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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: 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. (1721R)

© 2015–2019 Cisco Systems, Inc. All rights reserved.
Preface

- Change History, on page iii
- About This Document, on page iii
- Audience, on page iii
- Related Documents, on page iv
- Communications, Services, and Additional Information, on page iv
- Documentation Feedback, on page iv

Change History

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

<table>
<thead>
<tr>
<th>Change</th>
<th>See</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Release of Document for Release 12.0(1)</td>
<td></td>
<td>January 2019</td>
</tr>
<tr>
<td>Added a field, Enable secure communication with VRU PIM</td>
<td>ICM Service Settings</td>
<td></td>
</tr>
</tbody>
</table>

About This Document

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

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

Audience

This guide is intended for managers, Unified CVP system managers, Cisco Unified Intelligent Contact Management Enterprise (Unified ICME)/Cisco Unified Intelligent Management Hosted (Unified ICMH) system managers, VoIP technical experts, and IVR application developers, who are familiar with the following:
• Configuring Cisco Gateways
• Configuring Cisco Unified Communications Manager
• ICM Configuration Manager and ICM Script Editor tools for call center operations and management

Related Documents

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

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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

Documentation Feedback

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

PREFACE

Preface iii
  Change History iii
  About This Document iii
  Audience iii
  Related Documents iv
  Communications, Services, and Additional Information iv
  Documentation Feedback iv

CHAPTER 1

Cisco Unified Customer Voice Portal 1
  Unified CVP 1
    Key Features and Benefits 2
  Operations Console 3
    Sign In to Operations Console 4
      Procedure 4
    My Account Screen 4
      User Information 5
      User Group Assignment 5
      Device Pool Selection 6
  Cisco Unified Customer Voice Portal Page 6
    Window Header 6
  Operations Console Menu Options 7
  More Information About Unified CVP 11
  Sign Out of Operations Console 12
    Procedure 12
  View System-Level Operation States 12
  Transfer Script and Media Files 14
Contents

Procedure 14
Error Handling 14
Control Center Operation 14
  View Devices by Type 15
    Procedure 15
  View Devices by Device Pool 16
    Procedure 16
  View Device Status 16
  View Device Statistics 21
    Procedure 21
  View Device Associations 22
    Procedure 22
  View Infrastructure Statistics 22
    Procedure 22
  Infrastructure Statistics 23
  Unified ICM Service Call Statistics 25
  IVR Service Call Statistics 28
  SIP Service Call Statistics 30
  View Gateway Statistics 33
    Gateway Statistics 33
  Unified CVP VXML Server Statistics 33
  Standalone Unified CVP VXML Server Statistics 36
  View Pool Statistics 36
    Procedure 36
  Unified CVP Reporting Server Statistics 37
  Pool Statistics Tab 38
  Sort Servers 39
    Procedure 39
  Edit Device Setup 39
    Procedure 39
  Start Server 40
    Procedure 40
  Shut Down Server 40
    Procedure 41
Device Pools 41
   Add Device Pool to Operations Console 42
      Procedure 42
   Edit Device Pool 42
      Procedure 42
   Delete Device Pool 43
      Procedure 43
   Add or Remove Device From Device Pool 43
      Procedure 43
   Find Device Pool 44
      Procedure 44
Import System Configuration 44
      Procedure 45
Export System Configuration 45
      Procedure 46
Location Feature 46
   View Location Information 50
      Procedure 50
   Insert Site Identifiers 50
      Procedure 51
Deploy Location Information 51
      Procedure 51
      Error Scenario Deployment 52
   Add Locations 53
      Procedure 53
   Edit Location Information 53
      Procedure 54
   Delete Location 54
      Procedure 54
Synchronize Location Information 55
      Procedure 55
      Synchronize Error Scenarios 56
   View Location Deployment or Synchronization Status 56
      Procedure 57
Find Location 57
Procedure 57

SIP Server Groups 57
View SIP Server Groups 58
Add SIP Server Group 62
Procedure 62
Delete SIP Server Group 64
Edit SIP Server Group 64
Procedure 64
Find SIP Server Groups 65
Deploy SIP Server Group Configurations 66
Procedure 66
View SIP Server Groups Deployment Status 67
Procedure 67

Behavior 67

Dialed Number Pattern 68
Add Dialed Number Pattern 69
Procedure 69
Delete Dialed Number Pattern 71
Procedure 71
Edit Dialed Number Pattern 72
Procedure 72
Find Dialed Number Patterns 74
Procedure 74
Deploy Dialed Number Pattern 74
Procedure 74
View Dialed Number Pattern Deployment Status 75
Procedure 75

Web Services 76
Set Up Web Services 76
Procedure 76
View Web Services Deployment Status 77
Procedure 77

IOS Setup 77
Contents

IOS Template Format 78
IOS Template Management 80
  Add New Template 80
  Delete Templates 80
  Edit Templates 81
  Copy Templates 81
  View Template Details 81
IOS Template Deployment 82
  Preview and Deploy Template 82
  Check Deployment Status 83
  Roll Back Deployment 83
Cisco VVB Setup 84
  Add New Template 84
    ASR and TTS Servers Setup 84
    Application Setup 85
    Triggers Setup 89
  Delete Template 90
  Edit Templates 90
  Copy Templates 91
  Deploy Template 91
  Check Deployment Status 91
Perform Courtesy Callback 92
  Procedure 92
  View Courtesy Callback Deployment Status 94
    Procedure 94
SIP Error Reason Code Mapping 95
  Configure SIP Error Reason Code Mapping 95
  View SIP Error Reason Code Mapping Deployment Status 96
    Procedure 96
Cloud Services 97
  Proxy Settings 97
    View Proxy Settings Deployment Status 98
Context Service Setup 98
  Context Service 98
Find Reporting Server 152
  Procedure 152
Unified CVP VXML Server Setup 152
  Add Unified CVP VXML Server 153
    Procedure 153
  Edit Unified CVP VXML Server 154
    Procedure 154
  Delete Unified CVP VXML Server 155
    Procedure 155
Unified CVP VXML Server General Properties 156
Unified CVP VXML Server Configuration Properties 157
Unified CVP VXML Server Infrastructure Settings 159
Inclusive and Exclusive VXML Reporting Filters 161
  Procedure 162
    VXML Inclusive and Exclusive Filter Rules 162
    VXML Filter Wildcard Matching Examples 163
    Inclusive and Exclusive VXML Reporting Filter Examples 163
VXML Application File Transfers 164
  Download Log Messages XML File 165
    Procedure 165
  Edit Log Messages XML File 166
Unified CVP Event Severity Levels 167
  Upload Log Messages XML File 167
    Procedure 168
  Apply Unified CVP VXML Server License 168
    Procedure 168
  Find Unified CVP VXML Server 169
    Procedure 169
Unified CVP VXML Server (Standalone) Setup 169
  Add Standalone Unified CVP VXML Server 170
    Procedure 170
  Delete Standalone Unified CVP VXML Server 171
    Procedure 171
  Edit Standalone Unified VXML Server 172
Procedure 172
Find Standalone Unified CVP VXML Server 173
Procedure 173
Apply Standalone Unified CVP VXML Server License 174
Procedure 174
Gateway Setup 174
Add Gateway 175
Procedure 175
Delete Gateway 178
Procedure 178
Edit Gateway 178
Procedure 178
Find Gateway 180
Procedure 180
Transfer Script and Media File to Gateway 180
Procedure 181
View Gateway Statistics 181
Procedure 181
Execute IOS Commands on Gateway 182
Procedure 182
Speech Server Setup 182
Add Speech Server 183
Procedure 183
Delete Speech Server 184
Procedure 184
Edit Speech Server 185
Procedure 185
Find Speech Server 186
Procedure 186
Apply Speech Server License 186
Procedure 186
Media Server Setup 187
Add Media Server 188
Procedure 188
Contents

Delete Media Server 189
Procedure 189
Deploy Media Server 190
Procedure 190
Edit Media Server 190
Procedure 190
Find Media Server 192
Procedure 192
Add and Remove Media Server From Device Pool 192
Procedure 192
View Deployment Status 193
Procedure 193
Unified Communications Manager Server Setup 193
Add Unified CM Server 194
Procedure 194
Edit Unified CM Server 196
Procedure 196
Delete Unified CM Server 198
Procedure 198
Find Unified CM Server 198
Procedure 198
Unified ICM Server Setup 199
Add Unified ICM Server 199
Procedure 199
Delete Unified ICM Server 200
Procedure 200
Edit Unified ICM Server 201
Procedure 201
Find Unified ICM Server 202
Procedure 202
SIP Proxy Server Setup 203
Add SIP Proxy Server 203
Procedure 203
Edit SIP Proxy Server 205
<table>
<thead>
<tr>
<th>Procedure</th>
<th>Service Types User Roles and User Group Associations</th>
<th>216</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Group Management</td>
<td>User Group Management</td>
<td>217</td>
</tr>
<tr>
<td>Add User Group</td>
<td>Add User Group</td>
<td>217</td>
</tr>
<tr>
<td>Procedure</td>
<td>Procedure</td>
<td>217</td>
</tr>
<tr>
<td>Edit User Groups</td>
<td>Edit User Groups</td>
<td>218</td>
</tr>
<tr>
<td>Procedure</td>
<td>Procedure</td>
<td>218</td>
</tr>
<tr>
<td>Assign Role to User Group</td>
<td>Assign Role to User Group</td>
<td>218</td>
</tr>
<tr>
<td>Procedure</td>
<td>Procedure</td>
<td>218</td>
</tr>
<tr>
<td>Delete User Group</td>
<td>Delete User Group</td>
<td>219</td>
</tr>
<tr>
<td>Procedure</td>
<td>Procedure</td>
<td>219</td>
</tr>
<tr>
<td>Find User Group</td>
<td>Find User Group</td>
<td>219</td>
</tr>
<tr>
<td>Procedure</td>
<td>Procedure</td>
<td>219</td>
</tr>
<tr>
<td>Unified CVP User Setup</td>
<td>Unified CVP User Setup</td>
<td>220</td>
</tr>
<tr>
<td>General User Information Settings</td>
<td>General User Information Settings</td>
<td>220</td>
</tr>
<tr>
<td>Secure Password Requirements</td>
<td>Secure Password Requirements</td>
<td>221</td>
</tr>
<tr>
<td>Add User Account</td>
<td>Add User Account</td>
<td>222</td>
</tr>
<tr>
<td>Procedure</td>
<td>Procedure</td>
<td>222</td>
</tr>
<tr>
<td>Edit User Account</td>
<td>Edit User Account</td>
<td>222</td>
</tr>
<tr>
<td>Procedure</td>
<td>Procedure</td>
<td>223</td>
</tr>
<tr>
<td>Delete User Account</td>
<td>Delete User Account</td>
<td>223</td>
</tr>
<tr>
<td>Procedure</td>
<td>Procedure</td>
<td>223</td>
</tr>
<tr>
<td>Find User Account</td>
<td>Find User Account</td>
<td>224</td>
</tr>
<tr>
<td>Procedure</td>
<td>Procedure</td>
<td>224</td>
</tr>
<tr>
<td>Add or Remove User From Device Pool</td>
<td>Add or Remove User From Device Pool</td>
<td>224</td>
</tr>
<tr>
<td>Procedure</td>
<td>Procedure</td>
<td>224</td>
</tr>
<tr>
<td>Assign User to User Group</td>
<td>Assign User to User Group</td>
<td>225</td>
</tr>
<tr>
<td>Procedure</td>
<td>Procedure</td>
<td>225</td>
</tr>
</tbody>
</table>

---

**CHAPTER 4**

**Bulk Administration** | 227
---|---
**Bulk Administration File Transfer (BAFT)** | 227
**Transfer License Files Using BAFT** | 227
**Transfer Scripts and Media Files Using BAFT** | 228
**Transfer VXML Applications Using BAFT** | 229
SNMP Agent Setup 231

Simple Network Management Protocol Support 231
SNMP Basics 231
SNMP Management Information Base (MIB) 232
Set Up SNMP 233
Import Previously Configured Windows SNMP v1 Community Strings 233

SNMP v1/v2c Agent Setup 234

SNMP v1/v2c Community String Setup 234
Add SNMP v1/v2C Community String 235
Procedure 235
Edit SNMP v1/v2C Community String 235
Procedure 235
SNMP v1/v2c Community String Settings 236
Assign SNMP Entity to Device 237
Procedure 237
Find SNMP v1/v2c Community String 237
Procedure 237
Delete SNMP v1/v2c Community String 238
Procedure 238
SNMP v1/v2 Notification Destination Setup 238
SNMP v1/v2 Notification Destination Settings 239
Add SNMP v1/v2c Notification Destination 239
Procedure 239
Edit SNMP v1/v2C Notification Destination 240
Procedure 240
Delete SNMP v1/v2C Notification Destination 240
Procedure 240
Find SNMP v1/v2C Notification Destination 241
Procedure 241

SNMP v3 Agent Setup 241

SNMP v3 User Setup 242
Find SNMP v3 User 242
Unified CVP

Unified CVP provides Voice over IP (VoIP) routing services for the Cisco Unified Intelligent Contact Management Enterprise (Unified ICME) and Cisco Unified Contact Center Express (UCCX) products. Unified ICME provides the services necessary to determine where calls should be routed, whether to ACDs, specific agents, or to VRUs, but the routing services themselves must be provided by an external routing client.

Traditionally, ICM routing clients were various Public Switch Telephone Network (PSTN) network switches, or customer-provided ACDs. Unified CVP makes it possible for Unified ICME to use VoIP gateways as routing clients as well. This functionality carries a number of advantages, not the least of which is that call traffic can be handled over the IP network rather than by the PSTN carrier, which reduces costs and provides greater network bandwidth.

Unified CVP supports all the features of existing PSTNs and adds additional features. For example, Unified CVP provides a Voice Response Unit (VRU) platform, which includes the ability to prompt for and collect basic data from the caller before delivering the call. Unified CVP enhances this traditional PSTN feature with the use of its own VXML Interactive Voice Response (IVR) application platform. Also, Unified CVP can...
"park" calls by providing voice prompts or hold music to callers who are waiting in queue for an agent in Unified ICME.

A typical deployment of the Unified CVP solution requires operating, administering, managing, and provisioning multiple servers and IOS components. The Operations Console is a web-based console that enables users to centrally operate, administer, maintain, and provision the Unified CVP solution.

**Related Topics**
- Operations Console, on page 3
- Control Center Operation, on page 14

## Key Features and Benefits

Unified CVP is a web-based platform that provides carrier-class Interactive Voice Response (IVR) and Internet Protocol (IP) switching services over Voice Over IP (VoIP) networks.

Unified CVP includes these features:

- **IP-based services:**
  - **Switching** - Unified CVP can transfer calls over an IP network.
  - **Takeback** - Unified CVP can take back a transferred call for further IVR treatment or transfer.
  - **IVR Services** - The classic prompt-and-collect functions: "Press 1 for Sales, 2 for Service," for example.
  - **Queuing** - Calls can be "parked" on Unified CVP for prompting or music on hold, while waiting for a call center agent to be available.
  - **Voice Enabled IVR Services** - Unified CVP provides for sophisticated self-service applications, such as banking, brokerage, or airline reservations.

- **Compatibility with Other Cisco Call Routing and VoIP Products** - Specifically, Cisco Unified Intelligent Contact Management Hosted (Unified ICMH) or Unified ICME, Cisco Gateways, and Cisco IP Contact Center (IPCC).

- **Compatibility with Cisco Unified Communications Manager (Unified CM)** - Unified CM manages and switches VoIP calls among IP phones. When combined with Unified ICME, Unified CM becomes the IPCC product.

- **Compatibility with the PSTN** - Calls can be moved onto an IP-based network for Unified CVP treatment and then moved back out to a PSTN for further call routing to a call center.

- **Carrier-Class Platform** - Unified CVP is a reliable, redundant, and scalable platform, which allows it to work with service provider and large enterprise networks.

- **Reporting** - Unified CVP stores detailed call records in a reporting database using a well-documented schema. You can design and run custom reports using the ODBC-compliant reporting tool of your choice.

- **Operations Console** - A web-based console from which you can centrally operate, administer, maintain, and provision the Unified CVP solution.

- **Call Routing Support** - Unified CVP provides call routing services for SIP (RFC 3261).

- **VXML Services** - Unified CVP provides a platform for developing powerful, speech-driven interactive applications accessible from any phone.
The VXML platform includes:

- The Cisco Unified CVP VXML Server, a J2EE- and J2SE-compliant application server that dynamically drives the caller experience.
- The Cisco Unified Call Studio, a drag-and-drop graphical user interface (GUI) for the rapid creation of advanced voice applications.

## Operations Console

The Operations Console is a web-based interface from which you can configure the Unified CVP components in the Unified CVP solution. You can monitor and manage the following Unified CVP components directly from the Operations Console:

- Unified CVP Call Server
- Unified CVP Reporting Server
- Unified CVP VXML Server
- Unified CVP VXML Server (standalone)

The Operations Console manages component configurations. It also provides the ability to distribute Call Studio applications to Unified CVP VXML Servers, perform Reporting DB administration, and deploy licenses to all of the CVP devices listed above. Finally, the Operations Console provides basic visual indications as to which managed components are functioning properly and which are having problems.

Use the buttons and menus in the Operations Console to navigate through the web pages. The browser buttons are not supported.

---

**Note**

Do not use the Back button in your browser to navigate back to the pages that you have visited previously.

The Operations Console provides access to the following operations:

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

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

You can perform the following tasks to get started with the Operations Console:

- Logging in to the Operations Console
- Using the Cisco Unified Customer Voice Portal Page
- Getting Acquainted with the Operations Console Menus
• Where to Find More Information
• Logging out from the Operations Console
• Viewing System-Level Operation States
• Transferring Script and Media Files
• Using the Control Center

Sign In to Operations Console

To log in to the Operations Console, perform the following procedure.

Before You Begin

If this is the first time you are logging into the Operations Console after installing the Unified CVP software, you will need the password for the default Administrator account that was created during installation.

The inactivity session timeout for the Operations Console (when no activity is performed in the browser) is set to 60 minutes. If the browser is inactive for more than 60 minutes, you are required to login again.

Procedure

To log in to the Operations Console:

---

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 userID in the Username field.

The first time you log in after installing the Unified CVP software, enter Administrator, the default user account.

Step 3

In the Password field, enter your password.

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

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

The main Cisco Unified Customer Voice Portal window opens.

Step 4

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

---

Related Topics

Sign Out of Operations Console, on page 12

My Account Screen

The My Account screen displays the settings for the account of the user who is currently logged in.
You can view the device pools and user groups to which you are assigned.

**Related Topics**
- User Information, on page 5
- User Group Assignment, on page 5
- Device Pool Selection, on page 6

## User Information

### Table 1: User Information 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>User Information</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>Name of the user account. The user logs in to the Operations Console using this name. After logging in, the username is displayed in the upper right portion of the screen. You cannot change the username when editing a user account.</td>
<td>None</td>
<td>Valid names include uppercase and lowercase letters in the alphabet, the numbers 0 through 9, a dash, and an underscore.</td>
<td>No</td>
</tr>
<tr>
<td>Old Password</td>
<td>Old password for the user account.</td>
<td>None</td>
<td>Any text that follows the Secure Password Requirements</td>
<td>No</td>
</tr>
<tr>
<td>Password</td>
<td>New password for the user account. User must type this password to log into the Operations Console.</td>
<td>None</td>
<td>Any text that follows the Secure Password Requirements</td>
<td>No</td>
</tr>
<tr>
<td>Reconfirm Password</td>
<td>Retype the password for this user account 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>Firstname</td>
<td>(Optional) First name of the user.</td>
<td>None</td>
<td>Valid names include uppercase and lowercase letters in the alphabet, the numbers 0 through 9, a dash, and an underscore.</td>
<td>No</td>
</tr>
<tr>
<td>Lastname</td>
<td>(Optional) Last name of the user.</td>
<td>None</td>
<td>Valid names include uppercase and lowercase letters in the alphabet, the numbers 0 through 9, a dash, and an underscore.</td>
<td>No</td>
</tr>
<tr>
<td>E-mail</td>
<td>(Optional) e-mail address of the user.</td>
<td>None</td>
<td>Valid e-mail address</td>
<td>No</td>
</tr>
</tbody>
</table>

## User Group Assignment

To add/remove a user to/from a user group:
Step 1 To add a user to a group, select the user group from the Available pane, and then click the right arrow to move the user group to the Selected pane.

Step 2 To remove a user from a group, select the user from the Selected pane, and then click the left arrow to move the user group to the Available pane.

Step 3 Click Save.

---

Device Pool Selection

To add a user to or remove a user from a device pool:

Step 1 Select User Management > User.

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

Step 2 Perform one of the following steps:

- Select a user by clicking on the name in the Username list.
- Select the radio button preceding the name.

Step 3 Select Edit

The Edit User window opens to the General tab.

Step 4 Select the Device Pools tab.

Step 5 Select the device pool from the Available pane, and then click the right arrow to move the pool to the Selected pane.

Step 6 To remove a user from a device pool, perform the following steps:

a) Select the device pool from the Selected pane.

b) Select the left arrow to move the device pool to the Available pane.

**Note** A user must always be associated with at least one device pool.

Step 7 Select Save.

---

Cisco Unified Customer Voice Portal Page

The main Cisco Unified Customer Voice Portal page is displayed when you log in to the Operations Console. Navigation to the entire website is provided with the menu bar at the top of the screen.

**Related Topics**

- Operations Console Menu Options, on page 7
- More Information About Unified CVP, on page 11

---

Window Header

The window header, which displays at the top of each Operations Console window, contains the following fields:

Window header fields:
• Logged in as - User account for the user who is currently logged in.
• My Account - User who is currently logged in. See My Account Screen, on page 4.
• Logout - Logs you out from the console. See Sign Out of Operations Console, on page 12.
• About - Displays the Welcome window.
• Documentation Search - Searches the Ops Console documentation for a keyword.

**Operations Console Menu Options**

Use the Operations Console menu options to configure Unified CVP components and users.

---

**Note**

Selecting an item from the menu bar launches the respective page.
<table>
<thead>
<tr>
<th>Menu</th>
<th>Options</th>
<th>Use To</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Control Center</td>
<td>View the status of Cisco Unified Customer Voice Portal environment in a network control center. View the status and statistics by Device Type or Device Pools, logical groups of devices in Cisco Unified Customer Voice Portal solution. Initiate Start, Shutdown, or Graceful Shutdown actions on devices in the control center.</td>
</tr>
<tr>
<td></td>
<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).</td>
</tr>
<tr>
<td></td>
<td>Import System Configuration</td>
<td>Import a previously-saved Operations Console Server configuration file and apply it to the current system.</td>
</tr>
<tr>
<td></td>
<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.</td>
</tr>
<tr>
<td></td>
<td>Location</td>
<td>Add, edit, synchronize, and delete Unified CM location information.</td>
</tr>
<tr>
<td></td>
<td>SIP Server Groups</td>
<td>Configure server groups for SIP and view Call Server deployment status.</td>
</tr>
<tr>
<td></td>
<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.</td>
</tr>
<tr>
<td></td>
<td>Web Services</td>
<td>Configure Diagnostic Portal servlet credentials.</td>
</tr>
<tr>
<td></td>
<td>IOS Configuration</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>
</tr>
<tr>
<td></td>
<td>VVB Configuration</td>
<td>Configure Virtualized Voice Browser and associate it with device pools.</td>
</tr>
<tr>
<td></td>
<td>Courtesy Callback</td>
<td>Courtesy Callback reduces the time callers have to wait on hold/in queue and allows the system to offer callers who meet certain criteria.</td>
</tr>
<tr>
<td></td>
<td>SIP Error Reason Code Mapping</td>
<td>Configure SIP reason code to ISUP cause code mapping.</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 Unified CVP Call Server general and infrastructure settings; specify call services settings for each deployment model; associate Unified CVP Call Servers with device pools and the SIP Proxy Server; and apply licenses to a Unified CVP Call Server.</td>
</tr>
<tr>
<td></td>
<td>Unified CVP Reporting Server</td>
<td>Configure Unified CVP Reporting Server general and infrastructure settings, associate Unified CVP Reporting Servers with Unified CVP Servers, specify reporting properties, and associate Unified CVP Reporting Servers with device pools. Perform Reporting database administration: schedule database backups and purges; manage database and reporting user names and passwords; apply licenses to a Unified CVP Reporting Server.</td>
</tr>
<tr>
<td></td>
<td>Unified CVP VXML Server</td>
<td>Configure Unified CVP VXML Server general and infrastructure settings; specify primary and backup Unified CVP Call Servers; enable Unified CVP VXML Server reporting and specify VoiceXML data filters; associate Unified CVP VXML Servers with device pools; and apply licenses and transfer scripts to a VXML Server.</td>
</tr>
<tr>
<td></td>
<td>Unified CVP VXML Server (standalone)</td>
<td>Configure Unified CVP VXML Server (standalone) general settings; associate Unified CVP VXML Server (standalone) with device pools; and apply licenses and transfer scripts to a Unified CVP VXML Server (standalone).</td>
</tr>
<tr>
<td></td>
<td>Note</td>
<td>A Unified CVP VXML Server (standalone) handles calls that arrive through a VoiceXML gateway. (No statistics are provided when the Unified CVP VXML Server is configured this way.) Also, you cannot configure a database to and capture data from Unified CVP VXML Server (standalone) applications.</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></td>
<td>Virtualized Voice Browser</td>
<td>Configure Virtualized Voice Browser and associate it with device pools.</td>
</tr>
<tr>
<td></td>
<td>Speech Server</td>
<td>Speech Server provides speech recognition and synthesis services. You can add a pre-configured Speech Server to the Operations Console.</td>
</tr>
<tr>
<td></td>
<td>Media Server</td>
<td>Configure Media Server general settings and associate a Media Server with device pools.</td>
</tr>
<tr>
<td></td>
<td>Note</td>
<td>Media Server administers the media files that contain messages and prompts callers hear.</td>
</tr>
<tr>
<td></td>
<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>
</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>Unified ICM</td>
<td>Configure ICM Server general settings and associate the ICM Server with device pools.</td>
</tr>
<tr>
<td></td>
<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>
</tr>
<tr>
<td></td>
<td>Unified IC</td>
<td>Configure CUIS Server general settings and associate the CUIS Server with device pools.</td>
</tr>
<tr>
<td></td>
<td>Device Past Configuration</td>
<td>Allows you to view the past 10 saved configurations of a selected device that are currently stored in the Operations Console database.</td>
</tr>
<tr>
<td></td>
<td>Device Versions</td>
<td>View version information for the Unified CVP Call Server, Unified CVP Reporting Server, Unified CVP VXML Server, and Unified CVP VXML Server (standalone).</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, script files, and VXML applications to multiple devices at a time.</td>
</tr>
<tr>
<td>SNMP</td>
<td>V1/V2c</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>V3</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>System Group</td>
<td>Configure the MIB2 System Group system contact and location settings, and associate the MIB2 System Group with devices.</td>
</tr>
<tr>
<td>Tools</td>
<td>SNMP Monitor</td>
<td>Launch the SNMP Monitor application in a new browser window.</td>
</tr>
<tr>
<td>Help</td>
<td>Configure</td>
<td>Specify the URLs that launch the SNMP Monitor.</td>
</tr>
<tr>
<td></td>
<td>Contents</td>
<td>Display the table of contents for the help system.</td>
</tr>
<tr>
<td></td>
<td>This Page</td>
<td>Displays help on the current screen.</td>
</tr>
</tbody>
</table>
More Information About Unified CVP


The following table lists the documents available in the Unified CVP documentation set.

<table>
<thead>
<tr>
<th>For More Information on...</th>
<th>Refer to...</th>
</tr>
</thead>
</table>
Sign Out of Operations Console

To log out from the Operations Console, perform the following procedure.

Procedure

To log out from the Operations Console:

Click **Logout** in the screen header at the top of the screen.

You are logged out and the main Cisco Customer Voice Portal window opens.

---

**Related Topics**

- [Sign In to Operations Console](#), on page 4

---

View System-Level Operation States

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

*Table 2: Description of States Displayed in the Status Window*

<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>
</tbody>
</table>
### Failed Deployment Reasons

<table>
<thead>
<tr>
<th>State</th>
<th>Reasons</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

### Failed Synchronization Reasons

<table>
<thead>
<tr>
<th>State</th>
<th>Reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The reasons for a <strong>failed synchronization</strong> state are listed below:</td>
</tr>
<tr>
<td></td>
<td>• Device not accessible</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, you must deploy the changed configuration again.
Transfer Script and Media Files

You can transfer a single script or media file at a time from the Operations Console.

Procedure

To transfer a script or media file:

Step 1  From the Device Management menu, select the type of server to which to transfer the script file. For example, to transfer a script or media file to a Gateway, select **Device Management > Gateway**.

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

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

Step 3  Select **File Transfer** in the toolbar and then click **Scripts and Media**.

The Scripts and Media File Transfer page opens, listing the host name and IP address for the selected device. Script and Media files currently stored in the Operations Server database are listed in the Select From available Script Files box.

Step 4  If the script or media file is not listed in the Select From Available Script Files box:
- a) Click **Select a Script or Media File from Your Local PC**.
- b) Enter the file name in the text box or click **Browse** to search for the script or media file on the local file system.

Step 5  If the script or media file is listed in the Select From Available Script and media Files box, select the script or media file.

Step 6  Click **Transfer** to send the file to the device.

The script or media file is transferred to the selected server.

Error Handling

The Operations Console performs two types of validations:

- **Client Side** - Validations using Javascript, which runs within the web browser. You must enable Javascript in the browser.
- **Server Side** - Validations that are run on the server side. These are extensive validations that include the client side validations and any business validations.

Client side validation errors display at the top of the page just below the Menu bar.

Control Center Operation

Use the control center to view and manage the devices in the Unified CVP solution from a central place. You can view the status of an individual device or all the devices that belong to a group of devices. You can also shut down and start VXML, Reporting, and Call Servers; and view detailed statistics for each of these devices.

You can perform the following tasks from the Control Center:
View Devices by Type

You can view groups of devices by type (for example, Call Server, or Reporting Server). Devices of the selected device type are listed in the right pane of the Control Center.

Related Topics
- Start Server, on page 40
- Shut Down Server, on page 40
- Edit Device Setup, on page 39
- View Device Status, on page 16

Procedure

To view devices by type:

**Step 1** Select System > Control Center.
The Control Center window opens.

**Step 2** Select the Device Type tab.
Devices types are listed in the Device Type tab.

**Step 3** Select the type of device to display.
Only devices of the selected type are listed in the Devices tab in the right pane.

---

**View Devices by Device Pool**

You can view groups of devices by device pool (for example, the devices in the San Jose pool). If a device belongs to more than one device pool, that device is listed in each device pool.

**Related Topics**
- Start Server, on page 40
- Shut Down Server, on page 40
- Edit Device Setup, on page 39
- View Device Status, on page 16

**Procedure**

To view devices by device pool:

**Step 1** Select **System > Control Center**.

**Step 2** Select the **Device Pool** tab and then select a device pool from the list.
Devices that belong to the selected device pool display on the **General** tab.

**Step 3** Sort the devices by Hostname, IP Address, Device Type, Status, or Active Calls by clicking the desired column header.
Only the devices listed on the current page are sorted. For example, if you select a Call Server device pool and then click the **IP Address** column header, the call servers displayed on the current screen are sorted by the IP address.

**Step 4** Select the desired refresh interval from the **Refresh** drop-down menu.
By default, pool statistics are not refreshed.

**Step 5** Click individual device in a device pool to display or edit the device configuration.

---

**View Device Status**

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

All CVP devices, Unified CVP Call Servers, Unified CVP Reporting Servers, and Unified CVP VXML Servers, report current operating status. The status of some devices, such as IOS devices, Unified CM, ICM
servers, SIP proxy servers display as N/A (Not Applicable) because the Operations Console does not monitor these device types.

The following tables describes the fields in the Control Center.

**Table 3: Device Status Fields in the Control Center**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>The hostname assigned to the device.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address for the server.</td>
</tr>
<tr>
<td>Device Type</td>
<td>The category of the device, for example: Unified CVP Call Servers, Unified CVP Reporting Servers, or Unified CVP VXML Servers.</td>
</tr>
<tr>
<td>Actions</td>
<td>Icons that indicate operations that you can perform on a selected device. Not all actions are available for all devices. Available actions include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Statistics</strong> - Data on current activities and activities that occur during an interval.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unapplied Changes</strong> - Indicates that configuration changes that have been saved to the Operations Console database have not yet been applied to the device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Link to an External Administration Page</strong> - Displays a web-based administration page from which you can administer a server. Available for Unified CM, SIP proxy servers, and ICM Servers.</td>
</tr>
</tbody>
</table>
The current operating status for a selected device.

- The Device is up and running.

CVP Service Internal States:

- **In Service** - The service is running.
- **In Service (Warning Threshold Reached)** - The service is running and the warning threshold has been reached.
- **In Service (Critical Threshold Reached)** - The service is running and the critical threshold has been reached.

- Device is not running or has no communication with local WebServicesManager service.

CVP Service Internal States:

- **Disabled** - The service has not been configured.
- **Stopped** - The service is not running.
- **Error Scenario (not an internal state)** - Where local WebServicesManager service has no message bus communication with device.

- One or more of the device services are functioning partially.

CVP Service Internal States:

- **Starting** - The service is starting.
- **Partial Service** - The service has been configured and started, but is not running at full service.

Partial service may be attributed to waiting on a dependency (such as the IVR and SIP service waiting for ICM to connect to the VRU PIM), not licensed, or license usage critical.

- **Stopping** - The service is stopping.
- **Not Reachable**

- The device could not be reached from Operations Console.

Common reasons for not reachable status are:

- Machine shutdown.
- WebServicesManager service on the device is down.
- Security is enabled for device but invalid certificate configuration.
Field | Description
--- | ---
Active Calls | The total number of calls currently running in the device.
  - `<Integer Value>` - The number of calls for devices such as Unified CVP Call Server, Unified CVP Reporting Server, and Unified CVP VXML Server.
  - `N/A` - Not applicable for device types such as gateway, Unified CM Server, Virtualized Voice Browser and so on.

Context Service Status | Context service connectivity status for the selected device.
  - Context Service States:
    - `N/A` - Device is not registered or context service not applicable for the device type.
    - `Up` - Device is registered with Context Service and no issues.
    - `Down` - Device is registered with Context Service and has connectivity issue.

Sometimes, the actual device status can be resultant of more than one CVP service state for the corresponding device. For example, the Unified CVP Call Service device status in Control Center is actually an aggregation of SIP, ICM, and IVR service states.

The following table describes device status that is specific to each CVP device type.

**Table 4: CVP Device Status**

<table>
<thead>
<tr>
<th>CVP Device</th>
<th>Description</th>
</tr>
</thead>
</table>
| Unified CVP Call Server | • **Up**
  All configured services (ICM/IVR/SIP) are in the In Service state and report the same to the Operations Console.

  • **Down**
  At least one of the configured services (ICM/IVR/SIP) is deemed stopped (or disabled), and none of these services are in the Not Reachable state.

  • **Partial**
  At least one of the configured services (ICM/IVR/SIP) is running at Partial Service, and neither of these services are in the Down or Not Reachable state.

  **Note** If the device status is Partial, the status of the individual services are shown in the Partial state Details. Click the Partial status in Control Center to view the tool tip; it describes each service state.

  • **Not Reachable**
  At least one of the configured services (ICM/IVR/SIP) is deemed Not Reachable.
  If the Unified CVP Call Server is configured with no services (SIP/IVR/ICM) active, its status in Control Center will always be Not Reachable.
### View Device Status

<table>
<thead>
<tr>
<th>CVP Device</th>
<th>Description</th>
</tr>
</thead>
</table>
| Unified CVP Reporting Server | • **Up**  
The reporting service is running as reported by Central Controller on the Unified CVP Call Server machine.  

• **Down**  
If the reporting service is deemed Stopped (or disabled) as reported by Central Controller on the Unified CVP Call Server machine or the WebServicesManager, an associated Unified CVP Call Server machine has no communication with Central Controller.  

  • The WebServicesManager on the Unified CVP Call Server has not received state events from the Controller for the reporting subsystem.  

  • The Unified CVP Reporting Server is unable to communicate with Central Controller on the Unified CVP Call Server machine; Central Controller has no knowledge of state events and, therefore, cannot communicate state events to Operations Console.  

In either scenario, even if the Unified CVP Reporting Server is up and running and the WebServicesManager on the Unified CVP Reporting Server is up and running, the Operations Console still shows the status of the Unified CVP Reporting Server as Down when there is no communication with Control Controller.  

• **Partial**  
The reporting service is not in the Up, Down, or Not Reachable state. Unified CVP Reporting Server indicates a partial status when, for example, the reporting data buffer file is full and all new messages are written in memory in a buffer queue.  

• **Not Reachable**  
The Operations Console is unable to communicate to the WebServicesManager co-located with the associated Unified CVP Call Server (for example, the WebServicesManager service on the device is down).
In both cases, the Operations Console communicates with the WebServicesManager co-located on the Unified CVP VXML Server (or standalone) server machine. The WebServicesManager on the device runs the Unified CVP VXML Server status script to retrieve device status and the number of active calls.

- **Up**
  
  If the WebServicesManager gets a valid number for the number of active calls after running the status script. Zero (0) is a valid number.

- **Not Reachable**
  
  In addition to other reasons for the Not Reachable state, the Unified CVP VXML Server (or standalone) goes into this state if WebServicesManager does not get a valid number for active calls after running the status.

There is no Partial or Down status for Unified CVP VXML Servers and Unified CVP VXML Server (standalone).

### View Device Statistics

You can view realtime, interval, and aggregate data for Unified CVP devices.

