THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California. NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2016 Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface xiii
  Change History xiii
  About This Document xiii
  Organization xiv
  Related Documentation xv
  Document Conventions xvi
  Audience xvi
  Support xvii
  Documentation Feedback xvii

CHAPTER 1 Preconfiguration 1
  Prerequisites for Call Flow Model Configuration 1
    Design Prerequisites 1
  Preconfiguration Tasks 2
    Network Information 2
    Unified CVP Installation 3
    Route Calls Through the Network to the VRU 4
    Ethernet Switch/Server NIC, Gateways and Call Server Settings 4
    Apply Contact Center Gateway Debug Settings 5
    Network VRU Types 5
    SIP Dialed Number Pattern Matching Algorithm 7
  Additional Configuration Instructions 7
    Order of Device Operations 7
    Manage Devices 8

CHAPTER 2 Unified CVP Call Flow Models 9
  Common Tasks for Unified CVP Call Flow Models 9
Call Services for Call Flow Models 9
Standalone Call Flow Model 10
  Configure VXML Server Standalone Call Flow Model 12
  Enable Reporting for Standalone Call Flow Model 13
  Enable ICM Lookup for Standalone Call Flow Model 13
Comprehensive Call Flow Model 14
  Comprehensive Call Flow Model for ICME 15
  Comprehensive Call Flow Model for ICMH 17
Set Up Comprehensive Call Flow Model Using SIP for ICME and ICMH 20
DNS Zone File Configuration for Comprehensive Call Flow Model 25
REFER Transfers 27
Comprehensive Call Flows for Pre-Routed Calls 28
  Calls Arriving at ICME Through a Pre-Route-Only NIC 29
  Calls Originated by Unified CM 30
  Calls Originated by an ACD or Call Routing Interface 33
Call Director Call Flow Model 35
  Call Director Call Flow Model for Unified ICME 37
  Call Director Call Flow Model for Unified ICMH 38
Set Up Call Director Call Flow Model 39
  Examples: Ingress Gateway Configuration 45
  DNS Zone File Configuration for Call Director Call Flow Model 47
VRU-Only Call Flow Model with NIC Routing 48
  Type 8 VRU-Only Call Flow Model for ICME 50
  Type 8 VRU-Only Call Flow Model for ICMH 51
Set Up Type 8 VRU-Only Call Flow Model for ICME and ICMH 52
  Type 7 VRU-Only Call Flow Model Network VRU for ICMH 56
  Set Up Type 3 or 7 VRU-Only Call Flow Model Network VRU for ICMH 57
Set Up sendtooriginator Setting in the SIP Service of a Call Server 60

CHAPTER 3  Operations Console 63
  Sign In to Operations Console 64
  Sign Out of Operations Console 64
  Operations Console Menus and Options 65
  System-Level Operation States 70
# Configuration Guide for Cisco Unified Customer Voice Portal, Release 10.0(1)

## Contents

### CHAPTER 4

**Call Server Configuration** 73

- Configure Call Server 73
- Call Server Settings 74
  - General Settings 74
  - ICM Service Settings 75
  - SIP Service Settings 78
    - Ring No Answer Settings with SIP 89
    - Valid Format for Dialed Numbers 89
  - IVR Service Settings 90
- Device Pool 93
  - Add or Remove Device From Device Pool 93
- Infrastructure Service Settings 94
  - License Thresholds 97

### CHAPTER 5

**VXML Server Configuration** 99

- Configure VXML Server (Standalone) 99
- Configure VXML Server 100
- Configure VXML Server (Standalone) with ICM Lookup Call Flow Model 101
- Configure the Unified CVP VXML Server (Standalone) Call Flow Model (Without ICM Lookup) 102
- Takeback and Transfer in VoiceXML Scripts 104
  - Configure Two B-Channel Transfer 104
  - Configure Hookflash Relay 105
  - Configure SIP REFER 107
- VXML Server Settings 107
  - General Settings 107
  - Configuration Settings 109
  - Add VXML Server to Device Pool 111
    - Infrastructure Service Settings 111
  - Voice XML Service 113
- VXML Server Reporting 113
  - Enable Reporting for Standalone Call Flow Model 114
  - Inclusive and Exclusive VXML Reporting Filters 115
  - VXML Inclusive and Exclusive Filter Rules 115
### Contents

- **VXML Filter Wildcard Matching Examples** 116
- **Configure Inclusive and Exclusive VXML Reporting Filters** 116
- **QoS for VXML Server** 116
  - Create Policy Based QoS 117
- **VXML Server with Unified ICME** 117
  - Integrate VoiceXML Scripts with Unified ICME Scripts 117
  - Correlate Unified CVP and Unified ICME Logs with Unified CVP VXML Server Logs 118
- **Error Codes for VXML Server** 119

---

**CHAPTER 6**

**Reporting Server Configuration** 121

- Configure Reporting Server 121
- **Reporting Server Settings** 122
  - General Settings 122
  - Reporting Properties Settings 123
- **Add or Remove Device From Device Pool** 124
- **Infrastructure Settings** 124

---

**CHAPTER 7**

**Unified ICM Configuration** 129

- Configure Unified ICM Server 129
- **ICM Server Settings** 130
  - General Settings 130
  - Add Unified ICM to Device Pool 130
- **Configure ICM Settings for Standalone Call Flow Model** 130
- **Configure ICM Settings for Comprehensive Call Flow Model for ICME and ICMH** 132
  - Configure Common Unified ICMH for Unified CVP Switch Leg 135
  - Define Unified CVP ECC Variables 137
  - Metadata ECC Variable 143
  - **Common Configuration for Differentiating VRUs Based on Dialed Number** 144
- **Configure ICM Settings for Call Director Call Flow Model** 145
- **Configure ICM Settings for VRU-Only Call Flow Model: Type 8** 147
- **Configure ICM Settings for VRU-Only Call Flow Model: Type 7** 154
- **Pass Data to Unified ICME** 157
  - Configure the Connections 157
  - Configure a Gateway for IP to TDM Calls 157
Contents

Chapter 12: Gateway Configuration 205
  Configure Gateway 205
  Gateway Settings 206
    General Settings 206
    Activate Gateway Configuration 207
    Add Gateway to Device Pool 207
  Configure Gateway Settings for Standalone Call Flow Model 207
    Example: Gateway Settings for Standalone Call Flow Model 208
    Example: Dial-Peer for Standalone Call Flow Model 209
  Configure Gateway Settings for Comprehensive Call Flow Model 210
  Configure Gateway Settings for Call Director Call Flow Model 220
  Configure Gateway Settings for VRU-Only Call Flow Model: Type 8 224
  Configure Gateway Settings for VRU-Only: Type 7 228
  Transfer Script and Media File to Gateway 230

Chapter 13: SIP Proxy Server Configuration 231
  Configure SIP Proxy Server 231
  SIP Proxy Server Settings 232
    General Settings 232
    Add SIP Proxy Server to Device Pool 234

Chapter 14: System Configuration 235
  System Tab Options 235
  Import System Configuration 236
  Export System Configuration 237
  Location Configuration 238
    Prerequisites for Location Configuration 242
    Deploy Location Information 242
    Add Location 243
  SIP Server Group Configuration 243
    Add SIP Server Groups 243
CHAPTER 15

Unified CVP Security 277

Prerequisites for Securing Communication Between CVP Components 277

Communications Security Between Unified CVP Components 278
Secure JMX Communications Between CVP Components 278
Exchange Certificates Between Systems 279
Enable Security on Unified CVP Devices 281
Certificate Authority Signed Certificates 281
  Add a Certificate Signed by a Certificate Authority to the Keystore 282
  Add a Certificate Signed by a Certificate Authority for HTTPS Web Access 283
Secure Communications Between Unified CVP and IOS Devices 284
HTTPS Support for Unified CVP 284
  Set Up Tomcat to Present CA-Signed Certificates to Inbound HTTPs Clients 284
Sensitive Customer Information 286

CHAPTER 16
Unified ICME Warm Consult Transfer/Conference to Unified CVP 287
  Configure Unified ICME Warm Consult Transfer/Conference to Unified CVP 288
  Minimal Component Version Requirement 289
  Warm Transfer with SIP Calls 289
  Set Up Unified ICME Warm Consult Transfer 290

CHAPTER 17
Transfer and Queue Calls with Unified CVP 293
  IVRs From Perspective of Unified ICME 293
  Call Transfer Using Unified CVP in Comprehensive Mode 294
    Call Transfer Using SIP Service 294
    Example: Transfer Call to a Label 294
    Example: Queue and Transfer Call to a Skill Group 296
    Example: Network Transfer Script 300
  Call Transfer From Agent to Agent 300
    Configure Network Transfer From IP Phone 301
    Configure Network Transfer From CTI OS Agent Desktop 301
  Example of IP Transfer 302
  CLI Field on Outgoing Transfers 302
    Configure CLI Override 302
  Unified CCE Reroute on No Answer Configuration for Unified CVP 303
    Reroute on No Answer Operation for Unified CCE with Unified IP IVR 303
    Reroute on No Answer Operation with Unified CVP 304
    Reroute on No Answer Agent Desk Settings Configuration 304
Configure High Availability for Unified CVP 329
Server Groups 329
  Configure Server Groups 329
  Server Groups Diagnostics 330
Redundancy and Failover for Unified CVP 331
  Redundancy for VXML Server Applications 331
  Redundancy for Micro-App-Based Applications 331
    IVR Service Failover Mechanism 332
Configure Speech Server 333
Application Control Engine for Load Balancing in Unified CVP 333
  General Probes 335
  Unified CVP Media Servers 335
ASR/TTS Servers 337
ASR and TTS Server Location Setup 338
  Specify an ASR and TTS Server Location Globally on the Gateway 338
  Specify an ASR and TTS Server Location with an Individual VoiceXML Document 339
    com.cisco.tts-server 340
    com.cisco.asr-server 340
  Set Up the VoiceXML Document Properties 340
  Example Gateway Configuration for MRCPv2 with Failover 340
Unified CVP Call Servers 341
Unified CVP VXML Servers 342

CHAPTER 19
Java Runtime Environment Minor Update 345

CHAPTER 20
Tomcat Update 347
  Tomcat Update 347
Preface

- Change History, page xiii
- About This Document, page xiii
- Organization, page xiv
- Related Documentation, page xv
- Document Conventions, page xvi
- Audience, page xvi
- Support, page xvii
- Documentation Feedback, page xvii

Change History

This table lists and links to changes made to this guide and gives the dates those changes were made.

<table>
<thead>
<tr>
<th>Change</th>
<th>Date</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial release of document</td>
<td>December 12, 2013</td>
<td></td>
</tr>
<tr>
<td>Java Runtime Environment Minor</td>
<td>September 17, 2014</td>
<td>Java Runtime Environment Minor Update, on page 345</td>
</tr>
<tr>
<td>Update</td>
<td>December 2, 2015</td>
<td>Tomcat Update, on page 347</td>
</tr>
<tr>
<td>Tomcat Update</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

About This Document

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.

# Organization

## Table 1: Organization of Cisco Unified Customer Voice Portal Guide

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preconfiguration, on page 1</td>
<td>Provides prerequisites, preconfiguration, and references for understanding and planning a Unified CVP implementation, and check-off lists for the various call flow model options available for Unified CVP.</td>
</tr>
<tr>
<td>Unified CVP Call Flow Models, on page 9</td>
<td>Provides high-level call flow model overviews, high-level sets of instructions for configuring specific call flow models.</td>
</tr>
<tr>
<td>Operations Console, on page 63</td>
<td>Describes the interface that is required for configuration of required and additional Unified CVP component.</td>
</tr>
<tr>
<td>Call Server Configuration, on page 73</td>
<td>Describes how to configure Call Server and its configuration settings.</td>
</tr>
<tr>
<td>VXML Server Configuration, on page 99</td>
<td>Describes how to configure VXML Server and its configuration settings.</td>
</tr>
<tr>
<td>Reporting Server Configuration, on page 121</td>
<td>Describes how to configure Reporting Server and its configuration settings.</td>
</tr>
<tr>
<td>Unified ICM Configuration, on page 129</td>
<td>Describes how to configure Unified ICM Server, its configuration settings on Operations Console, and configuration for various Unified CVP call flow models.</td>
</tr>
<tr>
<td>Unified Communications Manager Configuration, on page 161</td>
<td>Describes how to configure Unified Communications Server and its configuration settings.</td>
</tr>
<tr>
<td>SIP Devices Configuration, on page 165</td>
<td>Describes how to set up Ingress gateway and Call Server for redundant proxy server.</td>
</tr>
<tr>
<td>Media Server Configuration, on page 173</td>
<td>Describes how to configure Media Server and its configuration settings.</td>
</tr>
<tr>
<td>Speech Server Configuration, on page 201</td>
<td>Describes how to configure Speech Server and its configuration settings.</td>
</tr>
</tbody>
</table>
Table 2: Related Documentation for Unified CVP Configuration

<table>
<thead>
<tr>
<th>Document Name</th>
<th>Link</th>
</tr>
</thead>
</table>
Document Conventions

Table 3: Document Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong> font</td>
<td>Boldface font is used to indicate commands, such as user entries, keys,</td>
</tr>
<tr>
<td></td>
<td>buttons, and folder and submenu names. For example:</td>
</tr>
<tr>
<td></td>
<td>• Choose <strong>Edit &gt; Find</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Finish</strong>.</td>
</tr>
<tr>
<td><strong>italic</strong> font</td>
<td>Italic font is used to indicate the following:</td>
</tr>
<tr>
<td></td>
<td>• A syntax value that the user must replace. Example: IF ( <em>condition</em>,</td>
</tr>
<tr>
<td></td>
<td><em>true-value, false-value</em> )</td>
</tr>
<tr>
<td><strong>window</strong> font</td>
<td>Window font, such as Courier, is used for the following:</td>
</tr>
<tr>
<td></td>
<td>• Text as it appears in code or that the window displays. Example:</td>
</tr>
<tr>
<td></td>
<td><code>&lt;html&gt;&lt;title&gt;Cisco Systems,Inc. &lt;/title&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td><code>&lt; &gt;</code></td>
<td>Angle brackets are used to indicate the following:</td>
</tr>
<tr>
<td></td>
<td>• For arguments where the context does not allow italic, such as ASCII output.</td>
</tr>
<tr>
<td></td>
<td>• A character string that the user enters but that does not appear on the window such as a password.</td>
</tr>
</tbody>
</table>

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
Support

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Documentation Feedback

Provide your comments about this document to:

mailto:ccbu_docfeedback@cisco.com
Preconfiguration

- Prerequisites for Call Flow Model Configuration, page 1
- Preconfiguration Tasks, page 2
- Additional Configuration Instructions, page 7
- Order of Device Operations, page 7
- Manage Devices, page 8

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

- 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Have network information. See Network Information, on page 2.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Perform ring no answer settings with SIP. See Ring No Answer Settings with SIP, on page 89.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Install Cisco Unified Intelligent Contact Management (ICM), Cisco Unified Communications Manager (CM), VXML and ingress gateways.</td>
</tr>
<tr>
<td>Step 5</td>
<td>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 63.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Route calls through the network to the VRU. See Route Calls Through the Network to the VRU, on page 4.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Configure ethernet switch/server NIC, gateways, and Call Server settings. See Ethernet Switch/Server NIC, Gateways and Call Server Settings, on page 4.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Apply contact center gateway debug settings. Apply Contact Center Gateway Debug Settings, on page 5.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Check the network VRU types. See the Network VRU Types, on page 5.</td>
</tr>
<tr>
<td>Step 10</td>
<td>Refer to the SIP dialed number pattern matching algorithm. See SIP Dialed Number Pattern Matching Algorithm, on page 7.</td>
</tr>
<tr>
<td>Step 11</td>
<td>Obtain licenses for the required Unified CVP components.</td>
</tr>
<tr>
<td>Step 12</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.
- 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 135.

Unified CVP Installation

• Install the Unified CVP software. For the installation procedures of Unified CVP components, see the http://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 Unified CVP reporting, see Reporting Guide for Cisco Unified Customer Voice Portal.

• 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.
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 4: Call Flows Using Network VRUs and Customer VRU

<table>
<thead>
<tr>
<th>Call Flows</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using Network VRUs of Type 7 or 10</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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 5: Ethernet Switch/Server NIC, Gateways and Call Server Settings

<table>
<thead>
<tr>
<th>Ethernet Switch Speed</th>
<th>Server/Gateway NIC Speed</th>
<th>Speed/Duplex Setting for Switch Port</th>
<th>Speed/Duplex Setting for Server/GW NIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000 Mb</td>
<td>1000 Mb</td>
<td>1000/Full</td>
<td>1000/Full</td>
</tr>
<tr>
<td>1000 Mb</td>
<td>1000 Mb</td>
<td>Auto/Auto</td>
<td>Auto/Auto</td>
</tr>
<tr>
<td>1000 Mb</td>
<td>100 Mb</td>
<td>100 Mb/Full</td>
<td>100 Mb/Full</td>
</tr>
</tbody>
</table>
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 execute 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.
- 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 28. 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 135. 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 137. 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 143. 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 144. 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 165 and Set Up Call Server with Redundant Proxy Servers, on page 165.

Order of Device Operations

Based on your call flow model, set up the device operations in the following order.
Table 6: Order of Devices

<table>
<thead>
<tr>
<th>Device Operations</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Deployment</td>
<td>• SIP Proxy Server device (optional)</td>
</tr>
<tr>
<td></td>
<td>• Unified CVP Call Server device</td>
</tr>
<tr>
<td></td>
<td>• Unified CVP VXML Server device</td>
</tr>
<tr>
<td></td>
<td>• Unified CVP Reporting Server device</td>
</tr>
<tr>
<td></td>
<td>• Other Devices (for example, Gateways and Unified CM)</td>
</tr>
<tr>
<td>System Configuration</td>
<td>• SIP Server Groups</td>
</tr>
<tr>
<td></td>
<td>• Dialed Number Pattern</td>
</tr>
<tr>
<td></td>
<td>• Locations</td>
</tr>
<tr>
<td></td>
<td>• Courtesy Callback</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>• Transfer of licenses (required)</td>
</tr>
<tr>
<td></td>
<td>• Transfer of VXML applications (required)</td>
</tr>
<tr>
<td></td>
<td>• Bulk transfer of default Gateway files (required)</td>
</tr>
</tbody>
</table>

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** Transfer license.
**Step 5** Restart Unified CVP device to activate license.
**Step 6** Verify that Unified CVP devices are active in Operations Console.
**Step 7** Deploy system-level configuration, Dialed Number Pattern, SIP Server Groups, Locations, and Courtesy Callback, and verify their statuses.
**Step 8** Save and deploy the SNMP Configuration.
Unified CVP Call Flow Models

After understanding the Prerequisites for Call Flow Model Configuration, on page 1, select one of the following call flow models for Unified Customer Voice Portal (CVP) implementation.

- Common Tasks for Unified CVP Call Flow Models, page 9
- Standalone Call Flow Model, page 10
- Comprehensive Call Flow Model, page 14
- Comprehensive Call Flows for Pre-Routed Calls, page 28
- Call Director Call Flow Model, page 35
- VRU-Only Call Flow Model with NIC Routing, page 48
- Set Up sendtooriginator Setting in the SIP Service of a Call Server, page 60

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 7: Call Services for Call Flow Models*

<table>
<thead>
<tr>
<th>Call Flow Model</th>
<th>Required Call Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehensive Call Flow Model, on page 14</td>
<td>ICM, IVR, SIP</td>
</tr>
<tr>
<td>VRU-Only Call Flow Model with NIC Routing, on page 48</td>
<td>ICM, IVR</td>
</tr>
<tr>
<td>Call Director Call Flow Model, on page 35</td>
<td>ICM, IVR</td>
</tr>
<tr>
<td>Standalone Call Flow Model, on page 10</td>
<td>No Service</td>
</tr>
</tbody>
</table>
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 8: Required and Optional Unified CVP Components for Standalone Call Flow Model**

<table>
<thead>
<tr>
<th>CVP components</th>
<th>Related topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required CVP components</strong></td>
<td></td>
</tr>
<tr>
<td>VXML Server</td>
<td>• VXML Server Configuration, on page 99</td>
</tr>
<tr>
<td>Ingress Gateway</td>
<td>• Gateway Configuration, on page 205</td>
</tr>
<tr>
<td></td>
<td>• Example: Gateway Settings for Standalone Call Flow Model, on page 208</td>
</tr>
<tr>
<td></td>
<td>• Call Survivability, on page 308</td>
</tr>
<tr>
<td>VoiceXML Gateway</td>
<td>• Gateway Configuration, on page 205</td>
</tr>
<tr>
<td></td>
<td>• Example: Gateway Settings for Standalone Call Flow Model, on page 208</td>
</tr>
<tr>
<td>Operations Console</td>
<td>Operations Console, on page 63</td>
</tr>
<tr>
<td>Call Server</td>
<td>• Call Server Configuration, on page 73</td>
</tr>
<tr>
<td></td>
<td>• REFER Transfers, on page 27</td>
</tr>
<tr>
<td>Media Servers</td>
<td>Media Server Configuration, on page 173</td>
</tr>
<tr>
<td><strong>Optional CVP components</strong></td>
<td></td>
</tr>
<tr>
<td>Reporting Server</td>
<td>Reporting Server Configuration, on page 121</td>
</tr>
<tr>
<td>Speech Servers</td>
<td>Speech Server Configuration, on page 201</td>
</tr>
<tr>
<td>Unified ICM Enterprise</td>
<td>Unified ICM Configuration, on page 129</td>
</tr>
</tbody>
</table>

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 [Configure VXML Server (Standalone)](#) on page 99 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 execute 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 48.

---

**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.

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

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

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 executed 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.

**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.
   
   **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 settings.
   For gateway settings, see the Example: Gateway Settings for Standalone Call Flow Model, on page 208.

c) Configure the service settings on the gateway.
   See the Example: Gateway Settings for Standalone Call Flow Model, on page 208.

d) Configure a dial-peer, which will call the service to reach the Unified CVP VXML Server.
   See the Example: Dial-Peer for Standalone Call Flow Model, on page 209.

e) (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.
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 12.

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 73

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 Configure VXML Server, on page 100

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.

Step 8
Click Save and Deploy.

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 12.

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 Configure Call Server, on page 73.

**Step 5** Configure the VXML Server.
For more information on configuring a VXML Server, see Configure VXML Server, on page 100.

**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 ToExtVXML0 - 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 157.

---

**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 15 and Comprehensive Call Flow Model for ICMH, on page 17 sections. In these call flow models, both the Voice Gateway and the Call Server have two legs for the same call:

- **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 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 IOS 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.

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.

---

**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 2: Comprehensive Call Flow Model for ICME Using SIP Without a Proxy Server**

**Figure 3: Comprehensive Call Flow Model for ICME Using SIP With a Proxy Server**
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 27 and Set Up sendtooriginator Setting in the SIP Service of a Call Server, on page 60.

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 30 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 4: Comprehensive Call Flow Model for ICMH Using SIP Without a Proxy Server**

**Figure 5: 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 27 and Set Up sendtooriginator Setting in the SIP Service of a Call Server, on page 60.

Table 9: Required and Optional CVP Components for Comprehensive Call Flow Model

<table>
<thead>
<tr>
<th>CVP components</th>
<th>Related topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required CVP components</strong></td>
<td></td>
</tr>
<tr>
<td>Operations Console</td>
<td>Operations Console, on page 63</td>
</tr>
<tr>
<td>Ingress Gateway</td>
<td>• Gateway Configuration, on page 205</td>
</tr>
<tr>
<td></td>
<td>• Configure Gateway Settings for Comprehensive Call Flow Model, on page 210</td>
</tr>
<tr>
<td></td>
<td>• Call Survivability, on page 308</td>
</tr>
<tr>
<td>VoiceXML Gateway</td>
<td>• Gateway Configuration, on page 205</td>
</tr>
<tr>
<td></td>
<td>• Configure Gateway Settings for Comprehensive Call Flow Model, on page 210</td>
</tr>
<tr>
<td></td>
<td>• Call Survivability, on page 308</td>
</tr>
<tr>
<td>Unified ICME</td>
<td>• Unified ICM Configuration, on page 129</td>
</tr>
<tr>
<td></td>
<td>• Comprehensive Call Flow Model for ICME, on page 15</td>
</tr>
<tr>
<td></td>
<td>• Comprehensive Call Flows for Pre-Routed Calls, on page 28</td>
</tr>
<tr>
<td></td>
<td>• Calls Arriving at ICME Through a Pre-Route-Only NIC, on page 29</td>
</tr>
<tr>
<td></td>
<td>• Calls Originated by Unified CM, on page 30</td>
</tr>
<tr>
<td></td>
<td>• Calls Originated by an ACD or Call Routing Interface, on page 33</td>
</tr>
<tr>
<td></td>
<td>• Configure ICM Settings for Comprehensive Call Flow Model for ICME and ICMH, on page 132</td>
</tr>
<tr>
<td></td>
<td>• Define Unified CVP ECC Variables, on page 137</td>
</tr>
<tr>
<td>CVP components</td>
<td>Related topics</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Unified ICMH</td>
<td>• Unified ICM Configuration, on page 129</td>
</tr>
<tr>
<td></td>
<td>• Comprehensive Call Flow Model for ICMH, on page 17</td>
</tr>
<tr>
<td></td>
<td>• Configure ICM Settings for Comprehensive Call Flow Model for ICME and ICMH, on page 132</td>
</tr>
<tr>
<td></td>
<td>• Configure Common Unified ICMH for Unified CVP Switch Leg, on page 135</td>
</tr>
<tr>
<td></td>
<td>• Define Unified CVP ECC Variables, on page 137</td>
</tr>
<tr>
<td>Call Server</td>
<td>• Call Server Configuration, on page 73</td>
</tr>
<tr>
<td></td>
<td>• REFER Transfers, on page 27</td>
</tr>
<tr>
<td>Optional CVP components</td>
<td></td>
</tr>
<tr>
<td>Speech Servers</td>
<td>Speech Server Configuration, on page 201</td>
</tr>
<tr>
<td>SIP Proxy Server</td>
<td>SIP Proxy Server Configuration, on page 231</td>
</tr>
<tr>
<td>Media Servers</td>
<td>Media Server Configuration, on page 173</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>DNS Zone File Configuration for Comprehensive Call Flow Model, on page 25</td>
</tr>
<tr>
<td>Reporting Server</td>
<td>Reporting Server Configuration, on page 121</td>
</tr>
</tbody>
</table>

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 210 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-uas section to be your Proxy Server and point the session target of the dial-peer to the sip-server global variable.

**Note**

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

2. 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.
Note
See the SIP Devices Configuration, on page 165 and SIP Dialed Number Pattern Matching Algorithm, on page 7 for detailed information.

Step 5 Perform Steps 6 to 10 of the Configure Gateway Settings for Comprehensive Call Flow Model, on page 210 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 147 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.
- The URLs to the media servers in the VXML returned by the IVR Service can be controlled so that they are either HTTP or HTTPS URLs. This property is a boolean property called Use Security for Media Fetches. By default, it is set to "false". A value of "true" means generate HTTPS URLs to media servers and a value of "false" means generate HTTP URLs to media servers.
  
  This property is only applicable, if the following condition is true:

  In the Unified ICME script, the media server (specified in ECC variable call.user.microapp.media_server) is not set to a URL that explicitly specifies an HTTP or HTTPS scheme. 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 210 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 210 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 210 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) **Dialled 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 137.

**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.
  - Use the greater than (>) and 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 89 for format and precedence information.

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

See **SIP Devices Configuration**, on page 165 and **SIP Dialed Number Pattern Matching Algorithm**, on page 7 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  "9191919191>" 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 7 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 249.

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.

DNS Zone File Configuration for Comprehensive Call Flow Model

DNS Zone File Linux NAMED Configuration Example

```
rington=1 IN A 10.86.129.20
rington=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
```
DNS Zone File Configuration for Comprehensive Call Flow Model

Characteristics for the VRU Leg for Comprehensive Call Flow Model

Use the following commands to provide voice treatment:
new-call is a required name.

Continue with the VRU Leg Example.

```plaintext
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 execute further call control operations after this kind of label has been executed. 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 query; 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 hang up 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:

```plaintext
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 executed 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 get executed. In such a case, the call is transferred to Unified CVP,
and the routing script continues executing 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 normal 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 29.
- Calls Originated by Unified CM, on page 30.
- Calls Originated by an ACD or Call Routing Interface, on page 33.

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 10: Procedure for Different Releases of ICME

<table>
<thead>
<tr>
<th>ICME Release</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| 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. |
<table>
<thead>
<tr>
<th>ICME Release</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICME Release 7.0 onwards</td>
<td>1. Configure Type 7 and Type 10 Network VRUs.</td>
</tr>
<tr>
<td></td>
<td>2. In the PG Explorer tool, assign all Unified CVP Call Servers to the Type 7 Network VRU.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>5. In the System Information configuration tool, configure the Type 10 Network VRU as the system default Network VRU.</td>
</tr>
<tr>
<td></td>
<td>6. Associate all micro-application VRU scripts with the Type 10 Network VRU.</td>
</tr>
</tbody>
</table>

**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 execute 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 into 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.
For information about Consultative Warm Transfer, see Unified ICME Warm Consult Transfer/Conference to Unified CVP, on page 287.

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.
<table>
<thead>
<tr>
<th>ICME Release</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified ICME Release 7.0 onwards</td>
<td>1 Configure a single Type 10 Network VRU and defined as the default system Network VRU in the System Information tool.</td>
</tr>
<tr>
<td></td>
<td>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 &quot;Network Routing Number,&quot; which must be associated with each Unified CVP Call Server routing client.</td>
</tr>
<tr>
<td></td>
<td>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 execute any micro-applications.</td>
</tr>
</tbody>
</table>

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 execute any micro-applications.
<table>
<thead>
<tr>
<th>ICME Release</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified ICME Release 7.1 onwards</td>
<td>1  Configure two Network VRUs: one Type 7 and one Type 10.</td>
</tr>
<tr>
<td></td>
<td>2  In the PG Explorer tool, assign the Unified CVP Call Servers to the Type 7 Network VRU.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>5  Configure the Type 10 Network VRU as the system default Network VRU in the System Information configuration tool.</td>
</tr>
<tr>
<td></td>
<td>6  Associate all micro-application VRU scripts with the Type 10 Network VRU.</td>
</tr>
</tbody>
</table>

**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 11: Procedure for Different Releases of ICME

<table>
<thead>
<tr>
<th>ICME Release</th>
<th>Tasks</th>
</tr>
</thead>
</table>
| 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. |
<table>
<thead>
<tr>
<th>ICME Release</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICME Release 7.0 onwards</td>
<td>1 Configure two Network VRUs: one Type 7 and one Type 10.</td>
</tr>
<tr>
<td></td>
<td>2 In the PG Explorer tool, assign all Unified CVP Call Servers to the Type 7 Network VRU.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>5 Configure the Type 10 Network VRU as the system default Network VRU in the System Information configuration tool.</td>
</tr>
<tr>
<td></td>
<td>6 Associate all micro-application VRU scripts with the Type 7 Network VRU.</td>
</tr>
</tbody>
</table>

**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 12: Required and Optional CVP Components for Call Director Call Flow Model

<table>
<thead>
<tr>
<th>CVP components</th>
<th>Related topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required CVP components</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Call Server | • Call Server Configuration, on page 73  
• REFER Transfers, on page 27 |
| Unified ICME | • Unified ICM Configuration, on page 129  
• Call Director Call Flow Model for Unified ICME, on page 37  
• Call Director Call Flow Model for Unified ICMH, on page 38  
• Configure ICM Settings for Call Director Call Flow Model, on page 145  
• Define Unified CVP ECC Variables, on page 137 |
| Ingress Gateway | • Gateway Configuration, on page 205  
• Configure Gateway Settings for Call Director Call Flow Model, on page 220  
• Call Survivability, on page 308 |
| Operations Console | Operations Console, on page 63 |
| **Optional CVP components** | |
| Reporting Server | Reporting Server Configuration, on page 121 |
| SIP Proxy Server, if Call Server is configured to use SIP signaling | SIP Proxy Server Configuration, on page 231 |

This section describes the following Call Director call flow models:

• Call Director Call Flow Model for Unified ICME, on page 37  
• Call Director Call Flow Model for Unified ICMH, on page 38
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 6: Call Director Call Flow Model for ICME Using SIP Without a Proxy Server**

**Figure 7: Call Director Call Flow Model for ICME Using SIP With a Proxy Server**
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 8: Call Director Call Flow Model for ICMH Using SIP Without a Proxy Server**

**Figure 9: 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 27 and Set Up sendtooriginator Setting in the SIP Service of a Call Server, on page 60.

---

**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 210 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-uasection 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 165 and SIP Dialed Number Pattern Matching Algorithm, on page 7 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 47 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 165.

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 166 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 execute 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 Devices Configuration, on page 165 and SIP Dialed Number Pattern Matching Algorithm, on page 7 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 7 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.
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
Examples: Ingress Gateway Configuration

```text
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-receive
!
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
!
!
!
application
service cvp-survivability flash:cvp-survivability.tcl
!
!
!
application
service ringtone flash:ringtone.tcl
!
!
!
application
gateway

timer receive-rtcp 6
!
ip rtp 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 relax 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
SRV 1 1 5060 ringtone-2.sox.cisco.com.

SRV 1 1 5060 ringtone-2.sox.cisco.com.

SRV 1 1 5060 vxml-2.sox.cisco.com.
SRV 1 1 5060 vxml-3.sox.cisco.com.

SRV 2 1 5060 vxml-2.sox.cisco.com.
SRV 1 1 5060 vxml-3.sox.cisco.com.

SRV 2 1 5060 cvp-2.sox.cisco.com.
SRV 3 1 5060 cvp-3.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
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.

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

<table>
<thead>
<tr>
<th>Required CVP components</th>
<th>Related topics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 13: Required and Optional CVP Components for VRU Call Flow Model**
### CVP components

<table>
<thead>
<tr>
<th>CVP components</th>
<th>Related topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Server (with IVR and ICM Services enabled)</td>
<td>• Call Server Configuration, on page 73</td>
</tr>
<tr>
<td></td>
<td>• REFER Transfers, on page 27</td>
</tr>
<tr>
<td>VoiceXML Gateway</td>
<td>• Gateway Configuration, on page 205</td>
</tr>
<tr>
<td></td>
<td>• Configure Gateway Settings for VRU-Only: Type 7, on page 228</td>
</tr>
<tr>
<td>Operations Console</td>
<td>Operations Console, on page 63</td>
</tr>
<tr>
<td>Unified ICME</td>
<td>• Unified ICM Configuration, on page 129</td>
</tr>
<tr>
<td></td>
<td>• Comprehensive Call Flow Model for ICME, on page 15</td>
</tr>
<tr>
<td></td>
<td>• Calls Arriving at ICME Through a Pre-Route-Only NIC, on page 29</td>
</tr>
<tr>
<td></td>
<td>• Calls Originated by Unified CM, on page 30</td>
</tr>
<tr>
<td></td>
<td>• Calls Originated by an ACD or Call Routing Interface, on page 33</td>
</tr>
<tr>
<td></td>
<td>• Define Unified CVP ECC Variables, on page 137</td>
</tr>
<tr>
<td></td>
<td>• Configure Common Unified ICMH for Unified CVP Switch Leg, on page 135</td>
</tr>
</tbody>
</table>

### Optional CVP components

<table>
<thead>
<tr>
<th>Optional CVP components</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VXML Server</td>
<td>VXML Server Configuration, on page 99</td>
</tr>
<tr>
<td>Speech Servers</td>
<td>Speech Server Configuration, on page 201</td>
</tr>
<tr>
<td>Media Servers</td>
<td>Media Server Configuration, on page 173</td>
</tr>
<tr>
<td>Reporting Server</td>
<td>Reporting Server Configuration, on page 121</td>
</tr>
</tbody>
</table>

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

- Type 8 VRU-Only Call Flow Model for ICME, on page 50
- Type 8 VRU-Only Call Flow Model for ICMH, on page 51
- Configure Gateway Settings for VRU-Only: Type 7, on page 228
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.

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

- 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.

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.

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
- survivability.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 TranslationRouteToVRUnodeto 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 137.

**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**:

1. Configure the Reporting Server.
2. Select a Call Server to associate with this Reporting Server.
3. 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

---

**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 51. 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 12: 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.

Set Up Type 3 or 7 VRU-Only Call Flow Model Nnetwork 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 52 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 137.

**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:

1. If necessary, differentiate VRUs (Unified CVPs) based on dialed number.
2. Define customers and their Network VRU.

For more information, see Common Configuration for Differentiating VRUs Based on Dialed Number, on page 144.

**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:

1. 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).

2. 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.

3. 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

4. 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.)
5 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.

1 Configure the Reporting Server.

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

3 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**.

---

**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 `sendtooriginator` settings, then the call is routed to the `sip:<label>@<host portion from header of incoming invite>` SIP URL.
• The setting on the IOS gateway for signaling forward unconditional is required only if ISDN call variables need 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.
Set Up sendtooriginator Setting in the SIP Service of a Call Server
Operations Console

Operations Console is one of the Cisco Unified Customer Voice Portal (CVP) components and a web-based interface using which you can configure other Unified CVP components and devices in the Unified CVP solution. Use Operations Console to perform the following tasks:

- Monitor and manage the Unified CVP components and additional components that make Unified CVP a solution.
- Manage component configurations.
- Distribute Call Studio applications to Unified CVP VXML Servers.
- Perform Reporting database administration.
- Deploy licenses to the CVP devices.

Operations Console provides access to the following operations:

- **Health Monitoring:** Use any SNMP-standard monitoring tool to get a detailed visual and tabular representation of the health of the solution network. All the Unified CVP product components and most Unified CVP solution components also issue SNMP traps and statistics that can be delivered to any standard SNMP management station or monitoring tool.

- **Direct administration of individual IOS-based components:** Administrators can select an individual gateway for direct administration using secure shell (ssh). Configurations that are modified using secure shell, or by accessing those components directly without using the Operations Server, can be uploaded to the Operations Server backup for later use.

- **Error handling:** Operations Console is used for the following two types of validations:
  - **Client Side** - Validations using Javascript that run within the web browser. Client side validation errors appear below the Menu bar on the Operations Console page.

    ![Note](enable-javascript-in-browser)

    **Note** Enable Javascript in the browser.

  - **Server Side** - Validations that are run on the server side. These are extensive validations that include the client side validations and any business validations.

- [Sign In to Operations Console](#), page 64
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 14: Operations Console—Menus and Options

<table>
<thead>
<tr>
<th>Menu</th>
<th>Options</th>
<th>Use To</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Device Pool</td>
<td></td>
<td>Create, modify, and delete device pool names and descriptions for logical groups of devices (for example, all devices located in a geographical region).</td>
</tr>
<tr>
<td>Import System Configuration</td>
<td></td>
<td>Import a previously-saved Operations Console Server configuration file and apply it to the current system.</td>
</tr>
<tr>
<td>Export System Configuration</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Location</td>
<td></td>
<td>Add, edit, synchronize, and delete Unified CM location information.</td>
</tr>
<tr>
<td>SIP Server Groups</td>
<td></td>
<td>Configure server groups for SIP and view Call Server deployment status.</td>
</tr>
<tr>
<td>Web Services</td>
<td></td>
<td>Configure Diagnostic Portal servlet credentials.</td>
</tr>
<tr>
<td>Dialed Number Pattern</td>
<td></td>
<td>Configure the Dialed Number Patterns for a destination. You can define the dialed numbers for the Error Tone, Ring Tone, and other destinations.</td>
</tr>
<tr>
<td>IOS Configuration</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Use To

<table>
<thead>
<tr>
<th>Menu</th>
<th>Options</th>
<th>Use To</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Courtesy Callback</td>
<td>Configure allowed and denied dialed numbers, maximum callbacks per number, and Call Server deployment.</td>
</tr>
<tr>
<td>Menu</td>
<td>Options</td>
<td>Use To</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Device Management</td>
<td>Unified CVP Call Server</td>
<td>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; and apply licenses to a Call Server.</td>
</tr>
<tr>
<td></td>
<td>Unified CVP Reporting Server</td>
<td>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; apply licenses to a Reporting Server.</td>
</tr>
<tr>
<td></td>
<td>Unified CVP VXML Server</td>
<td>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 apply licenses and transfer scripts to a VXML Server.</td>
</tr>
<tr>
<td></td>
<td>Unified CVP VXML Server (standalone)</td>
<td>Configure VXML Server (standalone) general settings; associate VXML Server (standalone) with device pools; and apply licenses and transfer scripts to a VXML Server (standalone).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Gatekeeper</td>
<td></td>
<td>Configure a Gatekeeper and add this device to the Device Pool.</td>
</tr>
<tr>
<td>Gateway</td>
<td></td>
<td>Configure Gateway general settings; associate Gateways with device pools; execute a subset of IOS commands; view gateway statistics; and transfer files.</td>
</tr>
<tr>
<td>Device Past Configurations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Menu</td>
<td>Options</td>
<td>Use To</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Review and Restore past device configurations.</td>
</tr>
<tr>
<td>Media Server</td>
<td>Configure Media Server general settings and associate a Media Server with device pools.</td>
<td>A Media Server administers the media files that contain messages and prompts callers hear.</td>
</tr>
<tr>
<td>Unified CM</td>
<td>Configure Unified CM general settings; specify the URL to the Unified CM Device Administration page; and associate the Unified CM with device pools.</td>
<td></td>
</tr>
<tr>
<td>Unified ICM</td>
<td>Configure ICM Server general settings and associate the ICM Server with device pools.</td>
<td></td>
</tr>
<tr>
<td>SIP Proxy Server</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Unified IC</td>
<td>Configure CUIS Server general settings and associate the CUIS Server with device pools.</td>
<td></td>
</tr>
<tr>
<td>Device Past Configurations</td>
<td>Review and Restore past device configurations.</td>
<td></td>
</tr>
<tr>
<td>Device Versions</td>
<td>View version information for the Call Server, Reporting Server, VXML Server, and VXML Server (standalone).</td>
<td></td>
</tr>
<tr>
<td>User Management</td>
<td>User Roles</td>
<td>Create, modify, and delete user roles. Assign SuperUser, Administrator, or Read Only access privileges to roles.</td>
</tr>
<tr>
<td></td>
<td>User Groups</td>
<td>Create, modify, and delete user groups. Assign roles to user groups.</td>
</tr>
<tr>
<td></td>
<td>Users</td>
<td>Manage Unified CVP users, and assign them to groups and roles.</td>
</tr>
<tr>
<td>Bulk Administration</td>
<td>File Transfer</td>
<td>Transfer license files and script files to multiple devices at a time. The File Transfer submenu consists of the following options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Licenses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Scripts and Media</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• VXML Applications</td>
</tr>
</tbody>
</table>
### Use To

<table>
<thead>
<tr>
<th>Menu</th>
<th>Options</th>
<th>Use To</th>
</tr>
</thead>
</table>
| 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 15: Description of States Displayed in the Status Window*

<table>
<thead>
<tr>
<th>State</th>
<th>Reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Indicates that the operation was successful.</td>
</tr>
<tr>
<td>Pending</td>
<td>Indicates that the operation has not yet been executed.</td>
</tr>
<tr>
<td>In Progress</td>
<td>Indicates that the operation is in progress.</td>
</tr>
<tr>
<td>State</td>
<td>Reasons</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Failed</td>
<td>The reasons for a <strong>failed deployment</strong> state are listed below:</td>
</tr>
<tr>
<td></td>
<td>• Unable to locate IP address in the database</td>
</tr>
<tr>
<td></td>
<td>• General database failure</td>
</tr>
<tr>
<td></td>
<td>• The call server was not deployed</td>
</tr>
<tr>
<td></td>
<td>• Unknown error</td>
</tr>
<tr>
<td></td>
<td>• Notification error: Contact administrator</td>
</tr>
<tr>
<td></td>
<td>• Could not write to properties file</td>
</tr>
<tr>
<td></td>
<td>• The Call Server device is using an unknown version of the Unified CVP software</td>
</tr>
<tr>
<td></td>
<td>• The Call Server device is using an older version of the Unified CVP software</td>
</tr>
<tr>
<td></td>
<td>• Configuration not removed from the database</td>
</tr>
<tr>
<td></td>
<td>This failure has multiple reasons:</td>
</tr>
<tr>
<td></td>
<td>• Could not write to properties file</td>
</tr>
<tr>
<td></td>
<td>• Device has not been deployed</td>
</tr>
<tr>
<td></td>
<td>• General failure</td>
</tr>
<tr>
<td></td>
<td>• Unable to access the Database</td>
</tr>
<tr>
<td></td>
<td>The reasons for a <strong>failed synchronization</strong> state are listed below:</td>
</tr>
<tr>
<td></td>
<td>• Device is inaccessible</td>
</tr>
<tr>
<td></td>
<td>• Authentication failure</td>
</tr>
<tr>
<td></td>
<td>• Web service is not available on the device</td>
</tr>
<tr>
<td></td>
<td>• General database error</td>
</tr>
<tr>
<td></td>
<td>• General error</td>
</tr>
<tr>
<td></td>
<td>• Unknown host address</td>
</tr>
<tr>
<td></td>
<td>• SOAP service error</td>
</tr>
</tbody>
</table>

**Note** If you make any configuration changes after your initial deployment of any System-level configuration tasks, deploy the changed configuration again.
CHAPTER 4

Call Server Configuration

- Configure Call Server, page 73
- Call Server Settings, page 74

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 74.  
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 75.  
b) SIP. See **SIP Service Settings**, on page 78.  
c) IVR. See **IVR Service Settings**, on page 90.  
d) Device Pool. See **Add or Remove Device From Device Pool**, on page 93.  
e) Infrastructure. See **Infrastructure Service Settings**, on page 94.

**Step 5**  
Click **Save & Deploy**.  
*Note*  
Click **Save** to save the changes on the Operations Console and configure the Call Server later.
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 16: Call Server General Tab Configuration Settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default Value</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the Call Server.</td>
<td>None</td>
<td>Valid IP address</td>
<td>No</td>
</tr>
<tr>
<td>Hostname</td>
<td>The hostname of the Call Server.</td>
<td>None</td>
<td>A valid DNS name, which includes the uppercase and lowercase letters, the numbers 0 through 9, and a dash</td>
<td>No</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the Call Server.</td>
<td>None</td>
<td>0 to 1024 characters</td>
<td>No</td>
</tr>
<tr>
<td>Enable Secure Communication with the Ops Console</td>
<td>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.</td>
<td>None</td>
<td>Enabled or Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Enable this option after you configure secure communications. For more information, see Secure Communications Between Unified CVP and IOS Devices, on page 284</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Version</td>
<td>Lists the Release and Build Number for this device.</td>
<td>Read-only</td>
<td>Read-only</td>
<td>No</td>
</tr>
</tbody>
</table>

Turn On Services
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 17: ICM Service Configuration Settings**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default Value</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Configuration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VRU Connection Port</td>
<td>The Port Number on which the Intelligent Call Management (ICM) Service listens for a TCP connection from the ICM PIM.</td>
<td>5000</td>
<td>Any valid TCP/IP connection port</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Maximum Length of DNIS

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default Value</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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. <strong>Note</strong> 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.</td>
<td>10</td>
<td>Integer. Valid input for this field is 1 to 99999 characters.</td>
<td>No</td>
</tr>
</tbody>
</table>

### Translation Routed DNIS Pool

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default Value</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Enter a single DNIS number for translation routed calls. Validation for DNIS field are:</td>
<td>None</td>
<td>Integer up to 32 characters</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• The DNIS must be a positive integer and can begin with a zero.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The first and the last values for the DNIS range must be of the same length.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• You cannot add a DNIS or DNIS range that already exists or overlaps with DNIS or is in the range of a DNIS.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 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.

### 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.

<table>
<thead>
<tr>
<th>Default Value</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Integer</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### 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.

<table>
<thead>
<tr>
<th>Default Value</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Integer</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### 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.

<table>
<thead>
<tr>
<th>Default Value</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>Integer</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### 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.

<table>
<thead>
<tr>
<th>Default Value</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>Integer</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**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>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default Value</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select QoS Level</td>
<td>Select the Quality of Service level between the ICM Service and the ICM VRU PIM.</td>
<td>cs3</td>
<td>The drop-down list has the following values: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, ef</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>For more information, see <em>Implementing Quality of Service Policies with DSCP</em> (Document ID: 10103) at <a href="http://www.cisco.com/warp/public/105/dscpvalues.html">http://www.cisco.com/warp/public/105/dscpvalues.html</a>.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The default QoS setting between ICM and ICM VRU PIM is CS3.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Trunk Utilization**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default Value</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Gateway Trunk Reporting</td>
<td>Check this check box to enable gateway trunk reporting.</td>
<td>None</td>
<td>Not applicable</td>
<td>No</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>While adding or editing a gateway, you can use the optional field, <strong>Trunk Group ID</strong> to customize the trunk group ID for each gateway.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Gateway Ports</td>
<td>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.</td>
<td>700</td>
<td>1 to 1500</td>
<td>Yes</td>
</tr>
<tr>
<td>Available</td>
<td>The list of gateways available for trunk reporting.</td>
<td>None</td>
<td>Not applicable</td>
<td>No</td>
</tr>
<tr>
<td>Selected</td>
<td>The list of gateways selected for trunk reporting.</td>
<td>All Gateways Selected</td>
<td>Not applicable</td>
<td>No</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
<td>Default</td>
<td>Range</td>
<td>Restart Required</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td><strong>Configuration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Outbound Proxy</td>
<td>If you want to use a Cisco Unified SIP Proxy Server, in the Enable outbound proxy field, select Yes. Else, select No.</td>
<td>No</td>
<td>Yes or No</td>
<td>Yes</td>
</tr>
<tr>
<td>Enable Outbound Proxy</td>
<td>If you want to use a Cisco Unified SIP Proxy Server, in the Enable outbound proxy field, select Yes. Else, select No.</td>
<td>Yes</td>
<td>Yes or No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
| 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. | No      | Yes or No      | Yes             |
| 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. | None    | 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             |
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound SRV domain name/Server group name (FQDN)</td>
<td>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. <strong>Example:</strong> Outbound calls made from CVP SIP service are addressed to the URL of sip:&lt;label&gt;@&lt;srvfqdn&gt;. A server, such as Redundant Proxy Server, can route calls using this configuration.</td>
<td>None</td>
<td>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.</td>
<td>Yes</td>
</tr>
<tr>
<td>DN on the Gateway to play the ringtone</td>
<td>Enter the dialed number configured on the gateway to play the ringtone, which is dedicated VoIP dial peer.</td>
<td>9191</td>
<td>Any valid label</td>
<td>No</td>
</tr>
<tr>
<td>DN on the Gateway to play the error tone</td>
<td>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, execute the <code>sh run</code> command on the gateway and look for the dial peer that matches the incoming dialed number.</td>
<td>9292</td>
<td>Any valid label</td>
<td>No</td>
</tr>
</tbody>
</table>
### Property Description Default Range Restart Required

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
</table>
| 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**
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static routes for local routing without an outbound proxy - Dialed Number (DN)</td>
<td>In the <strong>Dialed Number (DN)</strong> text box, enter a dialed number. The <strong>Static routes for local routing without an outbound proxy - Dialed Number (DN)</strong> 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 <strong>Dialed Number (DN)</strong> and <strong>IP Address/Hostname/Server Group Name</strong> fields so that the local static route is complete. Click <strong>Add</strong> to create a proxy route using the DN and the IP address or hostname entered in the <strong>IP Address/Hostname/Server Group Name</strong> fields. The newly created proxy route is added to the list of proxy routes displayed in the box below the <strong>Add</strong> button.</td>
<td>None</td>
<td>Dialed number pattern, destination must be format of NNN.NNN.NNN.NNN or a hostname. See <a href="#">Valid Format for Dialed Numbers, on page 89</a></td>
<td>No</td>
</tr>
<tr>
<td>IP Address/Hostname/Server Group Name</td>
<td>Enter an IP address, hostname, or server group name.</td>
<td>None</td>
<td>Valid IP address, hostname, or SRV domain name</td>
<td>No</td>
</tr>
</tbody>
</table>

**Advanced Configuration**

**General**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound proxy port</td>
<td>Enter a value for port on which the SIP service sends requests to the outbound proxy server.</td>
<td>5060</td>
<td>Any available port number. Valid port numbers are integers between 1 and 65535.</td>
<td>Yes</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
<td>Default</td>
<td>Range</td>
<td>Restart Required</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Outgoing transport type</td>
<td>Select a transport type for outgoing SIP requests. Select <strong>TCP</strong> when reliability is important or packet size is an issue. Select <strong>UDP</strong> 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.</td>
<td>TCP</td>
<td>TCP and UDP</td>
<td>Yes</td>
</tr>
<tr>
<td>Incoming transport type</td>
<td>The type of transport the SIP Service uses to listen for incoming SIP requests.</td>
<td>UDP+TCP</td>
<td>UDP+TCP</td>
<td>Yes</td>
</tr>
<tr>
<td>Time to wait for ICM</td>
<td>The maximum number of milliseconds to wait for ICM to send further instructions.</td>
<td>2000</td>
<td>50 to 5000</td>
<td>No</td>
</tr>
<tr>
<td>SIP info tone duration</td>
<td>The maximum number of milliseconds for tone durations sent in when sending Dual Tone Multi-Frequency (DTMF) *8 outpulse digits to the gateway.</td>
<td>100 milliseconds</td>
<td>50 to 2000</td>
<td>No</td>
</tr>
<tr>
<td>SIP info comma duration</td>
<td>The maximum number of milliseconds to pause for each comma in the label when sending DTMF to the gateway.</td>
<td>100 milliseconds</td>
<td>50 to 2000</td>
<td>No</td>
</tr>
</tbody>
</table>

**Note**
SIP info comma duration is a pause between the *8 and the number. For example, four commas imply four times the value.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic Type Descriptor (GTD) Parameter Forwarding</td>
<td>Enter a value for passing GTD (UUI) data to ICM in a new call.</td>
<td>UUS</td>
<td>48 characters</td>
<td>No</td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepend digits</td>
<td>From the <strong>Prepend digits</strong> 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.</td>
<td>0</td>
<td>0 to 20 digits</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> • When Unified ICM returns a label, Unified CVP prepends the stripped digits before initiating the transfer.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If you customized the <strong>Prepend Digits</strong> 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 <strong>Save &amp; Deploy</strong> to ensure the values of both Operations Console and Call Server devices are in sync.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP Retransmission Count</td>
<td>From the <strong>UDP Retransmission Count</strong> drop-down list, select an option to set the UDP retry count for SIP retries.</td>
<td>2</td>
<td>1 to 6</td>
<td>No</td>
</tr>
<tr>
<td>Use Error Refer</td>
<td>Check the <strong>Use Error Refer</strong> check box to enable the SIP Use Error Refer property. Else, keep the check box unchecked.</td>
<td>Checked</td>
<td>Checked or unchecked</td>
<td>No</td>
</tr>
</tbody>
</table>
### SIP Service Settings

#### Call Server Configuration

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS Gateway Options Dynamic Routing</td>
<td>Check the <strong>IOS Gateway Options Dynamic Routing</strong> 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.</td>
<td>Checked</td>
<td>Checked or unchecked</td>
<td>No</td>
</tr>
<tr>
<td>IOS Gateway Options Reporting</td>
<td>Check the <strong>IOS Gateway Options Reporting</strong> check box to identify if trunk utilization reporting and resource availability on a router basis is required after the call is completed.</td>
<td>Checked</td>
<td>Checked or unchecked</td>
<td>No</td>
</tr>
</tbody>
</table>

### QoS

Select QoS level

Select the Quality of Service (QoS) level between the SIP Service and the SIP Proxy Server. **Note** For more information, see the Enterprise QoS Solution Reference Network Design Guide.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>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 89.</td>
<td>None</td>
<td>Dialed Number pattern, destination</td>
<td>No</td>
</tr>
</tbody>
</table>

### SIP Header Passing (to ICM)

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>255 characters</td>
<td>None</td>
<td>255 characters</td>
<td>No</td>
</tr>
</tbody>
</table>

### Dialed Number (DN) patterns

This field is optional for list addition.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>255 characters</td>
<td>None</td>
<td>255 characters</td>
<td>No</td>
</tr>
</tbody>
</table>
## Patterns for sending calls to the originator - Dialed Number (DN)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patterns for sending calls to the originator - Dialed Number (DN)</td>
<td>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 &quot;User Agent&quot; 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:&lt;label&gt;@&lt;host portion of from header of incoming invite&gt;. 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). <strong>Note</strong> For Send To Originator to work properly, the call must be originated by TDM and have survivability configured on the pots dial peer.</td>
<td>None</td>
<td>24 characters. See Valid Format for Dialed Numbers, on page 89.</td>
<td>No</td>
</tr>
</tbody>
</table>
## SIP Service Settings

### Patterns for RNA timeout on outbound SIP calls

**Description**

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.

**Default**

None

**Range**

24 characters. See **Valid Format for Dialed Numbers**, on page 89.

**Restart Required**

No

### Timeout

**Description**

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.

**Default**

60 seconds

**Range**

5 to 60

**Restart Required**

No

### Custom ringtone patterns - Dialed Number (DN)

**Description**

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, execute the **sh run command on the gateway and look for the dial peer that matches the incoming dialed number.**

**Default**

None

**Range**

24 characters. See **Valid Format for Dialed Numbers**, on page 89.

**Restart Required**

No
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 89.
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
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 2 or 3 seconds greater than the Unified ICME Agent Desk Setting RNA timeout. A greater value provides time to signal the agent after the ICM Router picks the agent through the link with the Peripheral Gateway. The range of RNA value is from 5 to 60 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.
- 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 executed. 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 19: IVR Service Settings**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CVP H.323 Service Configuration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heartbeat timeout</td>
<td>Enter the number of seconds after which the heartbeat times out.</td>
<td>120</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IOS Voice Browser Configuration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
<td>Default</td>
<td>Range</td>
<td>Restart Required</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>---------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Last Access Timeout (seconds)</td>
<td>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.</td>
<td>7320</td>
<td>0 to 2147483647</td>
<td>No</td>
</tr>
<tr>
<td>Media Server Timeout</td>
<td>Enter the number of seconds the Gateway should wait to connect to the HTTP Media Server before timing out.</td>
<td>4</td>
<td>0 to 2147483647</td>
<td>No</td>
</tr>
<tr>
<td>Media Server Retry Attempts</td>
<td>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.</td>
<td>0</td>
<td>0 to 2147483647</td>
<td>No</td>
</tr>
<tr>
<td>ASR/TTS Server Retry Attempts</td>
<td>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.</td>
<td>0</td>
<td>0 to 2147483647</td>
<td>No</td>
</tr>
</tbody>
</table>

Note: The backup media server is defined on the gateway as <mediaserver>-backup.

Note: The backup ASR and TTS servers are defined on the gateway as asr-<locale>-backup and tts-<locale>-backup.
### IVR Service Settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>IVR Service Timeout</td>
<td>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 <code>fetchtimeout</code> property within the bootstrap VXML in flash memory on the Gateway.</td>
<td>7</td>
<td>0 to 2147483647</td>
<td>No</td>
</tr>
<tr>
<td>IVR Service Retry Attempts</td>
<td>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.</td>
<td>0</td>
<td>0 to 2147483647</td>
<td>No</td>
</tr>
<tr>
<td>Use Backup ASR/TTS Servers</td>
<td>Click <strong>Yes</strong> if an ASR/TTS Server is unavailable so that the gateway attempts to connect to the backup ASR/TTS server. Else click <strong>No</strong>.</td>
<td><strong>Yes</strong></td>
<td>Yes or No</td>
<td>No</td>
</tr>
<tr>
<td>Use Backup Media Servers</td>
<td>Click <strong>Yes</strong> if the Media Server is unavailable so that the gateway attempts to connect to the backup Media Server. Else click <strong>No</strong>.</td>
<td><strong>Yes</strong></td>
<td>Yes or No</td>
<td>No</td>
</tr>
<tr>
<td>Use hostnames for default Media/VXML servers</td>
<td>Click <strong>No</strong> to use IP address VXML Server and Media Server. Click <strong>Yes</strong> to use hostnames instead of IP addresses.</td>
<td>No</td>
<td>Yes or No</td>
<td>No</td>
</tr>
<tr>
<td>Use Security For Media Fetches</td>
<td>Click <strong>No</strong> to generate HTTP URLs to Media Servers. Click <strong>Yes</strong> to generate HTTPS URLs to Media Servers. <strong>Note</strong> 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.</td>
<td>No</td>
<td>Yes or No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Advanced
### 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>From the <strong>Device Management</strong> menu, select a device to add to the Device Pool.</td>
</tr>
</tbody>
</table>

**Example:**
To add a Call Server to a device pool, select 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 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 20: Infrastructure Service Configuration Settings**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration: Thread Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Threads</td>
<td>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.</td>
<td>500</td>
<td>100 to 1000</td>
<td>No</td>
</tr>
<tr>
<td>Statistics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**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).

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 minutes</td>
<td>10 to 1440 minutes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Log File Properties**

- **Max Log File Size**
Enter the maximum size of a log file in megabytes before a new log file is created.

Default: 10 MB
Range: 1 through 100 MB
Restart Required: 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.

Default: 20,000 MB
Range: 500 to 500000 MB
Restart Required: 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.

Default: None
Range: Valid IP address or hostname.
Restart Required: No

- **Primary Syslog Server Port Number**
Enter a port number of Primary Syslog Server.

Default: None
Range: Any available port number. Valid port numbers are integers between 1 and 65535.
Restart Required: 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.

Default: None
Range: Valid IP address or hostname.
Restart Required: No
### Call Server Configuration

#### Infrastructure Service Settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Backup Syslog Server Port Number</td>
<td>Enter a port number of Primary Backup Syslog Server.</td>
<td>None</td>
<td>Any available port number. Valid port numbers are integers between 1 and 65535.</td>
<td>No</td>
</tr>
</tbody>
</table>

#### 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

| Critical Threshold | Percentage of licenses in use required to reach Critical licensing state. See License Thresholds, on page 97. | 97% | Positive integer less than or equal to 100 and greater than the Warning threshold. | No |
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.
VXML Server Configuration

- Configure VXML Server (Standalone), page 99
- Configure VXML Server, page 100
- Configure VXML Server (Standalone) with ICM Lookup Call Flow Model, page 101
- Configure the Unified CVP VXML Server (Standalone) Call Flow Model (Without ICM Lookup), page 102
- Takeback and Transfer in VoiceXML Scripts, page 104
- VXML Server Settings, page 107
- Voice XML Service, page 113
- VXML Server Reporting, page 113
- Inclusive and Exclusive VXML Reporting Filters, page 115
- Error Codes for VXML Server, page 119

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 107.
b) **Device Pool** tab. For more information about adding, deleting and editing device pool, see Add or Remove Device From Device Pool, on page 93.

**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.

---

## Configure VXML Server

**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 73.

**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 required:

a) General. See *General Settings*, on page 107.

b) Configuration. See *Configuration Settings*, on page 109.

c) Device Pool. See Add or Remove Device From Device Pool, on page 93.

d) Infrastructure. See *Infrastructure Service Settings*, on page 111.

**Step 4** Click **Save & Deploy**.
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 CVFBackupVXMLServer 12.34.567.890
param CVPSelfService-port 7000
param CVPSelfService-app [name of application on the VXML Server, exactly how it appears]
param CVFPrimaryVXMLServer 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-npe
codec g711ulaw
!
dial-peer voice [dial-peer unique ID] pots /* for TDM originated calls */
service [gateway application name]
```
**Configure the Unified CVP VXML Server (Standalone) Call Flow Model (Without ICM Lookup)**