**Related Topics**

- Infrastructure Statistics, on page 23
- Unified ICM Service Call Statistics, on page 25
- IVR Service Call Statistics, on page 28
- SIP Service Call Statistics, on page 30
- View Gateway Statistics, on page 33
- Unified CVP VXML Server Statistics, on page 33
- Standalone Unified CVP VXML Server Statistics, on page 36
- Unified CVP Reporting Server Statistics, on page 37

**Procedure**

To view device statistics:

**Step 1** Select System > Control Center.

**Step 2** From the Device Type tab in the left pane, select the type of device for which you want to view statistics.

**Step 3** From the Devices tab, select a device by checking the radio button preceding it.

**Step 4** Select Statistics either in the Actions column or in the toolbar.

Statistics for the selected device are reported in a new statistics result window. All event statistics are sent to an SNMP manager, if one is configured. The log messages XML file, CVPLogMessages.xml, defines the severity, destination (SNMP management station or Syslog server), and possible resolution for Unified CVP log messages.
View Device Associations

The Operations Console supports the association of CVP Call Servers with Unified CVP VXML Servers and/or CVP Reporting Servers.

Procedure

To view devices associated with a Call Server:

Step 1  Select System > Control Center.
        The Control Center window opens.

Step 2  Click the hostname of a Call Server.
        The Edit CVP Call Server Configuration window opens.

Step 3  From the toolbar, click Device Associations.
        The Device Association page lists the VXML Server, Reporting Server, and Courtesy Callback Reporting Server associated with this Call Server.

View Infrastructure Statistics

You can view realtime, interval, and aggregate data for Unified CVP devices.

Related Topics

    Edit Log Messages XML File, on page 166

Procedure

To view infrastructure statistics:

Step 1  Select System > Control Center.
Step 2  Select the Device Type tab.
Step 3  Select the type of device for which you want infrastructure statistics.
        Devices of the selected type display in the Devices tab.

Step 4  Select the device by checking the radio button preceding it.
Step 5  Select Statistics in the toolbar.
Step 6  Select the Infrastructure tab.
        Statistics for the selected device are reported in a new window. All event statistics are sent to an SNMP manager, if one is configured. The log messages XML file, CVPLogMessages.xml, defines the severity, destination (SNMP management station or Syslog server), and possible resolution for Unified CVP log messages.
**Infrastructure Statistics**

Unified CVP infrastructure statistics include realtime and interval data on the Java Virtual Machine (JVM), threading, and licensing.

You can access these statistics by selecting Control Center from the System menu and then selecting a device. See View Infrastructure Statistics for more information.

Access infrastructure statistics either by:

- Selecting **System > Control Center**, selecting a device, clicking the **Statistics** icon in the toolbar, and then selecting the **Infrastructure** tab.

- Selecting a device type from the **Device Management** menu, selecting a device. Click **Edit > Statistics > Infrastructure**.

The following table describes infrastructure statistics.

*Table 5: Infrastructure Statistics*

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Realtime Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Ports Available</td>
<td>The number of ports available for the processing of new calls. Exactly one port license is used per call, independent of the call's traversal through the individual call server services.</td>
</tr>
<tr>
<td>Current Port Usage</td>
<td>The number of port usage currently in use on the call server. Exactly one port usage is used per call, independent of the call's traversal of the individual call server services.</td>
</tr>
<tr>
<td>Current Port Usage State</td>
<td>The threshold level of port usage. There are four levels: safe, warning, critical, and failure. An administrator may set the required percentage of port licenses in use needed to reach a given threshold level, with the exception of the failure level which is reached when the number of ports checked out is equal to the total number of ports.</td>
</tr>
<tr>
<td><strong>Interval</strong></td>
<td></td>
</tr>
<tr>
<td>Start Time</td>
<td>The time the system started collecting statistics for the current interval.</td>
</tr>
<tr>
<td>Duration Elapsed</td>
<td>The amount of time that has elapsed since the start time in the current interval.</td>
</tr>
<tr>
<td>Interval Duration</td>
<td>The interval at which statistics are collected. The default value is 30 minutes.</td>
</tr>
<tr>
<td>Total New Port Usage Requests</td>
<td>The number of port usage checkout requests made in the current interval. For each port license checkout request, whether it checks out a new port license or not, this metric is increased by one.</td>
</tr>
</tbody>
</table>
The average number of port usage checkout requests made per minute in the current interval. This metric is calculated by dividing the port license requests metric by the number of minutes elapsed in the current interval.

The maximum number of ports used during this time interval.

The time the service started collecting statistics.

The amount of time that has elapsed since the service start time.

The number of port checkout requests made since the system was started. For each port checkout request, whether it checks out a new port or not, this metric is increased by one.

The average number of port checkout requests made per minute since the system was started. This metric is calculated by dividing the aggregate port license requests metric by the number of minutes elapsed since the system was started.

The peak number of simultaneous ports used since the start of the system. When a port checkout occurs, this metric is set to the current ports in use metric if that value is greater than this metric's current peak value.

The number of port checkout requests that were denied since the start of the system. The only reason a port checkout request would be denied is if the number of port licenses checked out at the time of the request is equal to the total number of ports available. When a port checkout is denied, the call does not receive regular treatment (the caller may hear a busy tone or an error message).

The following table describes thread pool system statistics. The thread pool is a cache of threads, used by Unified CVP components only, for processing of relatively short tasks. Using a thread pool eliminates the waste of resources encountered when rapidly creating and destroying threads for these types of tasks.

### Table 6: Thread Pool Realtime Statistics

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Realtime Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Idle Threads</td>
<td>The number of idle threads waiting for some work.</td>
</tr>
<tr>
<td>Active Threads</td>
<td>The number of running thread pool threads currently processing some work.</td>
</tr>
<tr>
<td>Core Pool Size</td>
<td>The number of thread pool threads that are never destroyed, regardless of their idle period.</td>
</tr>
</tbody>
</table>

---

*Infrastructure Statistics*

*Administering Guide for Cisco Unified Customer Voice Portal, Release 12.0(1)
<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Pool Size</td>
<td>The maximum number of thread pool threads that can exist simultaneously.</td>
</tr>
<tr>
<td>Largest Pool Size</td>
<td>The peak number of thread pool threads simultaneously tasks with some work to process.</td>
</tr>
</tbody>
</table>

The following table describes Java Virtual Machine statistics.

**Table 7: Java Virtual Machine (JVM) Realtime Statistics**

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Realtime Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Peak Memory Usage</td>
<td>The greatest amount of memory used by the Java Virtual machine since startup. The number reported is in megabytes and indicates the peak amount of memory ever used simultaneously by this Java Virtual Machine.</td>
</tr>
<tr>
<td>Current Memory Usage</td>
<td>The current number of megabytes of memory used by the Java Virtual Machine.</td>
</tr>
<tr>
<td>Total Memory</td>
<td>The total amount of memory in megabytes available to the Java Virtual Machine. The number reported is in megabytes and indicates the how much of the system memory is available for use by the Java Virtual Machine.</td>
</tr>
<tr>
<td>Available Memory</td>
<td>The amount of available memory in the Java Virtual Machine. The number reported is in megabytes and indicates how much of the current system memory claimed by the Java Virtual Machine is not currently being used.</td>
</tr>
<tr>
<td>Threads in Use</td>
<td>The number of threads currently in use in the Java Virtual Machine. This number includes all of the Unified CVP standalone and thread pool threads, as well as those threads created by the Web Application Server running within the same JVM.</td>
</tr>
<tr>
<td>Peak Threads in Use</td>
<td>The greatest amount of threads ever used simultaneously in the Java Virtual Machine since startup. The peak number of threads ever used by the Java Virtual Machine includes all Unified CVP standalone and thread pool threads, as well as threads created by the Web Application Server running within the same JVM.</td>
</tr>
<tr>
<td>Uptime</td>
<td>The length of time that the Java Virtual Machine has been running. This time is measured in hh:mm:ss and shows the amount of elapsed time since the Java Virtual Machine process began executing.</td>
</tr>
</tbody>
</table>

**Unified ICM Service Call Statistics**

The ICM Service call statistics include data on calls currently being processed by the ICM service, new calls received during a specified interval, and total calls processed since start time.

Access ICM Service statistics either by:
• Selecting System > Control Center, selecting a Unified CVP Call Server, clicking the Statistics icon in the toolbar, and then selecting the ICM tab.

• Selecting Device Management > Unified CVP Call Server, selecting a Unified CVP Call Server, clicking the Statistics icon in the toolbar, and then selecting the ICM tab.

The following table describes ICM Service call statistics.

Table 8: ICM Service Call Statistics

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Realtime Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Active Calls</td>
<td>The current number of calls being serviced by the Unified ICM Server for a Unified CVP Call Server. This value represents a count of calls currently being serviced by the ICM for the Unified CVP Call Server for follow-on routing to a Contact Center agent.</td>
</tr>
<tr>
<td>Active SIP Call Legs</td>
<td>The Unified ICM Server can accept Voice over IP (VoIP) calls that originate using the Session Initiation Protocol (SIP). Active SIP Call Legs indicates the current number of calls received by the Unified ICM Server from the Unified CVP Call Server using the SIP protocol.</td>
</tr>
<tr>
<td>Active VRU Call Legs</td>
<td>The current number of calls receiving Voice Response Unit (VRU) treatment from the Unified ICM Server. The VRU treatment includes playing pre-recorded messages, asking for Caller Entered Digits (CED), or Speech Recognition Techniques to understand the customer request.</td>
</tr>
<tr>
<td>Active ICM Lookup Requests</td>
<td>Calls originating from an external Unified CVP VXML Server need call routing instructions from the Unified ICM Server. Active Lookup Requests indicates the current number of external Unified CVP VXML Server call routing requests sent to the ICM Server.</td>
</tr>
<tr>
<td>Active Basic Service Video Calls Offered</td>
<td>The current number of simultaneous basic service video calls being processed by the ICM service where video capability was offered.</td>
</tr>
<tr>
<td>Active Basic Service Video Calls Accepted</td>
<td>The current number of simultaneous calls that were accepted as basic service video calls and are being processed by the ICM service.</td>
</tr>
<tr>
<td><strong>Interval Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Start Time</td>
<td>The time at which the current interval has begun.</td>
</tr>
<tr>
<td>Duration Elapsed</td>
<td>The amount of time that has elapsed since the start time in the current interval.</td>
</tr>
<tr>
<td>Interval Duration</td>
<td>The interval at which statistics are collected. The default value is 30 minutes.</td>
</tr>
<tr>
<td>New Calls</td>
<td>The number of new calls received by the Intelligent Contact Management (ICM) application for follow-on Voice Response Unit (VRU) treatment and routing to a Contact Center agent during the current interval.</td>
</tr>
</tbody>
</table>
The Intelligent Contact Management (ICM) application has the ability to accept Voice over IP (VoIP) calls that originate via the Session Initiation Protocol (SIP). Interval SIP Call Legs is an interval specific snapshot metric indicating the number of calls received by the ICM application via SIP during the current interval.

The number of calls receiving Voice Response Unit (VRU) treatment from the Intelligent Contact Management (ICM) application. The VRU treatment includes playing pre-recorded messages, asking for Caller Entered Digits (CED), or speech recognition techniques to understand the customer request during the current interval.

Calls originating in an external Unified CVP VXML Server need call routing instructions from the Intelligent Contact Management (ICM) application. Interval Lookup Requests is an interval specific metric indicating the number of external Unified CVP VXML Server call routing requests sent to the ICM application during the current interval.

The number of offered basic service video calls processed by the ICM service during the current interval.

The number of basic service video calls accepted and processed by the ICM service during the current interval.

The time the service started collecting statistics.

The amount of time that has elapsed since the service start time.

The total number of new calls received by the ICM application for follow-on VRU treatment and routing to a Contact Center agent since system start time.

The ICM application has the ability to accept VoIP calls that originate via the SIP. Total SIP Switch Legs is a metric indicating the total number of calls received by the ICM application via SIP since system start time.

The total number of calls that have received VRU treatment from the ICM application since system start time. The VRU treatment includes playing pre-recorded messages, asking for CED or Speech Recognition Techniques to understand the customer request.

Calls originating in an external Unified CVP VXML Server need call routing instructions from the ICM application. Total Lookup Requests is a metric indicating the total number of external Unified CVP VXML Server call routing requests sent to the ICM application since system start time.

The total number of newly offered basic service video calls processed by the ICM service since system start time.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Call Legs</td>
<td>The Intelligent Contact Management (ICM) application has the ability to accept Voice over IP (VoIP) calls that originate via the Session Initiation Protocol (SIP). Interval SIP Call Legs is an interval specific snapshot metric indicating the number of calls received by the ICM application via SIP during the current interval.</td>
</tr>
<tr>
<td>VRU Call Legs</td>
<td>The number of calls receiving Voice Response Unit (VRU) treatment from the Intelligent Contact Management (ICM) application. The VRU treatment includes playing pre-recorded messages, asking for Caller Entered Digits (CED), or speech recognition techniques to understand the customer request during the current interval.</td>
</tr>
<tr>
<td>ICM Lookup Requests</td>
<td>Calls originating in an external Unified CVP VXML Server need call routing instructions from the Intelligent Contact Management (ICM) application. Interval Lookup Requests is an interval specific metric indicating the number of external Unified CVP VXML Server call routing requests sent to the ICM application during the current interval.</td>
</tr>
<tr>
<td>Basic Service Video Calls Offered</td>
<td>The number of offered basic service video calls processed by the ICM service during the current interval.</td>
</tr>
<tr>
<td>Basic Service Video Calls Accepted</td>
<td>The number of basic service video calls accepted and processed by the ICM service during the current interval.</td>
</tr>
<tr>
<td>Aggregate Statistics</td>
<td></td>
</tr>
<tr>
<td>Start Time</td>
<td>The time the service started collecting statistics.</td>
</tr>
<tr>
<td>Duration Elapsed</td>
<td>The amount of time that has elapsed since the service start time.</td>
</tr>
<tr>
<td>Total Calls</td>
<td>The total number of new calls received by the ICM application for follow-on VRU treatment and routing to a Contact Center agent since system start time.</td>
</tr>
<tr>
<td>Total SIP Call Legs</td>
<td>The ICM application has the ability to accept VoIP calls that originate via the SIP. Total SIP Switch Legs is a metric indicating the total number of calls received by the ICM application via SIP since system start time.</td>
</tr>
<tr>
<td>Total VRU Call Legs</td>
<td>The total number of calls that have received VRU treatment from the ICM application since system start time. The VRU treatment includes playing pre-recorded messages, asking for CED or Speech Recognition Techniques to understand the customer request.</td>
</tr>
<tr>
<td>Total ICM Lookup Requests</td>
<td>Calls originating in an external Unified CVP VXML Server need call routing instructions from the ICM application. Total Lookup Requests is a metric indicating the total number of external Unified CVP VXML Server call routing requests sent to the ICM application since system start time.</td>
</tr>
<tr>
<td>Total Basic Service Video Calls Offered</td>
<td>The total number of newly offered basic service video calls processed by the ICM service since system start time.</td>
</tr>
</tbody>
</table>
The total number of new basic service video calls accepted and processed by the ICM service since system start time.

IVR Service Call Statistics

The IVR service call statistics include data on calls currently being processed by the IVR service, new calls received during a specified interval, and total calls processed since the IVR service started.

Access IVR Service statistics either by:

- Selecting **System > Control Center**, selecting a Call Server, clicking the **Statistics** icon in the toolbar, and then selecting the **IVR** tab.

- Selecting **Device Management > Unified CVP Call Server**, and selecting a Unified CVP Call Server. Click **Edit > Statistics > IVR**.

The following table describes the IVR Service call statistics.

**Table 9: IVR Service Call Statistics**

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Basic Service Video Calls Accepted</td>
<td>The total number of new basic service video calls accepted and processed by the ICM service since system start time.</td>
</tr>
</tbody>
</table>

**Realtime Call Statistics**

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Calls</td>
<td>The number of active calls being serviced by the IVR service.</td>
</tr>
<tr>
<td>Active HTTP Requests</td>
<td>The number of active HTTP requests being serviced by the IVR service.</td>
</tr>
</tbody>
</table>

**Interval Statistics**

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>The time the system started collecting statistics for the current interval.</td>
</tr>
<tr>
<td>Duration Elapsed</td>
<td>The amount of time that has elapsed since the start time in the current interval.</td>
</tr>
<tr>
<td>Interval Duration</td>
<td>The interval at which statistics are collected. The default value is 30 minutes.</td>
</tr>
<tr>
<td>Peak Active Calls</td>
<td>Maximum number of active calls handled by the IVR service at the same time during this interval.</td>
</tr>
<tr>
<td>New Calls</td>
<td>New Calls is a metric that counts the number of New Call requests received from the IOS Gateway Service. A New Call includes the Switch leg of the call and the IVR leg of the call. This metric counts the total number of New Call Requests received by the IVR Service during this interval.</td>
</tr>
<tr>
<td>Statistic</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Calls Finished</td>
<td>A Call is a metric that represents the Switch leg of the CVP call and the IVR leg of the CVP call. When both legs of the call are finished, this metric increases. Calls Finished is a metric that counts the number of CVP Calls that have finished during this interval.</td>
</tr>
<tr>
<td>Average Call Latency</td>
<td>The average amount of time in milliseconds it took the IVR Service to process a New Call or Call Result Request during this interval.</td>
</tr>
<tr>
<td>Maximum Call Latency</td>
<td>The maximum amount of time in milliseconds it has taken for the IVR Service to complete the processing of a New Call Request or a Request Instruction Request during this time interval.</td>
</tr>
<tr>
<td>Minimum Call Latency</td>
<td>The minimum amount of time in milliseconds it took for the IVR Service to complete the processing of a New Call Request or a Request Instruction Request during this time interval.</td>
</tr>
<tr>
<td>Peak Active HTTP Requests</td>
<td>Active HTTP Requests is a metric that indicates the current number of simultaneous HTTP requests being processed by the IVR Service. Peak Active Requests is a metric that represents the maximum simultaneous HTTP requests being processed by the IVR Service during this time interval.</td>
</tr>
<tr>
<td>Total HTTP Requests</td>
<td>The total number of HTTP Requests received from a client by the IVR Service during this time interval.</td>
</tr>
<tr>
<td>Average HTTP Requests/second</td>
<td>The average number of HTTP Requests the IVR Service receives per second during this time interval.</td>
</tr>
<tr>
<td>Peak Active HTTP Requests/second</td>
<td>HTTP Requests per Second is a metric that represents the number of HTTP Requests the IVR Service receives each second from all clients. Peak HTTP Requests per Second is the maximum number of HTTP Requests that were processed by the IVR Service in any given second. This is also known as high water marking.</td>
</tr>
</tbody>
</table>

**Aggregate Statistics**

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>The time the service started collecting statistics.</td>
</tr>
<tr>
<td>Duration Elapsed</td>
<td>The amount of time that has elapsed since the service start time.</td>
</tr>
<tr>
<td>Total New Calls</td>
<td>New Calls is a metric that counts the number of New Call requests received from the IOS Gateway Service. A New Call includes the Switch leg of the call and the IVR leg of the call. Total New Calls is a metric that represents the total number of new calls received by the IVR Service since system startup.</td>
</tr>
<tr>
<td>Peak Active Calls</td>
<td>The maximum number of simultaneous calls processed by the IVR Service since the service started.</td>
</tr>
</tbody>
</table>
SIP Service Call Statistics

The SIP service call statistics include data on calls currently being processed by the SIP service, new calls received during a specified interval, and total calls processed since the SIP service started.

Access SIP service statistics either by:

- Selecting System > Control Center, selecting a Unified CVP Call Server, clicking the Statistics icon in the toolbar, and then selecting the SIP tab.
- Selecting Device Management > Unified CVP Call Server and selecting a Call Server. Click Edit > Statistics > SIP.

The following table describes the SIP Service call statistics.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realtime Statistics</td>
<td></td>
</tr>
<tr>
<td>Active Calls</td>
<td>A real time snapshot metric indicating the count of the number of current calls being handled by the SIP service.</td>
</tr>
<tr>
<td>Total Call Legs</td>
<td>The total number of SIP call legs being handled by the SIP service. A call leg is also known as a SIP dialog. The metric includes incoming, outgoing, and ringtone type call legs. For each active call in the SIP service, there will be an incoming call leg, and an outgoing call leg to the destination of the transfer label.</td>
</tr>
<tr>
<td>Active Basic Service Video Calls Offered</td>
<td>The number of basic service video calls in progress where video capability was offered.</td>
</tr>
<tr>
<td>Active Basic Service Video Calls Answered</td>
<td>The number of basic service video calls in progress where video capability was answered.</td>
</tr>
<tr>
<td>Active Agent Whisper Calls</td>
<td>The number of active whisper call legs.</td>
</tr>
<tr>
<td>Active Agent Greeting Calls</td>
<td>The number of active greeting call legs.</td>
</tr>
</tbody>
</table>

Interval Statistics
<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>The time the system started collecting statistics for the current interval.</td>
</tr>
<tr>
<td>Duration Elapsed</td>
<td>The amount of time that has elapsed since the start time in the current interval.</td>
</tr>
<tr>
<td>Interval Duration</td>
<td>The interval at which statistics are collected. The default value is 30 minutes.</td>
</tr>
<tr>
<td>New Calls</td>
<td>The number of SIP Invite messages received by Unified CVP in the current interval. It includes the failed calls as well as calls rejected due to the SIP service being out of service.</td>
</tr>
<tr>
<td>Connects Received</td>
<td>The number of CONNECT messages received by SIP service in order to perform a call Transfer, in the last statistics aggregation interval. Connects Received includes the regular Unified CVP transfers as well as Refer transfers. Any label coming from the ICM service is considered a CONNECT message, whether it is a label to send to the VRU or a label to transfer to an agent.</td>
</tr>
<tr>
<td>Avg Latency Connect to Answer</td>
<td>The period of time between the CONNECT from ICM and when the call is answered. The metric includes the average latency computation for all the calls that have been answered in the last statistics aggregation interval.</td>
</tr>
<tr>
<td>Failed SIP Transfers (Pre-Dialog)</td>
<td>The total number of failed SIP transfers since system start time. When Unified CVP attempts to make a transfer to the first destination of the call, it sends the initial INVITE request to set up the caller with the ICM routed destination label. The metric does not include rejections due to the SIP Service not running. The metric includes failed transfers that were made after a label was returned from the ICM Server in a CONNECT message.</td>
</tr>
<tr>
<td>Failed SIP Transfers (Post-Dialog)</td>
<td>The number of failed re-invite requests on either the inbound or outbound legs of the call during the interval. After a SIP dialog is established, re-INVITE messages are used to perform transfers. Re-invite requests can originate from the endpoints or else be initiated by a Unified CVP transfer from the Unified ICME script. This counter includes failures for both kinds of re-invite requests.</td>
</tr>
<tr>
<td>Basic Service Video Calls Offered</td>
<td>The number of basic service video calls offered in the current interval.</td>
</tr>
<tr>
<td>Basic Service Video Calls Answered</td>
<td>The number of basic service video calls answered in the current interval.</td>
</tr>
<tr>
<td>Whisper Announce Answered</td>
<td>The number of calls for which whisper announcement was successful during the interval.</td>
</tr>
<tr>
<td>Whisper Announce Failed</td>
<td>The number of calls for which whisper announcement was failed during the interval.</td>
</tr>
<tr>
<td>Statistic</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Agent Greeting Answered</td>
<td>The number of calls for which agent greeting was successful during the interval.</td>
</tr>
<tr>
<td>Agent Greeting Failed</td>
<td>The number of calls for which agent greeting was failed during the interval.</td>
</tr>
<tr>
<td><strong>Aggregate Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Start Time</td>
<td>The time the service started collecting statistics.</td>
</tr>
<tr>
<td>Duration Elapsed</td>
<td>The amount of time that has elapsed since the service start time.</td>
</tr>
<tr>
<td>Total New Calls</td>
<td>The number of SIP Invite messages received by Unified CVP since system start time. It includes the failed calls as well as calls rejected due to the SIP service being out of service.</td>
</tr>
<tr>
<td>Connects Received</td>
<td>The number of CONNECT messages received by SIP service in order to perform a Unified CVP Transfer, since system start time. Connects Received includes the regular Unified CVP transfers as well as Refer transfers. Any label coming from the ICM service is considered a CONNECT message, whether it is a label to send to the VRU or a label to transfer to an agent.</td>
</tr>
<tr>
<td>Avg Latency Connect to Answer</td>
<td>The period of time between the CONNECT from ICM and when the call is answered. The metric includes the average latency computation for all the calls that have been answered since system start up time.</td>
</tr>
<tr>
<td>Failed SIP Transfers (Pre-Dialog)</td>
<td>The total number of failed transfers on the first CVP transfer since system start time. A SIP dialog is established after the first CVP transfer is completed. The metric does not include rejections due to SIP being out of service. The metric includes failed transfers that were made after a label was returned from the ICM in a CONNECT message.</td>
</tr>
<tr>
<td>Failed SIP Transfers (Post-Dialog)</td>
<td>The number of failed re-invite requests on either the inbound or outbound legs of the call since start time. After a SIP dialog is established, re-INVITE messages are used to perform transfers. Re-invite requests can originate from the endpoints or else be initiated by a Unified CVP transfer from the Unified ICME script. This counter includes failures for both kinds of re-invite requests.</td>
</tr>
<tr>
<td>Total Basic Service Video Calls Offered</td>
<td>The total number of basic service video calls offered since system start time.</td>
</tr>
<tr>
<td>Total Basic Service Video Calls Answered</td>
<td>The total number of basic service video calls answered since system start time.</td>
</tr>
<tr>
<td>Total Whisper Announce Answered</td>
<td>The total number of call for which whisper announce was successful since the system start time.</td>
</tr>
<tr>
<td>Statistic</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Total Whisper Announce Failed</td>
<td>The total number of calls for which whisper announce failed since the system start time.</td>
</tr>
<tr>
<td>Total Agent Greeting Answered</td>
<td>The total number of calls for which agent greeting was successful since the system start time.</td>
</tr>
<tr>
<td>Total Agent Greeting Failed</td>
<td>The total number of calls for which agent greeting failed since the system start time.</td>
</tr>
</tbody>
</table>

**View Gateway Statistics**

Gateway statistics include the number of active calls, available memory, and CPU utilization.

Access Gateway statistics either by:

**Procedure**

- Selecting **System > Control Center**, selecting a Gateway, and then clicking the **Statistics** icon in the toolbar.
- Selecting **Device Management > Gateway**, selecting a Gateway, and then clicking the **Statistics** icon in the toolbar.

**Gateway Statistics**

The following table describes Gateway statistics.

*Table 11: Gateway Statistics*

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Calls</td>
<td>Number of currently active calls handled by the gateway. For example, Total call-legs: 0 no active calls</td>
</tr>
<tr>
<td>Free Memory</td>
<td>Free memory, for example: Processor memory free: 82% I/O memory free: 79%</td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>CPU utilization, for example: CPU utilization for five seconds: 1%/0%; one minute: 1%; five minutes: 1%</td>
</tr>
</tbody>
</table>

**Unified CVP VXML Server Statistics**

The Operations Console displays realtime, interval, and aggregate Unified CVP VXML Server statistics.

- VXML Statistics are not available if the Unified CVP VXML Server is deployed as standalone.
To view VXML Statistics, at least one deployed Unified CVP VXML Server application must be configured with the CVPDataFeed logger.

Access Unified CVP VXML Server statistics either by:

- Selecting **System > Control Center**, selecting a VXML Server, and then clicking the **Statistics** icon in the toolbar.
- Selecting **Device Management > Unified CVP VXML Server**, and selecting a Unified CVP VXML Server. Click **Edit > Statistics**.

The following table describes the statistics reported by the Unified CVP VXML Server.

**Table 12: VXML Server Statistics**

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port Usage Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Total Ports</td>
<td>The total number of licensed ports for this Unified CVP VXML standalone server.</td>
</tr>
<tr>
<td>Port Usage Expiration Date</td>
<td>The date when the licensed ports expires for this Unified CVP VXML standalone server.</td>
</tr>
<tr>
<td>Available Ports</td>
<td>The number of port licenses available for this Unified CVP VXML standalone server.</td>
</tr>
<tr>
<td>Total Concurrent Callers</td>
<td>The number of callers currently interacting with this Unified CVP VXML standalone server. <strong>Note</strong> The Total Concurrent Callers statistics is not applicable for applications having only audio elements.</td>
</tr>
<tr>
<td><strong>Real Time Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Active Sessions</td>
<td>The number of current sessions being handled by the Unified CVP VXML Server.</td>
</tr>
<tr>
<td>Active ICM Lookup Requests</td>
<td>The number of current ICM requests being handled by the Unified CVP VXML Server.</td>
</tr>
<tr>
<td><strong>Interval Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Start Time</td>
<td>The time at which the current interval begins.</td>
</tr>
<tr>
<td>Duration Elapsed</td>
<td>The amount of time that has elapsed since the start time in the current interval.</td>
</tr>
<tr>
<td>Interval Duration</td>
<td>The interval at which statistics are collected. The default value is 30 minutes.</td>
</tr>
<tr>
<td>Sessions</td>
<td>The total number of sessions in the Unified CVP VXML Server in the current interval.</td>
</tr>
<tr>
<td>Statistic</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reporting Events</td>
<td>The number of events sent to the Unified CVP Reporting Server from the Unified CVP VXML Server in the current interval.</td>
</tr>
<tr>
<td>ICM Lookup Requests</td>
<td>The number of requests from the Unified CVP VXML Server to the ICM Service in the current interval.</td>
</tr>
<tr>
<td>ICM Lookup Responses</td>
<td>The number of responses to both failed and successful ICM Lookup Requests that the ICM Service has sent to the Unified CVP VXML Server in the current interval. In the case that multiple response messages are sent back to the Unified CVP VXML Server to a single request, this metric will increment per response message from the ICM Service.</td>
</tr>
<tr>
<td>ICM Lookup Successes</td>
<td>The number of successful requests from the Unified CVP VXML Server to the ICM Service in the current interval.</td>
</tr>
<tr>
<td>ICM Lookup Failures</td>
<td>The number of requests from the Unified CVP VXML Server to the ICM Service in the current interval. This metric will be incremented in the case an ICM failed message was received or in the case the Unified CVP VXML Server generates the failed message.</td>
</tr>
</tbody>
</table>

**Aggregate Statistics**

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>The time at which the current interval has begun.</td>
</tr>
<tr>
<td>Duration Elapsed</td>
<td>The amount of time that has elapsed since the start time in the current interval.</td>
</tr>
<tr>
<td>Total Sessions</td>
<td>The total number of sessions in the Unified CVP VXML Server since startup.</td>
</tr>
<tr>
<td>Total Reporting Events</td>
<td>The total number of reporting events sent from the Unified CVP VXML Server since startup.</td>
</tr>
<tr>
<td>Total ICM Lookup Requests</td>
<td>The total number of requests from the Unified CVP VXML Server to the ICM Service. For each ICM lookup request, whether the request succeeded or failed, this metric will be increased by one.</td>
</tr>
<tr>
<td>Total ICM Lookup Responses</td>
<td>The total number of responses the ICM Service has sent to the Unified CVP VXML Server since startup. For each ICM lookup response, whether the response is to a succeeded or failed request, this metric will be increased by one. In the case that multiple response messages are sent back to the Unified CVP VXML Server to a single request, this metric will increment per response message from the ICM Service.</td>
</tr>
<tr>
<td>Total ICM Lookup Successes</td>
<td>The total number of requests from the Unified CVP VXML Server to the ICM Service since startup. For each ICM lookup request that succeeded, this metric will be increased by one.</td>
</tr>
</tbody>
</table>
Standalone Unified CVP VXML Server Statistics

The Operations Console displays realtime, interval, and aggregate Unified CVP VXML (Standalone) Server statistics.

Access Unified CVP VXML (Standalone) Server statistics either by:

- Selecting **System > Control Center**, selecting a Unified CVP VXML (Standalone) sever, and then clicking the icon in the toolbar.
- Selecting **Device Management > Unified CVP VXML (Standalone) Server**, and selecting a Unified CVP VXML (Standalone) server. Click **Edit > Statistics**.

The following table describes the statistics reported by the Unified CVP VXML (Standalone) Server.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total ICM Lookup Failures</td>
<td>The total number of requests from the Unified CVP VXML Server to the ICM Service since startup. For each ICM lookup request that failed, this metric will be increased by one. This metric will be incremented if an ICM failed message was received or if theUnified CVP VXML Server generates a failed message.</td>
</tr>
</tbody>
</table>

### Port Usage Statistics

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Ports</td>
<td>The total number of licensed ports for this Unified CVP VXML standalone server.</td>
</tr>
<tr>
<td>Port Usage Expiration Date</td>
<td>The date when the licensed ports expires for this Unified CVP VXML standalone server.</td>
</tr>
<tr>
<td>Available Ports</td>
<td>The number of port licenses available for this Unified CVP VXML standalone server.</td>
</tr>
<tr>
<td>Total Concurrent Callers</td>
<td>The number of callers currently interacting with this VXML standalone server.</td>
</tr>
</tbody>
</table>

**Note**: The Total Concurrent Callers statistics is not applicable for applications having only audio elements.

### View Pool Statistics

Device Pool statistics summarize the statistics for the devices that belong to the currently selected device pool.

**Procedure**

To view device pool statistics:
**Unified CVP Reporting Server Statistics**

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

Access Reporting Server statistics either by:

- Choosing **System** > **Control Center**, selecting a Unified CVP Reporting Server, and then clicking the **Statistics** icon in the toolbar.
- Choosing **Device Management** > **Unified CVP Reporting Server**, and selecting a Unified CVP Reporting Server. Click **Edit** > **Statistics**.

The following table describes the Unified CVP Reporting Server statistics.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interval Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Start Time</td>
<td>The time the system started collecting statistics for the current interval.</td>
</tr>
<tr>
<td>Duration Elapsed</td>
<td>The amount of time that has elapsed since the start time in the current interval.</td>
</tr>
<tr>
<td>Interval Duration</td>
<td>The interval at which statistics are collected. The default value is 30 minutes.</td>
</tr>
<tr>
<td>VXML Events Received</td>
<td>The total number of reporting events received from the VXML Service during this interval. For each reporting event received from the VXML Service, this metric will be increased by one.</td>
</tr>
<tr>
<td>SIP Events Received</td>
<td>The total number of reporting events received from the SIP Service during this interval. For each reporting event received from the SIP Service, this metric will be increased by one.</td>
</tr>
<tr>
<td>IVR Events Received</td>
<td>The total number of reporting events received from the IVR service in the interval. For each reporting event received from the IVR service, this metric will be increased by one.</td>
</tr>
</tbody>
</table>
**Aggregate Statistics**

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>The time the service started collecting statistics.</td>
</tr>
<tr>
<td>Duration Elapsed</td>
<td>The amount of time that has elapsed since the service start time.</td>
</tr>
<tr>
<td>VXML Events Received</td>
<td>The total number of reporting events received from the VXML Service since the service started. For each reporting event received from the VXML Service, this metric will be increased by one.</td>
</tr>
<tr>
<td>SIP Events Received</td>
<td>The total number of reporting events received from the SIP Service since the service started. For each reporting event received from the SIP Service, this metric will be increased by one.</td>
</tr>
<tr>
<td>IVR Events Received</td>
<td>The total number of reporting events received from the IVR Service since the service started. For each reporting event received from the IVR Service, this metric will be increased by one.</td>
</tr>
<tr>
<td>Database Writes</td>
<td>The total number of writes to the database made by the Unified CVP Reporting Server since startup. For each write to the database by the Unified CVP Reporting Server, this metric will be increased by one.</td>
</tr>
</tbody>
</table>

**Pool Statistics Tab**

Device pool statistics report data on the devices contained within a device pool as described in the following table.

*Table 15: Pool Statistics*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of Servers in Different States</strong></td>
<td></td>
</tr>
<tr>
<td>Server Type</td>
<td>Unified CVP servers include: Call Servers, Unified CVP VXML Servers, Unified CVP VXML Servers (standalone), and Reporting Servers.</td>
</tr>
<tr>
<td>Total Devices</td>
<td>Total number of devices for each server type.</td>
</tr>
<tr>
<td>Up</td>
<td>Number of servers of each type that are up and running.</td>
</tr>
<tr>
<td>Down</td>
<td>Number of servers of each type that have down status.</td>
</tr>
<tr>
<td>Partial</td>
<td>Number of servers of each type that have partial status.</td>
</tr>
<tr>
<td>Not Reachable</td>
<td>Number of servers of each type that have a Not Reachable status.</td>
</tr>
</tbody>
</table>
### Percentage of Servers in Different States

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Type</strong></td>
<td>Unified CVP servers include: Call Servers, Unified CVP VXML Servers, Unified CVP VXML Servers (standalone), and Reporting Servers.</td>
</tr>
<tr>
<td><strong>Total Devices</strong></td>
<td>Total number of devices for each server type.</td>
</tr>
<tr>
<td><strong>Up</strong></td>
<td>Percentage of servers of each type that are up and running.</td>
</tr>
<tr>
<td><strong>Down</strong></td>
<td>Percentage of servers of each type that have down status.</td>
</tr>
<tr>
<td><strong>Partial</strong></td>
<td>Percentage of servers of each type that have partial status.</td>
</tr>
<tr>
<td><strong>Not Reachable</strong></td>
<td>Percentage of servers of each type that have an Unreachable status.</td>
</tr>
</tbody>
</table>

### Related Topics

- [View Pool Statistics](#), on page 36

### Sort Servers

You can choose to sort the servers in ascending and descending sort sequences: by their network status (up, down, partial, unreachable), hostname, IP address, device type, and by the number of active calls.

#### Procedure

To sort servers:

1. Select System > Control Center.
2. Select Device Pool and then select a device pool from the list.
   
   Devices that belong to the selected device pool display on the General tab.
3. To sort the list of servers, click the heading for the column you want to sort by. After you sort the column, up/down arrows appear in the column headings. Click the arrows to specify the sort order for the column.

### Edit Device Setup

You can edit the configuration of a device that has been added to the Operations Console.

#### Procedure

To edit the configuration of a device:

1. Select System > Control Center.
   
   The Control Center Network Map window opens to the General tab.
Step 2
Click on the device hostname or select the radio button preceding the hostname and then click **Edit** on the toolbar.

The Edit Configuration window for the selected device opens.