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

**Procedure**

1. **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
   ```

2. **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**  

**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**  

---

**Sample Gateway Configuration**

Unified CVP VXML Server:

```
application
  service CVPSelfService flash:CVPSelfServiceBootstrap.vxml
  service HelloWorld flash:CVPSelfService.tcl
param CVPPBackupVXMLServer 10.78.26.28
param CVPSelfService-app HelloWorld
param CVPSelfService-port 7000
param CVPPPrimaryVXMLServer 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:

- **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 execute further call control or IVR operations after the label has been executed.

Configure Two B-Channel Transfer

This procedure describes how 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 CVPPPrimaryVXMLServer 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 102 or Configure VXML Server (Standalone) with ICM Lookup Call Flow Model, on page 101 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
```

**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 21: VXML Server General Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Values</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>The IP address of the VXML Server</td>
<td>None</td>
<td>A valid IP address</td>
<td>No</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the VXML Server</td>
<td>None</td>
<td>A valid IP address</td>
<td>No</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Default</td>
<td>Values</td>
<td>Restart Required</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>---------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Hostname</td>
<td>The hostname of the VXML Server. Hostnames must be valid DNS names, which can include letters, the numbers 0 through 9, and a dash.</td>
<td>None</td>
<td>A valid DNS name, which includes uppercase and lowercase letters, the numbers 0 through 9, and a dash.</td>
<td>No</td>
</tr>
<tr>
<td>Description</td>
<td>Enter additional information about the VXML Server.</td>
<td>None</td>
<td>Up to 1024 characters</td>
<td>No</td>
</tr>
<tr>
<td>Trunk Group ID</td>
<td>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.</td>
<td>None</td>
<td>300&lt;br&gt;1 to 65535</td>
<td>No</td>
</tr>
<tr>
<td>Location ID</td>
<td>View the location ID for the Gateway.</td>
<td>None</td>
<td>Blank, if not assigned to a system-level configuration location.</td>
<td>No</td>
</tr>
<tr>
<td>Enable secure communication with the Ops console</td>
<td>Select to enable secure communications between the Operations Server and this component. The device is accessed using SSH and files are transferred using HTTPS.</td>
<td>None</td>
<td>Checked or unchecked</td>
<td>Yes</td>
</tr>
<tr>
<td>Device Version</td>
<td>Lists the release and build number for this device.</td>
<td>Read-only</td>
<td>Read-only</td>
<td>No</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Values</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Indicates whether or not 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.</td>
<td>Checked</td>
<td>Checked or unchecked</td>
<td>No</td>
</tr>
<tr>
<td>Enable Reporting for VXML Application Details</td>
<td>Indicates whether VXML application details are reported.</td>
<td>Unchecked</td>
<td>Checked and unchecked</td>
<td>No</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Default</td>
<td>Values</td>
<td>Restart Required</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>-----------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Max. Number of Messages</td>
<td>Define the maximum number of reporting messages that will be saved in a file if failover occurs. (Limited by amount of free disk space.)</td>
<td>100,000</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>QoS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Select QoS Level</td>
<td>The level of transmission quality and service availability for the VXML Server. For more information, see Implementing Quality of Service Policies with DSCP (Document ID: 10103) at <a href="http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml">http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml</a>.</td>
<td>cs3</td>
<td>The drop-down list contains the following values: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, and ef.</td>
<td>Yes</td>
</tr>
<tr>
<td>VXML Applications Details: Filters</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inclusive Filters</td>
<td>List of applications, element types, element names, element fields, and ECC variables to include in reporting data.</td>
<td>None</td>
<td>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 115.</td>
<td>Yes</td>
</tr>
<tr>
<td>Exclusive Filters</td>
<td>List of applications, element types, element names, and element fields, and ECC variables to exclude from reporting data.</td>
<td>None</td>
<td>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 115.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Add VXML Server to Device Pool

See Device Pool, on page 93 and Add or Remove Device From Device Pool, on page 93.

Infrastructure Service Settings

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

Table 23: VXML Server Infrastructure Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Values</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration: Thread Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Threads</td>
<td>The maximum thread pool size in the VXML Server Java Virtual Machine.</td>
<td>300</td>
<td>100 to 1000</td>
<td>Yes</td>
</tr>
<tr>
<td>Advanced</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statistics Aggregation Interval</td>
<td>Interval during which the VXML Server publishes statistics.</td>
<td>30 minutes</td>
<td>10 to 1440 minutes</td>
<td>Yes</td>
</tr>
<tr>
<td>Log File Properties</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max Log File Size</td>
<td>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.</td>
<td>10 MB</td>
<td>1 through 100 MB</td>
<td>Yes</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Default</td>
<td>Values</td>
<td>Restart Required</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Max Log Directory Size</td>
<td>Enter the maximum size of the directory containing VXML Server log files.</td>
<td>20,000 MB</td>
<td>500 to 500000 MB</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Modifying the value to a setting that is below the default value</td>
<td></td>
<td>• The value of Max Log File Size must be less</td>
<td></td>
</tr>
<tr>
<td></td>
<td>might cause logs to be rolled over quickly. Consequently, log entries might</td>
<td></td>
<td>than Max Log Directory Size.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>be lost, which can affect troubleshooting.</td>
<td></td>
<td>• The value of the Max Log File size must be</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>greater than 1.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• The value of Max Log directory Size or Max</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Log File Size must not be greater than 5000.</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration: Primary Syslog Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Values</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Syslog Server</td>
<td>Hostname or IP address of Primary Syslog Server to send syslog events from</td>
<td>None</td>
<td>Valid IP address or hostname.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>a CVP Application.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Syslog Server</td>
<td>Port number of Primary Syslog Server.</td>
<td>None</td>
<td>Any available port number. Valid port numbers</td>
<td>No</td>
</tr>
<tr>
<td>Server Port Number</td>
<td></td>
<td></td>
<td>are integers between 1 and 65535.</td>
<td></td>
</tr>
<tr>
<td>Primary Backup Syslog</td>
<td>Hostname or IP address of the Primary Backup Syslog Server to send syslog</td>
<td>None</td>
<td>Valid IP address or hostname.</td>
<td>No</td>
</tr>
<tr>
<td>Server</td>
<td>events from a CVP Application when the Syslog Server cannot be reached.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Backup Syslog</td>
<td>Port number of Primary Backup Syslog Server.</td>
<td>None</td>
<td>Any available port number. Valid port numbers</td>
<td>No</td>
</tr>
<tr>
<td>Server Port Number</td>
<td></td>
<td></td>
<td>are integers between 1 and 65535.</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration: Secondary Syslog Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Values</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary Syslog Server</td>
<td>Hostname or IP address of Secondary Syslog Server to send syslog events</td>
<td>None</td>
<td>Valid IP address or hostname.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>from a CVP Application.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 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 157](#).

### 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.

**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 12.

**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 73.

**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 Configure VXML Server, on page 100.

**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.

**Step 8** Click **Save and Deploy**.
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 24: Examples - VXML Filter Wildcard Matching

<table>
<thead>
<tr>
<th>Filter</th>
<th>What It Matches</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyApplication.voice.<em>.</em></td>
<td>Matches all voice elements in MyApplication</td>
</tr>
<tr>
<td><em>.voice.</em>.*</td>
<td>Matches all Voice elements in all applications</td>
</tr>
<tr>
<td>MyApplication.**.<em>.var</em></td>
<td>Matches all fields in MyApplication that start with the string <code>var</code></td>
</tr>
<tr>
<td>MyApplication.**.*.*3</td>
<td>Matches all fields in MyApplication that end with <code>3</code></td>
</tr>
<tr>
<td>MyApplication.**.*.SESSION:Company</td>
<td>Matches the Company session variable in MyApplication</td>
</tr>
</tbody>
</table>

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.

QoS for VXML Server

Quality of Service (QoS) is the measure of transmission quality and service availability of a network (or internetworks).
Create Policy Based QoS

This section describes how to create policy based QoS.

Procedure

**Step 1** From the Local Group Policy Editor on Windows 2012 R2 Standard Edition server, select Computer Configuration > Windows Settings.

**Step 2** In the Group Policy Object Editor window right-click the Policy-based QoS node, and click Create a new policy.

**Step 3** On the Policy-based QoS wizard specify a policy name. Specify a DSCP value, and click Next.

**Step 4** Select all application, and click Next.

**Step 5** Check the Any source IP address and Any destination IP address check box, and click Next.

**Step 6** If the policy is for Call Server QoS, then from the Select the protocol this QoS policy applies to drop-down list, select the same protocol that was set in the Outbound transport type on the Unified CVP Operations Console.
   If the policy is for VXML Server QoS, then from the Select the protocol this QoS policy applies to drop-down list, select TCP.

**Step 7** If the policy is for Call Server QoS, check the To destination port number or range check box. Assign the same port number as configured in the Port number for outgoing SIP requests in the Unified CVP Operations console. By default the port number is 5060.
   If the policy is for VXML Server QoS, check the From this source port number or range check box. Assign the port number 7000.

**Step 8** Click on Finish.

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:


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 execute the **HelloWorld** application. To execute 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:
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)`: 

- 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 ".":
  
  `concatenate("ICMInfoKeys="`, Call.RouterCallKey, ",", Call.RouterCallDay, ",", Call.RouterCallKeySequenceNumber)`.


## 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.
CHAPTER 6

Reporting Server Configuration

• Configure Reporting Server, page 121
• Reporting Server Settings, page 122

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 73.

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

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 122.
  b) Reporting Properties tab. For more information, see Reporting Properties Settings, on page 123.
c) **Device Pool** tab. For more information about adding, deleting, and editing device pool, see Add or Remove Device From Device Pool, on page 93.

d) **Infrastructure** tab. For more information, see Infrastructure Settings, on page 124.

**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.

---

# 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 25: Reporting Server—General Tab Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the Reporting Server.</td>
<td>None</td>
<td>Valid IP address</td>
<td>Yes</td>
</tr>
<tr>
<td>Hostname</td>
<td>The hostname of the Reporting Server machine.</td>
<td>None</td>
<td>Valid DNS name, which can include letters of the alphabet and numbers 0 through 9.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> No hyphen (-) is permitted in the hostname.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>An optional text description for the Reporting Server.</td>
<td>None</td>
<td>Up to 1024 characters.</td>
<td>No</td>
</tr>
<tr>
<td>Enable Secure Communication with the Operations Console</td>
<td>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.</td>
<td>Off</td>
<td>On or Off</td>
<td>No</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Default</td>
<td>Value</td>
<td>Restart Required</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>--------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Device Version</td>
<td>Lists the release and build number for this device.</td>
<td>None</td>
<td>None</td>
<td>No</td>
</tr>
<tr>
<td>Associate Call Servers</td>
<td>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.</td>
<td>None</td>
<td>A Call Server can be associated with only one Reporting Server.</td>
<td>No</td>
</tr>
</tbody>
</table>

### Reporting Properties Settings

Configure Reporting Server settings on the **Reporting Properties** tab.

**Table 26: Reporting Server—Reporting Properties Tab Configuration Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Reporting</td>
<td>Enables the Reporting Server to receive call data from the associated Call Server.</td>
<td>Yes</td>
<td>Yes or No</td>
<td>Yes</td>
</tr>
<tr>
<td>Max. File Size (MB):</td>
<td>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.</td>
<td>100</td>
<td>1 through 250 MB</td>
<td>No</td>
</tr>
<tr>
<td>QoS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 CVPCallServer 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 CVPCallServers 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 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 27: Reporting Server—Infrastructure Tab Configuration Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration: Thread Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Threads</td>
<td>(Required) The maximum thread pool size in the Reporting Server Java Virtual Machine.</td>
<td>500</td>
<td>100 to 1000</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statistics Aggregation Interval</td>
<td>The Reporting Server publishes statistics at this interval.</td>
<td>30 minutes</td>
<td>10 to 1440</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Log File Properties</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max Log File Size</td>
<td>(Required) Maximum size of the log file in megabytes.</td>
<td>10 MB</td>
<td>1 through 100 MB.</td>
<td>Yes</td>
</tr>
<tr>
<td>Max Log Directory Size</td>
<td>(Required) Maximum size of the directory containing Reporting Server log files.</td>
<td>20,000 MB</td>
<td>500 to 500,000 MB.</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you modify the value to a setting that is below the default value, the log entries might be lost, which can affect troubleshooting.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Configuration: Primary Syslog Settings</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Syslog Server</td>
<td>Hostname or IP address of Primary Syslog Server to send syslog events from a CVP Application.</td>
<td>None</td>
<td>Valid IP address or hostname.</td>
<td>No</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Default</td>
<td>Value</td>
<td>Restart Required</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Primary Syslog Server Port Number</td>
<td>Port number of Primary Syslog Server.</td>
<td>None</td>
<td>Any available port number. Valid port numbers are integers between 1 and 65,535.</td>
<td>No</td>
</tr>
<tr>
<td>Primary Backup Syslog Server</td>
<td>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.</td>
<td>None</td>
<td>Valid IP address or hostname.</td>
<td>No</td>
</tr>
<tr>
<td>Primary Backup Syslog Server Port Number</td>
<td>Port number of Primary Backup Syslog Server.</td>
<td>None</td>
<td>Any available port number. Valid port numbers are integers between 1 and 65,535.</td>
<td>No</td>
</tr>
</tbody>
</table>

**Configuration: Secondary Syslog Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary Syslog Server</td>
<td>Hostname or IP address of Secondary Syslog Server to send syslog events from a CVP Application.</td>
<td>None</td>
<td>Valid IP address or hostname.</td>
<td>No</td>
</tr>
<tr>
<td>Secondary Syslog Server Port Number</td>
<td>Port number of Secondary Syslog Server.</td>
<td>None</td>
<td>Any available port number. Valid port numbers are integers between 1 and 65,535.</td>
<td>No</td>
</tr>
<tr>
<td>Secondary Backup Syslog Server</td>
<td>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.</td>
<td>None</td>
<td>Valid IP address or hostname.</td>
<td>No</td>
</tr>
</tbody>
</table>
### Field | Description | Default | Value | Restart Required |
--- | --- | --- | --- | --- |
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 |
CHAPTER 7

Unified ICM Configuration

- Configure Unified ICM Server, page 129
- ICM Server Settings, page 130
- Configure ICM Settings for Standalone Call Flow Model, page 130
- Configure ICM Settings for Comprehensive Call Flow Model for ICME and ICMH, page 132
- Configure ICM Settings for Call Director Call Flow Model, page 145
- Configure ICM Settings for VRU-Only Call Flow Model: Type 8, page 147
- Configure ICM Settings for VRU-Only Call Flow Model: Type 7, page 154
- Pass Data to Unified ICME, page 157

Configure Unified ICM Server

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to Operations Console and click <strong>Device Management &gt; Unified ICM</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click <strong>Add New</strong>.</td>
</tr>
<tr>
<td>Note</td>
<td>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 <strong>Use As Template</strong> and perform Steps 3 to 6.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the <strong>General</strong> tab and enter the field values. See <strong>General Settings</strong>, on page 130.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) Click the <strong>Device Pool</strong> tab and add the Unified ICM Server to a device pool. See <strong>Add Unified ICM to Device Pool</strong>, on page 130.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of a Unified ICM Server</td>
<td>None</td>
<td>Valid IP address</td>
<td>No</td>
</tr>
<tr>
<td>Hostname</td>
<td>The name of the Unified ICM Server</td>
<td>None</td>
<td>Valid DNS name. It includes alphanumerical characters and a dash.</td>
<td>No</td>
</tr>
<tr>
<td>Description</td>
<td>Additional information about the Unified ICM Server</td>
<td>None</td>
<td>Up to 1024 characters</td>
<td>No</td>
</tr>
<tr>
<td>Device Admin</td>
<td>The URL for the Unified ICM Web configuration application.</td>
<td>None</td>
<td>Valid URL</td>
<td>No</td>
</tr>
</tbody>
</table>

Add Unified ICM to Device Pool

See Add or Remove Device From Device Pool, on page 93.

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.
### Procedure

#### Step 1
Create an application using Cisco Unified Call Studio and deploy it as a zip file.

**Note**
- For ICM Lookup, use the `ReqICMLabelElement`. 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 `ReqICMLabelElement`.
- For details on the `ReqICMLabelElement`, 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 73.

#### 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"
```
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) **Dialled 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.
      * 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 89.

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

For more information, see SIP Devices Configuration, on page 165 and SIP Dialed Number Pattern Matching Algorithm, on page 7.

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.

---

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
Define Unified CVP ECC Variables

Set up the ECC variables that Unified CVP uses to exchange information with Unified ICME/ICMH.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>On the ICM Configuration Manager, select Tools &gt; Miscellaneous Tools &gt; System Information and check the <strong>Enable expanded call context</strong> check box.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>On the ICM Configuration Manager, select Tools &gt; List Tools &gt; Expanded Call Variable List.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>In the Expanded Call Variable List window, enable the <strong>Add</strong> button by clicking <strong>Retrieve</strong>.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Click <strong>Add</strong>. The Attributes property tab is enabled.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Create each of the variables in the following table by clicking <strong>Save</strong> after defining each variable. <strong>Note</strong> If you change the configuration of any ECC variable with the Expanded Call Variable List tool, stop and restart the Unified CVP Call Server. <strong>Caution</strong> It is important that you enter the ECC's <strong>Name</strong> 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. <strong>Length</strong> values are more flexible. Unless the values listed in following table are noted as &quot;required,&quot; 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. <strong>Note</strong> 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 change the length of the ECC variables while the Unified CVP ICM Service is running, restart the Unified CVP ICM Service so that it works properly.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Click <strong>Save</strong> to apply your changes.</td>
</tr>
</tbody>
</table>

**Table 29: Micro-Application ECCs**

<table>
<thead>
<tr>
<th>Name</th>
<th>Length</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>POD.ID</td>
<td>Length: 36</td>
<td>Unique identifier for use with Cisco Context Service to propagate call or task context data.</td>
</tr>
<tr>
<td>Name</td>
<td>Length</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>user.CourtesyCallbackEnabled</td>
<td>Required for using Courtesy Callback. Length: 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Used to determine if Courtesy Callback must be offered to a caller. Valid values are: &quot;1&quot; = Yes, &quot;0&quot; = No</td>
</tr>
<tr>
<td>user.cvp_server_info</td>
<td>Length: 15</td>
<td>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</td>
</tr>
<tr>
<td>user.microapp.currency</td>
<td>Value: 6</td>
<td>Currency type.</td>
</tr>
<tr>
<td>user.microapp.error_code</td>
<td>Value: 2</td>
<td>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.</td>
</tr>
<tr>
<td>user.microapp.fetchaudio</td>
<td>Recommended length: 20; but length depends on the filename.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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: &quot;flash:holdmusic.wav&quot;</td>
</tr>
<tr>
<td>user.microapp.fetchdelay</td>
<td>Length: 1</td>
<td>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 &quot;blip&quot; sound heard in a normal network scenario Setting this value to zero plays hold music immediately, for a minimum of five seconds. Values: 1 to 9</td>
</tr>
<tr>
<td>Name</td>
<td>Length</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------</td>
<td>------------</td>
</tr>
<tr>
<td>user.microapp.fetchminimum</td>
<td>Length: 1</td>
<td>The minimum length of time to play audio specified by <code>user.microapp.fetchaudio</code>, 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</td>
</tr>
<tr>
<td>user.microapp.isPostCallSurvey</td>
<td>Length: 1</td>
<td>Used to determine if post call survey must be offered to a caller after the agent hangs up. Valid values: &quot;y&quot; or &quot;Y&quot; is &quot;Yes&quot; &quot;n&quot; or &quot;N&quot; is &quot;No&quot; Default value is &quot;Yes&quot;</td>
</tr>
<tr>
<td>user.microapp.locale</td>
<td>Value: 5</td>
<td>Locale, a combination of language and country which defines the grammar and prompt set to use.</td>
</tr>
</tbody>
</table>
| 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>" |
<p>| 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. |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Length</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>user.microapp.app_media_lib</td>
<td>Maximum length: 210 characters Recommended length: 10</td>
<td>Directory for all application-specific media files and grammar files. You can also set this value to &quot;.&quot; (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 &quot;.&quot;, the path: <a href="http://server/locale/..//hello.wav">http://server/locale/..//hello.wav</a> would really be: <a href="http://server/hello.wav">http://server/hello.wav</a></td>
</tr>
<tr>
<td>user.microapp.grammar_choices</td>
<td>Configurable on Unified ICM. Maximum length: 210 characters.</td>
<td>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 (/).</td>
</tr>
<tr>
<td>user.microapp.inline_tts</td>
<td>Configurable on the ICM. Maximum length: 210 characters.</td>
<td>Specifies the text for inline Text To Speech (TTS).</td>
</tr>
</tbody>
</table>

**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 157.
<table>
<thead>
<tr>
<th>Name</th>
<th>Length</th>
<th>Definition</th>
</tr>
</thead>
</table>
| 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" |
<table>
<thead>
<tr>
<th>Name</th>
<th>Length</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>user.microapp.ToExtVXML</td>
<td>210</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information on user.microapp.ToExtVXML variable length, see the Configure the CCE Script for Courtesy Callback section.</td>
</tr>
<tr>
<td>user.microapp.FromExtVXML</td>
<td>210</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See Pass Data to Unified ICME, on page 157 for more information. For more information on user.microapp.FromExtVXML variable length, see the Configure the CCE Script for Courtesy Callback section.</td>
</tr>
<tr>
<td>user.microapp.override_cli</td>
<td></td>
<td>Configurable on Unified ICME/ICMH. Maximum length: 200 characters. Used by system to override the CLI field on outgoing transfers.</td>
</tr>
<tr>
<td>user.microapp.metadata</td>
<td></td>
<td>The variable length would normally 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 execution of that micro-application.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The user.microapp.metadata ECC variable is structured as follows: m</td>
</tr>
<tr>
<td>user.microapp.uui</td>
<td></td>
<td>Configurable on Unified ICME/ICMH. Maximum length: 131 characters. Used to pass user-to-user information back to Unified CVP from Unified ICME/ICMH.</td>
</tr>
</tbody>
</table>
**Metadata ECC Variable**

Following the Menu (M), Get Data (GD) and Get Speech (GS) micro-applications, Unified CVP returns information about the execution of that micro-application. 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>
<thead>
<tr>
<th>Metadata</th>
<th>ECC Variable Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>m</code></td>
<td>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 <code>m</code> being set to V or D, even if the entry was an invalid menu selection.)</td>
</tr>
<tr>
<td><code>con</code></td>
<td>000 to 100 - Indicates the ASR percent confidence level at which the voice input was finally recognized. This field is only valid if <code>m</code> is Voice (V).</td>
</tr>
<tr>
<td><code>tr</code></td>
<td>00 to 99 - Indicates how many tries were required. 01 means user responded successfully after the first prompt.</td>
</tr>
</tbody>
</table>
### ECC Variable Value Metadata

<table>
<thead>
<tr>
<th>Metadata</th>
<th>ECC Variable Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>to</td>
<td>00 to 99 - Indicates how many timeouts occurred. Does not include interdigit timeouts.</td>
</tr>
<tr>
<td>iv</td>
<td>00 to 99 - Indicates how many invalid entries were received, including interdigit timeouts.</td>
</tr>
<tr>
<td>duratn</td>
<td>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.</td>
</tr>
<tr>
<td>vru script name</td>
<td>Full name of the VRU script which was executed. This is the only variable length field.</td>
</tr>
</tbody>
</table>

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 vru script name 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 execution of each input micro-application.

### 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
   - **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) **Dialled 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 execute 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 165 and *SIP Dialed Number Pattern Matching Algorithm*, on page 7 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.

**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 52 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.
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 TranslationRouteToVRUnodetoconnectthecalltotheNetworkVRU.

**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 137.

**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 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:

1. Configure the Reporting Server.
2. Select a Call Server to associate with this Reporting Server.
3. 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
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

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 52 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>_<cvpl> 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
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 137*.

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 144.

**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**.
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 73. See the Unified ICME documentation for instructions on configuring the VRU PIM to connect to a VRU. For example, Unified CVP.

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.
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 the VXML 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.
Unified Communications Manager Configuration

- Configure Unified Communications Manager Server, page 161
- Unified CM Settings, page 162

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 162**.
- **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 93**.

**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 31: Unified CM Server—General Tab Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the Unified CM Server.</td>
<td>None</td>
<td>Valid IP address</td>
<td>No</td>
</tr>
<tr>
<td>Hostname</td>
<td>The name of the Unified CM Server.</td>
<td>None</td>
<td>Valid DNS names, includes letters in the alphabet, the numbers 0 through 9, and a dash.</td>
<td>No</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the Unified CM Server</td>
<td>None</td>
<td>Any text</td>
<td>No</td>
</tr>
<tr>
<td>Device Admin URL</td>
<td>The Administration URL for the Unified CM Server</td>
<td>None</td>
<td>A valid URL. The Operations Console validates the URL for syntax errors but does no validation for the existence of the URL.</td>
<td>No</td>
</tr>
</tbody>
</table>

**Enable Synchronization**

<table>
<thead>
<tr>
<th>Enable synchronization</th>
<th>Select to enable synchronization for location. If enabled, the Operations Console extracts or synchronizes the Unified CM location information from the Unified CM server.</th>
<th>Disabled When you enable this service, the default value of the Port is 8443.</th>
<th>Enabled or Disabled</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>User name to access the Unified CM AXL interface.</td>
<td>None</td>
<td>Valid Unified CM AXL username.</td>
<td>No</td>
</tr>
<tr>
<td>Password</td>
<td>Password to access the Unified CM AXL interface.</td>
<td>None</td>
<td>Valid Unified CM AXL password.</td>
<td>No</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Default</td>
<td>Value</td>
<td>Restart Required</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>--------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Retype the password to verify that you typed the password correctly.</td>
<td>None</td>
<td>Text must match the text entered in the Password field</td>
<td>No</td>
</tr>
<tr>
<td>Port</td>
<td>The port to which the Unified CM server connects while establishing initial contact.</td>
<td>8443</td>
<td>1 through 65,535</td>
<td>No</td>
</tr>
</tbody>
</table>
SIP Devices Configuration

- Set Up Ingress Gateway to Use Redundant Proxy Servers, page 165
- Set Up Call Server with Redundant Proxy Servers, page 165
- Local SRV File Configuration Example for SIP Messaging Redundancy, page 166
- Load-Balancing SIP Calls, page 166
- Set Up Ingress Gateway to Use Redundant Proxy Servers, page 166
- Set Up Call Server with Redundant Proxy Servers, page 166
- Cisco Unified SIP Proxy (CUSP) Configuration, page 166
- Configure Custom Streaming Ringtones, page 169

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).

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 25 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.

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).


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 tla 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 TUI 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
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 to 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 associate a dialed number pattern with a custom ringtone.