**Related Topics**
- Device Properties, on page 103
- Find Device, on page 105
- Past Device Setups in Operations Console Database, on page 211

### Start Server
You can start a Unified CVP Call Server, Unified CVP Reporting Server, or Unified CVP VXML Server from the Control Center.

**Related Topics**
- View Device Status, on page 16
- View Devices by Type, on page 15
- Shut Down Server, on page 40

### Procedure
To start a server:

**Step 1**
Select **System > Control Center**.
The Control Center window opens to the General tab.

**Step 2**
Select the Unified CVP Call Server, Unified CVP Reporting Server, or Unified CVP VXML Server to restart by clicking the radio button next to the server.

**Step 3**
Select **Start**.
The server starts; its state displays in the Status column on the General tab.

**Note**
By default, the device status is not refreshed. To set a refresh interval, select the desired interval from the Refresh drop-down menu.

### Shut Down Server
You can shut down a Unified CVP Call Server, Unified CVP Reporting Server, or Unified CVP VXML Server from the Control Center. A server instance enters the shutdown state as a result of a graceful shutdown or forced shutdown process.

During a graceful shutdown, running processes complete before the server is shut down. For example, if you want to stop the Unified CVP Call Server but want to complete the processing of calls in progress, you must choose Graceful Shutdown.

In a forceful shutdown, all processes are suspended immediately. If you were to shut down the Unified CVP Call Server forcefully, calls in progress will be immediately dropped.
**Procedure**

To shut down a server:

---

**Step 1** Select **System > Control Center**.

The Control Center window opens to the General tab.

**Step 2** Select the Unified CVP Call Server, Unified CVP Reporting Server, or Unified CVP VXML Server to shut down by clicking the radio button next to the server.

**Step 3** To shut down a server immediately, select **Shutdown**. To shut down a server gracefully, select **Graceful Shutdown**.

---

The selected server shuts down, and its status shows as Down in the Devices tab in the right pane of the Control Center window.

---

**Note**

Graceful Shutdown is not supported by Unified CVP VXML Server.

---

**Device Pools**

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

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

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

You can perform the following tasks using device pools:

- Adding a Device Pool
- Editing a Device Pool
- Deleting a Device Pool
- Adding or Removing a Device from a Device Pool
- Finding a Device Pool
Add Device Pool to Operations Console

This section describes how to add a device pool to the Operations Console.

Procedure

To add a device pool to the Operations Console:

1. **Step 1** Select System > Device Pool.
   The Find, Add, Edit, Delete Device Pools window opens.

2. **Step 2** Select Add New.

3. **Step 3** In the General tab, fill in a unique name for the device pool and add a description.
   - **Note** Device pool names must be valid DNS names, which can include letters in the alphabet, the numbers 0 through 9, and a dash.

4. **Step 4** Select Save to save the device pool.

**Related Topics**
- Device Pools, on page 41
- Delete Device Pool, on page 43
- Edit Device Pool, on page 42
- Add or Remove Device From Device Pool, on page 43
- Find Device Pool, on page 44

Edit Device Pool

You can change the name and description of any device pool, except the default device pool.

Procedure

To edit a device pool:

1. **Step 1** Select System > Device Pool.
   The Find, Add, Delete, Edit Device Pools window opens.

2. **Step 2** Select the device pool by clicking on its name in the device pool list or selecting the radio button preceding it and clicking Edit.
   The Edit Device Pool Configuration window opens to the General tab.

3. **Step 3** You can change the description. You cannot change the name of a device pool.

4. **Step 4** Select Save.

**Related Topics**
- Device Pools, on page 41
Delete Device Pool

This section describes how to delete a device pool from the Operations Console.

Procedure

To delete a device pool:

**Step 1** Select System > Device Pool.

The Find, Add, Edit, Delete Device Pools window opens.

**Step 2** Find the device pool by using the procedure in the Finding a Device Pool topic.

**Step 3** From the list of matching records, select the device pool that you want to delete.

**Step 4** Select Delete.

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

Add or Remove Device From Device Pool

This section describes how to delete a device pool from the device pool.

Procedure

To add or remove a device from a device pool:

**Step 1** From the Device Management menu, select the type of device you want to add to a device pool. For example, to add a Call Server to a device pool, select Unified CVP Call Server from the menu.

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

**Step 2** Select the device pool by clicking on its name in the device pool list or by selecting the radio button preceding it and clicking Edit.

**Step 3** Select the Device Pool tab.
Step 4 To add a device to a device pool, select the device pool from the Available pane, and then click the right arrow to move the pool to the Selected pane.

Step 5 To remove a device from a device pool, select the device pool from the Selected pane, and then click the left arrow to move the device pool to the Available pane.

Step 6 Click Save to save the changes to the Operations Console database. Some edit device screens have an Apply button. Click Apply to copy the configuration to the device.

---

**Find Device Pool**

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

**Procedure**

To find a device pool:

**Step 1** Select System > Device Pool.

The Find, Add, Delete, Edit Device Pools window lists the available device pools 10 at a time, sorted by name.

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

**Step 3** You can also filter the list by selecting an attribute such as Name; selecting a modifier such as begins with; entering your search term; and clicking Find.

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

---

**Import System Configuration**

In the event of disaster recovery, you can import a system configuration and apply a previously saved configuration.

The Unified CVP Operations Console supports the import of system-level configuration data.

When you import a database which was exported from an older version, the imported database is automatically upgraded to the latest version as indicated in the confirmation message.

**Note** The Unified CVP import operation does not back up or restore the CVP configuration of the VoiceBrowser or the sip.properties files. If a complete restore of Unified CVP server is required, you will need to manually restore some of the content of the sip.properties file as well as the VoiceBrowser configuration in addition to importing the system configuration using the Operations Console.
**Procedure**

To import a system configuration:

---

**Step 1** Stop the Cisco CVP WebServicesManager Service:

a) Select **Start > All Programs > Administrative Tools > Services.**
b) Select **Cisco CVP WebServicesManager.**
c) Select **Stop.**

**Step 2** Select **System > Import System Configuration.**

The Import System Configuration window opens.

**Step 3** If you know the file name, enter it in the Enter Configuration File text box. Otherwise, select **Browse to** and search for the configuration to import.

**Step 4** Select **Import.**

**Step 5** Restart the Cisco CVP OPSConsoleServer and Cisco CVP WebServicesManager Services on the machine and then log in to the Operations Console again:

a) Select **Start > All Programs > Administrative Tools > Services.**
b) Select **Cisco CVP OPSConsoleServer.**
c) Select **Restart.**
d) Select **Cisco CVP WebServicesManager.**
e) Select **Restart**

---

**Note**

All data in the Operations Console that is importing the configuration will be lost and replaced with the imported data.

**Related Topics**

[Export System Configuration](#), on page 45

---

**Export System Configuration**

Using Export System Configuration on the System menu, you can save and export all the configurations of the Operations Console to a single file on your local computer. This is particularly useful in a back up scenario. For example, if the Operations Console configuration file were to become corrupt, you can import the file and restore the Operations Console configuration without having to individually reconfigure each module. Consider exporting the database on a regular basis and also when you make major configuration changes to a device.

All Operations Console configuration data is exported, except for any files you have uploaded, including licenses and application scripts. The Operations Console supports the export of system-level configuration data.
The Unified CVP import and export operations do not back up or restore the CVP configuration of VoiceBrowser, sip.properties files, and Context Service data connection. If you must do a complete backup and record of the Unified CVP configuration, then you must manually back up the sip.properties file and the result of the VoiceBrowser `sall` command in addition to exporting the system configuration using the Operations Console.

**Procedure**

To export a system configuration:

1. Select `System > Export System Configuration`. The Export System Configuration window displays.
2. Select `Export`.
3. In the `Save As` dialog box, select the location to store the file.

**Note** You will probably save the configuration multiple times. Choose a naming convention that helps you identify the configuration, for example, include the current date and time in the file name.

**Related Topics**

*Import System Configuration*, on page 44

**Location Feature**

Use the Location feature to route calls locally to the agent available in the branch office, rather than routing calls to centralized or non-geographical numbers. This system-level feature allows you to select a Unified CM server and extract the Unified CM location information (location provider). Once the administrator initiates the synchronization, the system retrieves the location information for all available Unified CM servers which have been identified as sources for location information.

After you have enabled synchronization for a Unified CM server, information can be retrieved from any of the Unified CM servers that have been identified as sources for location information.

**Prerequisites:**

- Ensure that the device type (Gateway / Virtualized Voice Browser) is already configured.
- The device Location ID information, if configured in the Location configuration page, is displayed as a read-only field.
- Any configurable fields remain empty if they were not configured by the user.
If a location is associated with more than one Gateway / Virtualized Voice Browser, the system displays multiple rows of the same location information for each associated device.

All Unified CM servers enabled for synchronization are used during the synchronization task. If you do not want a particular Unified CM to be used when the synchronization task is performed, then disable synchronization for that Unified CM.

The following table describes the settings used to configure the Location feature.

### Table 16: Location Configuration Settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insertsiteidentifier</td>
<td>Three options are available to identify the site information:</td>
<td>Insert site</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>identifier</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>Locations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location Name (required)</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></td>
<td>Max length 128 characters</td>
<td></td>
<td></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>Max length 128 characters</td>
<td></td>
<td></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>Max length 128 characters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Property</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>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, or 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>
<tr>
<td>Associated Gateway</td>
<td>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.</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>No</td>
</tr>
<tr>
<td>Associated Virtualized Voice Browser</td>
<td>You can select Virtualized Voice Browsers from the available list to deploy location information. You can configure multiple Virtualized Voice Browsers per location. An instance of a Voice Browser can only be assigned to one location. When a Virtualized Voice Browser is associated with a location, the Virtualized Voice Browser configuration window displays the location as a read-only field.</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>No</td>
</tr>
</tbody>
</table>
### Status

The status indicates that the validity of 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.

### Call Server Deployment

You can select call servers from the Available list to deploy location information. One or more call servers can be selected and designated as Selected/Available.

| Configuration is deployed to all selected call servers | Not applicable | No |

You can perform the following tasks:

- **View Location Information**
- **Insert Site Identifiers**
View Location Information

Procedure

To view location-based information:

Step 1 Select System > Location.

Location information is listed on the Location tab. The Location tab displays the retrieved location information where you can edit and configure additional information.

If a location is associated with more than one Gateway / Virtualized Voice Browser, the same location information is presented in multiple rows. Only the associated device column differs.

Step 2 Click the required device to launch the device configuration window.

Related Topics
- Location Feature, on page 46
- Insert Site Identifiers, on page 50
- Deploy Location Information, on page 51
- Add Locations, on page 53
- Edit Location Information, on page 53
- Delete Location, on page 54
- Synchronize Location Information, on page 55
- View Location Deployment or Synchronization Status, on page 56
- Find Location, on page 57

Insert Site Identifiers

The Site Identifier insert applies to all selected call servers using the Location configuration.

Related Topics
- Location Feature, on page 46
- View Location Information, on page 50
- Deploy Location Information, on page 51
- Add Locations, on page 53
Procedure

To insert site identifiers:

Select System > Location.

Site identifier information is listed on the General tab.

Three options are available to identify the site information:

- Insert site identifier between the Network VRU label and the correlation ID
- Insert site identifier at the beginning of the Network VRU label
- Do not insert site identifier

Deploy Location Information

By default, location information is deployed to all associated Call Servers. You can choose to deploy location information to one or more Call Servers.

Related Topics

- Location Feature, on page 46
- View Location Information, on page 50
- Insert Site Identifiers, on page 50
- Add Locations, on page 53
- Edit Location Information, on page 53
- Delete Location, on page 54
- Synchronize Location Information, on page 55
- View Location Deployment or Synchronization Status, on page 56
- Find Location, on page 57

Procedure

To deploy location information:

Step 1 Selects System > Location.

Step 2 After making the required configuration changes, you have two options to save the configuration:

- Selects Save & Deploy in the bottom right corner of this page (or the Save & Deploy button in the toolbar above) to save the location information and initiate a deployment request to the selected Call Servers.
See View Location Deployment or Synchronization Status, on page 56 for details on viewing the status information.

- Selects **Save** to save three components to the database: the location information, information in the General tab, and the associated Call Servers.

**Caution** In the following cases, the Deployment Status displays a warning message:

- If you have only saved the configuration details and have not deployed them.
- If you have edited or deleted an existing configuration and have not deployed the changes.
- If you changed the call server association.

### Error Scenario Deployment

The following table provides the status, and workaround for the deployment error scenarios.

<table>
<thead>
<tr>
<th>Status</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unable to access the database.</td>
<td>Restart the Operations Console service.</td>
</tr>
<tr>
<td></td>
<td>Try again.</td>
</tr>
<tr>
<td></td>
<td>Contact your administrator.</td>
</tr>
<tr>
<td>General failure.</td>
<td>There is an unknown error in deployment.</td>
</tr>
<tr>
<td></td>
<td>Contact your administrator.</td>
</tr>
<tr>
<td>The device was not deployed.</td>
<td>Deploy the device first.</td>
</tr>
<tr>
<td></td>
<td>Try again.</td>
</tr>
<tr>
<td>The device was not deployed.</td>
<td>Cannot remove from the database.</td>
</tr>
<tr>
<td>The device could not be reached.</td>
<td>Check the network connection by pinging the device.</td>
</tr>
<tr>
<td></td>
<td>Check the firewall setting.</td>
</tr>
<tr>
<td></td>
<td>Turn off the firewall if the firewall is on.</td>
</tr>
<tr>
<td></td>
<td>If it is available, check if WebServicesManager service is on.</td>
</tr>
<tr>
<td></td>
<td>Try again later.</td>
</tr>
<tr>
<td>The device is using an unknown version of the Unified CVP software.</td>
<td>Upgrade to the compatible version, then deploy again.</td>
</tr>
<tr>
<td>The device is using an unknown version of the Unified CVP software.</td>
<td>Cannot remove.</td>
</tr>
</tbody>
</table>
## Add Locations

You can manually add location information for locations that do not exist in the Unified CM database.

### Related Topics
- Location Feature, on page 46
- View Location Information, on page 50
- Insert Site Identifiers, on page 50
- Deploy Location Information, on page 51
- Edit Location Information, on page 53
- Delete Location, on page 54
- Synchronize Location Information, on page 55
- View Location Deployment or Synchronization Status, on page 56
- Find Location, on page 57

### Procedure

To add locations:

1. **Step 1** Select System > Location.
2. **Step 2** On the Location tab, select Add New.
   
   The Location Configuration window opens.
3. **Step 3** Assign the Location, Site ID, Location ID, and the Unified CM IP Address as applicable to your configuration.
4. **Step 4** Optionally, select the required Gateway / Voice Browser by moving it/them to the Selected column.
5. **Step 5** Select Save or Cancel.

### Edit Location Information

You can only select a single location for this operation.

### Related Topics
- Location Feature, on page 46
- View Location Information, on page 50
- Insert Site Identifiers, on page 50
- Deploy Location Information, on page 51
- Add Locations, on page 53
- Delete Location, on page 54

### Workaround

If OAMP has deployed SIP Server Group to the call server, delete the call server, and re-create the call server with a SIP Subsystem; or, do not select Call Servers with No SIP when deploying SIP Server Group configuration.
Procedure

To edit the required location:

Step 1 Select System > Location.
Step 2 On the Location tab, select the required location in one of two ways:
  • Select the check box for the required location and click Edit.
  • Select the required location in the Location tab.
Step 3 Make the required changes and click Save or Cancel as applicable.

Delete Location

You can delete one or more locations at the same time.

Only manually-configured and invalid locations can be deleted.

Related Topics
  Location Feature, on page 46
  View Location Information, on page 50
  Insert Site Identifiers, on page 50
  Deploy Location Information, on page 51
  Add Locations, on page 53
  Edit Location Information, on page 53
  Synchronize Location Information, on page 55
  View Location Deployment or Synchronization Status, on page 56
  Find Location, on page 57

Procedure

To delete a location:

Step 1 Select System > Location.
Step 2 Select the required locations.
Step 3 On the Location tab, select Delete.
  A prompt window appears to confirm your intention.
Step 4 Respond to the prompt (Proceed with Delete? OK | Cancel).
  This prompt may differ if you select a location which cannot be deleted.
When you make your selection, the Location tab refreshes to display the results of your deletion in the message bar.

---

**Synchronize Location Information**

Location synchronization is a user-initiated task in the Operations Console. A single synchronization task runs in the background when initiated. When initiated, the system synchronizes and merges the location information for all Unified CM servers selected during the configuration. There are two sub-tasks to complete a synchronizing operation:

**Procedure**

- Synchronization: The system retrieves the location data from Unified CM database.
- Merge: The system merges the retrieved data with existing location data in the Operations Console database.

**What to do next**

The Location synchronization feature in the Operations Console only works with Unified CM.

**Related Topics**

- [Location Feature](#), on page 46
- [View Location Information](#), on page 50
- [Insert Site Identifiers](#), on page 50
- [Deploy Location Information](#), on page 51
- [Add Locations](#), on page 53
- [Edit Location Information](#), on page 53
- [Delete Location](#), on page 54
- [View Location Deployment or Synchronization Status](#), on page 56
- [Find Location](#), on page 57

**Procedure**

To synchronize and refresh the location information with the Unified CM server and merge the information with the Operations Console database:

1. **Step 1**
   Configure and save one or more Unified CM devices with synchronization enabled.

2. **Step 2**
   Select System > Location.

3. **Step 3**
   Select Synchronize.

   The synchronization process is initiated.

**Note**

Only one synchronization or deployment process can run at any given time. If one process is already running, you receive an error message stating the same.
Step 4  
Click **Refresh** to view the retrieved location information after the synchronization process is completed.

---

### Synchronize Error Scenarios

The following table provides the status, cause, and workaround for the synchronization error scenarios.

<table>
<thead>
<tr>
<th>Status</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not able to connect with the device.</td>
<td>Check the network connection by pinging the device.</td>
</tr>
<tr>
<td></td>
<td>If the device is connected, try again.</td>
</tr>
<tr>
<td>User credentials are not correct. User can't be authenticated.</td>
<td>Check the user credentials.</td>
</tr>
<tr>
<td>Host name is unknown. Check the host name.</td>
<td>The host name is not correct.</td>
</tr>
<tr>
<td></td>
<td>Verify the host name.</td>
</tr>
<tr>
<td>Web Service is not available on the device.</td>
<td>Determine if the AXL Web Service is available on the device.</td>
</tr>
<tr>
<td></td>
<td>Enable the AXL Web Service on the device.</td>
</tr>
<tr>
<td>General database failure.</td>
<td>Restart your Operations Console service.</td>
</tr>
<tr>
<td></td>
<td>Try again.</td>
</tr>
<tr>
<td></td>
<td>If the problem persists, contact your administrator.</td>
</tr>
<tr>
<td>General failure.</td>
<td>There is an unknown error in synchronization.</td>
</tr>
<tr>
<td></td>
<td>Contact your administrator.</td>
</tr>
</tbody>
</table>

---

### View Location Deployment or Synchronization Status

Deployment and Synchronization operations can be time consuming depending on the number of Call Servers or Unified CMs. When either process is running, you can select a status report to view the progress of the last initialized deployment or synchronization request.

---

**Note**

The Deployment and Synchronization operations are mutually exclusive. Only one synchronization or deployment process can run at any given time. If one process is already running, you cannot initiate another process and you receive an error message.

The following information applies to the Status window:

**Procedure**

- Unapplied changes (deployment status only) indicate that a Save operation took place since the last deployment operation.
- Only one call server can be deployed at any given time. The other call servers are either in the queue or in an already successful/failed state.
Procedure

To show deployment or synchronization results:

Step 1 Select **System > Location**.

Step 2 From the toolbar, select **Status**.

  - To view synchronization results, select **Synchronization Status**.
  - To view deployment results, select **Deployment Status**.

Step 3 Select **Refresh** to view the updated status information.

See **View System-Level Operation States, on page 12** for more details on each state.

Find Location

Procedure

To show deployment and/or synchronization results:

Step 1 Select **System > Location**.

Step 2 To scroll through multiple pages of the list, select the first, previous, next, and last page icons on the bottom left to view the next group of available notification destinations.

Step 3 You can filter the list by using the filter at the top right of the list. Select a field to search, a modifier (such as **Starts with**), and then select **Find**. The filter is not case-sensitive and wildcards are not allowed.

SIP Server Groups

In Unified CVP, you can add server groups at the system level to perform SIP dynamic routing.
A Server Group consists of one or more destination addresses (endpoints) and is identified by a Server Group domain name. This domain name is also known as the SRV cluster name, or Fully Qualified Domain Name (FQDN). Server Groups contain Server Group Elements.

**View SIP Server Groups**

**SIP Server Groups**
- General tab
- Heartbeat Properties tab
- Call Server Deployment tab

**General tab**
The General tab displays the list of SIP Server Groups and SIP Server Group Elements

<table>
<thead>
<tr>
<th><strong>Table 17: General Tab</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Column</strong></td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Number of Elements</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>Secure Port</td>
</tr>
<tr>
<td>Priority</td>
</tr>
<tr>
<td>Weight</td>
</tr>
</tbody>
</table>

**Note**
Clicking any of the column headers on this list sorts the list.

**Heartbeat Properties tab**
The Up and Down Endpoint Heartbeat Interval is between any two heartbeats; however, it is not between heartbeats to the same endpoint. The SIP Server Group does not wake up at specific interval and send a heartbeat for all elements since this approach can result in CPU utilization issues. It also takes more resources to track heartbeats for many endpoints. For example, for 3 total elements across all SIP Server Groups, to proactively send a heartbeat to each element at 30000ms (30 seconds) intervals, you have to set the Endpoint Heartbeat Interval to 10000ms (10 seconds). It is less deterministic for reactive mode since elements that are currently down can fluctuate so the heartbeat interval fluctuates with it. To turn off pinging when the element is UP, set the UP interval to zero (reactive pinging). To turn off pinging when the element is down, set the DOWN interval to zero (proactive pinging). To ping when the element is either UP or DOWN, set both the intervals to greater than zero (adaptive pinging).

### Table 18: Heartbeat Properties Tab

<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. Note Endpoints that are not in a Server Group can not use the heartbeat mechanism.</td>
<td>Disabled (unchecked)</td>
<td>Enabled or Disabled</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>3</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>800 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>Property</td>
<td>Description</td>
<td>Default</td>
<td>Value</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>---------</td>
<td>-------</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. <strong>Note</strong> PING is an alternate method; however, some SIP endpoints do not recognize PING and will not respond at all.</td>
<td>OPTIONS</td>
<td>OPTIONS or PING</td>
</tr>
</tbody>
</table>
Heartbeat Transport Type

During transportation, Server Group heartbeats are performed with a UDP or TCP socket connection. If the Operations Console encounters unreachable or overloaded callbacks invoked in the Server Group, that element is marked as being down for both UDP and TCP transports. When the element is up again, it is routable for both UDP and TCP.

**Note**

TLS transport is not supported.

<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.</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/or commas (,)</td>
</tr>
</tbody>
</table>
### Add SIP Server Group

**Procedure**

To add a SIP Server Group:

**Step 1**  
In the Operations Console, select **System > SIP Server Groups**.  
The SIP Server Groups window opens.

**Step 2**  
Select **Add New**.

**Step 3**  
Fill in the appropriate configuration settings:
Table 19: SIP Server Group Configuration Settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Server Group Configuration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Domain Name FQDN</td>
<td>The Server Group Fully Qualified Domain Name (FQDN).</td>
<td>None</td>
<td>Up to 128 characters Must be unique. Must be a Fully Qualified Domain Name.</td>
</tr>
<tr>
<td>SIP Server Group Elements</td>
<td>Enter the properties below and click Add to add the element to the SIP Server Group. Highlight any of the configured SIP Server Group Elements in the box below the property fields and; • To remove the element from the group, highlight the element and click Remove • To replace a selected element with the new element, edit the SIP Server Group Elements properties, highlight an existing element in the text box, and then click Replace.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address/Hostname</td>
<td>IP address or hostname of the Server Group Element.</td>
<td>None</td>
<td>Valid IP address or hostname</td>
</tr>
<tr>
<td>Port</td>
<td>Port number of the element.</td>
<td>5060</td>
<td>1 through 65535</td>
</tr>
<tr>
<td>Secure Port</td>
<td>The listening port for secure connection.</td>
<td>None</td>
<td>5061</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>
<td>10</td>
<td>1 through 2147483647</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>
<td>10</td>
<td>10 through 2147483647</td>
</tr>
</tbody>
</table>

Step 4

Select Save to save the SIP Server Group.

You are returned to the SIP Server Groups page. To deploy the SIP Server Groups, you must associate a Unified CVP Call Server. Select the Call Server Deployment tab, select a Unified CVP Call Server and then click Save & Deploy. See Deploy SIP Server Group Configurations, on page 66.

Related Topics

View SIP Server Groups
Delete SIP Server Group

If you only want to delete elements within the group, see Edit SIP Server Group, on page 64.

To delete a SIP Server Group:

**Step 1**
Select System > SIP Server Groups.
The SIP Server Group page opens.

**Step 2**
Find the SIP Server Group by using the procedure in Find SIP Server Groups, on page 65.

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

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

Edit SIP Server Group

To configure a SIP Server Group, you must first define a FQDN and add it to the list.

**Procedure**

To edit a SIP Server Group:

**Step 1**
In the Operations Console, select System > SIP Server Groups.
The SIP Server Groups Configuration window opens.

**Step 2**
On the Server Groups Configuration tab, define a FQDN for the server and select Add to add it to the list box.

**Step 3**
Fill in the appropriate configuration settings, as shown in the following table:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Server Group Configuration</td>
<td>The Server Group Fully Qualified Domain Name (FQDN). Note This field is not editable</td>
<td>None</td>
<td>Up to 128 characters</td>
</tr>
<tr>
<td>Server Domain Name FQDN</td>
<td></td>
<td>None</td>
<td>Must be unique.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Must be a Fully Qualified Domain Name.</td>
</tr>
</tbody>
</table>
### Find SIP Server Groups

To find a SIP Server Group:

**Step 1**
Select **System > SIP Server Groups**.

The SIP Server Groups Configuration window displays.

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

**Step 3**
You can also filter the list by selecting an attribute such as **SIP Server Group Name** then selecting a modifier, such as **begins with**, and entering your search term then clicking **Find**.
Deploy SIP Server Group Configurations

The Operations Console displays all configured SIP Server Groups. This section identifies the procedure to deploy a SIP Server Group.

Procedure

To deploy SIP Server Group configurations:

Step 1  In the Operations Console, select **System > SIP Server Groups**. The SIP Server Groups Configuration window opens.

Step 2  Click the **Call Server Deployment** tab.

Step 3  From the **Available** list box, select one or more Call Servers and use the arrow button to move your selection to the **Selected** list box.

Step 4  After making the required configuration changes, you have two options to save the configuration:

- Click **Save & Deploy** in the bottom right corner of this page (or the **Save & Deploy** button in the toolbar above) to save the SIP server information and initiate a deployment request to the selected devices.
  
  See **View SIP Server Groups Deployment Status, on page 67** for details on viewing the status information.

- Click **Save** to save the configuration to the Operations Console database.

Note  In the following cases, the Deployment Status displays a warning message:

- If you have only saved the SIP server details and have not deployed them.

- If you have edited or deleted an existing configuration and have not deployed the changes.

- If you changed the call server association.

- Only one deployment process can run at any given time. If one process is already running, you will not be able to initiate another process and you receive an error message stating the same.

A message displays to indicate the successful start of deployment process. The Operations Console saves the Call Server configuration to the Operations Console database and returns to display the new configuration in the list page.

- While deploying SIP Server Groups only the selected servers will be deployed. Any previous Call Servers deployed will be removed.

See **View System-Level Operation States, on page 12** for more details on each state.
View SIP Server Groups Deployment Status

The Operations Console displays all configured SIP Server Groups. If a deployment fails because the call server is not accessible (either not deployed or off line) or is not upgraded to the current version, the Operations Console issues a descriptive message.

Deployment operations can be time consuming, depending on the number of Call Servers. When either process is running, you can select a status report to view the progress of the last initialized deployment request.

---

**Note**

The Deployment operations are mutually exclusive. Only one deployment process can run at any given time. If one process is already running, you will not be able to initiate another process and you will receive an error message stating the same.

The following information applies to the Status window:

**Procedure**

To view Call Server deployment status:

**Step 1**

In the Operations Console, select **System > SIP Server Groups**.

The SIP Server Groups Configuration window opens.

**Step 2**

From the toolbar, click **Deployment Status**.

**Step 3**

Optionally, instead of Step 2, you can also click **Deployment Status** at the bottom right corner of the window.

The Operations Console provides status information for SIP Server Group (including the Operation Console's server time stamp). In case of a failure, the Operations Console provides a reason for the failure. See [View System-Level Operation States, on page 12](#) for more details on each state.

---

**Behavior**

*Table 21: When will CVP add SIP Element to UnreachableDestinationTable*

<table>
<thead>
<tr>
<th>Scenario</th>
<th>UDP</th>
<th>TCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>After exhausting retry count for outgoing SIP Invite message (No response to outgoing SIP invite)</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Table 22: When will CVP remove SIP Element from UnreachableDestinationTable

<table>
<thead>
<tr>
<th>Scenario</th>
<th>UDP</th>
<th>TCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>In cases of SIP error response to outbound SIP Invite - 503, 480, 600</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>In Proactive Options Ping Mode - no response to SIP Options ping</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TCP/UDP socket establishment mode</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Dialed Number Pattern

You can perform the following tasks on Dialed Number Patterns:

- **Add Dialed Number Pattern**
- **Delete Dialed Number Pattern**
- **Edit Dialed Number Pattern**
- **Collapse All** - Collapse all hierarchical table entries to display root entries only.
- **Expand All** - Expand all hierarchical table entries to display all entries.
- **Pagination** - The bottom of the list display contains pagination fields to go to a specific page, go to the first page, go to the previous page, go to the next page, and go to the last page in the table list.
- **View Dialed Number Pattern Deployment Status** The Call Server(s) do not require a restart for the changes to take affect after clicking the **Deploy** button.
- **View Dialed Number Pattern Deployment Status** Display the deployment status for the previous deployment to configured Call Servers.

You can select the **Display Pattern Type** to display all configured Dialed Number Patterns in a tree-hierarchy view. Available selections are:

- **Display All** (default)
- **Local Static Route**
- **Send Calls to Originator**
- **RNA Timeout for Outbound Calls**
- **Custom Ringtone**
• Post Call Survey for Incoming Calls

Once the view is selected, a table containing the Dialed Number Patterns for the respective, selected type displays. The current view for the dialed number system-level configuration list page is maintained until the user session expires, either by timeout or by signing out from the Operations Console, or until the dialed number pattern view type selection changes.

Each dialed number pattern is displayed as a row. Each dialed number pattern column type can be sorted alphabetically in ascending or descending order. The Dialed Number list is in hierarchical format which lets you collapse or expand individual entries. One or more root hierarchical rows can be selected using the check-boxes. All table entries are expanded by default or after certain operations like sorting, filtering, or pagination.

The column types are as follows:

**Dialed Number Pattern** - The actual dialed number pattern.

**Description** - The dialed number pattern description.

You may also use the filtering function to filter for specific Dialed Number Patterns. Only the Dialed Number Pattern itself is filterable by the standard constraint criteria (that is, begins with, contains, ends with, is exactly, is empty). The Dialed Number Pattern list also has sortable columns.

**Add Dialed Number Pattern**

**Procedure**

To add a new Dialed Number Pattern:

---

**Step 1**

In the Operations Console, select **System > Dialed Number Pattern**.

The Dialed Number Pattern window opens.

**Step 2**

Select **Add New**.

**Step 3**

Fill in the appropriate configuration settings:

**Table 23: Dialed Number Pattern Configuration Settings**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Configuration</td>
<td></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>Dialed Number Pattern</td>
<td>The actual Dialed Number Pattern.</td>
<td>None</td>
<td>Must be unique. Maximum length of 24 characters.</td>
</tr>
<tr>
<td></td>
<td></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>the letter X or period (.).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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>
</tbody>
</table>

### Dialed Number Pattern Types

<table>
<thead>
<tr>
<th>Enable Local Static Route</th>
<th>Enable local static routes on this Dialed Number Pattern.</th>
<th>Disabled</th>
<th>Maximum length of 128 characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If Local Static Routes are enabled:</td>
<td></td>
<td>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</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>contains a list of configured, supported devices. Once a selection is made,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>the IP Address/Hostname/Server Group Name field is automatically updated</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>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</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>which contains a list of configured, support devices. Once a selection is</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>made, the IP Address/Hostname/Server Group Name field is automatically</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>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</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Route to Device</strong> or <strong>Route to SIP Server Group</strong>, enter the IP address,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>hostname, or the server group name of the route.</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>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.</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>Cannot contain whitespace characters.</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> - Enter the survey dialed number pattern.</td>
<td>none</td>
<td>Maximum length of 24 characters. Accepts only alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Step 4**

Click **Save** to save the Dialed Number Pattern.

You are returned to the **Dialed Number Pattern** page. To deploy the Dialed Number Pattern configuration, click **Deploy** to deploy the configuration to all Unified CVP Call Server devices.

---

**Delete Dialed Number Pattern**

**Procedure**

Deleting a dialed number pattern deletes the entire dialed number pattern and all dialed number pattern types associated with that dialed number pattern. You can check one or more dialed number pattern check boxes and select **Delete**.

To delete a Dialed Number Pattern:

**Step 1**

Select **System** > **Dialed Number Pattern**.

The Dialed Number Pattern window opens.

**Step 2**

Find the Dialed Number Pattern.
Step 3 Select the radio button next to the Dialed Number Pattern that you want to delete and click Delete.

Step 4 When prompted to confirm the delete operation, click OK to delete or click Cancel to cancel the delete operation. If confirmed, the delete operation proceeds and a message displays the results. If canceled, no operation will occur. The end-user will be presented with an error message if the delete button is selected and no check boxes are checked.

### Edit Dialed Number Pattern

To edit a Dialed Number Pattern, you must first define a Dialed Number Pattern.

#### Procedure

To edit a Dialed Number Pattern:

**Step 1** In the Operations Console, select System > Dialed Number Pattern.

The Dialed Number Pattern Configuration window opens.

**Step 2** Select the Dialed Number Pattern and click Edit.

**Step 3** Modify the appropriate configuration settings:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Configuration</td>
<td></td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>Dialed Number Pattern</td>
<td>The actual Dialed Number Pattern. This field is read-only.</td>
<td>n/a</td>
<td>n/a</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>
</tbody>
</table>

Cisco Unified Customer Voice Portal

Administration Guide for Cisco Unified Customer Voice Portal, Release 12.0(1)
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Value</th>
</tr>
</thead>
</table>
| Enable Local Static Route                    | Enable local static routes on this Dialed Number Pattern. If Local Static Routes are enabled:  
  • Route to Device - Select the device from the drop down list which contains a list of configured, supported devices. Once a selection is made, the IP Address/Hostname/Server Group Name field is automatically updated with the IP Address of the selected device.  
  • Route to SIP Server Group - Select the device from the drop down list which contains a list of configured, support devices. Once a selection is made, the IP Address/Hostname/Server Group Name field is automatically updated with the IP Address of the selected device.  
  • IP Address/Hostname/Server Group Name - If you have not selected a Route to Device or Route to SIP Server Group, enter the IP address, hostname, or the server group name of the route. | Disabled | Maximum length of 128 characters  
Must be a valid IP address, hostname, or fully qualified domain name |
| Enable Send Calls to Originator              | Enables calls to be sent to originator. | Disabled | n/a |
| Enable RNA Timeout for Outbound Calls        | Enables Ring No Answer (RNA) timer for outbound calls.  
  • Timeout - Enter the timeout value in seconds. | Disabled | n/a  
Valid integer in the inclusive range from 5 to 60. |
| Enable Custom Ringtone                       | Enables customized ring tone.  
  • Ringtone media filename - Enter the name of the file that contains the ringtone. | Disabled | Maximum length of 256 characters  
Cannot contain whitespace characters |
| Enable Post Call Survey for Incoming Calls   | Enables post call survey for incoming calls.  
  • Survey Dialed Number Pattern - Enter the survey dialed number pattern. | Disabled | n/a  
Maximum length of 24 characters  
Accepts only alphanumeric characters |

**Step 4** Click **Save** to save changes to the Dialed Number Pattern.
You are returned to the **Dialed Number Pattern** page. To deploy the Dialed Number Pattern configuration, click **Deploy** to deploy the configuration to all Unified CVP Call Server devices.

---

**Find Dialed Number Patterns**

**Procedure**

To find a Dialed Number Pattern:

**Step 1** Select **System > Dialed Number Pattern** from the Main menu. The Dialed Number Pattern Configuration window opens.

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

**Step 3** You can also filter the list by selecting an attribute such as **Dialed Number Pattern Name** then selecting a modifier, such as **begins with**, and entering your search term then clicking **Find**.  

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

---

**Deploy Dialed Number Pattern**

You can deploy all configured dialed number patterns to all configured Unified CVP Call Server devices.

**Procedure**

To deploy Dialed Number Pattern configurations:

**Step 1** In the Operations Console select **System > Dialed Number Pattern**. The Dialed Number Pattern Configuration window opens.

**Step 2** Select one or more Dialed Number Patterns. Use the check box to the left of the Dialed Number Pattern column header to select all Dialed Number Patterns.

**Step 3** Click **Deploy** in the in the bottom right corner of this page to initiate a deployment request to the Unified CVP Call Servers.

**Note** In the following cases, the Deployment Status displays a warning message:

- No Unified CVP Call Server devices are configured
- A Dialed Number Pattern deployment is already in progress
You will receive a success message if at least one Unified CVP Call Server is configured, using the system-level configuration, and no dialed number pattern deployment task is currently in progress. No restart is required on a successful deployment to each Unified CVP Call Server device.

**Note**  
Only one deployment process can run at any given time. If one process is already running, you will not be able to initiate another process and you will receive an error message.

A message displays to indicate the successful start of deployment process. The Operations Console saves the Call Server configuration to the Operations Console database and returns to display the new configuration in the list page.

---

**View Dialed Number Pattern Deployment Status**

The Operations Console displays all configured Dialed Number Patterns. If a deployment fails because the Unified CVP Call Server is not accessible (either not deployed or offline) or is not upgraded to the current version, the Operations Console issues a descriptive message.

The Dialed Number Pattern Deployment Status page displays the last recorded deployment status per configured Unified CVP Call Server. You may refresh the page, view online help, or go back to the dialed number pattern list page. You may also sort (in alternating ascending and descending order) the Deployment Status table contents by the following column fields: Hostname, IP Address, Device Type Status, or Last Updated.

Deployment operations can be time consuming, depending on the number of Unified CVP Call Servers. When either process is running, you can select a status report to view the progress of the last initialized deployment request.

**Note**  
The Deployment operations are mutually exclusive. Only one deployment process can run at any given time. If one process is already running, you will not be able to initiate another process and you will receive an error message.

The following information applies to the Status window:

**Procedure**

- Unapplied changes (deployment status only) indicate that a Save operation took place since the last deployment operation.
- Only one Unified CVP Call Server can be deployed at any given time. The other call servers are either in the queue or in an already successful/failed state.

**Procedure**

To view Call Server deployment status:

**Step 1**  
In the Operations Console, select **System > Dialed Number Pattern**.

The Dialed Number Pattern Configuration window opens.

**Step 2**  
Select **Deployment Status** at the bottom right corner of the window.
The Operations Console provides status information for Dialed Number Pattern. In case of a failure, the Operations Console provides a reason for the failure.

**Web Services**

Unified CVP offers a Web Services-based framework to deliver a common user experience across all Cisco Unified Communications applications for features such as setting preferences, directories, and communication logs; setting serviceability parameters; and collecting, analyzing, and reporting on information necessary to manage and troubleshoot Cisco Unified Communications solution. This centralized framework enables consistency between Cisco Unified Communications applications and ensures a unified view of common serviceability operations.

The Web Services application handles API queries from external clients for CVP diagnostic information.

The Operations Console interfaces with the Web Services application in two ways:

- **Web Services User Management**: The Operation Console administrator can configure new Web Services users (users with the Web Services user role type). The Operations Console administrator can also manually push any configured Web Services users using the procedure identified in Set Up Web Services, on page 76.

  When you make Web Services user information changes and when you successfully deploy a device, all Web Services users are *automatically* pushed to the deployed Unified CVP devices listed below:

  - Unified CVP Call Server
  - Unified CVP Reporting Server
  - Unified CVP VXML Server
  - Unified CVP VXML Server (standalone)
  - CVP Remote Operations device

  External clients may connect to the Web Services application and authenticate themselves with these credentials.

- **List Application Servers**: The Operations Console currently stores configuration details for all devices in the database. The Operations Console writes this information to a device file which the Web Services application uses to reply to queries from external clients.

  To configure Web Services, see Set Up Web Services, on page 76.
  To view deployed Web Services configuration, see View Web Services Deployment Status, on page 77.

**Set Up Web Services**

You can manually deploy configured Web Services users to Unified CVP devices.

**Procedure**

To manually deploy Web Services configurations:
Step 1
Select System > Web Services.
The Web Services Configuration window opens.

Step 2
There is no configuration on the general tab. Optionally, select the Remote Operations Deployment tab to configure remote operations deployment.

Step 3
To associate Unified CVP Remote Operations with a third-party device, on the remote applications deployment tab:
Provide the IP Address and Hostname, and optionally a description, of the third-party device.
Click Add to add the device to the list of devices associated with this Unified CVP deployment's web services.

Note  The third-party device must have CVP Remote Operations installed.

Step 4
Click Save & Deploy in the bottom right corner of this page (or the Save & Deploy button in the toolbar above) to save and deploy the configuration to the impacted devices in the Operations Console database.
See View Web Services Deployment Status, on page 77 for details on viewing the status information.

View Web Services Deployment Status
You can verify the latest deployment status of the Web Services configuration. The deployment status is listed for each Unified CVP device.

Procedure
To view the deployment status of Web Services configurations:

Step 1
Select System > Web Services.
The Web Services Configuration window opens.

Step 2
From the toolbar, click Deployment Status.
The Web Services Deployment Status window displays the device IP address and current status.
See View System-Level Operation States, on page 12 for more details on each state.

IOS Setup
The Operations Console supports the ability to configure IOS gateways using templates. Templates are text files that contain the IOS commands required for use in a Unified CVP deployment. You can deploy the configuration defined in the template to a gateway right from the Operations Console. You can also rollback the configuration on the gateway to the point immediately before the template was deployed.
There is only one level of rollback. If you deploy a template (Template A) and then deploy another template (Template B), you can only roll back to Template A.

You can use the included default templates or create custom templates. The templates are text files that can be edited locally and then uploaded to the Operations Console.

The templates contain variables that are placeholders for configuration data. The variables can reference data that is in the Operations Console database as well as reference data that is outside of the Operations Console database, if it is accessible to the Operations Console (such as some portions of the Unified ICM database). The variables are replaced with the actual values of the data when the template is sent to the IOS Gateway.

Templates are located in the following directories on the Operations Console server:

- **Default Templates** - `%CVP_HOME%\OpsConsoleServer\IOSTemplates\default`
- **Custom Templates** - `%CVP_HOME%\OpsConsoleServer\IOSTemplates\custom`

IOS Configuration consists of:

- Template Management - Add, Delete, Edit, Copy, and View details about templates.
- Template Deployment - preview & deploy, view deployment status, and rollback template deployments.

See Also:

- IOS Template Format
- IOS Template Management
- IOS Template Deployment

**IOS Template Format**

The IOS template must have a specific format to be accepted by the Operations Console:

- The second should be a configure terminal command, such as:
  
  `conf t`

See [View Template Details](#) for examples of the remaining configuration. With the exception of variables, all of the commands use standard IOS syntax.

The variables that can be used are detailed below:
<table>
<thead>
<tr>
<th>Component</th>
<th>Variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified CVP Call Server</td>
<td>• %CVP.Device.CallServer.General.IP Address%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.CallServer.ICM.Maximum Length of DNIS%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.CallServer.ICM.New Call Trunk Group ID%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.CallServer.ICM.Pre-routed Call Trunk Group ID%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.CallServer.SIP.Outbound SRV Domain Name/Server Group Domain Name (FQDN)%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.CallServer.SIP.Outbound Proxy Port%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.CallServer.SIP.Port number for Incoming SIP Requests%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.CallServer.SIP.DN on the Gateway to play the ringtone%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.CallServer.SIP.DN on the Gateway to play the error tone%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.CallServer.SIP.Generic Type Descriptor (GTD) Parameter Forwarding%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.CallServer.SIP.PrependDigits - Number of Digits to Strip and Prepend%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.CallServer.SIP.UDP Retransmission Count%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.CallServer.IVR.Media Server Retry Attempts%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.CallServer.IVR.IVR Service Timeout%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.CallServer.IVR.Call Timeout%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.CallServer.IVR.Media Server Timeout%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.CallServer.IVR.ASR/TTS Server Retry Attempts%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.CallServer.IVR.IVR Service Retry Attempts%</td>
</tr>
<tr>
<td>Unified CVP Reporting Server</td>
<td>%CVP.Device.ReportingServer.General.IP Address%</td>
</tr>
<tr>
<td>Unified CVP VXML Server</td>
<td>%CVP.Device.VXMLServer.General.IP Address%</td>
</tr>
<tr>
<td>Gateway</td>
<td>• %CVP.Device.Gateway.Target.IP Address%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.Gateway.Target.Trunk Group ID%</td>
</tr>
<tr>
<td></td>
<td>• %CVP.Device.Gateway.Target.Location ID%</td>
</tr>
<tr>
<td>SIP Proxy Server</td>
<td>%CVP.Device.SIPProxyServer.General.IP Address%</td>
</tr>
</tbody>
</table>
**IOS Template Management**

You use this page to manage IOS templates.

You can perform the following tasks:

**Add New Template**

To add a new template:

**Step 1**
Select System > IOS Configuration > IOS Template Management.

The IOS Template Management page opens.

**Step 2**
From the toolbar, select Add New.

The IOS Template Configuration page opens.

**Step 3**
Click Browse to browse to a template file on your local computer. Provide a name for the template and an optional description. Click Save to upload the template file to the Operations Console.

*Note* The file you select to upload must be of a valid file format or the upload fails. See IOS Template Format, on page 78 for details on the format required and the variables that you can use in your template.

A message is displayed confirming successful upload if the file is valid.

**Delete Templates**

*Note* You cannot delete default templates. Only custom templates can be deleted.

To delete templates:

**Step 1**
Select System > IOS Configuration > IOS Template Management.

The IOS Template Management page opens.

**Step 2**
Select the checkboxes next to the templates you want to delete.

**Step 3**
From the toolbar, select Delete.
A confirmation appears. Select **OK** to proceed and delete any custom templates selected.

---

**Edit Templates**

You can edit templates. You can change the description of any template. You can edit the body of custom templates from within the browser. You cannot edit the body of default templates.

**Step 1** Select **System > IOS Configuration > IOS Template Management**.

The IOS Template Management window opens.

**Step 2** Select the check box next to the template you want to **Edit**.

**Step 3** From the toolbar, select **Edit**.

The IOS Template Configuration page appears.

**Step 4** Optionally, edit the description field.

**Step 5** If this is a custom template, then you can check the **Enable template modification** check box to allow for editing of the template body. See **IOS Template Format, on page 78** for details about template syntax. You can undo any unsaved changes you made to the body by clicking **Undo Template Body Changes**.

**Step 6** Select **Save** to save the template when you complete your changes.

---

**Copy Templates**

You can copy templates to create a new template to which you can make modifications. For instance, it is not possible to edit the body of a default template, however, you can copy a default template and then edit the body of the copy.

**Step 1** Select **System > IOS Configuration > IOS Template Management**.

The IOS Template Management window opens.

**Step 2** Select the checkbox next to the template that you want to **Copy**.

**Step 3** From the toolbar, select **Copy**.

The Copy IOS Template screen opens.

**Step 4** Edit the Name and Description for the copy.

**Step 5** Optionally, check the box entitled **Enable template modification** and make changes to the copy. You can also make changes later. See **Edit Templates, on page 81**.

**Step 6** Select **Save** to create the copy with the changes you made.

---

**View Template Details**

To view the details of a template:
Step 1 Select **System > IOS Configuration > IOS Template Management**.
The IOS Template Management page opens.

Step 2 Select **Details** in the details column for the template you want to view.
The IOS Template Details page opens.
The name and the template body of the template is displayed. See **IOS Template Format, on page 78** for details about template syntax.

---

**IOS Template Deployment**

The IOS Template Deployment pages allow you to deploy a gateway configuration template to a gateway. The template provisions the gateway and substitutes any variables in the template with source devices that you choose when you deploy.

From this page you can:

- Preview 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:

Step 1 Select **System > IOS Configuration > IOS Template Deployment**.
The IOS Template Deployment page opens.

Step 2 In the **Select Template** panel, select the template that you want to deploy.

Step 3 In the **Associate Source Device(s)** panel, select the devices to be replaced with device variables in the template.

Step 4 In the **Associated Gateways** panel, deselect any of the gateways that will not receive the template deployment. By default, all gateways are selected.

Step 5 Click **Preview and Deploy** to validate and preview the template to the selected gateways with the selected settings.

After clicking **Preview and Deploy**, the script is validated. If there is an error in the script, or there is a variable in the script for which a device is required, but no device was selected from the **Associate Source Device(s)** panel, then errors are listed on the IOS Template Preview Page. Even if you click **Deploy** at this point, the template is not deployed, and the status page shows a failure due to an invalid template.

Once the preview screen appears, you can perform one of three actions:

- If the template is valid or invalid, click **enable template modification** and edit the template on this screen. Click **Verify** to verify your changes as valid, or click **Undo All Changes** to revert the template to the way it was before you began editing.

- If the template is valid, click **Deploy** to deploy the template to the selected gateways,
• If the template is valid, click **Save and Deploy** to save the template and deploy the template to the selected gateways. If this is an existing custom template, then any changes you made are saved to this custom template. If this is a default template, then the template is copied to a new custom template and saved.

---

**Check Deployment Status**

To check the status of a template deployment:

**Step 1**
Select **System > IOS Configuration > IOS Template Deployment**.
The IOS Template Deployment window opens.

**Step 2**
From the toolbar, select **Deployment Status**.
The IOS Template Deployment - Deployment Status window opens.
The status page lists information about the attempted deployment. Click on the status message for any deployment for additional details.

---

**Roll Back Deployment**

---

**Note**
There is only one level of rollback. If you deploy a template (Template A) and then deploy another template (Template B), you can only roll back to Template A.

To Rollback a deployment:

**Step 1**
Select **System > IOS Configuration > IOS Template Deployment**.
The IOS Template Deployment window opens.

**Step 2**
From the toolbar, click **Deployment Status**.
The IOS Template Deployment - Deployment Status window opens.

**Step 3**
Check the check box next to the deployment you want to rollback and click **Rollback**.
A confirmation dialog opens. Read the warning and click **OK** to continue the rollback.
A status message is displayed stating that the rollback is in progress. You can refresh the status page by clicking **Refresh** to see the status of the rollback.
Cisco VVB Setup

The Operations Console supports the ability to configure Cisco Virtualized Voice Browser using templates. Templates are text files that contain the VVB settings required for deployment. You can deploy the configurations defined in the template to a VVB from the Operations Console.

You can use the included default templates or create custom templates. The templates are text files that can be copied and edited on the Operations Console.

You can use this page to manage VVB templates.

Add New Template

Step 1 Select System > VVB Configuration.
Step 2 From the toolbar, click Add New.
Step 3 In the General tab, enter a unique template name and description.
Step 4 Select the ASR Servers tab and configure server, port.

For configuration details, see ASR and TTS Servers Setup, on page 84.

Note All ASR Servers selected must have the same port number to access.

Step 5 Select the TTS Servers tab and configure server, port.

For configuration details, see ASR and TTS Servers Setup, on page 84.

Note All TTS Servers selected must have the same port number to access.

Step 6 Select the Applications tab and add new applications.

For configuration details, see Application Setup, on page 85.

Step 7 Select the Triggers tab and associate triggers for newly created applications.

For configuration details, see Triggers Setup, on page 89.

Step 8 Click Save to save the template file to the Operations Console.

ASR and TTS Servers Setup

You can configure ASR and TTS Servers using the following settings.
Table 25: ASR Servers Tab Configuration Settings

| Field            | Description                                                                                                                                                                                                                                                                                                                                                   | Default | Range     |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ASR / TTS Server Selection | Servers configured in Speech Servers page are listed in the Available Servers drop-down menu. Select the server from the drop-down list and click Add to select the server. To add a custom server which is not listed in the Speech Servers, you can type the hostname (FQDN) in the drop-down field and click Add to select the server. Cisco VVB uses the hostname to connect to these servers and VVB should be able to perform a DNS resolution for the hostname. | None    | None      |
| Port Number      | Provide the port number that is configured for communication.                                                                                                                                                                                                                                                                                                  |         | 1 to 65535 |

Application Setup

You can configure Applications using these settings.

Table 26: Application Tab Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Base Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>Provide an application name.</td>
<td>None</td>
<td>None</td>
<td>Alphanumeric .</td>
</tr>
<tr>
<td>Application Type</td>
<td>Select the application script type from the drop-down menu.</td>
<td>SelfService</td>
<td>SelfService, Comprehensive, VRU, Comprehensive, Error, Ringtone</td>
<td>None</td>
</tr>
<tr>
<td>Script</td>
<td>Description</td>
<td>Parameters</td>
<td>Default</td>
<td>Base Type</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>SelfService</td>
<td>The standalone call flow runs this scripting application.</td>
<td><em>VXML Application Name</em>—Application name that is present on the VXML server. Mandatory field to enter.</td>
<td>None</td>
<td>Alphanumeric</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Port</em>—Port on which the VXML server or load balancer is running.</td>
<td>7000</td>
<td>Numeric</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Primary VXML Server</em>—VXML server or load balancer IP address. Mandatory field.</td>
<td>None</td>
<td>IP Address or Domain Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Backup VXML Server</em>—VXML server backup server IP address.</td>
<td>None</td>
<td>IP Address or Domain Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Maximum Sessions</em>—Provide number of sessions you like to associate with this application.</td>
<td>25</td>
<td>Numeric</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> The number of sessions must be less or equal to the license provided by Cisco VVB.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Secured</em>—Select the check box to encrypt the communication between Cisco VVB and VXML server.</td>
<td>None</td>
<td>Boolean</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> If you have enabled secure communication, then ensure to:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Change the port number in the above field to 7443.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Upload the relevant certificate. To upload certificate, see <em>Upload certificate or certificate trust list</em> topic in <em>Cisco Unified Communications Operating System Administration Guide</em>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Restart Tomcat server and Engine from command line.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Script</td>
<td>Description</td>
<td>Parameters</td>
<td>Default</td>
<td>Base Type</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>Comprehensive</td>
<td>The comprehensive call flow runs this scripting application.</td>
<td>Sigdigit—Enable this parameter to use Significant Digits feature. Enter the number of digits that are used as sigdigit. When Cisco VVB receives a call, the CVP comprehensive service is configured to strip the digits, so that when the IVR leg of the call is set up, the original label is used on the incoming VoiceXML request.</td>
<td>None</td>
<td>Numeric</td>
</tr>
<tr>
<td></td>
<td>Maximum Sessions—Provide number of sessions you like to associate with this application.</td>
<td></td>
<td>25</td>
<td>Numeric</td>
</tr>
<tr>
<td></td>
<td>Note  The number of sessions must be less or equal to the license provided by Cisco VVB.</td>
<td></td>
<td></td>
<td>Boolean</td>
</tr>
<tr>
<td></td>
<td>Secured—Select the check box to encrypt the communication between Cisco VVB and VXML server. By default it is disabled.</td>
<td></td>
<td>None</td>
<td>Boolean</td>
</tr>
<tr>
<td></td>
<td>Note  If you have enabled secure communication, then ensure to:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Upload the relevant certificate. To upload certificate, see Upload certificate or certificate trust list topic in Cisco Unified Communications Operating System Administration Guide</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Restart Tomcat server and Engine from command line.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you are using a coresident VXML and Call Server, use CA-signed certificate.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Script</td>
<td>Description</td>
<td>Parameters</td>
<td>Default</td>
<td>Base Type</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>VRUComprehensive</td>
<td>The non-reference VRU call flow and VRU-only call flow runs this scripting application.</td>
<td><strong>PrimaryVXMLServer</strong>—VXML server or load balancer IP address.</td>
<td>&quot;&quot;</td>
<td>Alphanumeric</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>BackupVXMLServer</strong>—VXML backup server or load balancer IP address.</td>
<td>&quot;&quot;</td>
<td>Alphanumeric</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Port</strong>—Port on which VXML server or load balancer is running.</td>
<td>&quot;7000&quot;</td>
<td>Numeric</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>Ports 7000/7443 must be configured for interworking with CVP Release 11.5 and later. For earlier versions of CVP, configure ports 8000/8443.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Secured</strong>—Select the check box to encrypt the communication between Cisco VVB and VXML server.</td>
<td>false</td>
<td>Boolean</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>If you have enabled secure communication, then ensure to:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Change the port number in the above field to 7443.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Upload the relevant certificate. To upload certificate, see <em>Upload certificate or certificate trust list</em> topic in <em>Cisco Unified Communications Operating System Administration Guide</em>.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Restart Tomcat server and Engine from command line.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Sigdigit</strong>—Enable this parameter to use Significant Digits feature. Enter the number of digits that are used as sigdigit. When Cisco VVB receives a call, the CVP comprehensive service is configured to strip the digits, so that when the IVR leg of the call is set up, the original label is used on the incoming VoiceXML request.</td>
<td>0</td>
<td>Numeric</td>
</tr>
<tr>
<td>Script</td>
<td>Description</td>
<td>Parameters</td>
<td>Default</td>
<td>Base Type</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------</td>
<td>-------------------------------------------------</td>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>Error</td>
<td>This script is used to</td>
<td><strong>Maximum Sessions</strong>—Provide number of</td>
<td>25</td>
<td>Numeric</td>
</tr>
<tr>
<td></td>
<td>play error tone.</td>
<td>sessions you like to associate with this</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>application.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> The number of sessions must be less</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>or equal to the license provided by Cisco VVB.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Custom Error Prompt</strong>—Provide the custom</td>
<td>None</td>
<td>Numeric</td>
</tr>
<tr>
<td></td>
<td></td>
<td>error.wav file to play.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Prompt name field is case-sensitive.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The prompt file must be uploaded to Cisco VVB.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If custom prompts are not uploaded or found,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>the default prompt is played.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ringtone</td>
<td>This script is used to</td>
<td><strong>Maximum Sessions</strong>—Provide number of</td>
<td>25</td>
<td>Numeric</td>
</tr>
<tr>
<td></td>
<td>play ringtone.</td>
<td>sessions you like to associate with this</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>application.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> The number of sessions must be less</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>or equal to the license provided by Cisco VVB.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Triggers Setup**

You can associate trigger with the applications added in Applications tab.
### Table 27: Trigger Tab Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
</table>
| Dial Number Pattern        | A unique phone number. The value includes numeric characters, preceded or followed by the special character: *  
Examples of valid Directory Numbers: *12* or 12*23  
Examples of invalid Directory Numbers: 91X+, 91X?, 91!, 813510[^0-5] because this number contains a character other than numerical and allowed special characters, or 8]90[-, because this number does not conform with the rule that the square bracket ([ ]) characters enclose a range of values.  
**Note** For more information, see *Wildcards and Special Characters in Route Patterns and Hunt Pilots* section in the *Cisco Unified Communications Manager System Guide*. | None    |
| Application Name           | Select the application from the drop-down menu to associate trigger with the application and click Add. | None    |

### Delete Template

**Note** You cannot delete default templates. Only custom templates can be deleted.

**Step 1** Select **System > VVB Configuration**.

**Step 2** Select the templates you want to delete.

**Step 3** From the toolbar, select **Delete**.

A confirmation appears. Select **OK** to proceed and delete any custom templates selected.

### Edit Templates

You can edit and change description of any template. You can also edit custom templates within a browser, but you cannot edit the default templates.

**Step 1** Select **System > VVB Configuration**.
### Copy Templates

You can copy templates to create a new template to which you can modify. For instance, it is not possible to edit the body of a default template, however, you can copy a default template and then edit the body of the copy.

**Step 1** Select `System > VVB Configuration`.

**Step 2** Select the check box next to the template that you want to copy.

**Step 3** From the toolbar, select `Copy`.

The Copy VVB Template screen is displayed.

**Step 4** Edit the Name and Description, and for modifying other settings, see `Add New Template, on page 84`.

**Step 5** Select `Save` to create the copy with the changes you made.

### Deploy Template

To preview and deploy a template:

**Step 1** Select `System > VVB Configuration`.

**Step 2** From the `List of Template`, select the template that you want to deploy.

**Step 3** Click `Deploy` to deploy the selected template. You can verify the template body of the selected template.

**Step 4** In the `Associated Virtualized Voice Browsers` panel, move VVBs to `Selected` pane to deploy.

**Step 5** Click `Deploy` to deploy the template to the selected Voice Browsers.

If there is an error in the script, or there is a variable in the script for which a device is required, but no device was selected from the `Associate Source Device(s)` panel, then errors are listed on the VVB Template Preview page.

At this point, even if you attempt to deploy the template by clicking the `Deploy` button, the template will not be deployed, and the status page displays “Failure due to an invalid template”.

### Check Deployment Status

**Step 1** Select `System > VVB Configuration`.

**Step 2** From the toolbar, select `Deployment Status`.

The VVB Template Deployment - Deployment Status page is displayed.
The status page lists information about the attempted deployment. Click the status message for more details on deployment status.

---

**Perform Courtesy Callback**

The Courtesy Callback feature is available in Unified CVP. Courtesy Callback reduces the time callers have to wait on hold/in queue. The feature allows the system to offer callers who meet certain criteria, for example, callers with the possibility of being in queue for more than X minutes, the option to be called back by the system when the wait time would be considerably shorter.

If the caller decides to be called back by the system, then they leave their name and phone number. When the system determines that an agent is available (or will be available soon), then a call is placed back to the caller. The caller must answer the call and indicate that they are the caller. The caller is connected to the agent after a short wait.

**Procedure**

To configure Courtesy Callback:

**Step 1**
Select System > Courtesy Callback.

The Courtesy Callback Configuration window opens.

**Step 2**
Select the required Unified CVP Reporting Server (if configured) from the drop-down list.

**Note**
If you leave the selection blank, no Reporting Server is associated with the Courtesy Callback deployment.

**Step 3**
Optionally, enable the check box (default is disabled) next to the label Enable secure communication with the Courtesy Callback database to secure the communication between the Unified CVP Call Server and Unified CVP Reporting Server used for Courtesy Callback.

**Step 4**
In the Dialed Number Configuration section:

The Dialed Number Configuration of Courtesy Callback allows you to restrict the dialed numbers that callers can enter when they are requesting a callback. For example, it can stop a malicious caller from having Courtesy Callback dial 911. The table below lists the configuration options for the Dialed Number Configuration:

<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 Allowed Dialed Numbers field can be used for a callback. By default, this is unchecked. If no dialed numbers are present in the Allowed Dialed Numbers list box, then Courtesy Callback does not allow any callbacks.</td>
<td>Unchecked - Callbacks can only be sent to dialed numbers listed in the Allowed Dialed Numbers list.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allowed Dialed Numbers</td>
<td>The list of allowed dialed numbers to which callbacks can be sent. You can use dialed number patterns; for example, 978&gt; allows callbacks to all phone numbers in the area code 978.</td>
<td>Empty - If Allow Unmatched Dialed Numbers is not checked, and this list remained empty, then no callbacks can be made.</td>
</tr>
<tr>
<td></td>
<td>To Add/Remove Dialed Numbers:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• To remove a number from the list - Highlight the number and click Remove.</td>
<td></td>
</tr>
<tr>
<td>Denied Dialed Numbers</td>
<td>The list of denied dialed numbers to which callbacks are never sent. You can use dialed number patterns; for example, 555&gt; allows callbacks to all phone numbers in the area code 555.</td>
<td>The Denied Dialed Numbers window is prepopulated if your local language is &quot;en-us&quot;(United States, English). Be sure to add any additional numbers you want to deny.</td>
</tr>
<tr>
<td></td>
<td>To Add/Remove Dialed Numbers:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• To remove a number from the list - Highlight the number and click Remove.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Denied numbers takes precedence over allowed numbers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Wildcarded DN patterns can contain &quot;.&quot; and &quot;X&quot; in any position to match a single wildcard character.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Any of the wildcard characters in the set &quot;&gt;!*T&quot; match multiple characters but can only be used as trailing values because they always match all remaining characters in the string.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The highest precedence of pattern matching is an exact match, followed by the most specific wildcard match.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
</tbody>
</table>
The default value is 0, which is equivalent to an unlimited number of callbacks offered per calling number. The maximum value is 1000. This setting allows you to limit the number of calls, from the same calling number that are eligible to receive a callback. If this field is set to a positive number (X), then the courtesy callback “Validate” element only allows X callbacks per calling number to go through the “preemptive” exit state at any time. If there are already X callbacks offered for a calling number, new calls go through the “none” exit state of the “Validate” element. In addition, if no calling number is available for a call, the call always goes through the “none” exit state of the “Validate” element.

---

**Step 5**  
Click the **Call Server Deployment** tab to view a list of available call servers and to select a Unified CVP Call Server to associated with Courtesy Callback.

**Step 6**  
After making the required configuration changes, you have two options to save the configuration:

- **Click** **Save & Deploy** in the bottom right corner of this page (or the **Save & Deploy** button in the toolbar above) to save the Call Server information and initiate a deployment request to the selected devices.

  See the **View Courtesy Callback Deployment Status** section for details on viewing the status information.

- **Click** **Save** to save the configuration to the Operations Console database

---

**View Courtesy Callback Deployment Status**

You can verify the latest deployment status of the Courtesy Callback configuration using the Unified CVP Operations console. The deployment status is listed for each Unified CVP Call Server.

**Procedure**

To view the deployment status of Courtesy Callback configurations:

**Step 1**  
Select **System > Courtesy Callback**.

The configuration window opens.

**Step 2**  
From the toolbar, click **Deployment Status**.

TheCourtesy Callback Deployment Status window displays the device IP address and current status. Note that you can click **Refresh** to view the latest status.

In the following cases, the Deployment Status displays a warning message:

- If you have only saved the configuration details and have not deployed them.

- If you have edited or deleted an existing configuration and have not deployed the changes.
If you changed the call server association.

---

**SIP Error Reason Code Mapping**

In a REFER label transfer scenario, a call comes from the network to Cisco Unified Border Element (CUBE). The CUBE receives a REFER from Cisco Unified Customer Voice Portal (CVP) and starts a new INVITE toward refer-to number. If the call fails, CUBE receives a status message with q.850 Reason header which includes ISDN User Part (ISUP) cause codes. CUBE then starts a NOTIFY to Unified CVP with the Session Initiation Protocol (SIP) error string. Unified CVP maps the SIP code to ISUP cause code and sends back to CUBE in a BYE message and in-turn to network. This result is achieved by configuring the SIP reason code to ISUP cause code mapping under SIP Error Reason Code Mapping menu.

**Configure SIP Error Reason Code Mapping**

**Before you begin**

- Install Call Server 12.0(1).
- Ensure that the Call server is up and running.
- Check the **SIP Subsystem** check box to enable this service in the Call Server.

**Step 1**

In the Operations console, select **System > SIP Error Reason Code Mapping**.

**Step 2**

Enter the value of the error reason code in the **Error Reason Code (SIP)** field.

**Note**

- The value of Error Reason Code (SIP) must be unique and it can be a three-digit positive integer.
- The SIP Error Reason Code field must not be blank.

**Step 3**

Enter the value of ISUP cause code in the **Cause Code (ISUP)** field.

**Note**

- The ISUP cause code value must be two or three digit positive integers.
- The ISUP cause code field must not be blank.

**Step 4**

Perform one of the following options:

- Click **Add** to add the entries to the **Reason to Cause Code Mapping** list.
  
  **Note**
  
  A maximum of ten mapping entries are allowed.

  - Click **Remove** to remove an entry from the **Reason to Cause Code Mapping** list. Click **OK**.

**Step 5**

After changing the Error Reason Code Mapping configurations, you have two options to save the configuration:

- Click **Save** to save the configuration to the Operations Console derby database.
- Click **Save & Deploy** to deploy the configurations to all the Call Servers.
Step 6  Click **Deployment Status** to view the deployment status.
The SIP Error Reason Code Mapping - Deployment Status window displays the device IP address and the deployment status.

Step 7  Click **Refresh** to view the latest status.

**Caution**  The Deployment Status page displays a warning message, in the following cases:

- If you have saved the configuration details and have not deployed them.
- If you have edited or deleted an existing configuration detail, and have not deployed the changes.

---

**View SIP Error Reason Code Mapping Deployment Status**

The Operations Console displays the Unified CVP Call Server IP address and the deployment status. If a deployment fails because the Unified CVP Call Server is not accessible (either not deployed or offline) or is not upgraded to the current version, the Operations Console issues a descriptive message.

The **SIP Error Reason Code Mapping Deployment Status** page displays the last recorded deployment status per configured Unified CVP Call Server. You can refresh the page, view online help, or go back to the **SIP Error Reason Code Mapping Configuration** page. You can also sort (in either ascending and descending order) the Deployment Status table contents by the following column fields: **Hostname, IP Address, Device Type, Status, or Last Updated**.

Deployment operations can be time-consuming, depending on the number of Unified CVP Call Servers. When either process is running, you can select a status report to view the progress of the last initialized deployment request.

**Note**  Deployment operations are mutually exclusive. Only one deployment process can run at any given time. If a process is already running, you cannot start another process. You will receive an error message.

The following information applies to the Status window:

**Procedure**

- Unapplied changes (deployment status only) indicate that a Save operation took place since the last deployment operation.
- Only one Unified CVP Call Server can be deployed at any given time. The other call servers are either in queue or in a successful or failed state.

**Procedure**

To view the SIP error code mapping deployment status:

**Step 1**  From the Operations Console, select **System > SIP Error Reason Code Mapping**.
The Operations Console displays the **SIP Error Reason Code Mapping Configuration** page.

**Step 2**  Click **Deployment Status** at the bottom right corner of the window.
The Operations Console displays the Call Server IP address and the deployment status. If there is a failure, the Operations Console provides a reason for the failure.

---

## Cloud Services

### Proxy Settings

#### Prerequisite

- Install CVP 12.0(1).
- Ensure that the VXML servers are up and running.

#### Enabling Proxy Settings

1. **Step 1**  
   From the Operations Console, select **System > Cloud Services > Proxy Settings**.

2. **Step 2**  
   Enter the value of the Context Service Proxy.
   - The proxy hostname must be in the format: `hostname:port` or `IP_address:port`.
   - Leave the proxy setting column blank for a deployment that does not require a proxy for access.

3. **Step 3**  
   After changing the proxy configurations, save it. There are two options to save the configuration:
   - Click **Save** to save the configuration to the Operations Console derby database.
   - Click **Save & Deploy** to save and deploy the configurations to all the VXML servers.

4. **Step 4**  
   Click **Deployment Status** to view the current deployment status. The **Proxy Settings - Deployment Status** window displays the device IP address and the deployment status.

5. **Step 5**  
   Click **Refresh** to view the latest status.

#### Note

The **Deployment Status** page displays a warning message, in the following cases:

- If you have saved the configuration details and not deployed the changes.
- If you have edited or deleted an existing configuration and not deployed the changes.

---

### What to do next

Restart VXML service and Ops Console service.
View Proxy Settings Deployment Status

The Operations Console displays the Unified CVP VXML Server IP address and the deployment status. If a deployment fails because of any of the following reasons, then a descriptive message is displayed.

- Unified CVP VXML Server is not accessible (either not deployed or offline)
- Unified CVP VXML Server is not upgraded to the current version

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

Deployment operations can be time-consuming, depending on the number of Unified CVP VXML Servers. When a deployment process is running, you can select the status report.

---

**Note**

Deployment operations are mutually exclusive. Only one deployment process can run at any given time. If a process is already running, you cannot start another process. You will receive an error message.

The following information applies to the Status window:

- Unapplied changes (only deployment status) indicate that a Save operation took place since the last deployment operation.
- Only one Unified CVP VXML server can be deployed at any given time. The other VXML servers are either in queue or in a successful or failed deployment state.

Context Service Setup

**Context Service**

Cisco Context Service is a cloud-based omnichannel solution for Cisco Contact Center Express and Contact Center Enterprise. It enables you to capture your customer’s interaction history by providing flexible storage of customer-interaction data across any channel.

Context Service works with Cisco Customer Collaboration products. Context Service also provides an SDK interface for integration with your own applications or third-party applications to capture end-to-end customer-interaction data.

For more information about Context Service and to check service availability, see [https://cisco.com/go/contextservice](https://cisco.com/go/contextservice).

**Context Service Network Connectivity Requirements**

Context Service is a cloud-based service and requires that call center components using Context Service to be able to connect to the public Internet.

Context Service uses port 443 (HTTPS).

The following URLs must be whitelisted in your firewall so that your contact center components can connect to, and receive data from Context Service.
Use wildcard URLs in your allowed list because Context Service is accessed through multiple subdomains. Context Service subdomain names can dynamically change.

If you register Context Service by enabling the proxy setting option, configure the browser proxy with the URL specified in the Context Service Management Gadget. Refer to the following links to configure the proxy settings for the related browsers.

<table>
<thead>
<tr>
<th>Browser</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome</td>
<td><a href="https://support.google.com/chrome/answer/96815?hl=en">https://support.google.com/chrome/answer/96815?hl=en</a></td>
</tr>
</tbody>
</table>

Register Unified CVP with Context Service

You can register Unified CVP with Context Service.

Before you begin

Ensure that your web browser allows pop-ups.

If you are using Microsoft Internet Explorer, add a registry key `TabProcGrowth` with type of value String or DWORD (32-bit) and value set to 0 at:

```
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
```

Step 1 From the Operations Console, select **System > Cloud Services > Context Service**.
Step 2 Click **Save**.
Step 3 Click **Register**.
The Sign In Cisco WebEx page is displayed in a new browser tab or a new window based on your local browser settings.
Step 4 Enter your registered email address and click **Next**.
Step 5 Enter the Context Service username and password, and click **Sign In**.
The **Cloud Services** page is displayed.
Step 6 Click **Confirm**.
The **Context Service Management** page is displayed. If the registration is successful, the connection data is deployed on all running VXML servers in the pool.

**Note**

- If you add a VXML Server after registration, the connection data is automatically available on the VXML Server after you save and deploy the server settings. For more information about adding a VXML Server, see *Add Unified CVP VXML Server*, on page 153.

- The status of the deployment can be checked by clicking **Deployment status** button.

- Context Service is not supported in a VXML Server that is deployed in a standalone mode.

- The connection data expires after a predefined period. The Operations Console automatically generates a new connection data and deploys the connection data on all the VXML Servers in the pool.

If the registration is unsuccessful retry the registration process.

**Step 7**

Restart VXML service and Ops Console service.

---

**Related Topics**

- *Configure Context Service Connection Data in Call Studio*, on page 100
- *Deregister Context Service from Context Service*, on page 101

---

**Configure Context Service Connection Data in Call Studio**

You can configure Context Service connection data property to debug applications that interact with Context Service.

To debug a solution that uses Context Service, Call Studio requires your Context Service credentials and connection details.

**Before you begin**

Register Unified CVP with Context Service by using the Operations Console.

**Step 1**

From the Operations Console, select **System > Cloud Services > Context Service**.

**Step 2**

Click **Connection Data**.

The system displays the credential information in the Connection Data area below the **Connection Data** button. The connection data is selected by default.

**Note**

Carefully store the connection data. This data is the key to open your organization's data in the cloud.

**Step 3**

Copy the credentials onto the clipboard.

**Step 4**

Click **OK**.

**Step 5**

Launch Cisco Unified Call Studio.