<table>
<thead>
<tr>
<th>Table 32: Dialed Number Pattern Configuration Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Property</strong></td>
</tr>
<tr>
<td>General Configuration</td>
</tr>
</tbody>
</table>

```plaintext
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
```
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dialed Number Pattern</td>
<td>The actual Dialed Number Pattern.</td>
<td>None</td>
<td>Must be unique</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Maximum length of 24 characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Can contain alphanumeric characters,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>wildcard characters, such as exclamation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>point (!) or asterisk (*), single digit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>matches such as the letter X or period (.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Can end with an optional greater than</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(&gt; ) wildcard character</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the Dialed Number Pattern.</td>
<td>None</td>
<td>Maximum length of 1024 characters</td>
</tr>
<tr>
<td>Enable Custom Ringtone</td>
<td>Enables customized ring tone.</td>
<td>Disabled</td>
<td>Maximum length of 256 characters</td>
</tr>
<tr>
<td></td>
<td>• <strong>Ringtone media filename</strong> - Enter the name of the file that is to be</td>
<td>none</td>
<td>Cannot contain whitespace characters</td>
</tr>
<tr>
<td></td>
<td>played for the respective dialed number pattern. Provide the URL for the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>stream name in the following format:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>rtsp://&lt;streaming server IP address&gt;:&lt;port&gt;/&lt;directory&gt;/&lt;filename&gt;.rm</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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:

```bash
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 10

Media Server Configuration

- Configure Media Server, page 173
- Media Server Settings, page 174
- Media File Names and Types, page 175
- Location of Media Files, page 176
- Media File Address, page 176
- Locale Backward Compatibility, page 179
- System Media Files, page 180

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 174.
   b) Device Pool tab. For more information about adding, deleting and editing device pool, see Add or Remove Device From Device Pool, on page 93.

**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.
## Media Server Settings

### General Settings

**Table 33: Media Server—General Tab Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of Media Server</td>
<td>None</td>
<td>Valid IP address.</td>
<td>No</td>
</tr>
<tr>
<td>Hostname</td>
<td>The name of the Media Server</td>
<td>None</td>
<td>Follow naming conventions for hostnames.</td>
<td>No</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the Media Server</td>
<td>None</td>
<td>Up to 1,024 characters.</td>
<td>No</td>
</tr>
<tr>
<td>FTP Enabled</td>
<td>Indicates whether a Media Server has FTP Enabled. A Media Server, which that 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 to FTP the agent greeting recording.</td>
<td>Disabled</td>
<td>Select the check box to enable this feature.</td>
<td>No Use <strong>Test Sign-in</strong> button to verify the FTP credentials.</td>
</tr>
<tr>
<td>Anonymous Access</td>
<td>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).</td>
<td>Disabled</td>
<td>Select the check box to enable this feature. You must enable FTP to enable Anonymous Access.</td>
<td>No Use <strong>Test Sign-in</strong> button to verify the FTP credentials.</td>
</tr>
</tbody>
</table>
### 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 underscore 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 13: 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 executed. 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 34: Media File Address Components

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Location of Data</th>
<th>Description</th>
<th>Examples</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Server Set</td>
<td>ECC variable: user.microapp.media_server</td>
<td>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.</td>
<td>Base URL example: <a href="http://www.machine1.com/dir1/dirs/cust1">http://www.machine1.com/dir1/dirs/cust1</a></td>
<td>By convention, the service provider may include their customer names at the end of the Media Server set.</td>
</tr>
<tr>
<td>Locale</td>
<td>ECC variable: user.microapp.locale Default: en-us</td>
<td>This field is a combination of language and country with a default of en-us for English spoken in the United States.</td>
<td>en-us</td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Location of Data</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>The Media Library Type value passed from the VRU Script Name field. Valid options are:</td>
<td>The media library (directory) for the prompt is either the application prompt library defined by ECC variable <code>user.microapp.app_media_lib</code> (default &quot;app&quot;) or the system prompt library defined by ECC variable <code>user.microapp.sys_media_lib</code> (default &quot;sys&quot;).</td>
<td>A (user.microapp.app_media_lib= app_banking)</td>
</tr>
<tr>
<td>Media Library Type</td>
<td><strong>A</strong> - Application prompt library. <strong>S</strong> - System prompt library. <strong>V</strong> - External VXML. <strong>Default:</strong> A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Media Library Type</td>
<td>When the Media Library Type is V (external VXML), the VXML file will reside in the Application Prompt Library. 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 &quot;app&quot; directory, you must create an app directory in <code>./MediaFiles/en-us</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong></td>
<td></td>
</tr>
</tbody>
</table>
### 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

**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.

Based on the examples shown in the table above, a valid address for the Media File might be:


### 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 us" (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 35: System Media Files, Cardinal Numbers

<table>
<thead>
<tr>
<th>Symbol (where applicable)</th>
<th>Decimal Value</th>
<th>Media File Name</th>
<th>Media File Content</th>
<th>Data Play Back Types / When Media File Is Used</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>point</td>
<td>point</td>
<td>Number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>minus</td>
<td>minus</td>
<td>Number</td>
</tr>
<tr>
<td>0</td>
<td>48</td>
<td>0</td>
<td>zero</td>
<td>All except DOW</td>
</tr>
<tr>
<td>1</td>
<td>49</td>
<td>1</td>
<td>one (masculine version), uno (es-mx and es-es)</td>
<td>All except DOW</td>
</tr>
<tr>
<td>2</td>
<td>50</td>
<td>2</td>
<td>two</td>
<td>All except DOW</td>
</tr>
<tr>
<td>3</td>
<td>51</td>
<td>3</td>
<td>three</td>
<td>All except DOW</td>
</tr>
<tr>
<td>4</td>
<td>52</td>
<td>4</td>
<td>four</td>
<td>All except DOW</td>
</tr>
<tr>
<td>5</td>
<td>53</td>
<td>5</td>
<td>five</td>
<td>All except DOW</td>
</tr>
<tr>
<td>6</td>
<td>54</td>
<td>6</td>
<td>six</td>
<td>All except DOW</td>
</tr>
<tr>
<td>7</td>
<td>55</td>
<td>7</td>
<td>seven</td>
<td>All except DOW</td>
</tr>
<tr>
<td>Symbol (where applicable)</td>
<td>Decimal Value</td>
<td>Media File Name</td>
<td>Media File Content</td>
<td>Data Play Back Types / When Media File Is Used</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------</td>
<td>-----------------</td>
<td>-------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>8</td>
<td>56</td>
<td>8</td>
<td>eight</td>
<td>All except DOW</td>
</tr>
<tr>
<td>9</td>
<td>57</td>
<td>9</td>
<td>nine</td>
<td>All except DOW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10</td>
<td>ten</td>
<td>Same for the rest of all the numbers</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td>eleven</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td>twelve</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td>thirteen</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td>fourteen</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td>fifteen</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td>sixteen</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
<td>seventeen</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td>eighteen</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
<td></td>
<td>nineteen</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td>twenty</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td></td>
<td></td>
<td>twenty-one</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td></td>
<td></td>
<td>twenty-two</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
<td></td>
<td>twenty-three</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
<td></td>
<td>twenty-four</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td></td>
<td></td>
<td>twenty-five</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td></td>
<td></td>
<td>twenty-six</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td></td>
<td></td>
<td>twenty-seven</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td></td>
<td></td>
<td>twenty-eight</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td></td>
<td></td>
<td>twenty-nine</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td></td>
<td></td>
<td>thirty</td>
<td></td>
</tr>
<tr>
<td>Symbol (where applicable)</td>
<td>Decimal Value</td>
<td>Media File Name</td>
<td>Media File Content</td>
<td>Data Play Back Types / When Media File Is Used</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------</td>
<td>------------------</td>
<td>--------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>31</td>
<td>thirty-one</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>thirty-two</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>33</td>
<td>thirty-three</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>34</td>
<td>thirty-four</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>35</td>
<td>thirty-five</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>36</td>
<td>thirty-six</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>37</td>
<td>thirty-seven</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>38</td>
<td>thirty-eight</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>39</td>
<td>thirty-nine</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>forty</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>41</td>
<td>forty-one</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>42</td>
<td>forty-two</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>43</td>
<td>forty-three</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>44</td>
<td>forty-four</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>45</td>
<td>forty-five</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>46</td>
<td>forty-six</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>47</td>
<td>forty-seven</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>48</td>
<td>forty-eight</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>49</td>
<td>forty-nine</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>50</td>
<td>fifty</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>51</td>
<td>fifty-one</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>52</td>
<td>fifty-two</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>53</td>
<td>fifty-three</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>54</td>
<td>fifty-four</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symbol (where applicable)</td>
<td>Decimal Value</td>
<td>Media File Name</td>
<td>Media File Content</td>
<td>Data Play Back Types / When Media File Is Used</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------</td>
<td>----------------</td>
<td>-------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>55</td>
<td>fifty-five</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>fifty-six</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>fifty-seven</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>fifty-eight</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>fifty-nine</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>sixty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>sixty-one</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>sixty-two</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>sixty-three</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>sixty-four</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>sixty-five</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>66</td>
<td>sixty-six</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>67</td>
<td>sixty-seven</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>68</td>
<td>sixty-eight</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>69</td>
<td>sixty-nine</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>seventy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>71</td>
<td>seventy-one</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>72</td>
<td>seventy-two</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>73</td>
<td>seventy-three</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>74</td>
<td>seventy-four</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>75</td>
<td>seventy-five</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>76</td>
<td>seventy-six</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>77</td>
<td>seventy-seven</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>78</td>
<td>seventy-eight</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symbol (where applicable)</td>
<td>Decimal Value</td>
<td>Media File Name</td>
<td>Media File Content</td>
<td>Data Play Back Types / When Media File Is Used</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------</td>
<td>----------------</td>
<td>-------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>79</td>
<td>seventy-nine</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>eighty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>81</td>
<td>eighty-one</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>82</td>
<td>eighty-two</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>83</td>
<td>eighty-three</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>84</td>
<td>eighty-four</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>85</td>
<td>eighty-five</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>86</td>
<td>eighty-six</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>87</td>
<td>eighty-seven</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>eighty-eight</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>89</td>
<td>eighty-nine</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>90</td>
<td>ninety</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>ninety-one</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>92</td>
<td>ninety-two</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>93</td>
<td>ninety-three</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>94</td>
<td>ninety-four</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>95</td>
<td>ninety-five</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>96</td>
<td>ninety-six</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>ninety-seven</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>98</td>
<td>ninety-eight</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>99</td>
<td>ninety-nine</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>oh</td>
<td>oh</td>
<td></td>
<td></td>
<td>24TOD, Date</td>
</tr>
<tr>
<td>hundred</td>
<td>hundred</td>
<td></td>
<td></td>
<td>Number, 24TOD, Date, Currency</td>
</tr>
</tbody>
</table>
The table that follows lists the System Media File information for ordinal numbers.

**Table 36: System Media Files, Ordinal Numbers**

<table>
<thead>
<tr>
<th>Symbol (where applicable)</th>
<th>Decimal Value</th>
<th>Media File Name</th>
<th>Media File Content</th>
<th>Data Play Back Types / When Media File Is Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>1ord</td>
<td>first</td>
<td>Date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2ord</td>
<td>second</td>
<td>Date for all ordinal numbers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ord</td>
<td>third</td>
<td>Date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4ord</td>
<td>fourth</td>
<td>Date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5ord</td>
<td>fifth</td>
<td>Date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6ord</td>
<td>sixth</td>
<td>Date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7ord</td>
<td>seventh</td>
<td>Date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8ord</td>
<td>eighth</td>
<td>Date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9ord</td>
<td>ninth</td>
<td>Date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10ord</td>
<td>tenth</td>
<td>Date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11ord</td>
<td>eleventh</td>
<td>Date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symbol (when applicable)</td>
<td>Decimal Value</td>
<td>Media File Name</td>
<td>Media File Content</td>
<td>Data Play Back Types / When Media File Is Used</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------</td>
<td>-----------------</td>
<td>-------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>12ord</td>
<td>twelfth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>13ord</td>
<td>thirteenth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>14ord</td>
<td>fourteenth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>15ord</td>
<td>fifteenth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>16ord</td>
<td>sixteenth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>17ord</td>
<td>seventeenth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>18ord</td>
<td>eighteenth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>19ord</td>
<td>nineteenth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>20ord</td>
<td>twentieth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>21ord</td>
<td>twenty-first</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>22ord</td>
<td>twenty-second</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>23ord</td>
<td>twenty-third</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>24ord</td>
<td>twenty-fourth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>25ord</td>
<td>twenty-fifth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>26ord</td>
<td>twenty-sixth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>27ord</td>
<td>twenty-seventh</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>28ord</td>
<td>twenty-eighth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>29ord</td>
<td>twenty-nineth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>30ord</td>
<td>thirtieth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>31ord</td>
<td>thirty-first</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The table that follows lists the System Media File information for measurements.
### Table 37: System Media Files, Measurements

<table>
<thead>
<tr>
<th>Symbol (where applicable)</th>
<th>Decimal Value</th>
<th>Media File Name</th>
<th>Media File Content</th>
<th>Data Play Back Types / When Media File Is Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>½</td>
<td>189</td>
<td>one_half</td>
<td>one half</td>
<td>Char</td>
</tr>
<tr>
<td>¼</td>
<td>188</td>
<td>one_quarter</td>
<td>one quarter</td>
<td>Char</td>
</tr>
<tr>
<td>¾</td>
<td>190</td>
<td>three_quarters</td>
<td>three quarters</td>
<td>Char</td>
</tr>
<tr>
<td>A,a</td>
<td>65,97</td>
<td>a</td>
<td>A</td>
<td>Char</td>
</tr>
<tr>
<td>B,b</td>
<td>66,98</td>
<td>b</td>
<td>B</td>
<td>Char</td>
</tr>
<tr>
<td>C,c</td>
<td>67,99</td>
<td>c</td>
<td>C</td>
<td>Char</td>
</tr>
<tr>
<td>D,d</td>
<td>68,100</td>
<td>d</td>
<td>D</td>
<td>Char</td>
</tr>
<tr>
<td>E,e</td>
<td>69,101</td>
<td>e</td>
<td>E</td>
<td>Char</td>
</tr>
<tr>
<td>F,f</td>
<td>70,102</td>
<td>f</td>
<td>F</td>
<td>Char</td>
</tr>
<tr>
<td>G,g</td>
<td>71,103</td>
<td>g</td>
<td>G</td>
<td>Char</td>
</tr>
<tr>
<td>H,h</td>
<td>72,104</td>
<td>h</td>
<td>H</td>
<td>Char</td>
</tr>
<tr>
<td>I,i</td>
<td>73,105</td>
<td>i</td>
<td>I</td>
<td>Char</td>
</tr>
<tr>
<td>J,j</td>
<td>74,106</td>
<td>j</td>
<td>J</td>
<td>Char</td>
</tr>
<tr>
<td>K,k</td>
<td>75,107</td>
<td>k</td>
<td>K</td>
<td>Char</td>
</tr>
<tr>
<td>L,l</td>
<td>76,108</td>
<td>l</td>
<td>L</td>
<td>Char</td>
</tr>
<tr>
<td>M,m</td>
<td>77,109</td>
<td>m</td>
<td>M</td>
<td>Char</td>
</tr>
<tr>
<td>N,n</td>
<td>78,110</td>
<td>n</td>
<td>N</td>
<td>Char</td>
</tr>
<tr>
<td>O,o</td>
<td>79,111</td>
<td>o</td>
<td>O</td>
<td>Char</td>
</tr>
<tr>
<td>P,p</td>
<td>80,112</td>
<td>p</td>
<td>P</td>
<td>Char</td>
</tr>
<tr>
<td>Q,q</td>
<td>81,113</td>
<td>q</td>
<td>Q</td>
<td>Char</td>
</tr>
<tr>
<td>R,r</td>
<td>82,114</td>
<td>r</td>
<td>R</td>
<td>Char</td>
</tr>
<tr>
<td>S,s</td>
<td>83,115</td>
<td>s</td>
<td>S</td>
<td>Char</td>
</tr>
<tr>
<td>T,t</td>
<td>84,116</td>
<td>t</td>
<td>T</td>
<td>Char</td>
</tr>
<tr>
<td>Symbol (where applicable)</td>
<td>Decimal Value</td>
<td>Media File Name</td>
<td>Media File Content</td>
<td>Data Play Back Types / When Media File Is Used</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------</td>
<td>----------------</td>
<td>-------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>U, u</td>
<td>85,117</td>
<td>u</td>
<td>U</td>
<td>Char</td>
</tr>
<tr>
<td>V, v</td>
<td>86,118</td>
<td>v</td>
<td>V</td>
<td>Char</td>
</tr>
<tr>
<td>W, w</td>
<td>87,119</td>
<td>w</td>
<td>W</td>
<td>Char</td>
</tr>
<tr>
<td>X, x</td>
<td>88,120</td>
<td>x</td>
<td>X</td>
<td>Char</td>
</tr>
<tr>
<td>Y, y</td>
<td>89,121</td>
<td>y</td>
<td>Y</td>
<td>Char</td>
</tr>
<tr>
<td>Z, z</td>
<td>90,122</td>
<td>z</td>
<td>Z</td>
<td>Char</td>
</tr>
<tr>
<td>OE, oe</td>
<td>140,156</td>
<td>oe_140_156</td>
<td>Ligature OE</td>
<td>Char</td>
</tr>
<tr>
<td>Á, à</td>
<td>192,224</td>
<td>a_192_224</td>
<td>A grave</td>
<td>Char</td>
</tr>
<tr>
<td>Á, á</td>
<td>193,225</td>
<td>a_193_225</td>
<td>A acute</td>
<td>Char</td>
</tr>
<tr>
<td>Â, â</td>
<td>194,226</td>
<td>a_194_226</td>
<td>A circumflex</td>
<td>Char</td>
</tr>
<tr>
<td>Ä, ä</td>
<td>195,227</td>
<td>a_195_227</td>
<td>A tilde</td>
<td>Char</td>
</tr>
<tr>
<td>Ä, ä</td>
<td>196,228</td>
<td>a_196_228</td>
<td>A umlaut</td>
<td>Char</td>
</tr>
<tr>
<td>Ä, ä</td>
<td>197,229</td>
<td>a_197_229</td>
<td>A with ring above</td>
<td>Char</td>
</tr>
<tr>
<td>Æ, æ</td>
<td>198,230</td>
<td>ae_198_230</td>
<td>Ligature AE</td>
<td>Char</td>
</tr>
<tr>
<td>É, è</td>
<td>200,232</td>
<td>e_200_232</td>
<td>E grave</td>
<td>Char</td>
</tr>
<tr>
<td>É, é</td>
<td>201,233</td>
<td>e_201_233</td>
<td>E acute</td>
<td>Char</td>
</tr>
<tr>
<td>È, ê</td>
<td>202,234</td>
<td>e_202_234</td>
<td>E circumflex</td>
<td>Char</td>
</tr>
<tr>
<td>Ê, ê</td>
<td>203,235</td>
<td>e_203_235</td>
<td>E umlaut</td>
<td></td>
</tr>
<tr>
<td>I,i</td>
<td>204,236</td>
<td>i_204_236</td>
<td>I grave</td>
<td>Char</td>
</tr>
<tr>
<td>Í, í</td>
<td>205,237</td>
<td>i_205</td>
<td>I acute</td>
<td>Char</td>
</tr>
<tr>
<td>Í, í</td>
<td>206,238</td>
<td>i_206</td>
<td>I circumflex</td>
<td>Char</td>
</tr>
<tr>
<td>Í, í</td>
<td>207,239</td>
<td>i_207</td>
<td>I umlaut</td>
<td>Char</td>
</tr>
<tr>
<td>D</td>
<td>208</td>
<td>char_208</td>
<td>character 208</td>
<td>Char</td>
</tr>
</tbody>
</table>
The table that follows lists the System Media File information for month values.

**Table 38: System Media Files, Months**

<table>
<thead>
<tr>
<th>Symbol (where applicable)</th>
<th>Decimal Value</th>
<th>Media File Name</th>
<th>Media File Content</th>
<th>Data Play Back Types / When Media File Is Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>ð</td>
<td>240</td>
<td>char_240</td>
<td>character 240</td>
<td></td>
</tr>
<tr>
<td>Õ,ø</td>
<td>210,242</td>
<td>o_210_242</td>
<td>O grave</td>
<td>Char</td>
</tr>
<tr>
<td>Õ,ö</td>
<td>211,243</td>
<td>o_211_243</td>
<td>O acute</td>
<td>Char</td>
</tr>
<tr>
<td>Õ,ô</td>
<td>212,244</td>
<td>o_212_244</td>
<td>O circumflex</td>
<td>Char</td>
</tr>
<tr>
<td>Õ,ö</td>
<td>213,245</td>
<td>o_213_245</td>
<td>O tilde</td>
<td>Char</td>
</tr>
<tr>
<td>Õ,ö</td>
<td>214,246</td>
<td>o_214_246</td>
<td>O umlaut</td>
<td>Char</td>
</tr>
<tr>
<td>x</td>
<td>215</td>
<td>multiply</td>
<td>multiplication sign</td>
<td>Char</td>
</tr>
<tr>
<td>Ø,ø</td>
<td>216,248</td>
<td>o_216_248</td>
<td>oh stroke</td>
<td>Char</td>
</tr>
<tr>
<td>Ú,û</td>
<td>217,249</td>
<td>u_217_249</td>
<td>U grave</td>
<td>Char</td>
</tr>
<tr>
<td>Ú,ü</td>
<td>218,250</td>
<td>u_218_250</td>
<td>U acute</td>
<td>Char</td>
</tr>
<tr>
<td>Ú,û</td>
<td>219,251</td>
<td>u_219_251</td>
<td>U circumflex</td>
<td>Char</td>
</tr>
<tr>
<td>Ú,ü</td>
<td>220,252</td>
<td>u_220_252</td>
<td>U umlaut</td>
<td>Char</td>
</tr>
<tr>
<td>Ÿ,ý</td>
<td>221,253</td>
<td>y_221_253</td>
<td>Y acute</td>
<td>Char</td>
</tr>
<tr>
<td>þ</td>
<td>222</td>
<td>char_222</td>
<td>character 222</td>
<td>Char</td>
</tr>
<tr>
<td>β</td>
<td>223</td>
<td>ss</td>
<td>double s</td>
<td>Char</td>
</tr>
<tr>
<td>±</td>
<td>247</td>
<td>divide</td>
<td>division sign</td>
<td>Char</td>
</tr>
<tr>
<td>þ</td>
<td>254</td>
<td>char_254</td>
<td>character 254</td>
<td>Char</td>
</tr>
<tr>
<td>Ÿ,ý</td>
<td>159,255</td>
<td>y_159_255</td>
<td>character 159 or 255</td>
<td>Char</td>
</tr>
</tbody>
</table>
The table that follows lists the System Media File information for month values.

**Table 39: System Media Files, Days**

<table>
<thead>
<tr>
<th>Symbol (where applicable)</th>
<th>Decimal Value</th>
<th>Media File Name</th>
<th>Media File Content</th>
<th>Data Play Back Types / When Media File Is Used</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Sunday</td>
<td>Sunday</td>
<td>DOW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monday</td>
<td>Monday</td>
<td>DOW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tuesday</td>
<td>Tuesday</td>
<td>DOW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wednesday</td>
<td>Wednesday</td>
<td>DOW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Thursday</td>
<td>Thursday</td>
<td>DOW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Friday</td>
<td>Friday</td>
<td>DOW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Saturday</td>
<td>Saturday</td>
<td>DOW</td>
</tr>
</tbody>
</table>
The table that follows lists the System Media File information for month values.

### Table 40: System Media Files, Time

<table>
<thead>
<tr>
<th>Symbol (where applicable)</th>
<th>Decimal Value</th>
<th>Media File Name</th>
<th>Media File Content</th>
<th>Data Play Back Types / When Media File Is Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>hour</td>
<td>hour</td>
<td></td>
<td></td>
<td>Etine, 24 TOD per locale, TOD per locale</td>
</tr>
<tr>
<td>hours</td>
<td>hours</td>
<td></td>
<td></td>
<td>Etine, 24 TOD per locale, TOD per locale</td>
</tr>
<tr>
<td>minute</td>
<td>minute</td>
<td></td>
<td></td>
<td>Etine</td>
</tr>
<tr>
<td>minutes</td>
<td>minutes</td>
<td></td>
<td></td>
<td>Etine</td>
</tr>
<tr>
<td>second</td>
<td>second</td>
<td></td>
<td></td>
<td>Etine, 24 TOD</td>
</tr>
<tr>
<td>seconds</td>
<td>seconds</td>
<td></td>
<td></td>
<td>Etine, 24 TOD</td>
</tr>
<tr>
<td>on</td>
<td>on</td>
<td></td>
<td></td>
<td>per locale (unused for en-us)</td>
</tr>
<tr>
<td>at</td>
<td>at</td>
<td></td>
<td></td>
<td>per locale (unused for en-us)</td>
</tr>
<tr>
<td>am</td>
<td>am</td>
<td></td>
<td></td>
<td>TOD</td>
</tr>
<tr>
<td>pm</td>
<td>pm</td>
<td></td>
<td></td>
<td>TOD</td>
</tr>
<tr>
<td>o'clock</td>
<td>o'clock</td>
<td></td>
<td></td>
<td>TOD</td>
</tr>
</tbody>
</table>

The table that follows lists the System Media File information for currency values.

---

**Note**

The customer’s Media Administrator may prefer to replace the contents of "currency_minus" (for the negative amount) and “currency_and” (the latter can even be changed to contain silence).

### Table 41: System Media Files, Currency

<table>
<thead>
<tr>
<th>Symbol (where applicable)</th>
<th>Decimal Value</th>
<th>Media File Name</th>
<th>Media File Content</th>
<th>Data Play Back Types / When Media File Is Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>currency_minus</td>
<td>minus</td>
<td></td>
<td></td>
<td>Currency</td>
</tr>
</tbody>
</table>
The table that follows lists the System Media File information for gaps of silence and miscellaneous phrases.

<table>
<thead>
<tr>
<th>Symbol (where applicable)</th>
<th>Decimal Value</th>
<th>Media File Name</th>
<th>Media File Content</th>
<th>Data Play Back Types / When Media File Is Used</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>currency_and</td>
<td>and</td>
<td>Currency</td>
</tr>
<tr>
<td>$</td>
<td>36</td>
<td>USD_dollar</td>
<td>dollar</td>
<td>Currency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>USD_dollars</td>
<td>dollars</td>
<td>Currency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>USD_dollar.wav</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>USD_dollars.wav</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td>Unified CVP uses the USD_dollar.wav and USD_dollars.wav media files; the dollar.wav and dollars.wav used by ISN Version 1.0 are no longer installed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$</td>
<td>36</td>
<td>CAD_dollar</td>
<td>dollar</td>
<td>Currency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CAD_dollars</td>
<td>dollars</td>
<td>Currency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HKD_dollar</td>
<td>dollar</td>
<td>Currency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HKD_dollars</td>
<td>dollars</td>
<td>Currency</td>
</tr>
<tr>
<td>€</td>
<td>162</td>
<td>cent</td>
<td>cent</td>
<td>Currency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cents</td>
<td>cents</td>
<td>Currency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>euro</td>
<td>euro</td>
<td>Currency</td>
</tr>
<tr>
<td>£</td>
<td>163</td>
<td>GBP_pound</td>
<td>pound</td>
<td>Currency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GBP_pounds</td>
<td>pounds</td>
<td>Currency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>penny</td>
<td>penny</td>
<td>Currency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pence</td>
<td>pence</td>
<td>Currency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MXN_peso</td>
<td>peso</td>
<td>Currency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MXN_pesos</td>
<td>pesos</td>
<td>Currency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>centavo</td>
<td>centavo</td>
<td>Currency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>centavos</td>
<td>centavos</td>
<td>Currency</td>
</tr>
</tbody>
</table>
### Table 42: System Media Files, Silence and Miscellaneous Phrases

<table>
<thead>
<tr>
<th>Symbol (where applicable)</th>
<th>Decimal Value</th>
<th>Media File Name</th>
<th>Media File Content</th>
<th>Data Play Back Types / When Media File Is Used</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>silence_.1_sec</td>
<td>(.1 second of silence)</td>
<td>Used for pauses where needed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>silence_.25_sec</td>
<td>(.25 second of silence)</td>
<td>Used for pauses where needed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>silence_.5_sec</td>
<td>(.5 second of silence)</td>
<td>Used for pauses where needed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>silence_1_sec</td>
<td>(1 second of silence)</td>
<td>Used for pauses where needed</td>
</tr>
</tbody>
</table>

The table that follows lists the System Media File information for ANSI characters.

### Table 43: System Media Files, ANSI Characters

<table>
<thead>
<tr>
<th>Symbol (where applicable)</th>
<th>Decimal Value</th>
<th>Media File Name</th>
<th>Media File Content</th>
<th>Data Play Back Types / When Media File Is Used</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>32</td>
<td>space</td>
<td>space</td>
<td>Char</td>
</tr>
<tr>
<td></td>
<td>33</td>
<td>exclamation_mark</td>
<td>exclamation mark</td>
<td>Char</td>
</tr>
<tr>
<td></td>
<td>34</td>
<td>double_quote</td>
<td>double quote</td>
<td>Char</td>
</tr>
<tr>
<td></td>
<td>35</td>
<td>pound</td>
<td>pound</td>
<td>Char</td>
</tr>
<tr>
<td></td>
<td>37</td>
<td>percent</td>
<td>percent</td>
<td>Char</td>
</tr>
<tr>
<td></td>
<td>38</td>
<td>ampersand</td>
<td>ampersand</td>
<td>Char</td>
</tr>
<tr>
<td></td>
<td>39</td>
<td>apostrophe</td>
<td>apostrophe</td>
<td>Char</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>open_parenthesis</td>
<td>open parenthesis</td>
<td>Char</td>
</tr>
<tr>
<td></td>
<td>41</td>
<td>close_parenthesis</td>
<td>close parenthesis</td>
<td>Char</td>
</tr>
<tr>
<td></td>
<td>42</td>
<td>asterisk</td>
<td>asterisk</td>
<td>Char</td>
</tr>
<tr>
<td></td>
<td>43</td>
<td>plus</td>
<td>plus</td>
<td>Char</td>
</tr>
<tr>
<td>Symbol (where applicable)</td>
<td>Decimal Value</td>
<td>Media File Name</td>
<td>Media File Content</td>
<td>Data Play Back Types / When Media File Is Used</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------</td>
<td>----------------</td>
<td>--------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>,</td>
<td>44</td>
<td>comma</td>
<td>comma</td>
<td>Char</td>
</tr>
<tr>
<td>-</td>
<td>45</td>
<td>hyphen</td>
<td>hyphen</td>
<td>Char</td>
</tr>
<tr>
<td>.</td>
<td>46</td>
<td>period</td>
<td>period</td>
<td>Char</td>
</tr>
<tr>
<td>/</td>
<td>47</td>
<td>slash</td>
<td>slash</td>
<td>Char</td>
</tr>
<tr>
<td>:</td>
<td>58</td>
<td>colon</td>
<td>colon</td>
<td>Char</td>
</tr>
<tr>
<td>;</td>
<td>59</td>
<td>semicolon</td>
<td>semicolon</td>
<td>Char</td>
</tr>
<tr>
<td>&lt;</td>
<td>60</td>
<td>less_than</td>
<td>less than</td>
<td>Char</td>
</tr>
<tr>
<td>=</td>
<td>61</td>
<td>equal</td>
<td>equal</td>
<td>Char</td>
</tr>
<tr>
<td>&gt;</td>
<td>62</td>
<td>greater_than</td>
<td>greater than</td>
<td>Char</td>
</tr>
<tr>
<td>?</td>
<td>63</td>
<td>question_mark</td>
<td>question mark</td>
<td>Char</td>
</tr>
<tr>
<td>@</td>
<td>64</td>
<td>at_symbol</td>
<td>at</td>
<td>Char</td>
</tr>
<tr>
<td>[</td>
<td>91</td>
<td>left_square_bracket</td>
<td>left square bracket</td>
<td>Char</td>
</tr>
<tr>
<td>\</td>
<td>92</td>
<td>backslash</td>
<td>backslash</td>
<td>Char</td>
</tr>
<tr>
<td>]</td>
<td>93</td>
<td>right_square_bracket</td>
<td>right square bracket</td>
<td>Char</td>
</tr>
<tr>
<td>^</td>
<td>94</td>
<td>caret</td>
<td>caret</td>
<td>Char</td>
</tr>
<tr>
<td>_</td>
<td>95</td>
<td>underscore</td>
<td>underscore</td>
<td>Char</td>
</tr>
<tr>
<td>`</td>
<td>96</td>
<td>single_quote</td>
<td>single quote</td>
<td>Char</td>
</tr>
<tr>
<td>{</td>
<td>123</td>
<td>open_brace</td>
<td>open brace</td>
<td>Char</td>
</tr>
<tr>
<td></td>
<td></td>
<td>124</td>
<td>pipe</td>
<td>pipe</td>
</tr>
<tr>
<td>}</td>
<td>125</td>
<td>close_brace</td>
<td>close brace</td>
<td>Char</td>
</tr>
<tr>
<td>~</td>
<td>126</td>
<td>tilde</td>
<td>tilde</td>
<td>Char</td>
</tr>
<tr>
<td>’</td>
<td>130</td>
<td>char_130</td>
<td>low single quote</td>
<td>Char</td>
</tr>
<tr>
<td>f</td>
<td>131</td>
<td>char_131</td>
<td>F with hook</td>
<td>Char</td>
</tr>
<tr>
<td>Symbol (where applicable)</td>
<td>Decimal Value</td>
<td>Media File Name</td>
<td>Media File Content</td>
<td>Data Play Back Types / When Media File Is Used</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------</td>
<td>----------------------</td>
<td>----------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>&quot;</td>
<td>132</td>
<td>low double quote</td>
<td>low double quote</td>
<td>Char</td>
</tr>
<tr>
<td>…</td>
<td>133</td>
<td>ellipsis</td>
<td>ellipsis</td>
<td>Char</td>
</tr>
<tr>
<td>†</td>
<td>134</td>
<td>char_134</td>
<td>character 134</td>
<td>Char</td>
</tr>
<tr>
<td>‡</td>
<td>135</td>
<td>char_135</td>
<td>character 135</td>
<td>Char</td>
</tr>
<tr>
<td>^</td>
<td>136</td>
<td>char_136</td>
<td>character 136</td>
<td>Char</td>
</tr>
<tr>
<td>‰</td>
<td>137</td>
<td>per_mille</td>
<td>per mile</td>
<td>Char</td>
</tr>
<tr>
<td>Š</td>
<td>138</td>
<td>char_138</td>
<td>character 138</td>
<td></td>
</tr>
<tr>
<td>&lt;</td>
<td>139</td>
<td>left_pointing_angle</td>
<td>left pointing angle</td>
<td>Char</td>
</tr>
<tr>
<td>’</td>
<td>145</td>
<td>left_single_quote</td>
<td>left single quote</td>
<td>Char</td>
</tr>
<tr>
<td>’</td>
<td>146</td>
<td>right_single_quote</td>
<td>right single quote</td>
<td>Char</td>
</tr>
<tr>
<td>“</td>
<td>147</td>
<td>left_double_quote</td>
<td>left double quote</td>
<td>Char</td>
</tr>
<tr>
<td>”</td>
<td>148</td>
<td>right_double_quote</td>
<td>right double quote</td>
<td>Char</td>
</tr>
<tr>
<td>·</td>
<td>149</td>
<td>bullet</td>
<td>bullet</td>
<td>Char</td>
</tr>
<tr>
<td>–</td>
<td>150</td>
<td>en_dash</td>
<td>en dash</td>
<td>Char</td>
</tr>
<tr>
<td>—</td>
<td>151</td>
<td>em_dash</td>
<td>em dash</td>
<td></td>
</tr>
<tr>
<td>“</td>
<td>152</td>
<td>small_tilde</td>
<td>small tilde</td>
<td>Char</td>
</tr>
<tr>
<td>™</td>
<td>153</td>
<td>trade_mark</td>
<td>trade mark</td>
<td>Char</td>
</tr>
<tr>
<td>Š</td>
<td>154</td>
<td>char_154</td>
<td>character 154</td>
<td>Char</td>
</tr>
<tr>
<td>›</td>
<td>155</td>
<td>char_155</td>
<td>character 155</td>
<td>Char</td>
</tr>
<tr>
<td>¡</td>
<td>161</td>
<td>exclamation_mark_inverted</td>
<td>inverted exclamation mark</td>
<td>Char</td>
</tr>
<tr>
<td>†</td>
<td>164</td>
<td>char_164</td>
<td>character 164</td>
<td>Char</td>
</tr>
<tr>
<td>†</td>
<td>166</td>
<td>broken_pipe</td>
<td>broken pipe</td>
<td>Char</td>
</tr>
<tr>
<td>§</td>
<td>167</td>
<td>section</td>
<td>section</td>
<td>Char</td>
</tr>
</tbody>
</table>
### Data Play Back

<table>
<thead>
<tr>
<th>Symbol (where applicable)</th>
<th>Decimal Value</th>
<th>Media File Name</th>
<th>Media File Content</th>
<th>Data Play Back Types / When Media File Is Used</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>¨</code></td>
<td>168</td>
<td>char_168</td>
<td>character 168</td>
<td>Char</td>
</tr>
<tr>
<td>©</td>
<td>169</td>
<td>copyright</td>
<td>copyright</td>
<td>Char</td>
</tr>
<tr>
<td>a</td>
<td>170</td>
<td>char_170</td>
<td>character 170</td>
<td>Char</td>
</tr>
<tr>
<td>«</td>
<td>171</td>
<td>left_double_angle_quote</td>
<td>left double angle quote</td>
<td>Char</td>
</tr>
<tr>
<td>¬</td>
<td>172</td>
<td>not</td>
<td>not</td>
<td>Char</td>
</tr>
<tr>
<td>¬</td>
<td>173</td>
<td>char_173</td>
<td>character 173</td>
<td>Char</td>
</tr>
<tr>
<td>®</td>
<td>174</td>
<td>registered</td>
<td>registered</td>
<td>Char</td>
</tr>
<tr>
<td>¯</td>
<td>175</td>
<td>char_175</td>
<td>character 175</td>
<td>Char</td>
</tr>
<tr>
<td>°</td>
<td>176</td>
<td>degree</td>
<td>degree</td>
<td>Char</td>
</tr>
<tr>
<td>±</td>
<td>177</td>
<td>plus_minus</td>
<td>plus or minus</td>
<td>Char</td>
</tr>
<tr>
<td>²</td>
<td>178</td>
<td>superscript_2</td>
<td>superscript two</td>
<td>Char</td>
</tr>
<tr>
<td>³</td>
<td>179</td>
<td>superscript_3</td>
<td>superscript three</td>
<td>Char</td>
</tr>
<tr>
<td>′</td>
<td>180</td>
<td>acute_accent</td>
<td>acute accent</td>
<td>Char</td>
</tr>
<tr>
<td>µ</td>
<td>181</td>
<td>micro</td>
<td>micro</td>
<td>Char</td>
</tr>
<tr>
<td>¶</td>
<td>182</td>
<td>paragraph</td>
<td>paragraph</td>
<td>Char</td>
</tr>
<tr>
<td>·</td>
<td>183</td>
<td>middle_dot</td>
<td>middle dot</td>
<td>Char</td>
</tr>
<tr>
<td>,</td>
<td>184</td>
<td>cedilla</td>
<td>cedilla</td>
<td>Char</td>
</tr>
<tr>
<td>¹</td>
<td>185</td>
<td>superscript_1</td>
<td>superscript one</td>
<td>Char</td>
</tr>
<tr>
<td>º</td>
<td>186</td>
<td>char_186</td>
<td>character 186</td>
<td>Char</td>
</tr>
<tr>
<td>»</td>
<td>187</td>
<td>right_double_angle_quote</td>
<td>right double angle quote</td>
<td>Char</td>
</tr>
<tr>
<td>¿</td>
<td>191</td>
<td>question_mark_inverted</td>
<td>inverted question mark</td>
<td>Char</td>
</tr>
</tbody>
</table>
## 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 44: Miscellaneous Media Files*

<table>
<thead>
<tr>
<th>Symbol (where applicable)</th>
<th>Decimal Value</th>
<th>Media File Name</th>
<th>Media File Content</th>
<th>Data Play Back Types / When Media File Is Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>v</td>
<td>invalid_entry_error</td>
<td>Your entry is invalid.</td>
<td>Error message</td>
</tr>
<tr>
<td>v</td>
<td>no_entry_error</td>
<td>Please make a selection.</td>
<td></td>
<td>Error message</td>
</tr>
<tr>
<td>v</td>
<td>system_error</td>
<td>We are currently experiencing technical difficulties with this site. Please try again later when we can service you much better.</td>
<td></td>
<td>Error message</td>
</tr>
<tr>
<td>v</td>
<td>critical_error</td>
<td>We are currently experiencing technical difficulties with this site. Please try again later when we can service you much better.</td>
<td></td>
<td>Error message</td>
</tr>
<tr>
<td>v</td>
<td>critical_error_ULaw</td>
<td>We are currently experiencing technical difficulties with this site. Please try again later when we can service you much better.</td>
<td></td>
<td>Error message</td>
</tr>
<tr>
<td>v</td>
<td>critical_error_ALaw</td>
<td>We are currently experiencing technical difficulties with this site. Please try again later when we can service you much better.</td>
<td></td>
<td>Error message</td>
</tr>
<tr>
<td>v</td>
<td>440beep</td>
<td>&lt;single beep tone&gt;</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>busy_tone</td>
<td>&lt;single busy tone&gt;</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>busy_tone30</td>
<td>&lt;busy tone 1 per second for 30 seconds&gt;</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>Symbol (where applicable)</td>
<td>Decimal Value</td>
<td>Media File Name</td>
<td>Media File Content</td>
<td>Data Play Back Types / When Media File Is Used</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>v</td>
<td>central</td>
<td>Central</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>credit_of</td>
<td>Credit Of</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>dash</td>
<td>dash</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>daylight</td>
<td>daylight</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>dialtone</td>
<td>&lt;4 seconds of dial tone&gt;</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>dialtone2fastbusy60</td>
<td>&lt;9 seconds of dialtone&gt; followed by &lt;30 seconds of fast busy tone&gt;</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>dot</td>
<td>dot</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>eastern</td>
<td>Eastern</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>ENTER_PHONE_NUMBER</td>
<td>Please enter the phone number.</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>fastbusy</td>
<td>&lt;a single fastbusy tone + silence (total of 1 second)&gt;</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>fastbusy60</td>
<td>30 seconds of &lt;fastbusy tone&gt;</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>FINISHED</td>
<td>When you have finished, press</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>goodbye</td>
<td>Goodbye</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>Mountain</td>
<td>Mountain</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>negative</td>
<td>negative</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>of</td>
<td>of</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>pmgr_sys</td>
<td>pmgr_sys</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>pacific</td>
<td>Pacific</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>positive</td>
<td>positive</td>
<td>Unused</td>
<td></td>
</tr>
</tbody>
</table>
### 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).
CHAPTER 11

Speech Server Configuration

- Configure Speech Server, page 201
- Speech Server Settings, page 202
- Generate G729 Prompts for Unified CVP, page 203
- Configuration, page 204

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 202.
   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 93.

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.
# Speech Server Settings

## General Settings

Table 45: Speech Server—General Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
<th>Reboot/Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the Speech Server.</td>
<td>None</td>
<td>Valid IP address</td>
<td>Yes - Reboot Speech Server</td>
</tr>
<tr>
<td>Hostname</td>
<td>The host name of the Speech Server.</td>
<td>None</td>
<td>Valid DNS name, includes letters, the numbers 0 through 9, and a dash</td>
<td>Yes - Reboot Speech Server</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the Speech Server.</td>
<td>None</td>
<td>Up to 1024 characters</td>
<td>No</td>
</tr>
<tr>
<td>License File Location</td>
<td>The path of the license file on the Speech Server. The Operations Console transfers the license file to this location.</td>
<td>None</td>
<td>Any text</td>
<td>Yes - Restart</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The license file is the license file for the respective Speech Server. The location must be the path to where the license file exists on the Speech Server. The license file must exist at that path before you can successfully save and deploy.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable secure communication with the Ops console</td>
<td>Select On to enable secure communications between the Operations Server and this component. Access the device using SSH and files are transferred using HTTPS.</td>
<td>None</td>
<td>On or Off</td>
<td>No</td>
</tr>
</tbody>
</table>
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.

Note
Nuance does not support text-to-speech (TTS) and Automatic Speech Recognition (ASR) with G.729 codec.

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 same server. It is also no longer necessary to configure the VoiceXML Gateway with the IP address of the Call Server's IVR service. When SIP is used, the SIP service inserts the URL of the Call Servers 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 Call Servers IVR service.

The following example illustrates the VoiceXML bootstrap service that is invoked when a call is received:

```plaintext
service bootstrap flash:bootstrap.tcl
paramspace english index 0
paramspace english language en
paramspace english location flash
paramspace english prefix en
```

With Unified CVP 4.0 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:

CHAPTER 12

Gateway Configuration

- Configure Gateway, page 205
- Gateway Settings, page 206
- Configure Gateway Settings for Standalone Call Flow Model, page 207
- Configure Gateway Settings for Comprehensive Call Flow Model, page 210
- Configure Gateway Settings for Call Director Call Flow Model, page 220
- Configure Gateway Settings for VRU-Only Call Flow Model: Type 8, page 224
- Configure Gateway Settings for VRU-Only: Type 7, page 228
- Transfer Script and Media File to Gateway, page 230

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 206.

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 93.

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>
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. 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 8000 <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 46: Unified ICM—General Tab Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of a Unified ICM Server</td>
<td>None</td>
<td>Valid IP address</td>
<td>No</td>
</tr>
<tr>
<td>Hostname</td>
<td>The name of the Unified ICM Server</td>
<td>None</td>
<td>Valid DNS name. It includes alphanumeric characters and a dash.</td>
<td>No</td>
</tr>
<tr>
<td>Description</td>
<td>Additional information of the Unified ICM Server</td>
<td>None</td>
<td>Up to 1024 characters</td>
<td>No</td>
</tr>
<tr>
<td>Device Admin URL</td>
<td>The URL for the Unified ICM Web configuration application.</td>
<td>None</td>
<td>Valid URL</td>
<td>No</td>
</tr>
</tbody>
</table>

### 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 93 and Add or Remove Device From Device Pool, on page 93.

### 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
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 rtpprofile 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:
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
   no local-allow
   no direct-toll
   no direct-inward-dial

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
   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
   • cv perror.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:
      
      ```
      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
      ```
      
      General, a non-DNS setup is: sip-server 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 47.

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 165 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, on page 329 section.

- The primary and backup servers must be configured. If using name resolution local to the Gateway (rather than DNS) specify:

  ip host as- <locale> <ASR server for locale>
  ip host as- <locale>-backup <backup ASR server for locale>
  ip host ts- <locale> <TTS server for locale>
  ip host ts- <locale>-backup <backup TTS server for locale>

  Example for English US, use:
  ip host as-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
If you are using Nuance Speech Server 5 and Nuance Vocalizer for Network 5, make changes to 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:

- **Change**: `<ssml_validation>strict</ssml_validation>`
  
  **To**: `<ssml_validation>warn</ssml_validation>`

- **Change**: `<install path>\Nuance Vocalizer for Network 5.0\config\ttsrshclient.xml`

- **Change**: `<install path>\Nuance Vocalizer for Network 5.0\config\ttssapi.xml`

If you are using Nuance Speech Server 10.0, 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>

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.
   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 165 and SIP Dialed Number Pattern Matching Algorithm, on page 7 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
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 debugging
no logging console
!
ip cef
!voice rtp send-receive
!
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 g729a
!
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 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 210 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 165 and [SIP Dialed Number Pattern Matching Algorithm](#) on page 7 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 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:**

```no
sip-ua
sip-server ipv4:xx.xx.xxx.xxx:5060
```

**DNS Setup:**

```no
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 47 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
host cvp4cc3.cisco.com 10.4.33.133
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
cvp4cc2.cisco.com
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
```
Step 5  On the Unified CM server, CCMAadmin 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 166 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>`
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 210 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
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
!
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 210 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

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

```plaintext
service timestamps debug datetime msec
service timestamps log datetime msec
service internal
logging buffered 99999999 debugging
no logging console
ip cef
go 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
!
```

**VoiceXML Gateway Configuration: Example of Dial-Peer for ICM VRU Label for Type 7**

The following example provides the configuration for an ICM VRU label dial-peer for the Type 7 Unified CVP VRU-Only call flow model:

```plaintext
dial-peer voice 777 voip
description ICM VRU label
deploy bootstrap
deploy codec codec 1
ingo called-number <your sendtovru label pattern here>
dtmf-relay rtp-nte
no vad
```
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.
SIP Proxy Server Configuration

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

Unified CVP works with RFC-3261-compliant SIP Proxy Servers and has been qualified with Cisco Unified SIP Proxy.

• Configure SIP Proxy Server, page 231
• SIP Proxy Server Settings, page 232

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 232.
   b) Device Pool. See Add or Remove Device From Device Pool, on page 93. For information on Device Pool, see Device Pool, on page 93.
Step 4 Click Save.
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 47: SIP Proxy Server General Tab Configuration Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>General IP Address</td>
<td>The IP address of a SIP Proxy server.</td>
<td>None</td>
<td>Valid IP address</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Hostname</td>
<td>The host name of the SIP Proxy server.</td>
<td>None</td>
<td>Valid DNS name includes uppercase and lowercase letters, the numbers 0 through 9, and a dash.</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Device Type</td>
<td>The type of proxy server.</td>
<td>Cisco Unified SIP Proxy</td>
<td>Cisco Unified SIP Proxy and Cisco Unified Presence.</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the SIP Proxy server.</td>
<td>None</td>
<td>Up to 1,024 characters.</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Device Admin URL</td>
<td>The Administration URL of SIP Proxy server.</td>
<td>None</td>
<td>A valid URL. The user interface (UI) validates the URL for syntax errors. However, it cannot validate a URL for website existence.</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Default</td>
<td>Range</td>
<td>Restart Required</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------</td>
<td>-----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Enable Serviceability</td>
<td>Check this check box to enable serviceability for SIP Proxy server.</td>
<td>Not Applicable</td>
<td>Unchecked</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Username</td>
<td>The username required to log in to the proxy server Serviceability.</td>
<td>Valid names containing uppercase and lowercase alphanumeric characters, period, dash and underscore.</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Port</td>
<td>The port on which Serviceability is configured on the SIP Proxy.</td>
<td>1 to 65535</td>
<td>8443</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>(For Device Type: Cisco Unified SIP Proxy)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Password</td>
<td>Enter a password. This is the first level of authentication for IOS.</td>
<td>Valid names containing uppercase and lowercase alphanumeric characters, period, dash and underscore.</td>
<td>Not Applicable</td>
<td></td>
</tr>
<tr>
<td>Enable Password</td>
<td>The password required to log in to SIP Proxy Serviceability. This is the second level of authentication for IOS.</td>
<td>Must be same as password on the SIP Proxy.</td>
<td>Not Applicable</td>
<td></td>
</tr>
<tr>
<td>(For Device Type: Cisco Unified SIP Presence)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>Enter a password.</td>
<td>Valid names containing uppercase and lowercase alphanumeric characters, period, dash and underscore.</td>
<td>Not Applicable</td>
<td></td>
</tr>
</tbody>
</table>
Add SIP Proxy Server to Device Pool

See Add or Remove Device From Device Pool, on page 93. For information on Device Pool, see Device Pool, on page 93.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirm Password</td>
<td>The password required to log in to SIP Proxy Serviceability.</td>
<td>Must be same as password on the SIP Proxy.</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>
System Configuration

- System Tab Options, page 235
- Import System Configuration, page 236
- Export System Configuration, page 237
- Location Configuration, page 238
- SIP Server Group Configuration, page 243
- Dialed Number Pattern Configuration, page 248
- Web Services Configuration, page 251
- IOS Configuration, page 252
- Courtesy Callback, page 258
- Courtesy Callback Configuration, page 260

System Tab Options

Table 48: System Tab Options

<table>
<thead>
<tr>
<th>System tab options</th>
<th>Use To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Center</td>
<td>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.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>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 93 and Add or Remove Device From Device Pool, on page 93.</td>
</tr>
</tbody>
</table>
### System tab options

<table>
<thead>
<tr>
<th>System tab options</th>
<th>Use To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import System Configuration</td>
<td>Import a previously-saved Operations Console Server configuration file and apply it to the current system. For details, see Import System Configuration, on page 236.</td>
</tr>
<tr>
<td>Export System Configuration</td>
<td>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 237.</td>
</tr>
<tr>
<td>Location</td>
<td>Add, edit, synchronize, and delete Unified CM location information.</td>
</tr>
<tr>
<td>SIP Server Groups</td>
<td>Configure server groups for SIP and view Call Server deployment status. For details, see Location Configuration, on page 238.</td>
</tr>
<tr>
<td>Web Services</td>
<td>Configure Diagnostic Portal servlet credentials. For details, see Deploy Web Services, on page 252.</td>
</tr>
<tr>
<td>Dialed Number Pattern</td>
<td>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 249.</td>
</tr>
</tbody>
</table>
| 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 252. |
| Courtesy Callback           | For details, see Configure Courtesy Callback, on page 260. |

### 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*. 

*Configuration Guide for Cisco Unified Customer Voice Portal, Release 10.0(1)*
• 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 Resource Manager Windows Service by performing the following steps:
   a) Select Start > All Programs > Control Panel Programs > Administrative Tools > Services.
   b) Click Cisco CVP Resource Manager.
   c) Click Stop.

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 Resource Manager, and click Restart.
   c) Select Cisco CVP WebServicesManager, and click Restart.

Step 7  Log in to the Operations Console.

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, including licenses and application 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select System &gt; Export System Configuration.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Export System Configuration page, click Export.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Save As dialog box, select a location to save the file.</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Table 49: Location Configuration Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>General</td>
</tr>
</tbody>
</table>
### Location Configuration

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insert Site Identifier</td>
<td>Select one of the following options to identify the site information:</td>
<td>Insert site identifier between the Network VRU label and the correlation ID</td>
<td>Not applicable</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• Insert site identifier between the Network VRU label and the correlation ID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Insert site identifier at the beginning of the Network VRU label</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Do not insert site identifier</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location Name</td>
<td>This is a user defined field.</td>
<td>Not applicable</td>
<td>a-z, A-Z, 0-9, _</td>
<td>No</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
<td>Max length 128 characters</td>
<td></td>
</tr>
<tr>
<td>Site ID (required)</td>
<td>The Site ID is a unique user-defined field.</td>
<td>Null</td>
<td>0-9, #</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Max length 128 characters</td>
<td></td>
</tr>
<tr>
<td>Location ID (required)</td>
<td>The Location ID is a unique user-defined field.</td>
<td>Null</td>
<td>a-z, A-Z, 0-9</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Max length 128 characters</td>
<td></td>
</tr>
<tr>
<td>Unified CM IP Address</td>
<td>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.</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>No</td>
</tr>
</tbody>
</table>

**Configuration Guide for Cisco Unified Customer Voice Portal, Release 10.0(1)**
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
<th>Restart Required</th>
</tr>
</thead>
</table>
| 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               |
### 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.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The status indicates if the location information is valid or invalid:</td>
<td>Not applicable</td>
<td>Valid or Invalid</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Call Server Deployment**
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 244.
        b) Heartbeat Properties. See Heartbeat Properties Settings, on page 244.
        c) Call Server Deployment. See Deploy Call Server, on page 247.
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.
General Settings

Table 50: SIP Server Group General Settings

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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 <strong>Collapse all</strong> and <strong>Expand all</strong> to collapse/expand all the elements within the server groups listed on the page.</td>
</tr>
<tr>
<td>Number of Elements</td>
<td>The number of elements contained in the group.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number of the element in the server group.</td>
</tr>
<tr>
<td>Priority</td>
<td>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.</td>
</tr>
<tr>
<td>Weight</td>
<td>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.</td>
</tr>
</tbody>
</table>

Heartbeat Properties Settings

Table 51: SIP Server Group Heartbeat Properties Settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Heartbeats to Endpoints</td>
<td>Select to enable the heartbeat mechanism. Heartbeat properties are editable only when this option is enabled.</td>
<td>Disabled (unchecked)</td>
<td>Enabled or Disabled</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Endpoints that are not in a Server Group can not use the heartbeat mechanism.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
<td>Default</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Number of failed Heartbeats for unreachable status</td>
<td>The number of failed heartbeats before marking the destination as unreachable.</td>
<td>1</td>
<td>1 through 5</td>
</tr>
<tr>
<td>Heartbeat Timeout (ms)</td>
<td>The amount of time, in milliseconds, before timing out the heartbeat.</td>
<td>500 milliseconds</td>
<td>100 through 3000</td>
</tr>
<tr>
<td>Up Endpoint Heartbeat Interval (ms)</td>
<td>The ping interval for heart beating an endpoint (status) that is up.</td>
<td>5000 milliseconds</td>
<td>5000 through 3600000</td>
</tr>
<tr>
<td>Down Endpoint Heartbeat Interval (ms)</td>
<td>The ping interval for heart beating an endpoint (status) that is down.</td>
<td>5000 milliseconds</td>
<td>5000 through 3600000</td>
</tr>
<tr>
<td>Heartbeat Local Listen Port</td>
<td>The heartbeat local socket listen port. Responses to heartbeats are sent to this port on CVP by endpoints.</td>
<td>5067</td>
<td>0 through 65000</td>
</tr>
<tr>
<td>Heartbeat SIP Method</td>
<td>The heartbeat SIP method.</td>
<td>OPTIONS</td>
<td>OPTIONS or PING</td>
</tr>
</tbody>
</table>

**Note**
PING is an alternate method; however, some SIP endpoints do not recognize PING and will not respond at all.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heartbeat Transport Type</td>
<td>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. When the element is up again, it is routable for both UDP and TCP. Note: TLS transport is not supported.</td>
<td>UDP</td>
<td>UDP or TCP</td>
</tr>
<tr>
<td>Overloaded Response Codes</td>
<td>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.</td>
<td>503,480,600</td>
<td>1 through 128 characters. Accepts numbers 0 through 9 and commas (,)</td>
</tr>
</tbody>
</table>
### 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 73.

- 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.**
Dialled 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 Dialled Number (DN) pattern is dial plan configured on one or multiple Call Servers and provides details on the call flow of dialled 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 dialled digits the router collects and forwards to telephony devices. For more information on Dial plans, see http://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 Dialled Number Patterns for the respective, selected type appear. The current view for the dialled 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 dialled number pattern view type selection changes.

Each dialled number pattern appears as a row. Each dialled number pattern column type can be sorted alphabetically in ascending or descending order. The Dialled 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:

Dialled Number Pattern - The actual dialled number pattern.

Description - The dialled number pattern description.

You may also use the filtering function to filter for specific Dialled Number Patterns. Only the Dialled Number Pattern itself is filterable by the standard constraint criteria (that is, begins with, contains, ends with, is exactly, is empty). The Dialled 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>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Configuration</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dialed Number Pattern</td>
<td>The actual Dialed Number Pattern.</td>
<td>None</td>
<td>Must be unique&lt;br&gt;Maximum length of 24 characters&lt;br&gt;Can contain alphanumeric characters, wildcard characters such as exclamation point (!) or asterisk (*), single digit matches such as the letter X or period (.)&lt;br&gt;Can end with an optional greater than (&gt;) wildcard character</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the Dialed Number Pattern.</td>
<td>None</td>
<td>Maximum length of 1024 characters</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
<td>Default</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable Local Static Route</td>
<td>Enable local static routes on this Dialed Number Pattern. If Local Static Routes are enabled:</td>
<td>Disabled</td>
<td>Maximum length of 128 characters Must be a valid IP address, hostname, or fully qualified domain name</td>
</tr>
<tr>
<td></td>
<td>• <strong>Route to Device</strong> - 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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Route to SIP Server Group</strong> - 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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Address/Hostname/Server Group Name</strong> - If you have not selected a <strong>Route to Device</strong> or <strong>Route to SIP Server Group</strong>, enter the IP address, hostname, or the server group name of the route.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Send Calls to Originator</td>
<td>Enables calls to be sent to originator.</td>
<td>Disabled</td>
<td>n/a</td>
</tr>
<tr>
<td>Enable RNA Timeout for Outbound Calls</td>
<td>Enables Ring No Answer (RNA) timer for outbound calls.</td>
<td>Disabled</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>• <strong>Timeout</strong> - Enter the timeout value in seconds.</td>
<td>none</td>
<td>Valid integer in the inclusive range from 5 to 60</td>
</tr>
<tr>
<td>Enable Custom Ringtone</td>
<td>Enables customized ring tone.</td>
<td>Disabled</td>
<td>Maximum length of 256 characters Cannot contain whitespace characters</td>
</tr>
<tr>
<td></td>
<td>• <strong>Ringtone media filename</strong> - Enter the name of the file that contains the ringtone.</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
<td>Default</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable Post Call Survey for Incoming Calls</td>
<td>Enables post call survey for incoming calls.</td>
<td>Disabled</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>• <strong>Survey Dialed Number Pattern</strong></td>
<td>none</td>
<td>Maximum length of 24 characters</td>
</tr>
<tr>
<td></td>
<td>- Enter the survey dialed number pattern.</td>
<td></td>
<td>Can contain alphanumeric characters, wildcard characters such as</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exclamation point (!) or asterisk (*), single digit matches such as</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>period (.) or X, and can end with an optional greater than (&gt;) wildcard</td>
</tr>
</tbody>
</table>

**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 252.

  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.

### Deploy Web Services

#### Before You Begin

Install Remote Operations on the third-party device.

#### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log in to the Operations Console and select <strong>System &gt; Web Services</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the <strong>Remote Operations Deployment</strong> tab and perform the following steps:</td>
</tr>
<tr>
<td></td>
<td>a) Enter the IP Address and Hostname.</td>
</tr>
<tr>
<td></td>
<td>b) (Optional) Enter the description of the third-party device.</td>
</tr>
<tr>
<td></td>
<td>c) Click <strong>Add</strong> to add the device to the list of devices associated with the Unified CVP deployment Web services.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Save &amp; Deploy</strong> to save and deploy the configuration to the impacted devices in the Operations Console database.</td>
</tr>
</tbody>
</table>

### 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 255
- Template Deployment. See **IOS Template Deployment**, on page 257.

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

**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 53: IOS Template Format

<table>
<thead>
<tr>
<th>Component</th>
<th>Variables</th>
</tr>
</thead>
</table>
| 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.Prepending Digits - 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%  |
### Component Variables

<table>
<thead>
<tr>
<th>Component</th>
<th>Variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Proxy Server</td>
<td><code>%CVP.Device.SIPProxyServer.General.IP Address%</code></td>
</tr>
<tr>
<td>Speech Server</td>
<td><code>%CVP.Device.Speech Server.General.IP Address%</code></td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td><code>%CVP.Device.Unified CM.General.IP Address%</code></td>
</tr>
<tr>
<td>Media Server</td>
<td><code>%CVP.Device.Media Server.General.IP Address%</code></td>
</tr>
</tbody>
</table>

**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 253 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 253 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.

---

**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 256.

**Step 6** Select Save.
**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.

**Preview and Deploy Template**

To preview (validate) and deploy a template:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Log in to the Operations Console and select System &gt; IOS Configuration &gt; IOS Template Deployment.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>In the Select Template panel, select the template that you want to deploy.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>In the Associate Source Device(s) panel, select the devices to be replaced with device variables in the template.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>In the Associated Gateways panel, deselect any of the gateways that will not receive the template deployment. By default, all gateways are selected.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

---

Courtsey Callback

TheCourtesy Callback 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 will be available soon), then a call is placed back to the caller.
The caller must answer the call and indicate that they are the caller. The caller is connected to the agent after a short wait.

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

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).

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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Log in to the Operations Console and select <strong>System &gt;Courtesy Callback</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Select the required Unified CVP Reporting Server, if configured, from the drop-down list. <strong>Note</strong>: If you leave the selection blank, no Reporting Server is associated with the Courtesy Callback deployment.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>(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.</td>
</tr>
</tbody>
</table>
| **Step 4** | In the **DIALED NUMBER Configuration** section: The DIALED NUMBER Configuration ofCourtesy 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 54: Configuration Options for Dialed Number Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Unmatched Dialed Numbers</td>
<td>This checkbox controls whether or not dialed numbers that do not exist in the <strong>Allowed Dialed Numbers</strong> field can be used for a callback. By default, this is unchecked. If no dialed numbers are present in the <strong>Allowed Dialed Numbers</strong> list box, thenCourtesy Callback does not allow any callbacks.</td>
<td>Unchecked - Callbacks can only be sent to dialed numbers listed in the <strong>Allowed Dialed Numbers</strong> list.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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. |
| 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.  
  • 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. |
### 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](https://sso.cisco.com/autho/forms/CDClogin.html).


**Procedure**

1. **Step 1**
   
   Login to the CVP OAMP Operations Console (from the CVP OAMP VM), using this syntax: https://<server_ip>:9443/oamp.

2. **Step 2**
   
   Copy survivability.tcl from the Operations Console to the flash memory of the gateway. Using the Operations Console, perform the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Number of Calls Per Calling Number</td>
<td>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 &quot;Validate&quot; element only allows X callbacks per calling number to go through the &quot;preemptive&quot; exit state at any time. If there are already X callbacks offered for a calling number, new calls go through the &quot;none&quot; exit state of the &quot;Validate&quot; element.</td>
<td>0</td>
</tr>
</tbody>
</table>
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 308 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:

```bash
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 Courtesy callback is not supported for calls having call back time of more than 100 minutes. So, callback will be cancelled for a call back time of more than 100 minutes. It is recommended to set the session expiration timer to a maximum value (7200), to support courtesy call back with call back time more than 30 minutes (default session expiration timer set in the gateway). The following set of configuration steps are suggested to achieve the same.

---

**Configure VXML Gateway forCourtesy 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** dropdown 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_cc_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 rtpc 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 rtpc 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
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, on page 121.

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 file copies to a Media Server.
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 theCourtesy 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.

1. Set the path for the storage of recorded caller names.
2. Select app.callflow.
3. 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.
4. 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, and then executes update-all-apps batch file, then executes 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 14: 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 forCourtesy 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 the 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 271 for details. Steps that refer to specific blocks are noted at the beginning of 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.

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://10.86.139:7000/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) On the CCE Admin Workstation, in the ICM Configuration Manager, use the Expanded Call Variable List tool.

b) Create user.CourtesyCallbackEnabled.

c) Set Maximum Length to 1.

d) Check Enabled.

e) 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 137.

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.

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 executed.
- 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 executed 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.
System Configuration

Configure the CCE Script for Courtesy Callback
CHAPTER 15

Unified CVP Security

This chapter describes security considerations for Unified CVP call flow model deployments.

Note

For detailed information about security issues in Unified ICME, see *Security Best Practices Guide for ICM and IPCC Enterprise Hosted Editions*.

- Prerequisites for Securing Communication Between CVP Components, page 277
- Communications Security Between Unified CVP Components, page 278
- Secure Communications Between Unified CVP and IOS Devices, page 284
- HTTPS Support for Unified CVP, page 284
- Sensitive Customer Information, page 286

Prerequisites for Securing Communication Between CVP Components

Secure JMX communications by importing the following certificates:

- Self-signed certificates that are created automatically from information that you specify during Unified CVP installation.
- Signed certificates available from a Certificate Authority (CA).

Assuming that you work on Windows 2012 R2 Standard Edition server, manage certificates using:

- The keystore, a database for keys and trusted certificate information. For all keystore operations:

  * Keystore resides in: %CVP_HOME%\conf\security\.keystore
  * Resource Manager keystore resides in: %CVP_HOME%\conf\security\.ormKeystore
  * Keystore password resides in: %CVP_HOME%\conf\security.properties
• The keytool, a command-line utility for managing keys and trusted certificates. The keytool is installed at `%CVP_HOME%/jre`.

**Note**

- On Windows systems, the keystore and the keytool passwords are in an access control list (ACL) protected folder. Hence, either an administrator or a user having administrator privileges can import trusted certificates.
- For more information about the keytool and keystores, see Java documentation.

---

### Communications Security Between Unified CVP Components

During the configuration of a Unified CVP device, the Operations Console Server uses Java Management Extensions (JMX) to communicate to the managed Unified CVP device. Use Operations Console to configure Unified CVP components and additional components. See Operations Console User Guide for Cisco Unified Customer Voice Portal.

Unified CVP installation uses a default JMX communications setting of non-secured, so communications are not encrypted. However, you can modify this setting to secure communications using Secure Sockets Layer (SSL).

**Note**

Modifying this setting requires that you stop and restart services.

---

### Secure JMX Communications Between CVP Components

Secure JMX communication by using SSL between the Unified CVP Operations Console service, a managed Unified CVP device, and other CVP-related JMX clients.

**Procedure**

**Step 1**

Stop the Unified CVP Operations Console service.

a) On a Windows system, Select **Start** > **Administrative Tools** > **Services**.

b) The **Services** window appears. In the list of Service names, highlight the Cisco services listed below:

- Cisco CVP CallServer
- Cisco CVP OPSConsoleServer
- Cisco CVP Resource Manager
- Cisco CVP VXMLServer
- Cisco CVP WebServicesManager
c) Click Stop to complete the secure communication setup.

**Step 2**
Perform steps in the Exchange Certificates Between Systems, on page 279 procedure on how to use the keystore and keytool Java tools to exchange trusted certificates between the Operations Console and the device being managed.

*Note* For information about prerequisites and assumptions regarding keystore and keytool, see Prerequisites for Securing Communication Between CVP Components, on page 277. For instructions about using these tools, see the Java documentation.

**Step 3**
 Restart the Cisco CVP OPSConsoleServer service.

*Note* Restart this procedure by selecting the Start link instead of Stop on the Windows system.

**Step 4**
Log in to Operations Console and select Device Management > <CVP Device>.

**Step 5**
Check the Enable secure communication with the Ops Console checkbox to enable security for devices that require secure communication. For more information, see Enable Security on Unified CVP Devices, on page 281.

*Note* • Checking this box for the selected CVP device enables security for all the servers on that box. You are prompted to restart the servers that have security enabled.

• After you have enabled secure communication between Unified CVP components, any devices or clients that are not set up for secure communication do not work until modified for secure communication. See Exchange Certificates Between Systems, on page 279 to complete the setup.

**Step 6**
Restart the Cisco CVP Resource Manager service on the Unified CVP device machines on which communications needs to be secure by selecting Start > Control Panel > Administrative Tools > Services.

---

**Exchange Certificates Between Systems**

The following procedures describes how to move certificates between keystores.

*Note* The keytool commands shown below use the JRE relative path for the Windows platform.

**Procedure**

**Step 1**
Import the Operations Console Server certificate as trusted on the managed Unified CVP device by performing the following steps:

a) Log in to the Operations Console Server, retrieve the keystore password from the security.properties file.

   *Note* The security.properties file resides in the %CVP_HOME%/conf directory.

b) Export the certificate from the keystore. Open a command prompt and navigate to the %CVP_HOME%/conf/security directory, and then enter the following command:

```
..\..\jre\bin\keytool -export -v -keystore .keystore -storetype JCEKS -alias oamp_certificate -file <oamp_cert_XXX>
```
**Note**  Retain the default `oamp_certificate` alias name.

- c) When prompted, enter the keystore password.
- d) Copy the exported certificate file `<oamp_cert_XXX>` from the Operations Console service to the `%CVP_HOME%\conf\security` folder on the machine where the Cisco Unified CVP Resource Manager service is running.
- e) Retrieve the keystore password from the `security.properties` file on the managed Unified CVP device.
- f) For Windows, import the Operations Console certificate `<oamp_cert_XXX>` into the keystore on the managed Unified CVP device.
- g) Open a command prompt and navigate to the `%CVP_HOME%\conf\security` directory, and then enter the following command:

```
..\..\jre\bin\keytool -import
-keystore .keystore -storetype JCEKS -trustcacerts -alias
<orm_oamp_certificate> -file <oamp_cert_XXX>
```

**Remember**  The file argument in angular brackets is the exported Operations Console certificate filename.

- h) When prompted, enter the keystore password and then enter yes to confirm.

**Step 2**  Import the managed Unified CVP device certificate as trusted in the keystore on the Operations Console Server by performing the following steps:

- a) Retrieve the keystore password from the `security.properties` file on the managed Unified CVP device.
- b) For Windows, export the Unified CVP device certificate from the keystore. Open a command prompt and navigate to the `%CVP_HOME%\conf\security` directory, and then enter the following command:

```
..\..\jre\bin\keytool -export -v
-keystore .ormKeystore -storetype JCEKS -alias orm_certificate -file
<orm_cert_file_XXX>
```

- c) Append an IP address to the file name to make it unique.
  
  The IP address can be replaced with any value to make it unique when copied to the Operations Console Server.

- d) Copy the exported certificate file `<orm_cert_file>` from the managed Unified CVP device to the `%CVP_HOME%\conf\security` folder on the Operations Console service.
- e) Retrieve the keystore password from the `security.properties` file in the Operations Console Server.
- f) Import the certificate `<orm_cert_file>` into the keystore on the Operations Console Server. Open a command prompt and navigate to the `%CVP_HOME%\conf\security` directory, and then enter the following command:

```
..\..\jre\bin\keytool -import -keystore .keystore -storetype
JCEKS -trustcacerts -alias <oamp_orm_certificate_XXX> -file
<orm_cert_XXX>
```

- g) Append an IP address to the certificate alias to make the alias unique in the keystore.
  
  The IP address can be replaced with any value as long as it makes the certificate name unique when imported to the keystore.

- h) Repeat Steps 1 and 2 for every machine where the Unified CVP Resource Manager service is running if the JMX communication from the Operations Console Server to that managed Unified CVP device needs to be secured.
For self signed certificates, import the certificate <orm_cert_file> (generated using the option "b" in Step 2) into the keystore on the CVP managed device. Open a command prompt, navigate to the %CVP_HOME%/conf/security directory, and then enter the following command:
```
..\..\jre\bin\keytool -import -keystore .keystore -storetype JCEKS -trustcacerts -alias <cvp_orm_certificate_XXX>-file <orm_cert_XXX>
```

---

### Enable Security on Unified CVP Devices

After you have completed the procedure described in Exchange Certificates Between Systems, on page 279, enable security on the Unified CVP components that you want to accept only secure SSL communications.

**Note**
For information about enabling security on additional Unified CVP components that form the Unified CVP solution, see the Secure Communications Between Unified CVP and IOS Devices, on page 284.

By default, the communication channel between the Operations Console and the Resource Manager on CVP devices is not secure after the Unified CVP installation. On the Operations Console, use the Device Management configuration page to enable or disable secure SSL communications.

**Note**
- Whenever you modify this security setting, restart the Unified CVP Resource Manager service on the machine where the device is running.
- The communication link between the Operations Console and the managed CVP device remains secure after you check the Enable secure communication with the Ops console checkbox.

---

#### Procedure

**Step 1**
Log in the Operations Console and select a device type from the Device Management menu.

**Step 2**
Click Add New or select an existing device name and click Edit. The General tab appears.

**Step 3**
Select the Enable secure communication with the Ops console checkbox.

**Step 4**
Click Save to save the settings in the Operations Server database and click Save and Deploy to apply the changes to the device.

**Step 5**
Restart the Unified CVP Resource Manager service on the machine where the device is running.

**Step 6**
Repeat Steps 1 to 5 for all Unified CVP components that accept the secure SSL communications.

---

### Certificate Authority Signed Certificates

This section describes how to perform the following tasks:
Add a Certificate Signed by a Certificate Authority to the Keystore

Follow the steps below to generate and import CA-signed certificates for secure communications between the Operations Console and the CVP Resource Manager on other devices in your Unified CVP solution.

Procedure

Step 1 Retrieve the keystore password from the security.properties file.
Step 2 Generate a Certificate Signing Request (CSR).
   a) From the %CVP_HOME%/conf/security directory, enter the following:
      ```bash
      ..\..\jre\bin\keytool -keystore .keystore -storetype JCEKS -certreq -keyalg RSA -sigalg MD5withRSA -alias orm_certificate -file ormcertreq.csr
      ```
      b) When prompted, enter the keystore password.
Step 3 Send the ormcertreq.csr certificate file to a CA for sign-off.
   After the certificate is signed, it is returned with a CA root certificate, and depending on the signing CA, some optional intermediate certificates.
Step 4 Install the signed certificate into keystore and enter the following commands to install the following certificates:
   a) Intermediate CA Certificates:
      ```bash
      keytool -keystore .keystore -storetype JCEKS -import -alias root -trustcacerts -file <filename_of_intermediate_CA_certs>
      ```
   b) Root certificates (not in the Unified CVP keystore by default):
      ```bash
      keytool -keystore .keystore -storetype JCEKS -import -alias root -trustcacerts -file <filename_of_root_cert>
      ```
      \[Note\] Check the contents of any root certificate file before installing it to your keystore as a trusted certificate.
      The Java root certificates are installed in %CVP_HOME%/jre/lib/security/cacerts.
   c) CA Signed Certificate:
      ```bash
      keytool -keystore .keystore -storetype JCEKS -import -alias orm_certificate -trustcacerts -file <filename_of_your_signed_cert_from_CA>
      ```
Step 5 Repeat Steps 1 to 4 on every machine running Unified CVP Services.
Add a Certificate Signed by a Certificate Authority for HTTPS Web Access

The following procedure describes how to present a Certificate Authority (CA)-signed certificate to inbound Operations Console HTTPS clients.

The certificate and private key used for Operations Console HTTPS are listed as follows:

- **Self-signed certificate**: `%CVP_HOME%\conf\security\oamp.crt`
- **Private key for self-signed certificate**: `%CVP_HOME%\conf\security\oamp.key`

**Before You Begin**

Install OpenSSL from [http://www.openssl.org](http://www.openssl.org) because OpenSSL is not included with Unified CVP. See the OpenSSL documentation for details.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Back up the <code>%CVP_HOME%\conf\security</code> folder.</td>
</tr>
</tbody>
</table>
| **Step 2** | Open the `security.properties` file to retrieve the `.keystore` password and copy and paste the value of this property when managing the `.keystore`.  
   a) Open the `%CVP_HOME%\conf\security.properties` file.  
   b) Enter the keystore password after keytool prompts you to enter it.  
   c) Copy the value of the `Security.keystorePW` property and paste it into the command-line window. |
| **Step 3** | Open a command prompt and navigate to the `%CVP_HOME%\conf\security` folder. |
| **Step 4** | Generate a Certificate Signing Request (CSR) by entering the following command:  
   ```  
   ..\..\jre\bin\keytool.exe -storepass <keystore_pwd> -storetype JCEKS -keystore .keystore -certreq -dname CN=<cvp.your.domain> -alias oamp_certificate -file oamp.csr  
   ``` |
| **Step 5** | Install the root certificate by entering the following command:  
   ```  
   ..\..\jre\bin\keytool.exe -storepass <keystore_pwd> -storetype JCEKS -keystore .keystore -import -v -trustcacerts -alias root -file ca.cer  
   ``` |
| **Step 6** | Install the CA signed certificate by entering the following command:  
   ```  
   ..\..\jre\bin\keytool.exe -storepass <keystore_pwd> -storetype JCEKS -keystore .keystore -import -v -trustcacerts -alias oamp_certificate -file oamp.cer  
   ``` |
| **Step 7** | Run the following command to check whether the certificate is imported:  
   ```  
   ..\..\jre\bin\keytool.exe -storepass <keystore_pwd> -storetype JCEKS -keystore .keystore -list  
   ``` |
| **Step 8** | Restart the Cisco CVP OPSConsoleServer.  
   | a) **Start > Control Panel > Administrative Tools**  
   | b) Right-click the Cisco CVP OPSConsoleServer service and then click **Restart**. |
Secure Communications Between Unified CVP and IOS Devices

To secure file transfer between Cisco Gateways and the Operations Console, import the Operations Console Server certificate on the IOS device during device configuration and enable SSH on the router. Otherwise, any user-requested action, such as file transfer to an IOS device, fails. For example, to copy a file to the IOS device through the Operations Console, SSH must be enabled on the device, else the task fails.

HTTPS Support for Unified CVP

Set Up Tomcat to Present CA-Signed Certificates to Inbound HTTPs Clients

Due to the large processing overhead of HTTPs, the Tomcat application server only achieves up to 100 simultaneous connections dependent on the configuration. See the Configuration Guide for Cisco Unified Customer Voice Portal at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-implementation-design-guides-list.html for details.

Procedure

Step 1 Open the `security.properties` file to retrieve the .keystore password and copy and paste the value of this property when managing the .keystore.

1. Open the `%CVP_HOME%\conf\security.properties` file, where `%CVP_HOME%` is the installation directory for Unified CVP. By default, Unified CVP is installed in `C:\Cisco\CVP`.

   **Note** The property file should contain the `Security.keystorePW` property.

2. Enter the keystore password after keytool prompts you to enter it.

3. Copy the value of the `Security.keystorePW` property and paste it into the command-line window.

   For example, if the `%CVP_HOME%\conf\security.properties` file contains the `Security.keystorePW` property line, the password to copy will be `{3X}E70bhM3Gy{ou.5AL!+4Ffm868`.

Step 2 Back up the `%CVP_HOME%\conf\security` directory.

Step 3 Open a command-line prompt window, and change to security configuration directory to `cd\cisco\cvp\conf\security`.