**Step 6**

Choose **Window > Preferences**.

**Step 7**

On the **Preferences** window, choose **Call Studio > Debug Preferences**.

**Step 8**

In the Context Service area, paste the connection data from the clipboard into the **Connection Data** field.

**Step 9**

Click **OK**.
Deregister Context Service from Context Service

**Step 1** From the Operations Console, select **System > Cloud Services > Context Service**.

**Step 2** Click **Deregister**.

The Sign In Cisco WebEx page is displayed in a new browser tab or a new window based on your local browser settings.

**Step 3** Enter your registered email address and click **Next**.

**Step 4** Enter the Context Service username and password, and click **Sign In**.

The Enable Collaboration Cloud Extensions page opens.

**Step 5** Click **Confirm**.

If deregistration is successful, the credential information is automatically removed from the running VXML Servers in the pool. If deregistration is unsuccessful, retry the deregistration process.

**Step 6** Restart all the running VXML Servers in the pool.

---

Context Service Connection Timeouts and Retries

The Context Service client provides two connection properties that significantly affect the user experience for your customers and agents.

- **TIMEOUT** defines how long the client waits for a response from Context Service. Defaults to 1200 ms.

- **RETRIES** defines how many times the client retries the request when a timeout is reached. Set values based on factors specific to your deployment; the location relative to your Context Service instance, Internet latency, and quality metrics for your organization. Defaults to 1.

Ideally, you set REQUEST_TIMEOUT to a value that is long enough that the client does not frequently hit this limit before receiving a reply from Context Service, but not so long that callers hear long periods of silence from the IVR. Context Service is a cloud service that runs over the Internet, and the latency of the Internet can be highly variable. However, latency generally has a floor value based on your physical proximity to the data center on which your Context Service instance is hosted. You can roughly determine your floor value by pinging your Context Service instance at the times you experience the lowest call volume. Your REQUEST_TIMEOUT must never be lower than this floor value. Setting REQUEST_TIMEOUT lower than this value typically triggers timeouts and initiates a retry.

The RETRIES property is used to retry the request after a timeout is reached. For instance, if you set RETRIES to 1, then when a timeout is reached the request is resent and the timeout timer restarts. If Context Service does not respond on that first retry, then the request fails. If there is an issue with your connection, then you are potentially doubling the wait defined in REQUEST_TIMEOUT when RETRIES is set to 1. The effect increases as you increase RETRIES. The default REQUEST_TIMEOUT is 1200 ms (1.2 seconds) and the default RETRIES is set to 1. This combination results in a 2.4 second wait (wait time = REQUEST_TIMEOUT + RETRIES * REQUEST_TIMEOUT). In a worst-case scenario, wait time can be significant if there are network issues between your client and Context Service and your timeouts or retries are set too high. The RETRIES property is intended to be used to handle network hiccups that infrequently occur. The default setting of 1 assumes that your REQUEST_TIMEOUT is sufficiently high enough that the request is normally serviced on the first request. If the first 1.2 seconds is not enough, then the request is retried once and another 1.2 seconds allotted to wait for a response.
Retries are not attempted for "create" or "update" operations. If these operations fail due to a timeout, then your app or script could potentially request the "create" or "update" operation again, return a failure, or perform some other operation.

In general, typical requests within the same geographical area take from 100ms to 300ms; however, your network environment, switching latency, and location in relation to Context Service instance can increase the response time from Context Service.

Your service quality target ultimately defines how high REQUEST_TIMEOUT is set above the floor latency value. Setting the value too high results in extended waits for the caller or agent when Internet latency is high. Setting the value too low initiates retry requests that increase the wait in an attempt that can ultimately fail during times of high latency.

You can improve the customer experience of waiting while the client is accessing Context Service by notifying the customer that you are looking up information. For example, you can play prompts such as "Wait a moment while I access your account details". If a timeout occurs and a retry is attempted you can play a prompt, such as "I'm still accessing your account details." You could also opt to play MoH during the wait times to prevent silence on the line.

Inevitably connections to Context Service can fail, possibly due to high Internet latency or connections issues to the Internet itself. In those cases, your IVR scripting must account for a failed connection attempt to the Context Service. Your scripts must be able to route to an agent (or continue with self-service) without the benefit of Context Service data.

**Editing the vxml.properties File**

You can change the default value of `VXML.ContextService.requestTimeout` and `VXML.ContextService.maxRetries` connection properties in the `vxml.properties` file.

---

**Step 1**
Browse to the `vxml.properties` file available in the following locations:
- If you are using comprehensive call flow:
  
  C:\Cisco\CVP\conf

- If you are using Call Studio debugger:
  
  C:\Cisco\CallStudio\eclipse\plugins\com.audiumcorp.studio.debug.runtime\AUDIUM_HOME\conf

**Step 2**
Open the `vxml.properties` file by using any plain-text editor.

**Step 3**
Change the value of `VXML.ContextService.requestTimeout` and `VXML.ContextService.maxRetries` connection properties.

**Step 4**
Save the `vxml.properties` file.

**Step 5**
Restart the VXML Server.

---
Managing Devices

• Device Properties, on page 103
• Find Device, on page 105
• Unified CVP Licensing, on page 107
• Unified CVP Call Server Setup, on page 108
• Unified CVP Reporting Server Setup, on page 137
• Unified CVP VXML Server Setup, on page 152
• Unified CVP VXML Server (Standalone) Setup, on page 169
• Gateway Setup, on page 174
• Speech Server Setup, on page 182
• Media Server Setup, on page 187
• Unified Communications Manager Server Setup, on page 193
• Unified ICM Server Setup, on page 199
• SIP Proxy Server Setup, on page 203
• Unified IC Server Setup, on page 207
• Past Device Setups in Operations Console Database, on page 211
• Device Versions, on page 212

Device Properties

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

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

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

• Offline View of Device Properties
• Online View of Device Properties

For more information, see Device Information Field Descriptions
Offline View of Device Properties

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

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

Online View of Device Properties

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

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

Device Information Field Descriptions

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

The following table describes the server window fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>The hostname assigned to the device.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the device.</td>
</tr>
</tbody>
</table>
### Device State

The state of the configuration of the device: configured or invalid.

The following device types can be in the configured or invalid state:

- Unified CVP Call Server
- Unified CVP Reporting Server
- Unified CVP VXML Server
- Unified CVP VXML Server (standalone)
- Speech Server

A configuration can become invalid if the device is reinstalled or errors occur during device creation. To clear this state, edit the device and click **Save & Deploy**.

All other devices in the Operations Console are always in the configured state.

### Description

An optional text description for the device.

### Related Topics

- [View Device Status](#), on page 16

---

## Find Device

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

See also [Display Device Statistics](#), on page 106.

### Step 1

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

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

### Step 2

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

### Step 3

You can also filter the list by selecting an attribute such as **Hostname**; then selecting a modifier, such as **begins with**; entering your search term; and then clicking **Find**.

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

---

## Procedure

To find a device:

### Step 1

From the **Device Management** menu, select the menu option for the type of device to find from the Device menu.
The Find, Add, Delete, Edit window lists the available devices of the type you selected, sorted by name, 10 per screen.

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

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

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

---

**Display Device Statistics**

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

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

The Find, Add, Delete, Edit window opens.

**Step 2**
Click **Edit**.

**Step 3**
Find the device by using the procedure in **Find Device, on page 105**.

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

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

The Statistics window opens.

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

---

**Procedure**

To get device statistics:

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

The Find, Add, Delete, Edit window opens.

**Step 2**
Click **Edit**.

**Step 3**
Find the device using the procedure shown in **Find Device, on page 105**.

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

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

The Statistics window opens.

**Step 6**
If there are multiple statistics options to choose, select the desired option from the Statistics drop-down menu.
The Operations Server displays the statistics in the window.

## Unified CVP Licensing

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

**Unified CVP licenses:**

- **Call Server** - The SIP Service and the IVR Service check at startup time to ensure that it is running on a system with a valid Call Server license.

- **Unified CVP VXML Server** - The Unified CVP VXML Server checks at startup time to ensure that it is running on a system with a valid Unified CVP VXML Server license.

- **Reporting Server** - The Reporting Server checks at startup time to ensure that it is running on a system with a valid Reporting Server license.

The Operations Server runs without requiring a license.

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

Port licensing is enforced as follows:

- **The Call Server** is licensed for a certain number of ports; SIP and IVR Services share this port pool.

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

  **Note**

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

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

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

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

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

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

- **IVR Service** - Creates the VXML pages that implement the Unified CVP Micro-applications, based on Run Script instructions received from ICM server. The IVR service functions as the Voice Response Unit (VRU) leg, and calls must be transferred to it from the SIP Service to execute micro-applications. The VXML pages created by this module are sent to the VXML Gateway to be executed. The IVR Service routes requests from the SIP Service to the ICM Service.

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

You can perform the following tasks:

- Add Unified CVP Call Server
- Edit Unified CVP Call Server
- Delete Unified CVP Call Server
- Find Unified CVP Call Server
- View Unified CVP Call Server Statistics
- Unified CVP Call Server Settings
- Apply Unified CVP Call Server License
- View Device Status

**Related Topics**

- Shut Down Server, on page 40
- Start Server, on page 40

Add Unified CVP Call Server

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

**Procedure**

To add a Unified CVP Call Server:
Step 1 Select **Device Management > Unified CVP Call Server**.

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

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

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

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

Step 3 Fill in the IP Address and Hostname fields.

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

Step 5 Turn on the Call Services required for the Call Flow you are using by checking the appropriate check boxes, and then click **Next**. See Call Services, on page 110.

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

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

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

Configuration Tabs:

- [Set Up ICM Service, on page 112](#)
- [Set Up SIP Service, on page 115](#)
- [Set Up IVR Service, on page 124](#)
- [Add or Remove Device From Device Pool, on page 43](#)
- [Set Up Infrastructure, on page 127](#)

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

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

You must apply a license to the Unified CVP Call Server before using it. See Apply Unified CVP Call Server License, on page 136.

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

**Related Topics**

- [Unified CVP Call Server Settings, on page 135](#)
- [View Unified CVP Call Server Statistics, on page 134](#)
- [View Device Status, on page 16](#)
- [Shut Down Server, on page 40](#)
- [Start Server, on page 40](#)
Call Services

Services Needed for CVP Call Flow Models

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

<table>
<thead>
<tr>
<th>Call Flow Model</th>
<th>Required Call Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehensive Call Flow Using SIP, on page 110</td>
<td>ICM, IVR, SIP</td>
</tr>
<tr>
<td>VRU-Only, on page 110</td>
<td>ICM, IVR</td>
</tr>
<tr>
<td>Call Director Using SIP, on page 110</td>
<td>ICM</td>
</tr>
<tr>
<td>Unified CVP VXML Server with ICM Lookup, on page 111</td>
<td>ICM</td>
</tr>
<tr>
<td>Unified CVP VXML Server Standalone Call Flow, on page 111</td>
<td>No Service</td>
</tr>
<tr>
<td>Basic Video Call Flow, on page 111</td>
<td>ICM, IVR, SIP</td>
</tr>
</tbody>
</table>

**Comprehensive Call Flow Using SIP**

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

**VRU-Only**

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

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

**Call Director Using SIP**

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

**Unified CVP VXML Server with ICM Lookup**

In this call flow model, the call server with the ICM Service enabled is required to route calls. The Reporting server is optional. Use a Reporting server if you want to generate reports that include Unified CVP VXML Server events. You can also use the ICM request label from the Unified CVP VXML Server to an ICM Server, if the ICM service is enabled on the Call Server. The Reporting server can be installed on the same physical machine as the Call Server. After you configure the Call Server, you must configure the Unified CVP VXML Server. See Unified CVP VXML Server Setup, on page 152.

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

Following are the features of the IVR application:

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

**Unified CVP VXML Server Standalone Call Flow**

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

For a Unified CVP VXML Server (standalone) with no connection to an ICM Server and no Reporting Server, configure the Call Server with no services enabled. If you need to make requests to an ICM server, without relinquishing control of the call or use Unified CVP reporting, you must configure the VXML Server to use a Call Server with at least the ICM Service enabled. See Unified CVP VXML Server Setup, on page 152.

After you configure the Call Server, you must configure the Unified CVP VXML Server as a Unified CVP VXML Server (standalone). See Unified CVP VXML Server (Standalone) Setup, on page 169.

**Basic Video Call Flow**

The Basic Video call flow model combines the Call Director and the VRU-Only call flow models, along with video capabilities that are only enabled during the caller-agent conversation. It provides initial prompt and collect, self-service IVR, queuing, and VoIP routing among UCCE and TDM agents.
This call flow model is almost identical to the Unified CVP Comprehensive SIP call flow model. The only change between the two call flow models is the addition of video-enabled endpoints for the calling and called parties (Cisco Unified Video Advantage (CUVA), Cisco Unified Personal Communicator (CUPC), and Cisco TelePresence). See the Configuration Guide for Cisco Unified Customer Voice Portal for additional information about CUVA and Cisco TelePresence.

Unified CVP Call Server Services Setup

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

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

Set Up ICM Service

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

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

Procedure

• Call Director
• VRU-Only
• Comprehensive

What to do next

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

Procedure

To configure the ICM Service:

Step 1 If you are adding a new Call Server, refer to Add Unified CVP Call Server, on page 108. If you want to change an existing Call Server, refer to Edit Unified CVP Call Server, on page 132.
Step 2  Fill in the appropriate configuration settings as described in **ICM Service Settings**, on page 113.

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

**ICM Service Settings**

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

**Table 29: ICM 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><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 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>
<tr>
<td>Maximum Length of DNIS</td>
<td>The maximum length of an incoming Dialed Number Identification Service (DNIS). Valid input for this field is 1 - 99999 characters. Look for this information in your network dial plan. For example, if the Gateway dial pattern is 1800******, the value of Maximum Length of DNIS should be 10. The number of DNIS digits from the PSTN must be less than or equal to the maximum length of DNIS field.</td>
<td>10</td>
<td>Integer</td>
<td>No</td>
</tr>
</tbody>
</table>
### ICM Service Settings

**Enable secure communication with VRU PIM**
- Enables secure communication between ICM and the Unified CVP Server.
- **Default**: No
- **Range**: NA
- **Restart Required**: Yes

### Translation Routed DNIS Pool

**Add**
- Enter a single DNIS number for translation routed calls. DNIS is a phone service that identifies which number the caller dialed.
- DNIS can be up to 32 characters in length.
- Validations for DNIS fields are as follows:
  - The DNIS must be a positive integer; DNIS can begin with a zero (0)
  - The start and end values for the DNIS range must be the same length
  - Users cannot add a DNIS or DNIS range that already exists or overlap with (or in) the range of a DNIS added previously
- **Default**: None
- **Range**: Integer
- **Restart Required**: No

**Add a Range**
- List of DNIS numbers for translation routed calls. Add a range of DNIS numbers, select **Add a Range**, enter the first DNIS number in the range, and then enter the last DNIS number in the range in the **to** field. Click **Add DNIS** to add the entered DNIS or DNIS range to the list of Configured DNIS numbers. Select a DNIS or DNIS range in the Configured DNIS box and click **Delete DNIS** to remove it from the list of Configured DNIS numbers.
- DNIS can be up to 32 characters in length.
- Valid input for DNIS range requires the first and last DNIS numbers in the range to be the same length. For example, a range from 100 to 900 is valid because each number is three characters in length.
- **Default**: None
- **Range**: Integer
- **Restart Required**: No

### Advanced Configuration

**New Call Service ID**
- Identifies calls to be presented to ICM software as a new call. New Call Service ID calls result in a NEW CALL message being sent to ICM software and the call being treated as a new call, even if it had been pre-routed by ICM software.
- **Default**: 1
- **Range**: Integer
- **Restart Required**: 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>Pre-routed Call Service ID</td>
<td>Identifies calls pre-routed with a translation route or correlation ID. Pre-routed Service ID</td>
<td>2</td>
<td>Integer</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>calls result in a REQUEST_INSTRUCTION message being sent to ICM software, which continues to run</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>the script for the call.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Call Trunk Group ID</td>
<td>Calls presented to ICM as new calls are sent with this Trunk Group ID as part of the NEW_CALL</td>
<td>100</td>
<td>Integer</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>message being sent to ICM.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pre-routed Call Trunk Group ID</td>
<td>Calls pre-routed with a Translation Route or correlation ID are sent with this Trunk Group</td>
<td>200</td>
<td>Integer</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>ID as part of the REQUEST_INSTRUCTION message to ICM.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Trunk Utilization**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Gateway Trunk Reporting</td>
<td>Check the 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>The Add Gateway (when adding or editing a gateway) contains an optional field, <strong>Trunk Group ID</strong>,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>that can be used 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</td>
<td>700</td>
<td>1-1500</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>deployment. This will be used to calculate the number of ports to report to the Unified ICM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Server for each gateway.</td>
<td></td>
<td></td>
<td></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>
</tbody>
</table>

### Set Up SIP Service

You must configure the SIP service if you add a new Call Server (Add Unified CVP Call Server, on page 108) or edit a Call Server (Edit Unified CVP Call Server, on page 132), and you use any of these call flow models (Call Services, on page 110):

- Call Director
- Comprehensive

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

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

---

**Step 1**
If you are adding a new Call Server, refer to Add Unified CVP Call Server, on page 108. If you want to change an existing Call Server, see Edit Unified CVP Call Server, on page 132.

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

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

---

**SIP Service Settings**

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

**Configuration**

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

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes and No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Use DNS SRV type query**
Select **Yes** to use DNS SRV for outbound proxy lookup. Otherwise, select **No**. See Load-Balancing SIP Calls, on page 131 for information on using DNS SRV for load-balancing SIP calls.

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

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes and No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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

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

See the Configuration Guide for Cisco Unified Custom Voice Portal for additional information about local SRV configuration.
### SIP Service Settings

**Default** | **Range** | **Restart Required**
---|---|---
None | Enabled or Disabled | No | Yes

**Outbound Proxy Host**

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

**Default** | **Range** | **Restart Required**
---|---|---
No | Valid IP Address | Yes

**Outbound SRV domain name/Server group name (FQDN)**

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

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

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

**DN on the Gateway to Play the Ringtone**

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

To learn the DN configured on the gateway to play ringtone, execute the `sh run` command on the gateway and look for the dial peer that matches the incoming dialed number. See Ringtone Dialed Number Learning on Gateway Example, on page 131.

**Default** | **Range** | **Restart Required**
---|---|---
9191 | Any valid label | No

**DN on the Gateway to Play the Error Tone**

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

To learn the DN configured on the gateway to play the error tone, execute the `sh run` command on the gateway and look for the dial peer that matches the incoming dialed number. See Ringtone Dialed Number Learning on Gateway Example, on page 131.

**Default** | **Range** | **Restart Required**
---|---|---
9292 | Any valid label | No

**Override System Dialed Number Pattern Configuration**

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

**Advanced Configuration**

**Outbound proxy port**
Specify the port to be used.

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>5060</td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>TCP or UDP</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Port number for incoming SIP requests**
Specify the port to be used for incoming SIP requests.

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>5060</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Incoming transport type**
Specifies the incoming transport type.

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP+UDP</td>
<td>TCP, UDP, TCP+UDP</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Time to wait for ICM instructions**
Specifies the wait time in milliseconds for ICM instructions. It is optional value for the list addition.
SIP info tone duration
Specifies the wait time in milliseconds for SIP info tone. It is optional value for the list addition.

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

Generic Type Descriptor (GTD) parameter Forwarding
To be added

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>UUS</td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0-20</td>
<td>No</td>
</tr>
</tbody>
</table>

UDP Retransmission Count
Specifies the number of UDP retransmission will be attempted.

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

Use Error Refer
Flag for play error tone when call fails to caller.

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>False</td>
<td>True or False</td>
<td>Yes</td>
</tr>
</tbody>
</table>

IOS Gateway Options Dynamic Routing

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>True or False</td>
<td>Yes</td>
</tr>
</tbody>
</table>

IOS Gateway Options Reporting
Reports on resource utilization.
### Security Properties

#### Incoming secure port
Specify the port to be used.

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>True or False</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Incoming secure protocol
This option is grayed out as it is prepopulated.

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS</td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

#### Outgoing secure protocol
This option is grayed out as it is prepopulated.

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS</td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

### Supported TLS Versions
This allows to select the versions of TLS to be supported for securing the SIP signaling on the IVR leg. The TLS versions currently supported are TLSv1.0, TLSv1.1, and TLSv1.2.

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS v1.2</td>
<td>TLSv1.0, TLSv1.1, and TLSv1.2</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

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

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

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

Cipher configuration is available only if TLS is enabled.

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>
If you are using CUBE version 16.6 and higher, you must manually change the crypto suite to 128 by enabling CLI on the dial-peer towards CVP as shown:

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

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

### SIP Header Passing (to ICM)

#### Header Name

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

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Maximum length of 210 characters</td>
<td>No</td>
</tr>
</tbody>
</table>

#### Parameter

This field is optional for list addition.

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Maximum length of 210 characters</td>
<td>No</td>
</tr>
</tbody>
</table>

### Local Static Routes

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

#### Dialed Number (DN)

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

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

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

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Dialed number pattern, destination (must be format of NNN.NNN.NNN.NNN or a hostname). See Valid Formats for Dialed Numbers, on page 131 for more information.</td>
<td>No</td>
</tr>
</tbody>
</table>
**IP Address/Hostname/Server Group Name**

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

**Note**

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

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Valid IP address, hostname, or SRV domain name</td>
<td>No</td>
</tr>
</tbody>
</table>

**DIALED NUMBER (DN) PATTERNS**

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

**Patterns for sending calls to the originator:**

**Dialed Number (DN)**

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

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

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

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

*Note*

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

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>See <a href="#">Valid Formats for Dialed Numbers</a> for more information.</td>
<td>No</td>
</tr>
</tbody>
</table>

**Patterns for RNA timeout on outbound SIP calls:**

---

Administration Guide for Cisco Unified Customer Voice Portal, Release 12.0(1)
- Dialed Number (DN)

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

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

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>See Valid Formats for Dialed Numbers, on page 131 for more information.</td>
<td>No</td>
</tr>
</tbody>
</table>

Timeout (Seconds)

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

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

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>60 seconds</td>
<td>5 - 60</td>
<td>No</td>
</tr>
</tbody>
</table>

Custom ringtone patterns:

Dialed Number (DN)

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

To learn the DN configured on the gateway to play ringtone, execute the `sh run` command on the gateway and look for the dial peer that matches the incoming dialed number. See Ringtone Dialed Number Learning on Gateway Example, on page 131.

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>See Valid Formats for Dialed Numbers, on page 131</td>
<td>No</td>
</tr>
</tbody>
</table>

Ringtone Media file name

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

The ringtone media file must be saved to the VXML Gateway. See Transfer Script and Media File to Gateway, on page 180 for more information.
Set Up IVR Service

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

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

Audio call flow models:
  • Call Director, using SIP protocol
  • VRU-Only
  • Comprehensive, using SIP protocol

Post Call Survey DNIS Mapping

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

Incoming Call Dialed Number (DN)

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

Survey Dialed Number (DN)

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

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

None | Dialed Number pattern, destination (must be in the form of NNN.NNN.NNN.NNN or a hostname). See Valid Formats for Dialed Numbers, on page 131 for more information. | No

None | Accepts only alphanumeric characters | No
The IVR Service creates VXML documents that implement the Micro-Applications based on Run Script instructions received by the ICM. The VXML pages are sent to the VXML Gateway to be executed. The IVR Service can also generate external VXML through the Micro-Applications to engage the Unified CVP VXML Server to generate the VXML documents.

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

**Before You Begin**

Configure the following servers before configuring the IVR Service:

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

**Procedure**

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

**Step 1**
If you are adding a new Call Server, refer to Add Unified CVP Call Server, on page 108. If you want to change an existing Call Server, refer to Edit Unified CVP Call Server, on page 132.

**Step 2**
Fill in the appropriate configuration settings as described in IVR Service Settings, on page 125

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

**IVR Service Settings**

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IOS Voice Browser Configuration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Access Timeout (seconds)</td>
<td>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 -2147483647</td>
<td>No</td>
</tr>
<tr>
<td>Media Server Timeout</td>
<td>The number of seconds the Gateway should wait to connect to the HTTP Media Server before timing out.</td>
<td>4</td>
<td>0 -2147483647</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>Media Server Retry Attempts</td>
<td>Maximum number of times the non-Unified CVP Voice Browser (IOS Voice Browser) or Unified CVP VXML Server attempts to connect to an HTTP Media Server to retrieve a single prompt. If the Voice Browser or Unified CVP VXML Server fails after the specified number of times, it will try the same number of times to retrieve the media from a backup media server before failing and reporting an error. The backup media server is defined on the gateway as <code>&lt;mediaserver&gt;-backup</code>.</td>
<td>0</td>
<td>0-2147483647</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 will try the same number of times to connect to a backup ASR/TTS server before failing and reporting an error. (The backup ASR and TTS servers are defined on the gateway as asr-&lt;locale&gt;-backup and tts-&lt;locale&gt;-backup.)</td>
<td>0</td>
<td>0-2147483647</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>0-2147483647</td>
<td>No</td>
</tr>
<tr>
<td>Use Backup ASR/TTS Servers</td>
<td>If you select Yes (default) and an ASR/TTS Server is unavailable, the Gateway attempts to connect to the backup ASR/TTS server.</td>
<td>Yes</td>
<td>Yes or No</td>
<td>No</td>
</tr>
<tr>
<td>Use Backup Media/VXML Servers</td>
<td>If you select Yes (default) and a media server is unavailable, the Gateway attempts to connect to the backup Media Server.</td>
<td>Yes</td>
<td>Yes or No</td>
<td>No</td>
</tr>
</tbody>
</table>
### Property Description

**Use hostnames for default Media/VXML servers**
If you select No (default), the IP address is used for the XML Server and Media Server. If you select Yes, the hostnames are used rather than IP addresses.

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes or No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Use Security For Media Fetches**
If you select No (default), HTTP URLs are generated to media servers.

*Note* The default setting is only applicable if the client is SIP Service and the media server is not set to a URL that explicitly specifies an HTTP/HTTPS scheme.

Select Yes to generate HTTPS URLs to media servers.

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes or No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Advanced Configuration

**Call timeout**
The number of seconds the IVR Service waits for a response from the SIP Service before timing out. This setting should be longer than the longest prompt, transfer or digit collection at a Voice Browser. If the timeout is reached, the call is cancelled but no other calls are affected. The only downside to making the number arbitrarily large is that if calls are being stranded, they will not be removed from the IVR Service until this timeout is reached.

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>7200</td>
<td>Must be 6 seconds or greater</td>
<td>No</td>
</tr>
</tbody>
</table>

**ASR/TTS use the same MRCP server**
Select this option if your ASR and TTS servers are on the same machine. Using this option helps to minimize the number of MRCP connections on the ASR/TTS server.

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes or No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Set Up Infrastructure

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

Step 1  If you are adding a new Call Server, refer to Add Unified CVP Call Server, on page 108. If you want to change infrastructure settings for an existing Call Server, refer to Edit Unified CVP Call Server, on page 132.

Step 2  Fill in the appropriate configuration settings as described in Infrastructure Settings, on page 128.

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

Infrastructure Settings

The following table describes the infrastructure configuration settings.

Table 31: 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>Maximum Threads</td>
<td>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>300</td>
<td>100 to 1000</td>
</tr>
<tr>
<td>Statistics</td>
<td>Statistics Aggregation Interval</td>
<td>Length of time (in minutes) during which system and service statistics are published to the log file and SNMP events are sent. Once published, the counters will reset and aggregate data for the next interval. Note that this is different than the real time snapshot statistics (for the number of concurrent calls). Realtime statistics are on-demand and have no intervals. Statistics Publishing Interval will be used for attributes like the number of calls in last interval, the number of transfers in last interval, and the number of HTTP sessions in last interval.</td>
<td>30 minutes</td>
<td>10 - 1440 minutes</td>
</tr>
<tr>
<td>Log File Properties</td>
<td>Max Log File Size</td>
<td>Maximum size of a log file in Megabytes before a new log file is created.</td>
<td>10 MB</td>
<td>1 through 100 MB</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>Max Log Directory Size</td>
<td>Maximum number of Megabytes to allocate for disk storage for log files.</td>
<td>20000 MB</td>
<td>500 - 500000 MB</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The log folder size divided by the log file size must be less than 5000.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>License Thresholds</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Critical Threshold</td>
<td>Percentage of licenses in use required to reach critical licensing state. See License Thresholds.</td>
<td>97%</td>
<td>Positive integer less than or equal to 100 and greater than the warning threshold.</td>
<td>No</td>
</tr>
<tr>
<td>Warning Threshold</td>
<td>Percentage of licenses in use required to reach warning licensing state. See License Thresholds.</td>
<td>94%</td>
<td>Positive integer less than the critical threshold and greater than the safe threshold.</td>
<td>No</td>
</tr>
<tr>
<td>Safe Threshold</td>
<td>Percentage of licenses in use required to reach safe licensing state. See License Thresholds.</td>
<td>90%</td>
<td>Positive integer less than the warning threshold and greater than 0.</td>
<td>No</td>
</tr>
</tbody>
</table>

**Configuration: Primary Syslog 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 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>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 65535.</td>
<td>No</td>
</tr>
</tbody>
</table>
SIP Transport Setting for UDP

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

### SIP Transport Setting for UDP

<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</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 65535.</td>
<td>No</td>
</tr>
<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 65535.</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>
<tr>
<td>Secondary Backup Syslog Server Port Number</td>
<td>Port number of Secondary 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>
and Retry Timeout settings are not effective when using TCP transport on SIP calls because of the persistent nature of the TCP connection.

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

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

## Load-Balancing SIP Calls

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

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

## Valid Formats for Dialed Numbers

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

- Use the period (.) or the X character for single-digit wildcard matching in any position.
- Use the greater than (), asterisk (*), or exclamation (!) character as a wildcard for 0 or more digits at the trailing end of a DN.
- Do not use the character T for wildcard matching.
- Dialed numbers must not be longer than 24 characters.
- The highest precedence of pattern matching is an exact match, followed by the most specific wildcard match. When the number of characters are matched equally by more than one wildcarded pattern, precedence is given from top to bottom of the configured DN list.

## Ringtone Dialed Number Learning on Gateway Example

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

```
sh run
paramspace english index 0
paramspace english language en
paramspace english location flash
service ringtone flash:ringtone.tcl
paramspace english prefix en
service ringtone
voice-class codec 1
```
License Thresholds

Three thresholds (safe, warning, and critical) describe the percentage of licenses in use required to reach their respective licensing state. If using a license or releasing a license causes the number of licenses currently in use to cross a threshold (in either direction), the state of licensing will be that of the threshold.

This does not always mean the state will change. For example, if there are 100 total licenses and the Safe, Warning, and Critical license thresholds are set to the defaults of 90%, 94%, and 97%, and there are 89 licenses in use, licenses are at a Safe level. When the licenses in use reach 94, license state changes from Safe to Warning level. If one more license is used (95), the license state remains at the Warning level. If three licenses are released (no longer in use), 92 licenses remain in use and the license state remains at the Warning level. Once the licenses in use reach the previous threshold (90), the state changes from Warning to Safe.

Edit Unified CVP Call Server

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

Related Topics

Add Unified CVP Call Server, on page 108
Apply Unified CVP Call Server License, on page 136
Shut Down Server, on page 40
Start Server, on page 40
Upload Log Messages XML File, on page 167
Download Log Messages XML File, on page 165
View Unified CVP Call Server Statistics, on page 134
View Device Status, on page 16

Procedure

To edit a Unified CVP Call Server:

Step 1 Select Device Management > Unified CVP Call Server.
The Find, Add, Delete, Edit window opens.

Step 2 Select a Unified CVP Call Server by clicking the link in the Hostname field or by clicking the radio button preceding it, and then clicking Edit.
The Edit Unified CVP Call Server Configuration window opens with the current settings displayed.

Step 3 If you have not already applied a license to the Unified CVP Call Server, select File Transfer in the toolbar and then click Licenses.
The Licenses page opens. See Applying a License to a Unified CVP Call Server.
Step 4  Change the desired configuration settings on the General tab as described in Unified CVP Call Server Settings, on page 135.
You cannot change the IP Address.

Step 5  Optionally, click the Change Type button to change the services that are turned on for this Unified CVP Call Server.

Step 6  Select the appropriate tab and change the desired settings:
  Configuration Tabs:
  • Set Up ICM Service, on page 112
  • Set Up IVR Service, on page 124
  • Set Up SIP Service, on page 115
  • Add or Remove Device From Device Pool, on page 43
  • Set Up Infrastructure, on page 127

Step 7  When you finish configuring the Unified CVP Call Server, click Save to save the settings, or click Save & Deploy to save the changes and apply them to the Unified CVP Call Server.

Step 8  If you changed a configuration setting that requires a restart, shut down and start the Unified CVP Call Server.
Configuration settings that require a restart of the Unified CVP Call Server are identified in Unified CVP Call Server Settings, on page 135.

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

Procedure
To delete a Unified CVP Call Server:

Step 1  Select Device Management > Unified CVP Call Server.
The Find, Add, Delete, Edit window opens.

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

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

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

To find a Unified CVP Call Server:

Step 1
Select Device Management > Unified CVP Call Server from the Main menu.
The Find, Add, Delete, Edit window lists the available Unified CVP Call Servers sorted by name, 10 at a time.

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

Step 3
You can also filter the list by selecting an attribute such as Hostname, selecting a modifier such as begins with, entering your search term, and then clicking Find.

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

View Unified CVP Call Server Statistics

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

Related Topics
- Unified ICM Service Call Statistics, on page 25
- SIP Service Call Statistics, on page 30
- IVR Service Call Statistics, on page 28
- Infrastructure Statistics, on page 23

Procedure

To view device statistics:

Step 1
Select Device Management > Unified CVP Call Server.
The Find, Add, Delete, Edit window opens.

Step 2
Find the Unified CVP Call Server by using the procedure in Find Unified CVP Call Server, on page 133.

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

Step 4
Click Edit.
The Edit Unified CVP Call Server Configuration window opens with the current settings displayed.

Step 5
Click the Statistics icon in the toolbar.
Statistics are reported for the selected device.
Unified CVP Call Server Settings

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

Table 32: Call Server Configuration Settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></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>
<td></td>
</tr>
<tr>
<td>Hostname</td>
<td>The hostname of the Call Server</td>
<td>None</td>
<td>A valid DNS name, which includes uppercase and lowercase letters in the alphabet, the numbers 0 through 9, and a dash</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>The description of the Call Server</td>
<td>None</td>
<td>0 - 1024 characters</td>
<td>No</td>
<td></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. You must configure secure communications before you enable this option. For more information, see the Configuration Guide for Cisco Unified Customer Voice Portal.</td>
<td>None</td>
<td>Enabled or Disabled</td>
<td>Yes</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>Read Only</td>
<td>Read Only</td>
</tr>
<tr>
<td>Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICM</td>
<td>Enables the Call Server to communicate with an ICM Server. The ICM Server must be configured in the Operations Console.</td>
<td>None</td>
<td>Not applicable</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>IVR</td>
<td>The IVR Service creates VXML pages that implement the Micro-Applications, based on Run Script instructions received from the ICM Server. The VXML pages are sent to the VXML Gateway to be executed.</td>
<td>None</td>
<td>Not applicable</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
### Apply Unified CVP Call Server License

When you are creating a new Unified CVP Call Server, you must apply a valid license file before configuring the server. You can browse and upload the license file to the Operations Console, and then transfer the license to the server. You can select either an existing license file in the Operations Console database or a new license file from your local PC. For more information on licensing, see Unified CVP Licensing, on page 107.

#### Procedure

To apply a license file:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select <strong>Device Management &gt; Unified CVP Call Server</strong>. &lt;br&gt;The Find, Add, Delete, Edit window lists any Unified CVP Call Servers that have been added to the Operations Console.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select a Unified CVP Call Server by clicking the link in the Hostname field or by clicking the radio button preceding it, and then clicking <strong>Edit</strong>. &lt;br&gt;The Edit Unified CVP Call Server Configuration window opens.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select <strong>File Transfer</strong> in the toolbar, and then click <strong>Licenses</strong>. &lt;br&gt;The File Transfer page opens.</td>
</tr>
<tr>
<td>Step 4</td>
<td>If the license file is not listed in the <strong>Select From Available License Files</strong> text box: &lt;br&gt;a) Click <strong>Select a license file from your local PC</strong>. &lt;br&gt;b) Enter the fully qualified file name in the text box or click <strong>Browse</strong> to search for the license file on the local file system.</td>
</tr>
<tr>
<td>Step 5</td>
<td>If the license is listed in the <strong>Select From Available License Files</strong> text box, select the license file.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>Transfer</strong> to transfer the selected license file to the Unified CVP Call Server.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Shut down and start the Unified CVP Call Server.</td>
</tr>
</tbody>
</table>
The Operations console renames the license file to `cvp.license` under the folder on the machine to which the file is transferred. If the file `cvp.license` already exists in the folder, the old `cvp.license` file will be deleted first, and then replaced with the new `cvp.license` file.

**Unified CVP Reporting Server Setup**

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

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

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

You can perform the following tasks:

**Procedure**

- Add Unified CVP Reporting Server
- Edit Unified CVP Reporting Server
- Delete Reporting Server
- Upload Log Messages XML File
- Download Log Messages XML File
- Apply Reporting Server License
- Find Reporting Server
- View Device Status

**Add Unified CVP Reporting Server**

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

**Before You Begin**

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

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

**Procedure**

- Hostname of the Call Servers associated with the Unified CVP Reporting Server
A Call Server can only be associated with one Unified CVP Reporting Server.

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

Procedure

To add a Unified CVP Reporting Server:

Step 1 Select Device Management > Unified CVP Reporting Server.

A window listing Unified CVP Reporting Servers opens.

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

Step 2 Click Add New.

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

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

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

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

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

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

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

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

Related Topics
- Delete Reporting Server, on page 151
- Edit Unified CVP Reporting Server, on page 143
- General Unified CVP Reporting Server Information Setup, on page 138
- Reporting Properties Setup, on page 140
- Add or Remove Device From Device Pool, on page 43
- Unified CVP Reporting Server Infrastructure Settings, on page 140
- Device Information Field Descriptions, on page 104

General Unified CVP Reporting Server Information Setup

You can configure settings that identify the Unified CVP Reporting Server, associate it with one or more Unified CVP Call Servers, and enable or disable security on the General Tab.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the Unified CVP Reporting Server</td>
<td>None</td>
<td>Valid IP address</td>
<td>Yes</td>
</tr>
<tr>
<td>Hostname</td>
<td>The host name of the Unified CVP Reporting Server machine</td>
<td>None</td>
<td>Valid DNS name, which can include letters in the alphabet, the numbers 0 through 9</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>An optional text description for the Unified CVP Reporting Server</td>
<td>None</td>
<td>Up to 1024 characters</td>
<td>No</td>
</tr>
<tr>
<td>Enable Secure Communication</td>
<td>Select to enable secure communications between the Operations Server and this component. The Unified CVP Reporting Server is accessed using SSH and files are transferred using HTTPS. You must configure secure communications before you enable this option. For more information, see the Configuration Guide for Cisco Unified Customer Voice Portal.</td>
<td>Off</td>
<td>On or Off</td>
<td>No</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>Read Only</td>
</tr>
</tbody>
</table>
### Reporting Properties Setup

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

**Table 34: 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(s).</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 used to record the data feed messages during a database failover. This can be limited by the amount of free disk space.</td>
<td>100</td>
<td>1 through 250 MB</td>
<td>No</td>
</tr>
</tbody>
</table>

### Unified CVP Reporting Server Infrastructure Settings

The Unified CVP Reporting Server publishes statistics on the number of reporting events received from the Unified CVP VXML Server, the SIP Service, and the IVR Service. It also publishes the number of times the Reporting Server writes data to the Reporting database. You can configure the interval at which the Reporting Server publishes these statistics, the maximum log file and directory size, and the details for recording syslog messages on the Reporting Server Infrastructure tab.
<table>
<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: 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>525</td>
<td>100 - 525</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 Unified CVP Reporting Server publishes statistics at this interval.</td>
<td>30 minutes</td>
<td>10 - 1440</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Log File Properties</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Max Log File Size            | (Required) Maximum size of the log file in megabytes. The log file name follows this format: CVP.DateStamp.SeqNum.log  
For example: CVP.2006-07-04.00.log  
After midnight each day, a new log file is automatically created with a new date stamp. When a log file exceeds the max log file size, a new one with the next sequence number is created, for example, when CVP.2006-07-04.00.log reaches 5 Mb, CVP.2006-07-04.01.log is automatically created. | 10 MB | 1 through 100 MB | Yes              |
<p>| Max Log Directory Size       | (Required) Maximum size of the directory containing Unified CVP Reporting Server log files.                                                                                                                   | 20000 MB | 500 - 500000 MB | Yes              |
| 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.                                  |         |          |                  |
| <strong>Configuration: Primary Syslog Settings</strong> |                                                                                                                                                                                                             |         |          |                  |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</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 a CVP Application.</td>
<td>None</td>
<td>Valid IP address or hostname.</td>
<td>No</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 65535.</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 65535.</td>
<td>No</td>
</tr>
</tbody>
</table>

**Configuration: Secondary Syslog 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>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 65535.</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>
<tr>
<td>Secondary Backup Syslog Server Port Number</td>
<td>Port number of Secondary 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>
Edit Unified CVP Reporting Server

Procedure

To edit a Unified CVP Reporting Server:

**Step 1**
Select Device Management > Unified CVP Reporting Server.
The Find, Add, Delete, Edit window opens.

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

**Step 3**
If you have not already applied a license, select File Transfer in the toolbar and then click **Licenses**.
The File Transfer page opens.

**Step 4**
On the **General** tab, change the desired general information. You cannot change the IP address of the Reporting Server.

**Step 5**
Select the **Reporting Properties** tab and edit the reporting properties.

**Step 6**
Optionally, you can select the **Device Pool** tab and add or remove the Reporting Server from a device pool.

**Step 7**
Optionally, you can select the **Infrastructure** tab and change log file and syslog settings.

**Step 8**
When you finish configuring the Unified CVP Reporting Server, click **Save** to save the settings in the Operations Console database. Click **Save & Deploy** to deploy the changes to the Unified CVP Reporting Server.

---

**Related Topics**

- Delete Reporting Server, on page 151
- Add Unified CVP Reporting Server, on page 137
- Reporting Properties Setup, on page 140
- Add or Remove Device From Device Pool, on page 43
- Find Reporting Server, on page 152
- Device Information Field Descriptions, on page 104

---

**Change Reporting Database User Password**

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

**Procedure**

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

**Procedure**

To change a reporting database user password:
Step 1  Select Device Management > Unified CVP Reporting Server.
The Find, Add, Delete, Edit window opens.

Step 2  Select a Reporting Server by clicking the link in the Hostname field or by clicking the radio button preceding it, and then clicking Edit.
The Edit Reporting Server Configuration window opens with the current settings displayed.

Step 3  Select the Database Administration menu in the toolbar, then select Change User Passwords.
The Reporting Server: Change User Passwords page opens, displaying the IP address and hostname for the currently selected Reporting Server.

Step 4  In the User field, use the drop-down menu to select the user whose password you want to change.
Step 5  In the Old Password field, enter the existing password for that user.
Step 6  In the New Password field, enter the new password.
        Note  Passwords must follow guidelines for secure passwords.
Step 7  In the Reconfirm Password field, retype the new password.
Step 8  Click Save & Deploy to save the changes to the Operations Console database and deploy them to the Reporting Server.

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

Add New Reporting Users
To add a new reporting user to the Reporting Server:

Step 1  Select Device Management > Unified CVP Reporting Server.
The Find, Add, Delete, Edit window opens.

Step 2  Select a Reporting Server by clicking the link in the Hostname field or by clicking the radio button preceding it, and then clicking Edit.
You can also search for a Reporting Server.
The Edit Reporting Server Configuration window opens.

Step 3  Select the Database Administration menu in the toolbar, and then select Manage Reporting Users.
The Reporting Server: Manage Users windows opens, listing the IP address and hostname for the selected Reporting Server.

Step 4  In the Manage Users pane, click Add User.
Step 5  Enter the name for the user in the Username field.
Step 6  Enter a password for the new user in the Password field.
Step 7  
Retype the password in the **Reconfirm Password** field.

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

---

**Change Reporting User Password**

To change a reporting user's password:

---

**Step 1**  
Select **Device Management > Unified CVP Reporting Server**.  
The Find, Add, Delete, Edit window opens.

**Step 2**  
Select a Reporting Server by clicking on the link in the Hostname field or by clicking the radio button preceding it, and then clicking **Edit**.  
You can also search for a Reporting Server.  
The Edit Reporting Server Configuration window opens.

**Step 3**  
Select the **Database Administration** menu in the toolbar, and then select **Manage Reporting Users**.  
The Reporting Server: Manage Users window opens, listing the IP address and hostname for the currently selected Reporting Server.

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

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

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

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

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

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

---

**Remove Reporting Users**

To remove a reporting user from the Reporting Server:

---

**Step 1**  
Select **Device Management > Unified CVP Reporting Server**.  
The Find, Add, Delete, Edit window opens.

**Step 2**  
Select a Reporting Server by clicking on the link in the Hostname field or by clicking the radio button preceding it, and then clicking **Edit**.  
You can also search for a Reporting Server.  
The Edit Reporting Server Configuration window opens.

**Step 3**  
Select **Database Administration** in the toolbar, then select **Manage Reporting Users**.  
The Reporting Server: Manage Users window opens, listing the IP address and hostname for the currently selected Reporting Server.
**Run Reporting Database Backup**

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

**Procedure**

To run a reporting database backup:

**Step 1**
Select Device Management > Unified CVP Reporting Server. The Find, Add, Delete, Edit window opens.

**Step 2**
Select a Reporting Server by clicking the link in the Hostname field or by clicking the radio button preceding it and then clicking Edit. The Reporting Server Configuration window opens with the current settings displayed.

**Step 3**
Select the Database Administration menu in the toolbar, then select Reporting Database Backups. The Reporting Server - Database Backup Activities page opens. The IP address and host name for the currently selected Reporting Server are listed.

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

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

**Related Topics**
- Change Reporting Database User Password, on page 143
- Set Up Reporting Database Delete, on page 147
- Cancel Reporting Database Backup, on page 146
- Reporting User Management, on page 144
- View Database Details, on page 149
- View Reporting Statistics, on page 150

**Cancel Reporting Database Backup**

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

To cancel a reporting database backup:

Step 1  Select Device Management > Unified CVP Reporting Server. 

The Find, Add, Delete, Edit window opens.

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

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

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

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

Step 4  Click Cancel Daily Backups. 

Step 5  Enter your cvp_dbadmin Password and Save & Deploy.

Related Topics

Change Reporting Database User Password, on page 143
Set Up Reporting Database Delete, on page 147
Reporting User Management, on page 144
View Database Details, on page 149
View Reporting Statistics, on page 150

Set Up Reporting Database Delete

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

Procedure

To configure Reporting Database Delete settings:

Step 1  Select Device Management > Unified CVP Reporting Server. 

The Find, Add, Delete, Edit window opens.

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

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

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

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

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

Step 5  Select the hours and minutes to run the delete each day.
Step 6 Enter your cvp_dbadmin password and click **Save & Deploy**.

---

**Related Topics**
- Run Reporting Database Backup, on page 146
- Cancel Reporting Database Backup, on page 146
- Change Reporting Database User Password, on page 143
- Reporting User Management, on page 144
- View Database Details, on page 149
- View Reporting Statistics, on page 150

---

**Reporting Data Category Deletion**

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

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

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

**Table 36: Number of Days to Retain Data Before Purging**

<table>
<thead>
<tr>
<th>Data Category</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call</td>
<td>Detailed information about calls received by Unified CVP.</td>
<td>30</td>
</tr>
<tr>
<td>Call Event</td>
<td>Call state change event messages published by the Call Server and Unified CVP VXML Server. SIP and IVR services publish call state change event messages when a SIP call changes its state. These states include call initiated, transferred, terminated, aborted, or an error state.</td>
<td>30</td>
</tr>
<tr>
<td>VXML Session</td>
<td>VXML session data includes application names, session ID, and session variables. Session variables are global to the call session on the Unified CVP VXML Server. Unlike element data, session data can be created and modified by all components (except the global error handler, hotevents, and XML decisions).</td>
<td>30</td>
</tr>
<tr>
<td>VXML Element</td>
<td>A VXML element is a distinct component of a voice application call flow whose actions affect the experience of the caller. A VXML element contains detailed script activity to the element level, such as, Call Identifiers, activity time stamp, VXML script name, name and type of the VXML element, and event type.</td>
<td>15</td>
</tr>
</tbody>
</table>
### Data Category | Description | Default
--- | --- | ---
VXML ECC Variable | Expanded Call Context (ECC) variables that are included in VXML data. Unified CVP uses ECC variables to exchange information with Unified ICME. | 15
VXML Voice Interact Detail | Application detailed data at the script element level from the Unified CVP VXML Server call services. This data includes input mode, utterance, interpretation, and confidence. | 15
VXML Session Variable | VXML session variables are global to the call session on the Unified CVP VXML Server. | 15
VXML Element Detail | The names and values of element variables. | 15
Callback | Retention days for Courtesy Callback reporting data | 15
Trunk Utilization Usage | Retention days for Gateway Trunk Utilization reporting data | 15

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

**VXML Session Data Categories:**
- VXML Element
  - VXML ECC Variable
  - VXML Voice Interact Detail
  - VXML Session Variable
  - VXML Element Detail

---

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

---

**View Database Details**

You can view the size of a Reporting database.

**Procedure**

To view database details:

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

The Find, Add, Delete, Edit window opens.

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

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

**Step 3**  
Select the **Database Administration** menu in the toolbar, and then select **Database Details**.
The Reporting Server - Disk Drives: Housing Database Files page opens, displaying the IP address and host name for the currently selected Reporting Server along with the following database information:

**Reporting Database Details:**

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

**Note** When the usage of the database increases beyond 200 GB, it starts occupying the head room space. In this scenario, the free size is shown as 0(zero) bytes.

- **Free size (MB)** - Amount of space that has not been taken by extents.
- **Used Size (MB)** - Data space used.
- **Extent size (MB)** - Space reserved for tables. This size may be greater than the total size.
- **% Free Size** - The percent of space that has not been extended (reserved). This might be greater than 100 percent.

---

**View Reporting Statistics**

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

**Procedure**

To get Reporting Server statistics:

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

The Find, Add, Delete, Edit window opens.

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

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

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

The **Unified CVP Reporting Server Statistics, on page 37** are listed in the Reporting tab.

---

**Related Topics**

- Run Reporting Database Backup, on page 146
- Cancel Reporting Database Backup, on page 146
- Change Reporting Database User Password, on page 143
- Set Up Reporting Database Delete, on page 147
- Reporting User Management, on page 144
- View Reporting Statistics, on page 150

---

**View Reporting Statistics**

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

**Procedure**

To get Reporting Server statistics:

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

The Find, Add, Delete, Edit window opens.

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

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

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

The **Unified CVP Reporting Server Statistics, on page 37** are listed in the Reporting tab.

---

**Related Topics**

- Run Reporting Database Backup, on page 146
- Cancel Reporting Database Backup, on page 146
Delete Reporting Server

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

Procedure

To delete a reporting server:

**Step 1** Select **Device Management > Unified CVP Reporting Server**. The Find, Add, Delete, Edit window displays.

**Step 2** Find the Reporting Server to delete by using the procedure in **Find Reporting Server, on page 152**.

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

**Step 4** Click **Delete**.

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

**Related Topics**

Add Unified CVP Reporting Server, on page 137

Apply Reporting Server License

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

**Related Topics**

Unified CVP Licensing, on page 107

Find Device, on page 105

Procedure

To apply a license file:

**Step 1** Select **Device Management > Unified CVP Reporting Server**. The Find, Add, Delete, Edit window lists any Reporting Servers that have been added to the Operations Console.

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

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

Procedure

To find a Reporting Server:

Step 1  Choose Device Management > Unified CVP Reporting Server.
A list of the available Reporting Servers appears, 10 devices per screen, sorted by name.

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

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

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

Unified CVP VXML Server Setup

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

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

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

You can perform the following tasks:

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

Add Unified CVP VXML Server

Before You Begin

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

Procedure

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

Note

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

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

Procedure

To add a Unified CVP VXML Server:
Step 1  Choose **Device Management > Unified CVP VXML Server**.
The Find, Add, Delete, Edit Unified CVP VXML Servers window opens.

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

Step 2  Click **Add New**.
The Unified CVP VXML Server Configuration window opens to the General Tab.

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

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

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

Configuration tabs:
- Unified CVP VXML Server Configuration Properties, on page 157
- Unified CVP VXML Server Infrastructure Settings, on page 159
- Add or Remove Device From Device Pool, on page 43

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

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

**Related Topics**
- Unified CVP VXML Server General Properties, on page 156
- Unified CVP VXML Server Configuration Properties, on page 157
- Unified CVP VXML Server Infrastructure Settings, on page 159
- Add or Remove Device From Device Pool, on page 43
- Shut Down Server, on page 40
- Start Server, on page 40

**Edit Unified CVP VXML Server**

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

**Procedure**

To edit a Unified CVP VXML Server configuration:

Step 1  Choose **Device Management > Unified CVP VXML Server**.
The Find, Add, Delete, Edit Unified CVP VXML Servers window opens.

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

Step 3  From the list of matching records, choose the Unified CVP VXML Server that you want to edit.
Step 4  Click **Edit**.
The Unified CVP VXML Server Configuration window opens to the General Tab.

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

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

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

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

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

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

## Related Topics
- [Delete Unified CVP VXML Server](#), on page 155
- [Add Unified CVP VXML Server](#), on page 153
- [Unified CVP VXML Server Configuration Properties](#), on page 157
- [Unified CVP VXML Server General Properties](#), on page 156
- [Unified CVP VXML Server Infrastructure Settings](#), on page 159
- [Find Unified CVP VXML Server](#), on page 169
- [Shut Down Server](#), on page 40
- [Start Server](#), on page 40
- [Device Information Field Descriptions](#), on page 104

## Delete Unified CVP VXML Server

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

### Procedure

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

**Step 1**  Choose **Device Management > Unified CVP VXML Server**.
The Find, Add, Delete, Edit Unified CVP VXML Servers window opens.

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

**Step 3**  Click **Delete**.

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

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

## Related Topics
- [Add Unified CVP VXML Server](#), on page 153
- [Transfer Script and Media Files](#), on page 14
Unified CVP VXML Server General Properties

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

Table 37: Unified CVP VXML Server General Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart/Reboot Needed</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 Unified CVP VXML Server</td>
<td>None</td>
<td>A valid IP address</td>
<td>No</td>
</tr>
<tr>
<td>Hostname</td>
<td>The host name of the Unified CVP VXML Server. Host names must be valid DNS names, which can include letters in the alphabet, the numbers 0 through 9, and a dash.</td>
<td>None</td>
<td>A valid DNS name, which includes uppercase and lowercase letters in the alphabet, the numbers 0 through 9, and a dash.</td>
<td>No</td>
</tr>
<tr>
<td>Description</td>
<td>The Unified CVP VXML Server description</td>
<td>None</td>
<td>Up to 1,024 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 Server and this component. The device is accessed using SSH and files are transferred using HTTPS. Configure secure communications before you enable this option. For more information, see the Configuration Guide for Cisco Unified Customer Voice Portal.</td>
<td>None</td>
<td>On or Off</td>
<td>Yes - reboot</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>Read Only</td>
</tr>
</tbody>
</table>

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

**Important**

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

## Unified CVP VXML Server Configuration Properties

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

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

**Table 38: Unified CVP VXML Server Configuration Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart/Reboot Needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Default</td>
<td>Range</td>
<td>Restart/Reboot Needed</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>---------</td>
<td>-------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Enable Reporting for this Unified CVP VXML Server</td>
<td>Indicates whether or not the Unified CVP VXML Server sends data to the Reporting Server. If disabled, no data is sent to the Reporting Server, and reports do not contain any VXML application data.</td>
<td>Enabled</td>
<td>Enabled (the default) or Disabled.</td>
<td>No</td>
</tr>
<tr>
<td>Enable Reporting for VXML Application Details</td>
<td>Indicates whether VXML application details are reported.</td>
<td>Disabled</td>
<td>Enabled or Disabled (the default).</td>
<td>No</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>
</tbody>
</table>

**VXML Applications Details: Filters**

| Inclusive Filters | List of applications, element types, element names, and element fields, and ECC variables to include in reporting data. | None | A semicolon-separated list of text strings. A wildcard character (*) is allowed within each element in the list. | Yes - Restart VXML Server |

**Note** For information about filter syntax and rules, see Inclusive and Exclusive VXML Reporting Filter Examples, on page 163.
# Unified CVP VXML Server Infrastructure Settings

**Table 39: VXML Server Infrastructure 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: 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 VXML Server Java Virtual Machine.</td>
<td>525</td>
<td>100 - 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 VXML Server publishes statistics at this interval.</td>
<td>30 minutes</td>
<td>10 - 1440</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Log File Properties</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Max Log File Size

(Required) Maximum size of the log file in Megabytes. The log file name follows this format:
CVP.DateStamp(SeqNum).log

**Example:**
CVP.2006-07-04.00.log

After midnight each day, a new log file is automatically created with a new date stamp. Also, when a log file exceeds the max log file size, a new one with the next sequence number is created, for example, when CVP.2006-07-04.00.log reaches 5 MB, CVP.2006-07-04.01.log is automatically created.

**Default:** 10 MB

**Range:** 1 through 100 MB

**Restart Required:** Yes

### Max Log Directory Size

(Required) Maximum size of the directory containing VXML Server log files.

**Note:** Modifying the value to a setting that is below the default value might cause logs to be rolled over quickly. Consequently, log entries might be lost, which can affect troubleshooting.

**Default:** 20,000 MB

**Range:** 500 - 500000 MB

**Restart Required:** Yes

---

### Configuration: Primary Syslog 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>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>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 65535.</td>
<td>No</td>
</tr>
</tbody>
</table>
### Inclusive and Exclusive VXML Reporting Filters

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

Data feed control is crucial for:
- Saving space in the reporting database.
- Preserving messaging communication bandwidth.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<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 65535.</td>
<td>No</td>
</tr>
</tbody>
</table>

#### Configuration: Secondary Syslog 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>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 65535.</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>
<tr>
<td>Secondary Backup Syslog Server Port Number</td>
<td>Port number of Secondary 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>
Procedure

To configure inclusive and exclusive filters for a Reporting Server:

Step 1
Choose Device Management > Unified CVP VXML Server.
The Find, Add, Delete, Edit Unified CVP VXML Servers window opens.

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

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

Step 4
Click Edit.
The Unified CVP VXML Server Configuration window opens to the General Tab.

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

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

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

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

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

Related Topics

- VXML Inclusive and Exclusive Filter Rules, on page 162
- Inclusive and Exclusive VXML Reporting Filter Examples, on page 163

VXML Inclusive and Exclusive Filter Rules

Inclusive and exclusive filters operate using the following rules:

- Filters are case sensitive.

- By default, all items except the Start, End, Subdialog_Start and Subdialog_End elements are filtered from reporting data unless they are added to an Inclusive Filter. The Subdialog_Start and Subdialog_End elements are never filtered from reporting data unless Reporting is disabled on the Unified CVP VXML Server.

- The Exclusive Filter takes precedence over the Inclusive Filter. For example, if an application name is in the Exclusive Filter, then the items of that applications are excluded from reporting data even if a particular field or element is listed in the Inclusive filter.

- The syntax for Inclusive/Exclusive filters is:
  Appname.ElementType.ElementName.FieldName
  or
  AppName.*.*.SESSION:Varname

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

**VXML FilterWildcard Matching Examples**

The table below provides examples of VXML filter wildcard matching.

*Table 40: Examples of 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>.</em>.var*</td>
<td>Matches all fields in MyApplication that start with the string var</td>
</tr>
<tr>
<td>MyApplication.<em>.</em>.*</td>
<td>Matches all fields in MyApplication that end with 3</td>
</tr>
<tr>
<td>MyApplication.<em>.</em>.SESSION:Company</td>
<td>Matches the Company session variable in MyApplication</td>
</tr>
</tbody>
</table>

**Inclusive and Exclusive VXML Reporting Filter Examples**

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

*Table 41: Examples of Inclusive and Exclusive VXML Filters for Reporting*

<table>
<thead>
<tr>
<th>Inclusive Filter</th>
<th>Exclusive Filter</th>
<th>Data the Unified CVP VXML Server Feeds To the Reporting Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application1.<em>.</em>.*</td>
<td>None</td>
<td>All Application1 data</td>
</tr>
<tr>
<td>Application1.<em>.</em>.*</td>
<td><em>.Element1.</em>;</td>
<td>All Application1 data, except Element1 and Element2</td>
</tr>
<tr>
<td></td>
<td><em>.Element2.</em></td>
<td></td>
</tr>
<tr>
<td>Application1.<em>.</em>.*</td>
<td><em>.Element1.</em>;</td>
<td>All Application1 data, except Element1, Element2, and Field1</td>
</tr>
<tr>
<td></td>
<td><em>.Element2.</em>;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>*.Field1</td>
<td></td>
</tr>
<tr>
<td>Application1.<em>.</em>.*</td>
<td><em>.voice.</em>.* which matches Element3 and Element4</td>
<td>All Application1 data, except Element3 and Element4</td>
</tr>
</tbody>
</table>
Data the Unified CVP VXML Server Feeds To the Reporting Server

<table>
<thead>
<tr>
<th>Inclusive Filter</th>
<th>Exclusive Filter</th>
<th>Data the Unified CVP VXML Server Feeds To the Reporting Server</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>*.Element1.*;</code></td>
<td><code>Application1.*.*</code></td>
<td>No data for Application1. Other Data for other applications, such as Application2, which contain Element1, Element2 and Field1, will be fed.</td>
</tr>
<tr>
<td><code>*.Element2.*;</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>*.Field1</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>*.voice.*.* which matches Element1, Element2, Element3, and Element4</code></td>
<td><code>*.Element3.*;</code></td>
<td>Only Element1 and Element2 and all applications.</td>
</tr>
<tr>
<td></td>
<td><code>*.Element4.*</code></td>
<td></td>
</tr>
<tr>
<td><code>*.voice.*.* which matches Element1 and Element2</code></td>
<td><code>*.Field1</code></td>
<td>Element1 and Element2, except for Field1, if it exists in those elements</td>
</tr>
<tr>
<td><code>*.Element1.*</code></td>
<td><code>None</code></td>
<td>Element1</td>
</tr>
<tr>
<td><code>*.Element1.*</code></td>
<td><code>*.Field1</code></td>
<td>Element1, except for Field1 if it exists in Element1</td>
</tr>
<tr>
<td><code>*.Field1</code></td>
<td><code>*.Element3.*;</code></td>
<td>Field1 in any elements except Element3 and Element4</td>
</tr>
<tr>
<td></td>
<td><code>*.Element4.*</code></td>
<td></td>
</tr>
</tbody>
</table>

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

- First, create an inclusive filter to include all information:
  ```
  MyApp.voice.*.*
  ```
- Then, create an exclusive filter to remove credit card and social security numbers information:
  ```
  MyApp.voice.*.CreditCard; MyApp.voice.*.SSN
  ```

### VXML Application File Transfers

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

To create an Archive file using Call Studio:

1. Right-click on a project in the Navigator view, and choose **Deploy**.
2. Under Deploy Destination, choose **Archive File**.
3. Enter the location and filename of the destination file in the **Archive File text** field.

**Note**

The filename must end with a ".zip" extension.
4. Click **Finish**.

Transferring a file is a two-step process:

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

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

1. From the main menu, select **Device Management > Unified CVP VXML Server (standalone)**. The Find, Add, Delete, Edit window lists any servers that have been added to the Operations Console.
2. Select a server by clicking on the link in its Hostname field or by clicking the radio button preceding it and then clicking **Edit**.
3. Select **File Transfer > VXML Applications** in the toolbar and then click **Applications**.
   - The VXML Application File Transfer page opens, listing the host name and IP address for the selected device. VXML applications currently stored in the Operations Server database are listed in the Select From available VXML applications box.
4. If the VXML application is not listed in the Select From available VXML application files box: Click **Select a VXML application file from Your Local PC**. Click **Browse** to search for the VXML application on the local file system.
5. If the VXML application is listed in the Select From available VXML applications box, select the VXML application.
6. Click **Transfer** to send the file to the device.
   - The VXML application is transferred to the selected server.

### Download Log Messages XML File

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

**Procedure**

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

---

**Step 1**

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

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

**Step 2**

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

**Step 3**

Select **File Transfer** in the toolbar and then click **Log Messages XML File Download**.

   - The Log Messages XML Download dialog box opens.

**Step 4**

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

### Edit Log Messages XML File

The log messages XML file, `CVPLogMessages.xml`, defines the severity, destination (SNMP management station or Syslog server) and possible resolution for Unified CVP log messages. This file also identifies an event type identifier and message text identifier for each event. The text for these identifiers is stored in the resource properties file, `CVPLogMessagesRes.properties`.

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

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

<table>
<thead>
<tr>
<th>Message Element</th>
<th>Possible Values</th>
<th>What it Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td><code>Resource=&quot;identifier&quot;</code></td>
<td>Identifies the event type described in the <code>CVPLogMessagesRes.properties</code> file.</td>
</tr>
<tr>
<td>Body</td>
<td><code>Resource=&quot;identifier&quot;</code></td>
<td>Identifies the message text described in the <code>CVPLogMessagesRes.properties</code> file.</td>
</tr>
<tr>
<td>Severity</td>
<td>0 to 6</td>
<td>Identifies the severity level of the event. See <a href="#">Unified CVP Event Severity Levels</a>, page 167.</td>
</tr>
<tr>
<td>SendToSNMP</td>
<td>True or false</td>
<td>Set to true, to send this message, when logged, to an SNMP manager, if one is configured.</td>
</tr>
<tr>
<td>SendToSyslog</td>
<td>True or false</td>
<td>Set to true to send this message, when logged, to a Syslog server, if one is configured.</td>
</tr>
</tbody>
</table>
### Unified CVP Event Severity Levels

The following table describes the available severity levels for Unified CVP events. You can set the severity level for an event by editing the log messages XML file, CVPLogMessages.xml, on the server that generates events. For instructions on editing this file, see [Edit Log Messages XML File, on page 166](#).

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

### Upload Log Messages XML File

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

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

**Step 1**  From the Device Management menu, select the type of server to which you want to upload a syslog XML file. For example, to upload a file to a Unified CVP VXML Server, select **Device Management > Unified CVP VXML Server**. The Find, Add, Delete, Edit window lists any servers that have been added to the control panel.

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

**Step 3**  Select **File Transfer** in the toolbar and then click **Log Messages XML File Upload**. The Log Messages XML Upload page opens.

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

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

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

**Related Topics**

- Upload Log Messages XML File, on page 167
- Edit Log Messages XML File, on page 166
- Shut Down Server, on page 40
- Start Server, on page 40

**Apply Unified CVP VXML Server License**

When you are creating a new Unified CVP VXML Server, you must apply a valid license file before using the server. You can browse for and upload the license file to the Operations Console, and then transfer the license to the Unified CVP VXML Server. Select either an existing license file in the Operations Console database or a new license file from your local PC. For information on licensing, see **Unified CVP Licensing**, on page 107.

Procedure

To apply a license file:

**Step 1**  Select **Device Management > Unified CVP VXML Server**. 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 **Licenses**. The File Transfer page displays, listing the Hostname and IP Address for the currently selected Unified CVP VXML Server.

**Step 4**  If the license file is not listed in the **Select From Available License Files** text box:
a) Click **Select a License File from Your Local PC**.
b) Enter the file name in the text box or click **Browse** to search for the license file on the local file system.

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

**Step 6**  
Click **Transfer** to transfer the selected license file to the selected device.

The license is applied to the selected server.

---

**Related Topics**

Find Unified CVP VXML Server, on page 169

---

**Find Unified CVP VXML Server**

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

**Procedure**

To find a Unified CVP VXML Server:

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

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

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

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

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

---

**Unified CVP VXML Server (Standalone) Setup**

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

You can perform the following tasks:

- Add Standalone Unified CVP VXML Server, on page 170
- Delete Standalone Unified CVP VXML Server, on page 171
- Edit Standalone Unified VXML Server, on page 172
- Find Standalone Unified CVP VXML Server, on page 173
Add Standalone Unified CVP VXML Server

Procedure

To add a Unified CVP VXML Server (standalone):

**Step 1**  
Choose Device Management > Unified CVP VXML Server (Standalone).  
The Find, Add, Delete, Edit Unified CVP VXML Server (standalone) window opens.  
*Note*  
To use an existing Unified CVP VXML Server as a template for creating the new Unified CVP VXML Server, select the Unified CVP VXML Server by clicking the radio button preceding it, and then click Use As Template.

**Step 2**  
Click Add New.  
The Unified VXML Server (standalone) Configuration window opens to the General Tab.

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

Table 42: Unified CVP VXML Server General Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart/Reboot Needed</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 Unified CVP VXML Server</td>
<td>None</td>
<td>A valid IP address</td>
<td>No</td>
</tr>
<tr>
<td>Hostname</td>
<td>The host name of the Unified CVP VXML Server. Host names must be valid DNS names, which can include letters in the alphabet, the numbers 0 through 9, and a dash.</td>
<td>None</td>
<td>A valid DNS name, which includes uppercase and lowercase 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 CVP VXML Server</td>
<td>None</td>
<td>Up to 1,024 characters</td>
<td>No</td>
</tr>
</tbody>
</table>
Delete Standalone Unified CVP VXML Server

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

Procedure

To delete a Unified CVP VXML Server (standalone):

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

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

**Step 2** Select the Unified CVP VXML Server (standalone) by clicking the radio button preceding it and then clicking Delete.

To narrow the list of servers see Find Standalone Unified CVP VXML Server, on page 173.

**Step 3** Click Delete.
**Edit Standalone Unified VXML Server**

**Procedure**

To edit a Unified CVP VXML Server (standalone):

**Step 1**  
Choose **Device Management > Unified CVP VXML Server (Standalone).**  
The Find, Add, Delete, Edit Unified CVP VXML Servers (standalone) window opens.

**Step 2**  
Select a server by clicking on the link in its Hostname field or by clicking the radio button preceding it and then clicking **Edit.**  
The Unified CVP VXML Server (standalone) Configuration window opens to the General Tab.

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

**Table 43: Unified CVP VXML Server General Configuration Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart/Reboot Needed</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 Unified CVP VXML Server.</td>
<td>None</td>
<td>A valid IP address</td>
<td>No</td>
</tr>
<tr>
<td>Note</td>
<td>This field is not editable.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hostname</td>
<td>The host name of the Unified CVP VXML Server. Host names must be valid DNS names, which can include letters in the alphabet, the numbers 0 through 9, and a dash.</td>
<td>None</td>
<td>A valid DNS name, which includes uppercase and lowercase 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 CVP VXML Server</td>
<td>None</td>
<td>Up to 1,024 characters</td>
<td>No</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Default</td>
<td>Range</td>
<td>Restart/Reboot Needed</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>---------</td>
<td>-------</td>
<td>-----------------------</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. You must configure secure communications before you enable this option. For more information, see the <em>Configuration Guide for Cisco Unified Customer Voice Portal</em>.</td>
<td>None</td>
<td>On or Off</td>
<td>Yes - reboot</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>Read Only</td>
</tr>
</tbody>
</table>

**Step 4**

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

**Related Topics**

- Delete Standalone Unified CVP VXML Server, on page 171
- Add Standalone Unified CVP VXML Server, on page 170
- Find Standalone Unified CVP VXML Server, on page 173
- VXML Application File Transfers, on page 164
- Apply Unified CVP VXML Server License, on page 168
- View Device Status, on page 16

**Find Standalone Unified CVP VXML Server**

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

**Related Topics**

- Add Standalone Unified CVP VXML Server, on page 170
- Edit Standalone Unified VXML Server, on page 172
- Delete Standalone Unified CVP VXML Server, on page 171

**Procedure**

To find a Unified CVP VXML Server (standalone):

**Step 1**

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

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

**Step 2**

If the list is long, click the first page, previous page, next page, and last page icons on the bottom right of the window to page through the list. Or, enter a page number in the **Page** field and press enter to go directly to the numbered page.
Step 3 You can also filter the list by selecting an attribute such as Hostname. Then select a modifier, such as begins with, enter your search term, and then click Find.

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

Apply Standalone Unified CVP VXML Server License

When you are creating a new Unified CVP VXML Server (standalone), you can apply a valid license file. If you do not apply a license file then the Unified CVP VXML Server (standalone) is limited to 30 active ports. You can browse for and upload the license file to the Operations Console, and then transfer the license to the Unified CVP VXML Server (standalone). Select either an existing license file in the Operations Console database or a new license file from your local PC. For information on licensing, see Unified CVP Licensing, on page 107.

Procedure

To apply a license file:

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

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

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 Licenses.

The File Transfer page displays, listing the Hostname and IP Address for the currently selected Unified VXML Server (Standalone).

Step 4 If the license file is not listed in the Select From Available License Files text box:

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

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

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

Step 6 Click Transfer to transfer the selected license file to the selected device.

The license is applied to the selected server.

Related Topics

Find Unified CVP VXML Server, on page 169

Gateway Setup

From the Device Management menu, Gateway option, you can add an IOS Gateway to the Operations Console. Once added, you can execute a subset of IOS Gateway commands on the Gateway from the Operations Console.
The Ingress Gateway is the point at which an incoming call enters the Unified CVP solution. It terminates TDM phone lines on one side and implements VoIP on the other side. It also provides for sophisticated call routing capabilities at the command of other Unified solution components. It works with SIP protocols, and also supports MGCP for use with Unified CM.

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

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

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

See Also:
• Add Gateway
• Delete Gateway
• Edit Gateway
• Find Gateway
• Execute IOS Commands on Gateway
• Transfer Script and Media File to Gateway
• View Gateway Statistics
• IOS Setup

Add Gateway

You can add an IOS Gateway to the Operations Console.

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

**Related Topics**

- **IOS Setup**, on page 77
- **Add or Remove Device From Device Pool**, on page 43

**Procedure**

To add a Gateway:

**Step 1**

Select **Device Management > Gateway**.

The Find, Add, Delete, Edit Gateways window opens.
**Step 2**  Click **Add New**.

The Gateway Configuration window opens.

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

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

*Table 44: Gateway Configuration General Settings*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the Gateway</td>
<td>None</td>
<td>Valid IP address</td>
</tr>
<tr>
<td>Hostname</td>
<td>The name of the Gateway</td>
<td>None</td>
<td>Valid DNS name, which can include letters in the alphabet, the numbers 0 through 9, and a dash</td>
</tr>
<tr>
<td>Device Type</td>
<td>The type of Gateway device</td>
<td>None</td>
<td>Valid Gateway devices listed in the drop-down menu</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the Gateway</td>
<td>None</td>
<td>Up to 1,024 characters</td>
</tr>
<tr>
<td>Trunk Group ID</td>
<td>If the Call Server associated with this Gateway has <strong>Enable Gateway Trunk Reporting</strong> checked on the ICM tab, then the Trunk Group ID is used for Gateway trunk reporting. 300</td>
<td>1 to 65535</td>
<td></td>
</tr>
<tr>
<td>Location ID</td>
<td>Read only. The location ID for this Gateway.</td>
<td>Blank if not assigned to a system-level configuration location.</td>
<td>Not editable</td>
</tr>
</tbody>
</table>
Table 45: Gateway Configuration Username and Password Settings

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

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

**Step 4** Optionally, you can select the **Device Pool** tab and add the Gateway to a device pool.
Step 5  When you finish configuring the Gateway, click **Save** to save the configuration.