Step 4 Create the certificate signing request to use the private key entry for your certificate,

   **Remember** Enter the keystore password when prompted.

Example:

- **Call Server**: `%CVP_HOME%\jre\bin\keytool.exe - certreq - alias callserver_certificate - storetype JCEKS - keystore .keystore - file callserver_certificate.csr`.

- **VXML Server**: `%CVP_HOME%\jre\bin\keytool.exe - certreq - alias vxml_certificate - storetype JCEKS - keystore .keystore - file vxml_certificate.csr`.
A new csr file is created on the file system.

Step 5  Give the certificate signing request file to a trusted Certificate Authority. They sign it and return one or more trusted certificates.

Step 6  Import the signed certificate file from your trusted Certificate Authority to the .keystore file, and enter in the keystore password when prompted.
If more than one certificate is delivered, certificates must be imported in order of the chained certificate hierarchy. For example: root, intermediate, signed certificate.

Example:

- **Call Server:** %CVP_HOME%\jre\bin\keytool.exe - import -v -alias callservcer_certificate -storetype JCEKS -trustcacerts -keystore .keystore -file signed_callservcer_certificate.crt

- **VXML Server:** %CVP_HOME%\jre\bin\keytool.exe - import -v -alias vxml_certificate -storetype JCEKS -trustcacerts -keystore .keystore -file signed_vxml_certificate.crt

---

**Secure Communications Between Unified CVP and IOS Devices**

To secure HTTPS between Cisco Gateways and Call Server and VXML Server to the gateway for HTTPS, import either the Call Server certificate or the VXML Server certificate on the IOS device during device configuration.

**Procedure**

Step 1  Do one of the following in the address bar of the web browser:

- To access the secure Call Server, enter https://<ServerIP>:8443/
- To access the secure VXML Server, enter https://<ServerIP>:7443/
- To access the secure Operations Console, enter https://<ServerIP>:9443/

*Note*  For the file transfer to work, you must upload the https://<ServerIP>:9443/ certificate to the IOS router.

The Security Alert dialog box appears.

Step 2  Click **View Certificate**.

Step 3  Select the **Details** tab.

Step 4  Click **Copy to File**.
The Certificate Export Wizard dialog appears.

Step 5  Click **Base-64 encoded X.509 (.CER)**, and then click **Next**.

Step 6  Specify a file name in the **File to 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 exported file in Notepad and copy the Operations Console certificate information that appears between the **--BEGIN CERTIFICATE--** and **--END CERTIFICATE--** tags to the IOS device.

**Step 10**  Access the IOS device in privileged EXEC mode.  
For more information, see the *Cisco IOS CLI documentation*.

**Step 11**  Access global configuration mode by entering configuration terminal.

**Step 12**  Create and enroll a trustpoint by entering the following commands:

```
crypto pki trustpoint xxxx
en terminal
exit
```

where `xxxx` is a trustpoint name.

The IOS device exits `conf t` mode and returns to privileged EXEC mode.

**Step 13**  Copy the certificate exported to the Notepad to the IOS device:

1. Enter `crypto pki auth <xxxx>`  
   where `xxxx` is the trustpoint name specified in the previous step.

2. Paste the certificate from the Notepad clipboard.

3. Enter `quit`.

   - A message displays describing the certificate attributes.
   - A confirmation prompt appears.

**Step 14**  Enter `yes`.  
A message indicates that the certificate is successfully imported.

---

**Sensitive Customer Information**

Use the VXML Server Inclusive and Exclusive filters to control the sensitive customer information, such as PIN numbers that are sent to the Reporting Server.  

By default, all items except the Start and End element are filtered from information the VXML Server feeds to the Reporting Server unless they are added to an Inclusive Filter. If you create Inclusive filters that are broad enough to allow sensitive information to be passed, you then have the option to perform the following tasks:

- Adjust the Inclusive filters so that the sensitive information is not included.
- Add Exclusive filters to prevent the sensitive information from being included.

For information on how to configure filters, see the Cisco Unified CVP Operations Console online help.
CHAPTER 16

Unified ICME Warm Consult Transfer/Conference to Unified CVP

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 289. For configuration procedure of Call Director and Comprehensive call flow models using SIP, see Unified CVP Call Flow Models, on page 9.

- Configure Unified ICME Warm Consult Transfer/Conference to Unified CVP, page 288
- Minimal Component Version Requirement, page 289
- Warm Transfer with SIP Calls, page 289
- Set Up Unified ICME Warm Consult Transfer, page 290
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.
Minimal Component Version Requirement

See the http://www.cisco.com/en/US/products/sw/custcosw/ps1006/prod_technical_reference_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.
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 the 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.

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

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.
Unified ICME Warm Consult Transfer/Conference to Unified CVP

Set Up Unified ICME Warm Consult Transfer
Transfer and Queue Calls with Unified CVP

- IVRs From Perspective of Unified ICME, page 293
- Call Transfer Using Unified CVP in Comprehensive Mode, page 294
- Call Transfer From Agent to Agent, page 300
- Example of IP Transfer, page 302
- CLI Field on Outgoing Transfers, page 302
- Unified CCE Reroute on No Answer Configuration for Unified CVP, page 303
- Call Survivability, page 308
- Enhanced Location Call Admission Control, page 316
- Locations-Based Call Admission Control Configuration, page 320
- UUI as Correlation ID, page 323
- External Transfers in Unified ICME, page 324
- Multicast Music on Hold (MMoH), page 325
- Post Call Survey for SIP, page 326

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 Unified CVP Call Flow Models, on page 9.

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 normal 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.

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 16: 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:
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 18: 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 19: VRU Script Execution*
Transfer and Queue Calls with Unified CVP

Example: Queue and Transfer Call to a Skill Group

From a VRIU script to play a menu to the caller such as “For banking, press 1. For savings, press 2. To speak to a customer service representative, press 0.”

If the Caller ID is not available (CED) is 0, then try to move the call to an appropriate agent group. This selection will result in a new VRIU screen or a call to an agent if available. If an agent is not available, the call will be put into a queue.

At the same time, queue the call into the set of agent skill groups with a higher priority.

While the call is in the queue waiting for an available agent, play an announcement to the caller. When the next available agent becomes available, play music, press 1. For the latest stock update, press 2. To return to the main menu of the automated system, press 3. To hear a duck quack, press 4. When the agent is available, depending on time and VRIU availability, the call will be sent to the next available agent based on routing rules.
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 20: 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 phones 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 ICM.

**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 NNNNNNNNN 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 the word `null` 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=null` 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 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 executed 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 unavailable 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

Specify the number of seconds in the Ring no answer time field in the Agent Desk Settings configuration and do not select the Ring no answer dialed number field. Set the timeout to the maximum time you want to allow the agent to answer a call; for example, 2 rings = 8 seconds. Set this timer shorter than the no answer timeout for router requery (refer to the following example).

Figure 21: Agent Desk Settings List

Setting the Ring No Answer Time causes the agent to be made unavailable after the Reroute On No Answer timer expires, but does not invoke the Reroute On No Answer mechanism to reroute the call.
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).

- 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; for example, less than 15 seconds (4 rings), such as 10 seconds. In any case, this timeout must be longer than the Re-route On No Answer timeout 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 "Not Ready" state due to the expiration of the 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 22: 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 23: Requery Mechanism**

![Diagram of 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 requeryd 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 normal 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 Reroute On No Answer timeout expires, Unified ICME makes the agent unavailable. The agent state does not change until the call gets taken away from the agent. The agent phone continues to ring and the agent can pick up the phone (if the agent does pick up the phone, the agent is left in Ready state after the call, even if it was after the Reroute On No Answer timer expires).
- 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 Not Ready state.
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 executes. When the routing script executes 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 executes the "Go To Script" node, script execution 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's 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 normally 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:

```bash
application
service survive flash:survivability.tcl
paramspace callfeature med-inact-det enable
```
And, then add the following parameters:

```plaintext
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:

```plaintext
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:

```plaintext
dial-peer voice XXXX pots
  service my-CVP-service
  incoming called-number NNNNN
  service my-CVP-service flash:CVPSelfService.tcl
  param CVFPrimaryVXMLServer my-VXML-server-IP
  param CVFBackupVXMLServer 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”:

```plaintext
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.tel 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-agentXDNIS
  • 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 5644478.

• 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-agent 0 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 aborting 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 aborting 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.

---

**Configuration Guide for Cisco Unified Customer Voice Portal, Release 10.0(1)**

Transfer and Queue Calls with Unified CVP
• **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:

```tcl
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.

  a) **Syntax Example**: refer-prefix "800 888 877 866 855"

### 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 normally be an 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.

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 452111111111 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 80099900000
port 7/0:D (or whatever port is desired)
#------------------------------------------
dial-peer voice 6 voip
incoming called-number 80099900000
codec g711ulaw (To force the call to g711ulaw on the outgoing
hairpin)
#------------------------------------------
service billing flash:survivability.tcl
param after-hours-agent0 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

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.

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).

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.)

   ![Find and List Locations](image)

   **Figure 24: 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 25: 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. Using Unified CM Administration, select Device > Device Settings > SIP Profile > Trunk Specific Configuration > Reroute Incoming Request to new Trunk based on > Call-Info header with the purpose equal to x-cisco-origIP.

6. 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 321.
• Prompt retrieval. See Prompt Retrieval, on page 321.

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:
  
  $20 \times 30 = 600 \text{ calls per hour} = 0.166 \text{ calls per second (CPS)}$

**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:

• $7000 \text{ bytes} \times 20 \text{ VoiceXML documents} \times 8 \text{ bits} = 1,120,000 \text{ bits per call}$

• $0.166 \text{ CPS} \times 1,120,000 \text{ bits per call} = 185.9 \text{ Kbps per remote site}$

**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:

\[
\begin{align*}
50 \text{ prompts} & \times 50,000 \text{ bytes} \times 8 \text{ bits} = 20,000,000 \text{ bits} \\
20,000,000 \text{ bits} / 900 \text{ seconds} &= 22.2 \text{ Kbps per branch}
\end{align*}
\]

**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:
- ivr prompt memory 15000
- http client cache memory file 500
- 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 datatime 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:

- 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 205.

**Debugging Tips**

**Debug Trace Settings for the Gateway**

On the gateway, enter the following code:

```
debg voip application script
debg 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,5900CFC,09FCI,,,,,,,y,UUS,3,3132333435

  --> This is the UUI that will become the Correlation
  ID12345GCI, 87c0c79d91dd1daa9c4000bfda207f2"
```

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 nnnn 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.

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 nnnn 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

Post Call Survey for SIP

A Post Call Survey takes place after normal 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 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 the normal call flow completes. 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 variable user.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.
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'.
Configure High Availability for Unified CVP

- Server Groups, page 329
- Redundancy and Failover for Unified CVP, page 331
- Configure Speech Server, page 333
- Application Control Engine for Load Balancing in Unified CVP, page 333

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.


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 26: 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`.

**Note** For ASR/TTS failover to function when using Custom VXML Applications, you require either an Application Control Engine (ACE) or any other supported load balancer.

Redundancy for Micro-App-Based Applications

When ACE 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.
For information about setting up the IVR Service to accommodate failover, see the Administration Guide for Cisco Unified Customer Voice Portal.

**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. |

### 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>From the Operations Console, select Device Management &gt; Speech Server.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
| **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 202.  
  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 93. |
| **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. |

### Application Control Engine for Load Balancing in Unified CVP

For configuration details, refer to the Cisco ACE 4700 Series Appliance Server Load-Balancing Configuration Guide.

ACE provides load-balancing services for HTTP, MRCP and RTSP traffic, but not for call control signaling SIP messages. As a load-balancing device, ACE determines which server in a set of load-balanced servers,
should receive the client request for service. Load balancing helps fulfill the client request without overloading either the server or the server farm as a whole. Also, by monitoring the state of each server and transferring a server's load to a working server during a server failure, ACE provides high availability support.

In this application of ACE, the engine is used primarily to direct initial session requests for a particular type of service. There are four types of services:

- http prompts
- ASR/TTS
- Unified CVP Call Server
- Unified CVP VXML Server

The following general approach applies to configuring each Unified CVP component type for use with ACE.

- **Real Servers** - One ACE real server is configured for each group of Unified CVP components (Call Servers, VXML Servers, etc.) that need ACE Load balancing. For general step-by-step guidelines for configuring Real Servers, refer to the Cisco ACE 4700 Series Appliance Server Load-Balancing Configuration Guide

- **Server Farms** - Typically, in data centers, servers are organized into related groups called server farms. Servers within server farms often contain identical content (referred to as mirrored content) so that if one server becomes inoperative, another server can take its place immediately. After you create and name a server farm, you can add existing real servers to it and configure other server-farm parameters, such as the load-balancing predictor, server weight, backup server, health probe, and so on. For general step-by-step guidelines for configuring server farms, refer to the Cisco ACE 4700 Series Appliance Server Load-Balancing Configuration Guide

- **Health Monitoring** - You can instruct the ACE servers to check the health of servers and server farms by configuring health probes (sometimes referred to as keepalives). After you create a probe, you assign it to a real server or a server farm. A probe can be one of many types, including TCP, ICMP, Telnet, or HTTP. The ACE server sends out probes periodically to determine the status of a load-balanced server, verifies the server response, and checks for other network problems that may prevent a client from reaching a server. For general step-by-step guidelines for configuring probes, refer to the Cisco ACE 4700 Series Appliance Server Load-Balancing Configuration Guide

- **Class-Map and Policy Map** - The ACE server uses several configuration elements to filter traffic and then to perform various actions on that traffic before making the load-balancing decision. These filtering elements and subsequent actions form the basis of a traffic policy for server load balancing. For general step-by-step guidelines for configuring traffic policies, refer to the Cisco ACE 4700 Series Appliance Server Load-Balancing Configuration Guide

Specific component-type configuration is covered in the following sections.
In this section, you will configure the probes and other configuration needed for the ACE server to ensure that each server in each server farm is operating properly, so that the ACE server can load balance between all the servers of each type that are usable at any given moment.

Figure 27: Application Control Engine for Load Balancing in Unified CVP

General Probes

In your ACE unit's configuration, create an ICMP probe to check for server connectivity. In the sub topics that follow you associate this probe with each of your real servers.

```
probe icmp PROBE_SERVICE_ICMP
  interval 5
  receive 3
  faildetect 1
  passdetect interval 5
  passdetect count 1
```

Unified CVP Media Servers

Media Servers are standard web servers that are responsible for serving Unified CVP prompt files to the voice gateway.

Create an HTTP Probe

The probe below is used to determine whether the Media Server is operating properly. A simple HTTP request is sent to the Media Server and the probe does a check for HTTP return code 200.

The Media Server probe sends an HTTP request to /index.html. The request is sent to the default HTTP port (80) and the IP address of the real server associated with the probe.
In the probe below, the following parameters are set. Set the actual values according to your own requirements. Refer to the Cisco ACE 4700 Series Appliance Server Load-Balancing Configuration Guide.

To create the HTTP probe for the media servers, place the following code in the configuration for the ACE server.

```
probe http PROBE_HTTP
interval 5
receive 3
faildetect 1
passdetect interval 5
passdetect count 1
request method get url /index.html
expect status 200 200
open 1
```

**Configure the Physical Servers**

Create a real server for every physical media server you would like to load balance. Associate the ICMP probe with each server by creating a section, as shown in the following example, for each media server in the server farm.

```
rserver host mediaServer1
ip address 10.1.1.1
probe PROBE_SERVICE_ICMP
inservice
rserver host mediaServer2
ip address 10.1.1.2
probe PROBE_SERVICE_ICMP
inservice
```

**Group Your Physical (Media) Servers**

In the ACE configuration file, create a server farm and associate servers with this farm. The following example applies the HTTP Probe to the server farm and the ACE server probes each media server in the server farm. However, you can also associate this probe with the physical server.

```
serverfarm host media_server_FARM
description Media Server Farm
probe PROBE_HTTP
rserver mediaServer1 80
inservice
rserver mediaServer2 80
inservice
```

**Class Map Configuration**

The configuration below defines a Layer 3 and a Layer 7 class-map.

- The Layer 3 class-map is used to define a Virtual IP and the allowed traffic port. This class map gets applied to the Layer 3/4 policy-map. Traffic sent to the virtual IP is directed by the ACE server to real media servers based on the load balancing policy.

- The Layer 7 class-map is used to filter traffic based on the URL pattern specified. This class-map is associated with a Layer 7 policy-map, which contains information about which servers to load balance.
When traffic entering the ACE server matches the class-map \texttt{L3\_Media\_Server\_VIP}, the ACE server applies the actions specified in \texttt{Media\_Server\_L7SLB}, which is defined below.

\begin{verbatim}
class-map match-all L3_Media_Server_VIP
  2 match virtual-address 10.1.1.3 tcp eq www

class-map type http loadbalance match-all L7_HTTP_CLASS
  2 match http url .*\
\end{verbatim}

**Policy Map Configuration**

In the code below, the layer 7 class map gets associated with the layer 7 policy map.

\begin{verbatim}
policy-map type loadbalance first-match Media_Server_L7SLB
  class L7_HTTP_CLASS
  serverfarm media_server_FARM

policy-map multi-match POLICY
  class L3_Media_Server_VIP
  loadbalance vip inservice
  loadbalance policy Media_Server_L7SLB
  loadbalance vip icmp-reply active
\end{verbatim}

**ASR/TTS Servers**

**Probe**

The probe below is used to determine whether the MRCP ASR/ TTS Server is up. The ACE server makes a connection to the MRCP port to validate that the ASR/TTS server is running. In the configuration below, a TCP probe is used. The probe waits for the configured 3 seconds to receive information from the server. The ASR/TTS service is considered down if the ACE server is unable to connect to port 554 for MRCP traffic.

In the probe below, the parameters are set. Set the actual values according to your own requirements. Refer to the *Cisco ACE 4700 Series Appliance Server Load-Balancing Configuration Guide*.

The following configuration example is part of the ACE server's configuration.

\begin{verbatim}
probe tcp PROBE_ASR_TTS
  port 554
  interval 5
  receive 3
  faildetect 1
  passdetect interval 5
  passdetect count 1
  open 1
\end{verbatim}

**Real Server and Server Farm Configuration**

The following code defines your physical servers and associates them with the ICMP probe.

\begin{verbatim}
rserver host asrtts1
  ip address 10.1.1.12
  probe PROBE\_SERVICE\_ICMP
  inservice

rserver host asrtts2
  ip address 10.1.1.13
  probe PROBE\_SERVICE\_ICMP
  inservice
\end{verbatim}
The following code defines your server farms and associates them with the PROBE_ASR_TTS probe. The servers in the server farm only accept connections on port 554.

```python
serverfarm host ASR
description ASR Farm
probe PROBE_ASR_TTS
rserver asrtts1 554
inservice
rserver asrtts2 554
inservice
serverfarm host TTS
description TTS Farm
probe PROBE_ASR_TTS
rserver asrtts1 554
inservice
rserver asrtts2 554
inservice
```

**Class-map Configuration**

Create a class-map that accepts connections only on port 554. (By default, rtsp maps to port 554.)

```python
class-map match-all ASR_CLASS_L3
2 match virtual-address 10.1.1.14 tcp eq rtsp

class-map match-all TTS_CLASS_L3
2 match virtual-address 10.1.1.18 tcp eq rtsp
```

**Policy-map Configuration**

```python
policy-map type loadbalance first-match ASR_POLICY_L7
class class-default
serverfarm ASR

policy-map type loadbalance first-match TTS_POLICY_L7
class class-default
serverfarm TTS
policy-map multi-match POLICY
class ASR_CLASS_L3
loadbalance vip inservice
loadbalance policy ASR_POLICY_L7
loadbalance vip icmp-reply active
class TTS_CLASS_L3
loadbalance vip inservice
loadbalance policy TTS_POLICY_L7
loadbalance vip icmp-reply active
inspect rtsp
```

**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 338
- Specify an ASR and TTS Server Location with an Individual VoiceXML Document, on page 339

**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 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.

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); or MRCP v2, which uses Session Initiation Protocol (SIP), for example:

```xml
<property name="com.cisco.tts-server" value="rtsp://tts-server1/synthesizer" />
<property name="com.cisco.tts-server" value="sip:mresources@mediaserver.com" />
```

**com.cisco.asr-server**

The "com.cisco.asr-server" allows a document to specify an external media server for automatic speech recognition 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.

The media server's URI can be formatted for Media Resource Control Protocol version 1 (MRCP v1) which uses RTSP or MRCP v2, which uses SIP, for example:

```xml
<property name="com.cisco.asr-server" value="rtsp://asr-server1/synthesizer" />
<property name="com.cisco.asr-server" value="sip:mresources@mediaserver.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 ACE server.

The ACE server 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.

Refer to the Cisco ACE 4700 Series Appliance Server Load-Balancing Configuration Guide.

To create the Call Server HTTP probe, place the following lines in the configuration for the ACE server:

```plaintext
probe http PROBE_CALLSERVER_HTTP
port 8000
interval 6
faildetect 1
passdetect interval 6
passdetect count 1
```
QoS for Unified CVP Call Server

Quality of Service (QoS) is the measure of transmission quality and service availability of a network (or internetworks).

For more information about defining QoS criteria, see the latest Enterprise QoS Solution Reference Network Design Guide.

For more information to create policy based QoS, see section Create Policy Based QoS, on page 117.

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.

```plaintext
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 ACE server.

The VXML Server probe sends an HTTP request to /CVP/Server?probe=true. If the VXML Server is up and in service, 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.

```plaintext
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
```

In order to get the "?", press CTRL-V before pressing the question mark 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 ACE server has chosen a particular VXML Server from the list of servers in a server farm, the ACE server continues to send all traffic for that session to the same VXML Server. To accomplish this, use a sticky group.

Refer to the Cisco ACE 4700 Series Appliance Server Load-Balancing Configuration Guide.

The following definitions apply to the settings shown below:

- **http-cookie**: Sticky method being used. In this method, when the ACE server examines a request for content, and determines through policy matching that the content is sticky, the ACE server examines any cookie or URL present in the content request. The ACE server uses the information in the cookie or URL to direct the content request to the appropriate server.

- **Cookie insert**: The ACE server inserts the cookie on behalf of the VXML Server upon the return request, so that the ACE server can perform cookie stickiness even when the VXML servers are not configured to set cookies. The cookie contains information that the ACE server uses to ensure persistence to a specific real server.

The following ACE server configuration code accomplishes the sticky function.

```
sticky http-cookie ACE_COOKIE VXMLServer_HTTP_STICKY
cookie insert
serverfarm vxmlserver
```

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
```
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 1.6.0_24 to 1.6.0_81.

Download the JREUpdate.zip from the following location:

http://software.cisco.com/download/release.html?mdfid=270563413&softwareid=280840592&release=10.5%281%29&relind=AVAILABLE&rellifecycle=&reltype=latest

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 1.6.0_81 to 1.7.0_45.

Procedure

Step 1  Download and install the preferred Java Development Kit (JDK) version on your personal machine.

Step 2  Copy the JRE folder from the installed JDK 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:\jdk1.7.0_67\jre.

Step 3  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 4  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 5  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.
Tomcat Update

Perform the following procedure to update Tomcat version on Call Server, Reporting Server, Operations Console, VXML Server, and Web Services Manager (WSM). For example, you can update from Tomcat version 7.0.24 to 7.0.47.

Before You Begin

• Save a backup copy of the Tomcat folder from the following locations:
  • For Call Server: C:\Cisco\CVP\CallServer
  • For Reporting 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 Tomcat service.

Step 2
Remove the Tomcat folder from the following locations:
  • For Call Server: C:\Cisco\CVP\CallServer
Step 3  Download the Tomcat binary apache-tomcat-7.0.47-windows-x86.zip file from the following location: https://archive.apache.org/dist/tomcat/tomcat-7.

Step 4  Right-click the apache-tomcat-7.0.47-windows-x86.zip file and extract the files to a known location on the local drive.

Step 5  Copy the apache-tomcat-7.0.47 folder to the following locations:
- For Call Server: C:\Cisco\CVP\CallServer
- For Reporting 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 6  Rename the folder apache-tomcat-7.0.47 to Tomcat.

Step 7  Copy the cvp.war 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\webapps
- For Reporting Server: C:\Cisco\CVP\CallServer\Tomcat\webapps
- For VXML Server: C:\Cisco\CVP\VXMLServer\Tomcat\webapps
- For Operations Console: C:\Cisco\CVP\OPConsoleServer\Tomcat\webapps
- For WSM: C:\Cisco\CVP\wsm\Server\Tomcat\webapps

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 Reporting 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

Step 9  Restart the following Tomcat services:
- Cisco CVP CallServer
- Cisco CVP OPSConsoleServer
- Cisco CVP VXMLServer
• Cisco CVP WebServicesManager

**Step 10** Ensure that the CVP Diag portal is up and running.

**Step 11** Check Tomcat and CVP logs for any exceptions.