---

**Delete Gateway**

**Procedure**

To delete a Gateway:

---

**Step 1** Select **Device Management > Gateway**.  
The Find, Add, Delete, Edit Gateways window opens.

**Step 2** Find the Gateway using the procedure in **Find Gateway, on page 180**.

**Step 3** Select the radio button next to the Gateway that you want to delete and click **Delete**.  
If this Gateway is assigned to a system-level configuration location or trunk utilization, then the association must be removed prior to deleting this Gateway.

---

**Edit Gateway**

**Related Topics**
- **Add or Remove Device From Device Pool**, on page 43
- **Execute IOS Commands on Gateway**, on page 182
- **View Gateway Statistics**, on page 181
- **Transfer Script and Media Files**, on page 14

**Procedure**

To edit a Gateway:

---

**Step 1** Select **Device Management > Gateway**.  
The Find, Add, Delete, Edit Gateways window opens.

**Step 2** Find the Gateway using the procedure in **Find Gateway, on page 180**.

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

**Step 4** Click the Gateway name to edit it.  
The **Gateway Configuration** window opens with the current settings displayed on the **General** tab.

**Step 5** Change the appropriate configuration settings.
### Table 46: Gateway Configuration General Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the Gateway.</td>
<td>None</td>
<td>Not editable</td>
</tr>
<tr>
<td>Note</td>
<td>This field is not editable.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hostname</td>
<td>The name of the Gateway</td>
<td>None</td>
<td>Valid DNS name, which can include letters in the alphabet, the numbers 0 through 9, and a dash</td>
</tr>
<tr>
<td>Device Type</td>
<td>The type of Gateway device</td>
<td>None</td>
<td>Valid Gateway devices are listed in the drop-down menu.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the Gateway</td>
<td>None</td>
<td>Up to 1,024 characters</td>
</tr>
<tr>
<td>Trunk Group ID</td>
<td>If the Call Server associated with this Gateway has <strong>Enable Gateway Trunk Reporting</strong> checked on the ICM tab, then the Trunk Group ID is used for Gateway trunk reporting.</td>
<td>300</td>
<td>1 to 65535</td>
</tr>
<tr>
<td>Location ID</td>
<td>Read only. The location ID for this Gateway.</td>
<td>Blank if not assigned to a system-level configuration location.</td>
<td>Not editable</td>
</tr>
<tr>
<td>Enable Secure Communication with the Ops console</td>
<td>Select <strong>On</strong> to enable secure communications between the Operations Server and this component. The device is accessed using SSH and files are transferred using HTTPS. Select only if security is enabled and configured on Gateway. You must configure secure communications before you enable this option. For more information, see the <em>Configuration Guide for Cisco Unified Customer Voice Portal</em>.</td>
<td>None</td>
<td>Enabled or disabled</td>
</tr>
</tbody>
</table>

### Table 47: Gateway Configuration Username and Password Settings

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

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

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

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

---

**Find Gateway**

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

**Procedure**

To find a Gateway:

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

The Find, Add, Delete, Edit Window lists the available Gateways, 10 at a time, sorted by name.

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

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

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

---

**Transfer Script and Media File to Gateway**

You can transfer a single script at a time from the Operations Console to one or more Gateways. If you want to transfer multiple scripts at a time, use the Bulk Administration File Transfer menu option. See **Bulk Administration File Transfer (BAFT)**, on page 227.

**Related Topics**

  Find Gateway, on page 180
Procedure

To transfer scripts between the Operations Console and a Gateway:

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

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

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

The Edit Gateway Configuration window opens.

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

The File Transfer window opens.

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

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

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

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

---

**View Gateway Statistics**

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

**Procedure**

To get Gateway statistics:

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

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

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

The Edit Gateway Configuration window opens to the General tab.

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

The Gateway Statistics Results window opens, displaying the selected statistics. If the statistics fill the display area, use the scroll bar to move forward and backward or up and down in the display. See **View Gateway Statistics, on page 33**.
Execute IOS Commands on Gateway

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

Procedure

To execute a Gateway commands:

- **Step 1**: Select Device Management > Gateway. The Find, Add, Delete, Edit Gateways window opens.
- **Step 2**: If you are editing an existing Gateway configuration, click Edit.
- **Step 3**: Select IOS Commands from the Gateway Configuration toolbar.
- **Step 4**: From the IOS Commands drop-down menu, select an IOS command to execute on the Gateway.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show version</td>
<td>Displays IOS version</td>
</tr>
<tr>
<td>Show startup-config</td>
<td>Displays startup-config</td>
</tr>
<tr>
<td>Show running-config</td>
<td>Displays running-config</td>
</tr>
</tbody>
</table>

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

Speech Server Setup

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

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

**Note**

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

You can perform the following tasks:
Add Speech Server

Procedure

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

Step 1
Select Device Management > Speech Server.
The Find, Add, Delete, Edit Speech Server window opens.

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

Step 2
Click Add New.
The Speech Server Configuration window opens.

Step 3
Fill in the appropriate configuration settings on the General tab as described in Speech Server Configuration Settings.
You can change the settings described in the following table to configure a Speech Server.

Table 49: Speech Server Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Reboot/Rerstart 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 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 in the alphabet, 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 1,024 characters</td>
<td>No</td>
</tr>
</tbody>
</table>
### Related Topics

- **Device Information Field Descriptions**, on page 104
- **Apply Speech Server License**, on page 186

### Delete Speech Server

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

#### Procedure

To delete a Speech Server:

**Step 1** Select **Device Management > Speech Server**. The Find, Add, Delete, Edit Speech Server window opens.

**Step 2** Select the Speech Server by clicking the radio button preceding it and then clicking **Delete**. To narrow the list of servers see **Find Speech Server**, on page 186.
Step 3 When prompted to confirm the delete operation, click **OK** to delete or click **Cancel** to cancel the delete operation.

---

**Edit Speech Server**

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

**Related Topics**

Find Speech Server, on page 186

**Procedure**

To edit a Speech Server:

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

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

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

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

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

**Table 50: Speech Server Configuration Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Reboot/Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<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>Note</td>
<td>This field is not editable.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hostname</td>
<td>The host name of the Speech Server</td>
<td>None</td>
<td>Valid DNS name, includes letters in the alphabet, 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 1,024 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>
</tbody>
</table>
Find Speech Server

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

Procedure

To find a Speech Server:

Step 1 Select Device Management > Speech Server.

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

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

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

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

Apply Speech Server License

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

Procedure

To apply a license file:
**Step 1**
Select **Device Management > Speech Server**.
The Find, Add, Delete, Edit Speech Server window opens.

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

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

**Step 4**
Select **File Transfer** in the toolbar and then click **Licenses**.
The License File Transfer page displays, listing the host name and IP address for the currently selected Speech Server.

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

**Step 6**
If the license file is not listed in the **Select From Available License Files** text box:
- a) Click **Select a License File from Your Local PC**.
- b) Enter the file name in the text box or click **Browse** to search for the license file on the local file system.

**Step 7**
Click **Transfer** to transfer the selected license file to the selected device.
The license is applied to the selected server.

**Related Topics**
Find Speech Server, on page 186

---

**Media Server Setup**

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

When you add and deploy Media Server(s) to the Operations Console, that information gets pushed to all the Call servers. It is similar to how WebServices information gets added to the CVP devices. This automatically populates the media servers in the FTP element of the Studio application. You can designate a default media server.

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

The Media Server must be an IIS web server on a separate machine, with FTP enabled. The Agent Greeting recording script requires the Media Server to have FTP enabled. This is done automatically with Unified CVP as long as the Media Server is configured with Add Media Server, on page 188. If it is not enabled, then make sure that Microsoft FTP Service Startup Type is set to Automatic and the status is Running. Using Tomcat on the Unified CVP VXML server is not a supported configuration as a Media Server, and the FTP element in the recording application fails if the FTP operation fails.
Add Media Server

Procedure

To add a Media Server:

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

**Step 1** Select Device Management > Media Server.
The Find, Add, Delete, Edit window opens.

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

**Step 2** Click Add New.
The Media Server Configuration window opens.

**Step 3** Fill in the appropriate configuration settings on the General tab.
The following table describes the fields that can be configured for a Media Server:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</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 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 RFC 1123 Section 2.1 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 that this media server has FTP Enabled. A media server that has FTP enabled is automatically populated as a session variable to the Unified CVP VXML Server. The default agent greeting recording application automatically uses the media servers defined in CVP OAMP that have FTP enabled to FTP the agent greeting recording.</td>
<td>Disabled</td>
<td>Select the check box to enable this feature.</td>
<td>No Use Test Sign-in button to verify the FTP credentials.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<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.</td>
<td>No Use Test Sign-in button to verify the FTP credentials.</td>
</tr>
<tr>
<td>Username and Password</td>
<td>These fields apply if FTP is enabled and Anonymous Access is disabled. In this case, enter the username and password.</td>
<td>None</td>
<td>Enter a valid username and password.</td>
<td>No Use Test Sign-in button to verify the FTP credentials.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Retype password.</td>
<td>None</td>
<td>Enter valid password.</td>
<td>No Use Test Sign-in button to verify the FTP credentials.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter a new port number or use the default port number (21).</td>
<td>21</td>
<td>Valid ports are 1 to 65535.</td>
<td>No Use Test Sign-in button to verify the FTP credentials.</td>
</tr>
</tbody>
</table>

---

**Step 4** Optionally, you can select the Device Pool tab and add the Media Server to a device pool. See Add and Remove Media Server From Device Pool, on page 192.

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

---

### Delete Media Server

**Procedure**

To delete a Media Server:

---

<table>
<thead>
<tr>
<th>Warning</th>
<th>You will receive a special prompt if you attempt to delete the default Media Server.</th>
</tr>
</thead>
</table>

---

| Note | Whenever you add, edit, or delete a Media Server, click the **Deploy** button to make the change effective. |
Step 1 Select **Device Management > Media Server**.
The Find, Add, Delete, Edit Media Server window opens.

Step 2 Select the Media Server by clicking the radio button preceding it and then clicking **Delete**. To narrow the list of servers see **Find Media Server**, on page 192.

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

**Related Topics**
- **Find Media Server**, on page 192

**Deploy Media Server**

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

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

**Procedure**

To deploy a Media Server to all Call Servers:

Step 1 Select **Device Management > Media Server**.
The Find, Add, Delete, Edit window opens.

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

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

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

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

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

Step 5 Restart the VXML Server.

**Edit Media Server**

**Procedure**

To edit a Media Server:

**Note** Whenever you add, edit, or delete a Media Server, click the **Deploy** button to make the change effective.
Step 1  Select **Device Management > Media Server**.
The Find, Add, Delete, Edit Media Server window opens.

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

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

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<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></td>
<td><strong>Note</strong> This field is not editable.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hostname</td>
<td>The name of the Media Server</td>
<td>None</td>
<td>Follow RFC 1123 Section 2.1 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 that this media server has FTP Enabled. A media server(s) that has FTP enabled is automatically populated as a session variable to the Unified CVP VXML Server. The default agent greeting recording application automatically uses the media servers defined in CVP OAMP that have FTP enabled for FTPping the agent greeting recording.</td>
<td>Disabled</td>
<td>Select the check box to enable this feature.</td>
<td>No, Use Test Sign-in 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.</td>
<td>No, Use Test Sign-in button to verify the FTP credentials.</td>
</tr>
</tbody>
</table>

**Table 52: Media Server Configuration Settings**
Find Media Server

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

**Procedure**

To find a Media Server:

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

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

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

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

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

**Add and Remove Media Server From Device Pool**

**Procedure**

To add or remove a Media Server from a device pool:
Step 1  Select Device Management > Media Server.
The Find, Add, Delete, Edit Media Server window opens.

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

Step 3  Click Edit.

Step 4  Select the Device Pool tab.

Step 5  To add a device to a device pool, select the device pool from the Available pane, and then click the right arrow to move the pool to the Selected pane.

Step 6  To remove a device from a device pool, select the device pool from the Selected pane, and then click the left arrow to move the device pool to the Available pane.

Step 7  Click Save.

View Deployment Status

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

Procedure

To view the status of the Media Server device list:

Step 1  Select Device Management > Media Server.
The Find, Add, Delete, Edit Media Server window opens.

Step 2  Click the Deployment Status button to view the status of the deployment of the default Media Server to each Call Server.
You must select the Deploy button to have the Media Server sent to the Call Servers.

Unified Communications Manager Server Setup

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

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

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

You can perform the following tasks:
Add Unified CM Server

Procedure

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

Table 53: Unified CM 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</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<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 not check that the site exists.</td>
<td>No</td>
</tr>
</tbody>
</table>

Enable Synchronization (See Synchronize Location Information, on page 55 for more information.)

<table>
<thead>
<tr>
<th>Enable synchronization</th>
<th>Select to enable synchronization for location. If enabled, the Operations Console extracts (synchronizes) the Unified CM location information from the Unified CM server.</th>
<th>Disabled</th>
<th>Enabled or Disabled</th>
<th>No</th>
</tr>
</thead>
</table>
### Field Description Default Range Restart Required

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</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>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 when establishing initial contact</td>
<td>8443</td>
<td>1 through 65535</td>
<td>No</td>
</tr>
</tbody>
</table>

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

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

**Step 2**  
Click **Add New**.

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

**Step 3**  
Fill in the appropriate configuration settings.

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

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

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

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

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

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

**Related Topics**

- [Device Information Field Descriptions](#), on page 104
- [Add or Remove Device From Device Pool](#), on page 43
- [Synchronize Location Information](#), on page 55
## Edit Unified CM Server

### Procedure

Use this procedure to edit a Unified CM Server.

See the following table for the Unified CM field descriptions

**Table 54: Unified CM 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>General</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<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><strong>Note</strong></td>
<td>This field is not editable.</td>
<td></td>
<td></td>
<td></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 not check that the site exists.</td>
<td>No</td>
</tr>
<tr>
<td>Enable Synchronization for Location</td>
<td><strong>(See Synchronize Location Information, on page 55 for more information.)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable synchronization</td>
<td>Select to enable synchronization for location. If enabled, the Operations Console extracts (synchronizes) the Unified CM location information from the Unified CM server.</td>
<td>Disabled</td>
<td>Enabled or Disabled</td>
<td>No</td>
</tr>
<tr>
<td>Username</td>
<td>User name to access the Unified CM AXL interface.</td>
<td>None</td>
<td>Valid names include uppercase and lowercase alphabetical letters, the numbers 0 through 9, a dash, and an underscore.</td>
<td>No</td>
</tr>
</tbody>
</table>
### Field | Description | Default | Range | Restart Required
---|---|---|---|---
Password | Password to access the Unified CM AXL interface | None | Any text that follows the requirements for choosing secure passwords. See General User Information Settings, on page 220. | No
Confirm Password | Retype the password to verify that you typed the password correctly | None | Text must match the text entered in the Password field | No
Port | The port to which the Unified CM server connects when establishing initial contact | 8443 | 1 through 65535 | No

**Step 1** Select **Device Management > Unified CM**.
The Find, Add, Delete, Edit Unified ICM Servers window opens.

**Step 2** Select the Unified CM Server that you want to edit. To narrow down the list of servers see Find Unified CM Server, on page 198.

**Step 3** Click **Edit**.
The Edit Unified CM Server Configuration window opens to the General tab with the current settings displayed.

**Step 4** Update the configuration settings as required.
See the Unified CM configuration settings field descriptions table for details.

**Note** Cisco AXL Web Service must be enabled on the Unified CM for synchronization to work.
To enable Cisco AXL Web Service on the Unified CM, perform the following steps:

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

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

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

**Related Topics**
Device Information Field Descriptions, on page 104
Find Unified CM Server, on page 198
Add or Remove Device From Device Pool, on page 43
Synchronize Location Information, on page 55
Delete Unified CM Server

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

Procedure

To delete a Unified CM Server:

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

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

**Step 2** Select the Unified CM Server that you want to delete. To narrow down the list of servers, see Find Unified CM Server, on page 198.

**Step 3** Click Delete.

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

Related Topics

Find Unified CM Server, on page 198
Synchronize Location Information, on page 55

Find Unified CM Server

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

**Related Topics**

Synchronize Location Information, on page 55

Procedure

To find a Unified CM Server:

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

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

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

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

**Note** The filter is not case sensitive, and wildcard characters are not allowed.
Unified ICM Server Setup

Unified CVP provides VoIP routing services for the Unified CCE and Unified CCX products. Unified ICM provides the services to determine where calls should be routed, whether to ACDs, specific agents, or to VRUs, but the routing services themselves must be provided by an external routing client.

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

Add Unified ICM Server

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

Related Topics

Add or Remove Device From Device Pool, on page 43  
Device Information Field Descriptions, on page 104

Procedure

To add an ICM Server:

Step 1  Select Device Management > Unified ICM.

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

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

Step 2  Click Add New.

The Unified ICM Server Configuration window opens.

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

Table 55: Unified ICM 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</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the 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, 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 ICM Server</td>
<td>None</td>
<td>Up to 1,024 characters</td>
<td>No</td>
</tr>
</tbody>
</table>
Step 4  
In the Unified ICM server, enter the information in the Enable Serviceability panel so that Serviceability information for this Unified ICM server is distributed using the web services manager feature of Unified CVP.

Table 56: Unified ICM Serviceability Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Data Range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Admin URL</td>
<td>The URL for the Unified ICM web configuration application.</td>
<td>None</td>
<td>Valid URL</td>
</tr>
<tr>
<td>Enable Serviceability</td>
<td>Check to enable this feature.</td>
<td>N/A</td>
<td>Not Checked</td>
</tr>
<tr>
<td>Username</td>
<td>The username required to sign in to Unified ICM Serviceability.</td>
<td>Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore.</td>
<td>N/A</td>
</tr>
<tr>
<td>Password/Confirm Password</td>
<td>The password required to sign in to Unified ICM Serviceability.</td>
<td>Any text that follows the requirements for choosing secure passwords. See General User Information Settings, on page 220</td>
<td>N/A</td>
</tr>
<tr>
<td>Port</td>
<td>The port on which Serviceability is configured on Unified ICM.</td>
<td>1 - 65535</td>
<td>7890</td>
</tr>
</tbody>
</table>

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

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

Delete Unified ICM Server

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

Related Topics
Find Unified ICM Server, on page 202

Procedure

To delete a Unified ICM Server:
Step 1  Select **Device Management > Unified ICM**.
The Find, Add, Delete, Edit window opens.

Step 2  Select the Unified ICM Server that you want to delete. To narrow the list of servers see Find Unified ICM Server, on page 202.

Step 3  Click **Delete**.

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

### Edit Unified ICM Server

**Related Topics**
- Add or Remove Device From Device Pool, on page 43
- Device Information Field Descriptions, on page 104
- Find Unified ICM Server, on page 202

## Procedure

To edit a Unified ICM Server:

Step 1  Select **Device Management > Unified ICM**.
The Find, Add, Delete, Edit Unified ICM Server window opens.

Step 2  Select the Unified ICM Server that you want to edit. To narrow the list of servers see Find Unified ICM Server, on page 202.

Step 3  Click **Edit**.
The Unified ICM Server Configuration window opens and displays the current settings.

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

<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</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the Unified ICM Server.</td>
<td>None</td>
<td>Valid IP address</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This field is not editable.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hostname</td>
<td>The name of the Unified ICM Server</td>
<td>None</td>
<td>Valid DNS name, 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 ICM Server</td>
<td>None</td>
<td>Up to 1,024 characters</td>
<td>No</td>
</tr>
</tbody>
</table>
Step 5

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Username</td>
<td>The username required to sign in to Unified ICM Serviceability.</td>
<td>N/A</td>
<td>N/A</td>
<td>Not Checked</td>
</tr>
<tr>
<td>Password/Confirm Password</td>
<td>The password required to sign in to Unified ICM Serviceability (for example, the web admin password).</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Port</td>
<td>The port on which Serviceability is configured on Unified ICM.</td>
<td>1 - 65535</td>
<td>7890</td>
<td></td>
</tr>
</tbody>
</table>

Table 57: Unified ICM Serviceability Fields

Step 6
Update the Device Pool tab settings.

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

Find Unified ICM Server

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

Procedure

To find a Unified ICM Server:

Step 1
Select Device Management > Unified ICM.

The Find, Add, Delete, Edit Unified ICM Servers window lists the available Unified ICM Servers.
Step 2 If the list is long, click the first page, previous page, next page, and last page icons on the bottom right of the window to page through the list. Or, you can enter a page number in the Page field and press enter to go to the numbered page.

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

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

SIP Proxy Server Setup

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

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

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

- Cisco Unified SIP Proxy

Add SIP Proxy Server

Related Topics

Add or Remove Device From Device Pool, on page 43
Device Information Field Descriptions, on page 104

Procedure

To add SIP Proxy Server:

Step 1 Select Device Management > SIP Proxy Server.

The Find, Add, Delete, Edit window opens.

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

Step 2 Click Add New.

The SIP Server Configuration window opens.

Step 3 Fill in the appropriate SIP Proxy Server configuration settings on the General tab.
Table 58: SIP Proxy Server 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>IP Address</td>
<td>The IP address of the 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 letters in the alphabet, 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</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 UI validates the URL for URL syntax errors, but no validation for site existence.</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

Table 59: SIP Proxy Server Serviceability Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Data Range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Serviceability</td>
<td>Check to enable this feature.</td>
<td>N/A</td>
<td>Not checked</td>
</tr>
<tr>
<td>Username</td>
<td>The username required to sign in to the proxy server's serviceability.</td>
<td>Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore.</td>
<td>N/A</td>
</tr>
<tr>
<td>Password</td>
<td>For Unified SIP Proxy Only. The password that matches the user password.</td>
<td>Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore.</td>
<td>Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Retype password.</td>
<td>Must match password on the SIP Proxy.</td>
<td>N/A</td>
</tr>
<tr>
<td>Port</td>
<td>The port on which Serviceability is configured on the SIP Proxy.</td>
<td>1 - 65535</td>
<td>8443</td>
</tr>
</tbody>
</table>

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

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

You can change an existing SIP Proxy Server configuration.

Procedure

To edit SIP Proxy Server:

Step 1  Select Device Management > SIP Proxy Server.
The Find, Add, Delete, Edit SIP Servers window opens.

Step 2  Select the SIP Proxy Server that you want to edit. If the list is too long, see Find SIP Proxy Server, on page 206.

Step 3  Click Edit.
The SIP Proxy Server Configuration window opens and displays the current settings.

Step 4  Fill in the appropriate configuration settings on the General tab.

Table 60: SIP Proxy Server 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>IP Address</td>
<td>The IP address of the SIP Proxy Server</td>
<td>None</td>
<td>Valid IP address</td>
<td>Not Applicable</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This field is not editable</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hostname</td>
<td>The host name of the SIP Proxy Server</td>
<td>None</td>
<td>Valid DNS name, includes</td>
<td>Not Applicable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>letters in the alphabet,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>the numbers 0 through 9,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>and a dash</td>
<td></td>
</tr>
<tr>
<td>Device Type</td>
<td>The type of proxy server</td>
<td>Cisco</td>
<td>Cisco Unified SIP Proxy</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 UI validates the URL for URL syntax errors, but no validation for site existence</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

Table 61: SIP Proxy Server Serviceability Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Data Range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Serviceability Checkbox</td>
<td>Check to enable this feature.</td>
<td>N/A</td>
<td>Not Checked</td>
</tr>
</tbody>
</table>
### Related Topics

[Device Information Field Descriptions](#), on page 104

## Delete SIP Proxy Server

Deleting a SIP Proxy Server deletes the configuration of the selected Proxy Server in the Operations Console database and removes the server from displayed list of SIP Proxy Servers.

**Procedure**

To delete a SIP Proxy Server:

1. Select [Device Management > SIP Proxy Server](#).
   
The Find, Add, Delete, Edit SIP Proxy Server window opens.
2. Select the radio button next to the SIP Proxy Server that you want to delete. If the list is too long, see [Find SIP Proxy Server](#), on page 206.
3. Click **Delete**.
4. When prompted to confirm the delete operation, click **OK** or click **Cancel**.

## Find SIP Proxy Server

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

**Procedure**

To find a SIP Proxy Server:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Data Range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username required to sign in to Unified ICM Serviceability.</td>
<td>Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore.</td>
<td>N/A</td>
</tr>
<tr>
<td>User Password/Enable Password</td>
<td>The password required to sign in to SIP Proxy Serviceability.</td>
<td>Must match password on Unified ICM</td>
<td>N/A</td>
</tr>
<tr>
<td>Port</td>
<td>The port on which Serviceability is configured on the SIP Proxy.</td>
<td>1 - 65535</td>
<td>8443</td>
</tr>
</tbody>
</table>

**Step 5**  (Optional) Select the **Device Pool** tab and update the device pool settings.

**Step 6**  When you finish configuring the SIP Proxy Server, click **Save**.
Step 1
Select **Device Management > SIP Proxy Server**.

The Find, Add, Delete, Edit SIP Proxy Servers window lists the available proxy servers of the type you selected, sorted by name, 10 at a time.

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

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

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

---

**Unified IC Server Setup**

The Unified Intelligence Center (Unified IC) Server is a device type in Operations Console for Unified CVP. To support a Unified CVP reporting solution, install and configure a Unified IC Server with the Unified CVP Reporting Server.

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

- Configured Unified IC Servers are listed in the Device Past Configurations table listing. Unified IC Server devices are only saved to the Operations Console database—they are not saved and deployed. Consequently, each Unified IC Server is listed as one past configuration entry.

- The Unified IC Server is a standalone device and is not integrated with Unified CVP. Therefore, the Unified IC Server is not displayed in the Device Versions table.

- A Unified IC Server device is not included as a selectable device in the SNMP menu option windows.

- If you select a Unified CVP Reporting Server for deletion and this server has a Unified IC Server association, a warning message prompts you to remove the association.

---

**Add Unified IC Server**

You can create a new Unified IC Server by using an existing Unified IC Server configuration as a template or by filling in its values from scratch.

**Related Topics**
- Unified IC Server Setup, on page 207
- Edit Unified IC Server, on page 209
- Delete Unified IC Server, on page 210
- Find Unified IC Server, on page 210
Procedure

To add a Unified IC Server to the Operations Console database and associate it with a Unified CVP Reporting Server:

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

All Unified IC Servers that have been added to the Operations Console are listed in the Find, Add, Delete, Edit Unified IC Servers list.

Step 2
Click **Add New**.

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

Step 3
Fill in the appropriate Unified IC Server configuration settings on the **General** tab.

**Table 62: General 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>IP Address</td>
<td>The IP address of the Unified IC</td>
<td>None</td>
<td>Valid IP address</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Hostname</td>
<td>The host name of the Unified IC</td>
<td>None</td>
<td>Valid DNS name, includes</td>
<td>Not Applicable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>letters in the alphabet, the numbers 0 through 9, and a dash</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>The description of the Unified IC</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 Unified IC</td>
<td>None</td>
<td>A valid URL. The UI validates the URL for URL syntax errors, but no validation for site existence</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

**Table 63: Unified IC Server Serviceability Fields**

| Field            | Description                                                      | Data Range                                                          | Default                     |
|------------------|------------------------------------------------------------------|                                                                   |                             |
| Enable Serviceability | Check to enable this feature.                                    | N/A                                                               | Not checked                 |
| Username         | The username required to sign in to the proxy server's serviceability. | Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore. | N/A                         |
| Password         | For Unified SIP Proxy Only. The password that matches the user password. | Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore. | Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore. |
| Confirm Password | Retype password.                                                 | Must match password on the SIP Proxy.                             | N/A                         |
### Field Description | Data Range | Default
--- | --- | ---
Port | The port on which Serviceability is configured on the SIP Proxy. | 1 - 65535 | 8443

**Step 4** Assigning Unified CVP Reporting Servers is optional. One Unified CVP Reporting Server can be assigned to multiple Unified IC Server devices. By associating a Reporting Server, you are tracking that this Reporting Server is being set up as a data source for Unified IC.

**Step 5** Click **Device Pool** to associate the Unified IC Server to a device pool.

The default device pool is automatically assigned to the newly-configured Unified IC Server. You can specifically assign the Unified IC Server to required device pool.

**Step 6** When you finish configuring the Unified IC Server, click **Save** to save the settings in the Operations Console database.

---

### Edit Unified IC Server

While you can edit any existing Unified IC Server device, you cannot change the IP address of a Unified IC Server. The same fields present when adding a Unified IC Server (see *Add Unified IC Server, on page 207*) are also displayed in the edit process.

**Related Topics**
- Unified IC Server Setup, on page 207
- Add Unified IC Server, on page 207
- Delete Unified IC Server, on page 210
- Find Unified IC Server, on page 210

**Procedure**

To edit an existing Unified IC Server:

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

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

**Step 2** Select a Unified IC Server by clicking on the link in its name field or by clicking the radio button preceding it, and then clicking **Edit**. To narrow the list of servers see *Find Unified IC Server, on page 210*.

All fields are pre-populated with existing configuration information if available: IP Address (read-only, required), Hostname (required), Description, Device Admin URL, and Reporting Server Assignment. Serviceability information is also present if configured. See *Add Unified IC Server, on page 207* for details on the fields.

**Step 3** (Optional) Select the **Device Pool** tab to add/remove devices the device pool.

**Step 4** When you finish configuring the Unified IC Server, click **Save** to save the settings in the Operations Console database.
Delete Unified IC Server

One Unified CVP Reporting Server can be assigned to several Unified IC Servers. Before the assigned Unified CVP Reporting Server can be deleted, these associated references in the Unified IC devices must also be removed. When you select a Unified CVP Reporting Server for deletion and that server has a Unified IC Server association, you receive a warning message prompting you to delete all Unified IC Server associations.

You can delete existing Unified IC Servers using the procedure specified in this section.

Related Topics
- Unified IC Server Setup, on page 207
- Add Unified IC Server, on page 207
- Edit Unified IC Server, on page 209
- Find Unified IC Server, on page 210

Procedure

To delete a Unified IC Server:

---

Step 1  Select Device Management > Unified IC.

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

Step 2  Select the required Unified IC Server by clicking the radio button preceding it, and then clicking Delete. To narrow the list of servers see Find Unified IC Server, on page 210.

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

---

Find Unified IC Server

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

Related Topics
- Unified IC Server Setup, on page 207
- Add Unified IC Server, on page 207
- Edit Unified IC Server, on page 209
- Delete Unified IC Server, on page 210

Procedure

To find a Unified IC Server:

---

Step 1  Select Device Management > Unified IC.

The Find, Add, Delete, Edit Unified IC Servers window lists the available Unified IC Servers, sorted by name.

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

You can view the past 10 saved configurations of a selected device that are currently stored in the Operations Console database.

Find Past Device Setup

To find a past configuration for a device, first find the device. As you probably have several devices in your network, the Operations Console lets you locate specific devices on the basis of specific criteria. Use the following procedure to locate a device.

Procedure

To find a past configuration for a device:

Step 1 Select Device Management > Device Past Configurations.
Step 2 If the list is long, click the first page, previous page, next page, and last page icons on the bottom right of the window to page through the list. Or, you can enter a page number in the Page field and press enter to go to the numbered page.
Step 3 You can also filter the list by selecting an attribute such as Hostname. Then select a modifier, such as begins with, enter your search term, and then click Find.
Note The filter is not case-sensitive, and wildcard characters are not allowed.

View Past Device Setup

Procedure

To view the details of a past configuration for a device:

Step 1 Select Device Management > Device Past Configurations.
Step 2 Select the device configuration by clicking the radio button preceding it and then clicking Past Configurations.
The List of Past Configurations window lists the configurations that have been saved for the selected device.
Step 3 Select a device past configuration to view by clicking the link in the description field or by clicking the radio button preceding it, and then clicking View.
Apply Past Device Setup

The Operations Console stores configurations for a device. You can select a previous device configuration and apply it to a device.

Procedure

To apply a past configuration to a device:

Step 1
Select Device Management > Device Past Configurations from the Main menu.

Step 2
Select the device configuration by clicking the radio button preceding it, and then clicking Past Configurations.

The List of Past Configurations window lists the configurations that have been saved for the selected device.

Step 3
Select a device past configuration to view by clicking the link in the description field or by clicking the radio button preceding it, and then clicking View.

Configuration details for the selected past configuration are displayed.

Step 4
Click Save to save the selected configuration to the database.

Note
If this is a Reporting Server, Call Server, VXML Server, Unified CVP VXML Server (standalone), or Speech Server, you must click Save & Deploy.

Device Versions

From the Device Management menu, Device Version option, you can view version information for the Call Server, Reporting Server, Unified CVP VXML Server, and Unified CVP VXML Server (standalone). Device version information is available for CVP specific devices only.

To view version information for CVP device types:

1. Select Device Management > Device Versions.

2. From the Select Device Type drop-down menu, select the CVP device type that you want version information about.

The table refreshes to display devices of the selected type and corresponding version data.
Managing Unified CVP Users

From the User Management menu, Users option, you can create one user account at a time. Unified CVP includes the Super User, Administrator, Read Only, and Serviceability Administration roles. You can assign users to any of these roles. The Unified CVP installation creates an Administrator account, which is assigned to the Super User role and a "wsmadmin" account which is assigned a Serviceability Administration role.

User groups are provided so that you can group users together. Assigning users to groups limits the operations users can perform from the Operations Console menus. For example, administrators for San Jose devices can belong to a user group called SanJose_Admins with Administrator privilege.

Device pools are logical groupings of devices, for example, SanJose-Gateways. If a user is configured with SanJose-Gateways as the device pool, then that user can operate only on devices in this device pool. The types of allowed operations also depends on which user group the user belongs to. For example, if a user belongs to SanJose_Admins, a group with Administrator privilege, then this user has Administrator privilege for devices in the SanJose-Gateways device pool.

Unified CVP includes four categories of access criteria:

- **Super User** - Allows any operation in the Operations Console. Only the Super User can create and delete Administrator accounts and assign device pools to any user. The Super User can view all devices because this account is associated with the "default" device pool.

- **Administrator** - Allows any operation in the Operations Console except deleting Administrator accounts. Administrators can only view devices in the device pools to which they have been associated. Administrators can disassociate themselves from a device pool, but cannot associate themselves to a device pool.

- **Read Only** - Allows read-only access to the Operation Console.

- **Serviceability Administration** - Allows Web Services authentication through the Unified System CLI tool and does not provide any privileges for the Operations Console. Only the Administrator can create and delete Web Services users. Whenever Web Services user information is changed or whenever a Unified CVP device is deployed successfully, the configured Web Services users are pushed to all deployed Unified CVP devices (see Web Services, on page 76).

Users roles that have Serviceability Administration applied cannot have any roles assigned that contain Super User, Administrator, or Read Only privileges.

• **User Role Management**, on page 214  
• **User Group Management**, on page 217  
• **Unified CVP User Setup**, on page 220
User Role Management

A user role is a logical group of privileges, also called access criteria, that determine the operations a user can perform. For example, you might create a role that grants an operator read-only access to the Reporting Server, but grants write access to the Unified CVP VXML Servers. You can do this by creating an operator user group and assigning that group the default Administrator privilege, which allows any operation except deleting accounts with superuser privilege. Then, create a device pool that contains all Unified CVP VXML Servers. Finally, assign the Unified CVP VXML Server device pool to the operator user group.

Add User Role

Related Topics
- Edit User Role, on page 214
- Delete User Roles, on page 216
- Assign Role to User Group, on page 218
- Assign User Role Access Criteria, on page 215
- Find User Role, on page 215

Procedure

To add a user role:

---

Step 1 Select User Management > User Roles from the Main menu.

The Find, Add, Delete, Edit window opens.

Step 2 Select Add New.

Step 3 On the General tab, fill in the name of the role in the Role Name field.

Step 4 Fill in descriptive text in the Description field, if desired.

Step 5 Select the Access Criteria tab and assign access criteria to the user role. See Assign User Role Access Criteria, on page 215.

A default Access Criteria of Administrator is applied to every new user role you create.

Step 6 When you finish configuring the user role, click Save to save the configuration.
---

Edit User Role

Related Topics
- Add User Role, on page 214
- Delete User Roles, on page 216
- Find User Role, on page 215
- Assign User Role Access Criteria, on page 215
Procedure

You can change the access criteria, which are privileges, assigned to a user role that has been added to the Operations Console.

**Step 1** Select **User Management > User Roles** from the Main menu.

The Find, Add, Delete, Edit Application User Roles window opens.

**Step 2** Select the desired Role Name link or select the user role from the list and click **Edit**. If you have a long list of user roles, see **Find User Role**, on page 215.

The Edit Application User Role window opens to the General tab.

**Step 3** Change the description for the user role, if desired.

**Step 4** Select the **Access Criteria** tab and change the access criteria assigned to the user role. See **Assign User Role Access Criteria**, on page 215.

**Step 5** When you finish configuring the user role, select **Save**.

**Assign User Role Access Criteria**

Access criteria are privileges that let users perform one or more operations using the Operations Console. Assign access criteria to a user role when:

**Procedure**

- **Add User Role**, on page 214
- **Edit User Role**, on page 214

**Related Topics**

- **Find User Role**, on page 215
- **Delete User Roles**, on page 216
- **Assign Role to User Group**, on page 218

**Procedure**

To assign access criteria to a user role:

**Step 1** Select **Access Criteria** tab.

**Step 2** Select the desired access criteria.

**Step 3** Click **Save** to save the user role with assigned access criteria to the Operations Console database.

**Find User Role**

The Operations Console lets you locate specific user roles on the basis of specific criteria. Use the following procedure to locate a user role:
Procedure

To find a user role:

---

**Step 1**  
Select User Management > User Roles.  
The Find, Add, Delete, Edit window opens.

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

**Step 3**  
Filter the list by selecting an attribute such as Role Name. Select a modifier, such as begins with. Enter your search term and click Find.

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

---

Delete User Roles

Deleting a user role deletes the configuration of the selected user role in the Operations Console database and removes the user role from the displayed list of user roles.

**Related Topics**

- Add User Role, on page 214
- Edit User Role, on page 214
- Find User Role, on page 215

Procedure

To delete a user role:

---

**Step 1**  
Select User Management > User Roles.  
The Find, Add, Delete, Edit Application User Roles window opens.

**Step 2**  
Find the user roles using the procedure shown in Find User Role, on page 215.

**Step 3**  
From the list of matching records, select the user roles that you want to delete.

**Step 4**  
Select Delete.

**Step 5**  
When prompted to confirm the delete operation, perform one of the following steps:

- Select OK to delete the operation.
- Select Cancel to cancel the operation.

---

Service Types User Roles and User Group Associations

In Unified CVP, the Operations Console allows you to add a new type of user role: a Web Services (Serviceability Administration) user role.
The Operation Console does not support a mix-and-match of various user roles. The existing Operations Console service type user roles (Super User, Administrator, and Read-only users) cannot co-exist with the Web service type user roles (Web Services users) within a single user group.

Whenever you add/modify/delete a Web Services user role, a current list of Web Services users is pushed to all deployed Unified CVP devices.

The end user receives a validation error in the following situations:

- When you edit any user role, the list of user groups associated with this user role are retrieved. If the user role changes and causes a mismatch of user role service types within any of its associated user groups.
- A role changes and causes a mismatch of user role service types within any of its associated users.

Users assigned a Web Services user role cannot log into the Operations Console.

## User Group Management

A user group is a collection of users to which you can assign one or more user roles. These groups limit the operations that users can perform to the Operations Console.

### Add User Group

**Related Topics**

- [Edit User Groups](#), on page 218
- [Assign Role to User Group](#), on page 218
- [Delete User Group](#), on page 219
- [Find User Group](#), on page 219

**Procedure**

To add a User Group:

1. **Step 1** Select **User Management > User Groups**.
   The Find, Add, Delete, Edit Application User Groups window opens.

2. **Step 2** Select **Add New**.

3. **Step 3** Fill in the name of the group in the **Group Name** field.

4. **Step 4** Fill in descriptive text in the **Description** field, if desired.

5. **Step 5** Select the **User Roles** tab and assign a user role to the user group. See [Assign Role to User Group](#), on page 218 for details.
   You must assign at least one user role to each user group you create.

   **Note** You cannot add a Web Service Role and an Operations Console user role to the same user group.

   **Note** Users assigned a Web Service Role cannot log in to the Operations Console.

6. **Step 6** When you finish configuring the user group, select **Save**.
Edit User Groups

You can change one or more settings for a user group that has been added to the Operations Console.

Related Topics
- Add User Group, on page 217
- Delete User Group, on page 219
- Find User Group, on page 219
- Assign Role to User Group, on page 218

Procedure

To edit a User Group:

Step 1
Select User Management > User Groups.
The Find, Add, Delete, Edit User Groups window opens.

Step 2
If you have a long list of user groups, see Find User Group, on page 219 to narrow the list of choices.

Step 3
Select the radio button next to the User Group name and click Edit or click the Group Name. See Assign Role to User Group, on page 218 for details.
The User Group Configuration window opens to the General tab.

Step 4
You can change the description for the group by editing the Description field.

Step 5
Select the User Roles tab and edit the assigned roles for this user group.

Step 6
When you finish configuring the user group, click Save.

Assign Role to User Group

A user role is a named collection of privileges that can be assigned to a user group. You can assign one or more user roles to a user group on the User Role tab. Assign a user role to a user group when you:

Procedure

- Add User Group, on page 217
- Edit User Groups, on page 218

Related Topics
- Find User Group, on page 219
- Delete User Group, on page 219
- Edit User Groups, on page 218
- User Role Management, on page 214

Procedure

To assign a user role to a user group:
Step 1  If you want to add a user role to a user group, select the user role from the Available pane, and then click the right arrow to move the user role to the Selected pane.

Step 2  To remove a user role from a user group, select the user role from the Selected pane, and then click the left arrow to move the user role to the Available pane.

Step 3  Click Save.

Delete User Group

Deleting a user group from the Operations Console deletes the configuration of the selected user group in the Operations Console database and removes the user group from the displayed list of user groups.

Related Topics
- Add User Group, on page 217
- Find User Group, on page 219
- Edit User Groups, on page 218

Procedure

To delete a user group from the Operations Console:

Step 1  Select User Management > User Groups.

The Find, Add, Delete, Edit Application User Groups window opens.

Step 2  Find the groups by using the procedure in Find User Group, on page 219.

Step 3  From the list of matching records, select the user groups that you want to delete.

Step 4  Select Delete.

Step 5  When prompted to confirm the delete operation, perform one of the following steps:
  - Select OK to delete the operation
  - Select Cancel to cancel the delete operation

Find User Group

The Operations Console lets you locate specific user groups on the basis of specific criteria. Use the following procedure to locate a user group.

Procedure

To find a user group:

Step 1  Select User Management > User Groups User Management.

The Find, Add, Delete, Edit Application User Groups Window lists the available user groups.
Step 2
If the list is long, you can perform one of the following steps:

- Select the first page, previous page, next page, and last page icons on the bottom right of the window to page through the list, or
- Enter a page number in the Page field and press Enter to go to the numbered page.

Step 3
To filter the list, perform the following steps:

a) Select an attribute, such as Group Name
b) Select a modified, such as begins with
c) Enter your search term
d) Select Find

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

Unified CVP User Setup

From the User Management menu, Users option, you can create one user account at a time. Unified CVP includes four roles: Super User, Administrator, and Read Only in the Operations Console Server type of role, and Serviceability Administration in the Web Services type of role. You can assign users to any of these roles; however, you cannot assign users to roles that include both the Operations Console type and the web services type. See Assign User Role Access Criteria, on page 215 for information about this restriction.

General User Information Settings

Configure general information about a Unified CVP user when you:

- Add User Account
- Edit User Account

Table 64: User Information 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>Username</td>
<td>Name of the user account. The user logs in to the Operations Console using this name. After logging in, the username is displayed in the upper right portion of the screen. You cannot change the username when editing a user account.</td>
<td>None</td>
<td>Valid names include uppercase and lowercase letters in the alphabet, the numbers 0 through 9, a dash, and an underscore.</td>
<td>No</td>
</tr>
</tbody>
</table>
### Secure Password Requirements

**Note**

Passwords must meet all the following criteria.

Passwords must only contain the following ASCII characters:

- Maximum password length is 80 characters.
- Minimum password length is 12 characters
- The password must contain characters from at least three of the following classes: lowercase characters, uppercase characters, digits, and special characters.
  - Lowercase letters (abcdefghijklmnopqrstuvwxyz)
  - Uppercase letters (ABCDEFGHIJKLMNOPQRSTUVWXYZ)
  - Digits (012345689)
  - Special characters: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
- No character in the password can be repeated more than three (3) times consecutively.
- Password must not repeat or reverse username. Password is not `cisco`, `ocsic`, or any variant obtained by changing the capitalization of letters therein.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>New password for the user account. User must type this password to log into the Operations Console.</td>
<td>None</td>
<td>Any text that follows the Secure Password Requirements</td>
<td>No</td>
</tr>
<tr>
<td>Reconfirm Password</td>
<td>Retype the password for this user account 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>Firstname</td>
<td>(Optional) First name of the user.</td>
<td>None</td>
<td>Valid names include uppercase and lowercase letters in the alphabet, the numbers 0 through 9, a dash, and an underscore.</td>
<td>No</td>
</tr>
<tr>
<td>Lastname</td>
<td>(Optional) Last name of the user.</td>
<td>None</td>
<td>Valid names include uppercase and lowercase letters in the alphabet, the numbers 0 through 9, a dash, and an underscore.</td>
<td>No</td>
</tr>
<tr>
<td>E-mail</td>
<td>(Optional) e-mail address of the user.</td>
<td>None</td>
<td>Valid e-mail address</td>
<td>No</td>
</tr>
<tr>
<td>Signed in User Password</td>
<td>The password used to log into the user account.</td>
<td>None</td>
<td>Valid e-mail address</td>
<td>No</td>
</tr>
</tbody>
</table>
Add User Account

Related Topics
- General User Information Settings, on page 220
- Add or Remove User From Device Pool, on page 224
- Edit User Account, on page 222
- Delete User Account, on page 223
- Find User Account, on page 224
- Add User Role, on page 214
- Add User Group, on page 217

Procedure

Before You Begin
When you are adding a new user for the first time after installing Unified CVP software, you must create at least one user role and user group before creating the user account. For information on performing these tasks, see Add User Role, on page 214, Add User Group, on page 217.

Note
You must create Device Pools to further limit access to devices. See Add Device Pool to Operations Console, on page 42.

To add a user account:

Step 1
Select User Management > Users.
The Find, Add, Delete, Edit Application Users window opens.

Step 2
Select Add New.

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

Step 4
Select the Device Pools tab and assign a Device Pool to the user. Each user must be assigned to at least one device pool. See Add or Remove User From Device Pool, on page 224.

Step 5
Select the User Group tab and add the user to one or more user groups. See Add User Group, on page 217.

Step 6
When you finish configuring the user, click Save.

Edit User Account

Related Topics
- Add User Account, on page 222
- Delete User Account, on page 223
- Find User Account, on page 224
- General User Information Settings, on page 220
- Add or Remove User From Device Pool, on page 224
Procedure

You can change one or more settings for a user account that has been added to the Operations Console.

**Step 1**
Select **User Management** > **Users**.

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

**Step 2**
Select the desired Username link or select radio button next to the username from and select **Edit**. You can reduce the list of users displayed. See *Find User Account, on page 224*.

The Edit User page opens to the General tab.

**Step 3**
Fill in the appropriate configuration settings on the General tab as described in *General User Information Settings, on page 220*.

**Step 4**
Select the Device Pools tab and assign a device pool to the user. See *Add or Remove User From Device Pool, on page 224*.

**Step 5**
Select the User Groups tab and add/remove the user to/from one or more user groups. See *Add User Group, on page 217*.

**Step 6**
When you finish configuring the user, select **Save**.

---

**Delete User Account**

You can delete one or more user accounts from the Operations Console. Deleting a user account from the Operations Console removes the user account data from the Operations Console database and from the displayed list of user accounts.

**Related Topics**

- *Add User Account, on page 222*
- *Find User Account, on page 224*
- *Edit User Account, on page 222*

**Procedure**

To delete a user account:

**Step 1**
Select **User Management** > **Users**.

The Find, Add, Delete, Edit Application Users window opens.

**Step 2**
From the list of users, select the user that you want to delete. You can reduce the list of users displayed. See *Find User Account, on page 224*.

**Step 3**
Select **Delete**.

**Step 4**
When prompted to confirm the delete operation, perform one of the following steps:

- Select **OK** to delete.
- Select **Cancel** to cancel the delete operation.
Find User Account

The Operations Console lets you locate users on the basis of specific criteria. Use the following procedure to locate an Operations Console user account.

**Related Topics**
- Add User Account, on page 222
- Delete User Account, on page 223
- Edit User Account, on page 222

**Procedure**

To find a user:

**Step 1**
Select **User Management > User**.

The Find, Add, Delete, Edit Application Users window opens.

**Step 2**
Perform one of the following steps:
- If the list is long, select the first page, previous page, next page, and last page icons on the bottom right of the window to page through the list.
- Enter a page number in the **Page** field and press Enter to go directly to the numbered page.

**Step 3**
Filter the list by performing the following steps:
- a) Select an attribute, such as **Username**.
- b) Select a modifier, such as **begins with**.
- c) Enter your search term.
- d) Select **Find**.

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

Add or Remove User From Device Pool

A device pool is a named collection of devices. You must add each user to at least one device pool. Users can be added to or removed from one or more device pools.

**Related Topics**
- Add User Account, on page 222
- Find User Account, on page 224
- Edit User Account, on page 222
- Device Pools, on page 41

**Procedure**

To add a user to or remove a user from a device pool:

**Step 1**
Select **User Management > User**.
The Find, Add, Delete, Edit Users window opens.

**Step 2**
Perform one of the following steps:
- Select a user by clicking on the name in the Username list.
- Select the radio button preceding the name.

**Step 3**
Select **Edit**
The Edit User window opens to the General tab.

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

**Step 5**
Select the device pool from the **Available** pane, and then click the right arrow to move the pool to the **Selected** pane.

**Step 6**
To remove a user from a device pool, perform the following steps:

a) Select the device pool from the **Selected** pane.
b) Select the left arrow to move the device pool to the **Available** pane.

**Note**
A user must always be associated with at least one device pool.

**Step 7**
Select **Save**.

---

**Assign User to User Group**

Assigning users to groups can limit the operations users can perform from the Operations Console menus. You must assign each user to at least one user group. Unified CVP includes four roles:

- **Super User** - a role with superuser privileges that allow any operation in the Operations Console.
- **Administrator** - can perform any operation in the Operations Console except deleting user accounts.
- **Serviceability Administration** - Allows Web Services authentication through the "Unified System CLI" tool and does not allow any privileges for the Operations Console.
- **ReadOnly** - Has Read-only access to the Operations console.

You add/remove a user to/from a user group when you:

- **Add User Account**, on page 222
- **Edit User Account**, on page 222

**Related Topics**
- **Find User Account**, on page 224
- **Delete User Account**, on page 223
- **Add User Role**, on page 214

**Procedure**

To add/remove a user to/from a user group:

**Step 1**
To add a user to a group, select the user group from the **Available** pane, and then click the right arrow to move the user group to the **Selected** pane.

**Step 2**
To remove a user from a group, select the user from the **Selected** pane, and then click the left arrow to move the user group to the **Available** pane.
Step 3  
Click Save.
Bulk Administration

Bulk Administration File Transfer (BAFT)

You can transfer multiple VXML application files and Script and Media files from the Operations Console to one or more devices in a single operation. One license file can be transferred to one or more devices in a single operation. Some types of files can only be transferred to certain types of devices. For example, license files can only be transferred to Unified CVP Call Servers, Unified CVP Reporting Servers, Unified CVP VXML Servers, and Speech Servers. Script and Media files can be transferred to Gateways. VXML Application files can be transferred to Unified CVP VXML Servers.

See also:

Transfer License Files Using BAFT

To transfer a license file:

**Step 1**
Select Bulk Administration > File Transfer > Licenses.
The File Transfer - Licenses window opens.

**Step 2**
In the Device Association panel, use the Select Device Type drop-down menu and select the type of device to which you want to transfer a license file.

**Step 3**
To select a device, perform the following steps:
Only devices of the selected type are displayed in the Available Devices box.

| Note | Click the check box Select all Unified CVP devices to move all servers listed in Available to Selected. |

**Example:**
For example, if you select Unified CVP Reporting Server, then only Unified CVP Reporting Servers are displayed in the Available box.

a) Select a device from the Available box.
b) Select the right arrow to move the device to the Selected box.

**Step 4**
To remove a device from the Selected Devices box, perform the following steps:
a) Select the device.
b) Select the left arrow to move the device to the **Available Devices** box.

c) You can check the **Select all Unified CVP Devices** check box to move all available devices to the selected devices column.

**Step 5**

In the **License File** portion of the screen, select the check box for the type of license you want to upload: a new license or a license from the managed files section.

- If you are selecting a new license then select **Browse** to select the license file from your local computer. (This license is added to managed files after the transfer finishes.)

**Step 6**

When you finish selecting devices and the license, click **Transfer**.

The file you selected is transferred to each selected device. Obtain the status of the transfer by selecting File Transfer Status. See View File Transfer Status, on page 229.

---

**Transfer Scripts and Media Files Using BAFT**

To transfer one or more script or media files:

**Step 1**

Select **Bulk Administration > File Transfer > Scripts and Media**.

The **File Transfer - Scripts and Media** window opens.

**Step 2**

In the **Device Association** panel, use the **Select Device Type** drop-down menu and select the type of device to which you want to transfer scripts and/or media files.

**Step 3**

Select a device from the **Available** box and click the right arrow to move the device to the **Selected** box.

**Step 4**

To remove a device from the **Selected Devices** box, select the device and click the left arrow to move the device to the **Available** box.

**Step 5**

In the **Script and Media Files** panel, select the radio button for the action you want to perform, then select or browse for the files you want to transfer.

There are three choices:

- **Default Gateway files** - the default gateway files are displayed in the list box. By default, all default files are selected. You can select or deselect one or more files using CTRL-click. Highlighted files are sent to the device(s) after you click transfer.

- **Managed files** - Managed files are non-default files that have already been transferred to a device from this Operations Console server. You can select or deselect one or more files using CTRL-click. Highlighted files are sent to the device(s) after you click transfer. You can optionally highlight files and then click **Delete Managed file** to remove the file from this Operations Console server and the managed files list.

- **Select new files** - You can click browse to select a new file to upload from your local computer. After you browse and select a file, another slot is made available to browse and upload, up to a limit of 10 files. After transfer, these files are displayed in the Managed Files section.

**Step 6**

When you finish selecting devices and files, select **Transfer**.
The selected file(s) is transferred to each selected device. You can view the status of the transfer by clicking File Transfer Status. See View File Transfer Status, on page 229.

---

### Transfer VXML Applications Using BAFT

To transfer one or more VXML applications:

**Step 1** Select **Bulk Administration > File Transfer > VXML Applications**.

The **File Transfer - VXML Application window opens**.

**Step 2** Select one or more Unified CVP VXML Servers and click the appropriate arrow to move them into the **Selected** panel.

The list of available Unified CVP VXML Servers to which you can transfer a VXML application is listed in the **Associated Unified CVP VXML Server(s) Available** panel.

**Step 3** In the **VXML Application Files** panel, select the radio button for the action that you want to perform, then select or browse for the files that you want to transfer.

There are two choices:

- **Select new files** - You can click browse to select a new VXML application to upload from your local computer. After you browse and select a VXML application, another slot is made available to browse and upload, up to a limit of 10 VXML applications. After the transfer finishes, these files are displayed in the **Managed Files** section.

- **Managed files** - Managed files are files that have already been transferred to a device from this Operations Console server. You can select or deselect one or more files using CTRL-click. Highlighted files are sent to the device(s) after you click **Transfer**. You can also highlight files and then click **Delete Managed file** to remove the file from this Operations Console server and the managed files list.

**Step 4** When you finish selecting devices, click **Transfer**.

The selected file(s) is transferred to each selected device. You can view the status of the transfer by clicking File Transfer Status. See View File Transfer Status, on page 229.

---

### View File Transfer Status

To view the status of a bulk administration file transfer:

**Step 1** Select **Bulk Administration > File Transfer** then **License Files, Scripts and Media Files**, or **VXML Application**.

**Step 2** Select the **File Transfer Status** button on the resulting page.

The status for the transfer is listed in the table.

Select **Refresh** to refresh the list of statuses.
View File Transfer Status

Bulk Administration
CHAPTER 5

SNMP Agent Setup

- Simple Network Management Protocol Support, on page 231
- SNMP Basics, on page 231
- SNMP Management Information Base (MIB), on page 232
- Set Up SNMP, on page 233
- Import Previously Configured Windows SNMP v1 Community Strings, on page 233
- SNMP v1/v2c Agent Setup, on page 234
- SNMP v3 Agent Setup, on page 241
- SNMP MIB2 System Group Setup, on page 248
- Syslog, on page 250

Simple Network Management Protocol Support

Simple Network Management Protocol (SNMP), an application layer protocol, facilitates the exchange of management information among network devices, such as nodes, routers, and so on. As part of the TCP/IP protocol suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth. The Unified CVP SNMP agent lets customers and partners to integrate with their existing SNMP network management system to provide instantaneous feedback on the health of their Unified CVP system.

The Call server, Unified CVP VXML Server, and Reporting server can send SNMP traps and statistics to any standard SNMP management station. You can configure a link to the administration web page for an SNMP monitoring tool and then access it by selecting SNMP Monitor from the Tools menu.

The SNMP menus from the Operations Console enable you to configure SNMP-associated settings, such as community strings, users, and notification destinations for V1, V2c, and V3. SNMP V3 offers improved security features.

SNMP Basics

An SNMP-managed network is comprised of managed devices, agents, and network management systems.

Key SNMP Components

- Managed device - A network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make it available by using SNMP.
• Agent - A network-managed software module that resides on a managed device. An agent contains local knowledge of management information and translates it into a form that is compatible with SNMP. Unified CVP uses a master agent and subagent components to support SNMP. The master agent acts as the agent protocol engine and performs the authentication, authorization, access control, and privacy functions that relate to SNMP requests. Likewise, the master agent contains a few MIB variables that relate to MIB-II. The SNMP master agent listens on port 161 and forwards SNMP packets for Vendor MIBs. The Unified CVP subagent interacts with the local Unified CVP only. The Unified CVP subagent sends notifications and SNMP response messages to the Master Agent for forwarding to a Network Management Station. The SNMP Master Agent communicates with the SNMP trap receiver (notification destination).

• Network Management System (NMS) - A SNMP management application (together with the PC on which it runs) that provides the bulk of the processing and memory resources that are required for network management. An NMS executes applications that monitor and control managed devices. Unified CVP works with any standard SNMP-based NMS.

SNMP Management Information Base (MIB)

SNMP allows access to Management Information Base (MIB), which is a collection of information that is organized hierarchically. MIBs comprise managed objects, which are identified by object identifiers. A MIB object, which contains specific characteristics of a managed device, comprises one or more object instances (variables). The Unified CVP Simple Network Management Protocol (SNMP) agent resides in each component and exposes the CISCO-CVP-MIB that provides detailed information about devices that are known to the Unified CVP subagent. The CISCO-CVP-MIB provides device information such as device registration status, IP address, description, and model type for the component.

The AIX Native agent by default listens on port 161 for Network Management Station requests. Upon installation of CVP, the AIX Native agent is reconfigured to listen on port 8161. The CVP SNMP Agent takes over listening on port 161. The CVP SNMP Agent acts as a proxy to the Native AIX Agent. The CVP SNMP Agent handles the forwarding of traps and statistics. SNMP Traps generated by the Native AIX Agent are sent to the CVP SNMP Agent and forwarded to all SNMP Notification targets that are configured using the Operations Console.

Unified CVP supports the following MIBs:

Supported MIBs:

• CISCO-CVP-MIB - Provides general information; server name and version number; and status and statistics for each component.

• HOST-RESOURCES-MIB - The Host Resources MIB found in Cisco SNMP is an implementation of the Host Resources MIB document, proposed standard RFC 1514 (https://www.ietf.org/rfc/rfc1514.txt). It is also compliant with Host Resources MIB, draft standard RFC 2790 (https://www.ietf.org/rfc/rfc2790.txt). This MIB defines objects that are useful for managing host systems and allows SNMP access to useful host information, such as the storage resources, process table, device information, and the installed software base.

• The System-level Managed Objects for Applications (SYSAPPL) MIB, RFC 2287 (https://www.ietf.org/rfc/rfc2287.txt), supports configuration, fault detection, performance monitoring, and control of application software. It provides for tables that define an application as a series of processes and services. This includes objects for applications installed on the system, elements and processes that are included in an application, and current and previously run applications.
Set Up SNMP

Table 65: SNMP Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install and configure the SNMP NMS.</td>
<td>SNMP product documentation that supports the NMS.</td>
</tr>
<tr>
<td>Import all previous SNMP configurations to the Operations Console.</td>
<td>Import Previously Configured Windows SNMP v1 Community Strings</td>
</tr>
<tr>
<td>If you are using SNMP v1/v2c, configure the community string.</td>
<td>SNMP v1/v2c Community String Setup</td>
</tr>
<tr>
<td>If you are using SNMP v3, configure the SNMP user.</td>
<td>SNMP v3 User Setup</td>
</tr>
<tr>
<td>Configure the notification destinations.</td>
<td>SNMP v1/v2 Notification Destination Setup</td>
</tr>
<tr>
<td>Configure the system contact and location for the MIB2 system group.</td>
<td>SNMP MIB2 System Group Setup</td>
</tr>
</tbody>
</table>

Import Previously Configured Windows SNMP v1 Community Strings

To import previously configured Windows SNMP V1 Community Strings:

Step 1
View the list of previously configured Windows SNMP V1 community strings by performing the following:
  a) Open the Windows Services viewer.
  b) Right-click **SNMP Service** and select **Properties**.
  c) Select the **Security** tab. This tab lists the accepted V1 community strings and the access granted for each string, and also lists the hosts from which SNMP packets are accepted.

**Note**
The accepted hosts apply to all community strings, whereas the Operations Console provides more granularity, allowing you to specify accepted hosts on a per-community string basis.

Step 2
Configure these community strings using the Operations Console:
  a) Open the Operations Console and select **SNMP | V1/V2C | Community String**.
  b) For each community string discovered above that has not already been configured in the Operations Console, add it by clicking **Add New**.

Perform the following actions:
- Enter the community string exactly as it appeared in step 1 above.
- Select **V1** as the version.
For Windows community strings with permission other than "Read Only," select Read Write in the Operations Console.

Select the device(s) on which this community string was seen in step 1.

SNMP v1/v2c Agent Setup

SNMP version 1 (SNMPv1), the initial implementation of SNMP that functions within the specifications of the Structure of Management Information (SMI), operates over protocols, such as User Datagram Protocol (UDP) and Internet Protocol (IP). The SNMPv1 SMI defines highly structured management information base tables (MIBs) that are used to group the instances of a tabular object (that is, an object that contains multiple variables). Tables contain zero or more rows, which are indexed to allow SNMP to retrieve or alter an entire row with a supported command. With SNMPv1, the NMS issues a request, and managed devices return responses. Agents use the Trap operation to asynchronously inform the NMS of a significant event.

As with SNMPv1, SNMPv2c functions within the specifications of the Structure of Management Information (SMI). MIB modules contain definitions of interrelated managed objects. The operations that are used in SNMPv1 are similar to those that are used in SNMPv2. The SNMPv2 Trap operation, for example, serves the same function as that used in SNMPv1, but it uses a different message format and replaces the SNMPv1 Trap.

You need to compile the Cisco CVP MIB with your SNMP network management application. The CVP MIB is located in the %CVP_HOME%/conf folder. You can also find the current list of supported MIBs at: https://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

The CVP MIB is defined using version 2 of the Structure of Management Information (SMI) and contains "Counter64" (64-bit integer) object types. While the CVP SNMP infrastructure supports version 1 of the SNMP protocol, SNMP v1 cannot query Counter64 object values. Hence, you must use SNMP v3 or SNMP v2c.

You can configure SNMP v1 support from the SNMP V1/V2c menu.

You can perform the following tasks:

- SNMP v1/v2c Community String Setup, on page 234
- SNMP v1/v2 Notification Destination Setup, on page 238

SNMP v1/v2c Community String Setup

Although SNMP community strings provide no security, they authenticate access to MIB objects and function as embedded passwords. Typically, one community string is used for read-only access to a network element.

You configure SNMP community strings for SNMP v1 and v2c only. SNMP v3 does not use community strings. Instead, version 3 uses SNMP users. These users serve the same purpose as community strings, but users provide security because you can configure encryption or authentication for them.
Add SNMP v1/v2C Community String

Related Topics
- SNMP v1/v2c Community String Settings, on page 236
- Find SNMP v1/v2c Community String, on page 237

Procedure

To add an SNMP v1/v2c community string:

Step 1 Select SNMPV1/V2cCommunity String. 
The Find, Add, Delete, Edit window lists the available SNMP community strings, sorted by name, 10 at a time.

Step 2 Select Add New. 
The V1/V2c SNMP Community String Configuration window opens to the General tab.

Step 3 Fill in the community string and verify that the default values for other fields are correct.

Step 4 Select the Devices tab and assign an SNMP community string to a device.

Step 5 Select Save to save the configuration to the Operations Console database, or select Save & Deploy to save the changes and apply the changes to the selected devices.

Edit SNMP v1/v2C Community String

Related Topics
- SNMP v1/v2c Community String Settings, on page 236
- Find SNMP v1/v2c Community String, on page 237

Procedure

You can change the name, the hosts to accept SNMP packets from, and the access privileges for an SNMP V1/V2C community string.

Step 1 Select SNMP > V1/V2c > Community String. 
The Find, Add, Delete, Edit Window lists the available SNMP community strings, sorted by name, 10 at a time.

Step 2 Select the SNMP community string to edit by checking the check box preceding it and selecting Edit. 
The Community String Configuration window opens to the General tab.

Step 3 Make the desired changes to the community string settings. You cannot change the name of the SNMP community string.

Step 4 Select the Devices tab and make desired changes to the assignment of the SNMP community string to a device.

Step 5 Click Save to save the configuration to the Operations Console database, or click Save & Deploy to save the changes and apply the changes to the selected devices.
# SNMP v1/v2c Community String Settings

The following table describes the fields that you can change to configure an SNMP v1/v2c community string.

### Table 66: SNMP v1/v2c Community String Configuration

<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>Community String Information</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Community String Name</td>
<td>You cannot change this name if you are editing a Community String.</td>
<td>None</td>
<td>Letters in the alphabet, the numbers 0 through 9, and a dash</td>
<td>No</td>
</tr>
<tr>
<td><strong>SNMP Version Information</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V1 or V2c</td>
<td>Select SNMP Version 1 or 2c agent</td>
<td>V1</td>
<td>V1 or 2c</td>
<td>No</td>
</tr>
<tr>
<td><strong>Host IP Addresses Information</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accept SNMP Packets From any Host or Accept SNMP Packets Only from these Hosts</td>
<td>Select hosts that are allowed to query or access the configured devices using this community string.</td>
<td>Accept SNMP Packets From Any Host</td>
<td>From any host or from only these hosts</td>
<td>No</td>
</tr>
<tr>
<td>Host IP Address</td>
<td>Enter the IP address of an SNMP management station from which SNMP agents accept SNMP packets. Enter the IP address and click <strong>Add</strong> to include the IP address in the list of Host IP Addresses. To remove an IP address from the list, select the IP address and click <strong>Remove</strong>.</td>
<td>None</td>
<td>Valid IP address</td>
<td>No</td>
</tr>
<tr>
<td><strong>Access Privileges</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Privileges</td>
<td>Choose the appropriate access level from the following list: Access Privileges:</td>
<td>ReadOnly</td>
<td>ReadOnly, ReadWrite</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• <strong>ReadOnly</strong> - The community string can only read the values of MIB objects.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ReadWrite</strong> - The community string can read and write the values of MIB objects.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Assign SNMP Entity to Device

Procedure

While you add or edit any of the following SNMP entities, you can add them to or remove them from one or more devices:

SNMP Entities:

- SNMP V1/V2C community strings
- SNMP V1/V2C or V3 notification destinations
- SNMP MIB-2 user groups
- SNMP V3 users

Step 1 Select the Devices tab.

Step 2 To add an SNMP V1/V2 community string to a device, perform the following steps:
   a) Select the device from the Available pane.
   b) Select the right arrow to move the device to the Selected pane.

Step 3 To remove an SNMP V1/V2 community string from a device, perform the following steps:
   a) Select the device from the Selected pane.
   b) Select the left arrow to move the device to the Available pane.

Step 4 Select Save to save the configuration to the Operations Console database. Select Save & Deploy to save the changes and apply the changes to the selected devices.

Find SNMP v1/v2c Community String

If you have several SNMP community strings in your network, the Operations Console lets you locate specific community strings on the basis of specific criteria. Use the following procedure to locate an SNMP community string.

Procedure

To find an SNMP V1/V2c community string:

Step 1 Select SNMP > V1/V2c > Community String.

The Find, Add, Delete, Edit Window lists the available SNMP community strings, sorted by name, 10 at a time.

Step 2 To scroll through the list, select Next to view the next group of available community strings.

Step 3 Select Previous to view the previous group of available community strings.

Step 4 To filter the list:
   a) Using the filter at the top right of the list, select a field to search.
   b) Select a modified (such as Starts with).
c) Select **Find**.

**Note** The filter is not case-sensitive and wildcards are not allowed.

**Step 5** From the second window drop-down list box, select one of the following search criteria:
- begins with
- contains
- ends with
- is exactly

**Step 6** Specify the appropriate search text, if applicable, and select **Find**.

---

**Delete SNMP v1/v2c Community String**

**Procedure**

To delete one or more SNMP V1/V2c community strings:

**Step 1** Select **SNMP > V1/V2c > Community String**.

The Find, Add, Delete, Edit Window lists the available SNMP community strings, sorted by name, 10 at a time.

**Step 2** To select the SNMP community string to delete, perform the following steps:
- a) Select the check box preceding the string.
- b) Select **Delete**.

**Step 3** When prompted to confirm the delete operation, perform one of the following steps:
- Select **OK** to delete the operation.
- Select **Cancel** to cancel the delete operation.

**Related Topics**

Find SNMP v1/v2c Community String, on page 237

---

**SNMP v1/v2 Notification Destination Setup**

You can configure different community strings for SNMP v1 and v2c depending on which protocol they wish to use on their network. If you use both SNMP v1 and v2c, you can configure one community string for v1 and another for v2.

You might have one management station (using SNMP v1) collecting notifications from one part of the network and another management station (using SNMP v2) collecting notifications from another part. In this case, when configuring a destination, you must specify the community string that correlates the SNMP version used to send the notification.
SNMP v1/v2 Notification Destination Settings

The following table describes the fields that you can change to configure the host and port to receive SNMP notifications.

Table 67: Notification Destination 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>Host IP Address Information</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host IP Address</td>
<td>IP address of host to receive SNMP notifications.</td>
<td>None</td>
<td>Valid IP address</td>
<td>No</td>
</tr>
<tr>
<td>Port Number</td>
<td>Port number to receive SNMP notifications.</td>
<td>162</td>
<td>Any available port number. Valid port numbers are integers between 1 and 65535</td>
<td>No</td>
</tr>
<tr>
<td><strong>Notification Destination Information</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notification Destination Name</td>
<td>When you are adding a notification destination, assign a name. You cannot change the Notification Destination Name.</td>
<td>None</td>
<td>Letters in the alphabet, the numbers 0 through 9, and a dash</td>
<td>No</td>
</tr>
<tr>
<td><strong>Community String Information</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Community String</td>
<td>Select the community string from the drop-down list.</td>
<td>None</td>
<td>Not applicable</td>
<td>No</td>
</tr>
</tbody>
</table>

Add SNMP v1/v2c Notification Destination

Procedure

To add an SNMP v1/v2c notification destination:

**Step 1** Select SNMP > V1/V2c > Notification Destination.

The Find, Add, Delete, Edit V1/V2c Notification Destinations Window lists the available SNMP notification destinations, sorted by name, 10 at a time.

**Step 2** Click Add New.

The V1/V2c Notification Destination Configuration window opens to the Configuration tab.

**Step 3** Fill in the fields on the configuration tab.

**Step 4** Select the Devices tab and assign the SNMP notification destination to a device.
Edit SNMP v1/v2C Notification Destination

Related Topics
- SNMP v1/v2 Notification Destination Settings, on page 239
- Assign SNMP Entity to Device, on page 237
- Find SNMP v1/v2C Notification Destination, on page 241

Procedure

To change an SNMP V1/V2C notification destination:

Step 1: Select SNMP > V1/V2c > Notification Destination. The Find, Add, Delete, Edit V1/V2C Notification Destinations Window lists the available SNMP notification destinations, sorted by name, 10 at a time.

Step 2: To select the SNMP notification destination to edit, perform the following steps:
   a) Select the check box preceding the destination.
   b) Select Edit. The Notification Destination Configuration window opens to the Configuration tab.

Step 3: Make the desired changes to the fields on the Configuration tab.

Note: You cannot change the name of the notification destination.

Step 4: Select the Devices tab and assign an SNMP entity to a device.
Step 5: Select Save to save the configuration to the Operations Console database, or click Save & Deploy to save and apply the changes to the selected devices.

Delete SNMP v1/v2C Notification Destination

Procedure

To delete one or more SNMP V1/V2c notification destinations:

Step 1: Select SNMP > V1/V2c > Notification Destination. The Find, Add, Delete, Edit V1/V2C Notification Destinations Window lists the available SNMP notification destinations, sorted by name, 10 at a time.
Step 2: To select the SNMP notification destination to delete, perform the following steps:
   a) Select the check box preceding the destination.
   b) Select Delete.

Step 3: When prompted to confirm the delete operation, select OK to delete or select Cancel to cancel the delete operation.

---

Find SNMP v1/v2C Notification Destination

The Operations Console lets you locate specific community strings on the basis of specific criteria. Use the following procedure to locate an SNMP notification destination.

Procedure

To find an SNMP V1/V2c notification destination:

---

Step 1: Select SNMP > V1/V2c > Notification Destination.

The Find, Add, Delete, Edit V1/V2c Notification Destinations window lists the available SNMP notification destinations, sorted by name, 10 at a time.

Step 2: To scroll through many pages of the list, click the first, previous, next, and last page icons on the bottom left to view the next group of available notification destinations.

Step 3: You can filter the list by performing the following steps:
   a) Using the filter at the top right of the list, select a field to search.
   b) Select a modifier (such as Starts With).
   c) Select Find.

   Note: The filter is not case-sensitive and wildcards are not allowed.

---

SNMP v3 Agent Setup

SNMP version 3 provides security features such as authentication (verifying that the request comes from a genuine source), privacy (encryption of data), authorization (verifying that the user allows the requested operation), and access control (verifying that the user has access to the objects requested.) To prevent SNMP packets from being exposed on the network, you can configure encryption with SNMPv3. Instead of using community strings like SNMP v1 and v2, SNMP v3 uses SNMP users, as described in the SNMP Community Strings and Users topic.

Configure SNMP v3 support from the SNMP V3 menu.

You can perform the following tasks:

- SNMP v3 User Setup, on page 242
- SNMP v3 Notification Destination Setup, on page 246
SNMP v3 User Setup

When you create SNMP users, match their SNMP user names to the user names you have already configured for the NMS.

You can perform the following tasks:

• Find SNMP v3 User, on page 242
• Add SNMP v3 User, on page 242
• Edit SNMP v3 User, on page 243

Find SNMP v3 User

Procedure

To find an SNMP user:

Step 1  Select SNMP > V3 > User.
The Find, Add, Delete, Edit Users window lists the available SNMP v3 users, sorted by name, 10 at a time.

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

Step 3  You can filter the list by selecting an attribute such as V3 Username. Then select a modifier, such as begins with, enter your search term, and then click Find.

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

Add SNMP v3 User

Related Topics

  SNMP v3 User Settings, on page 243
  Assign SNMP Entity to Device, on page 237

Procedure

To add an SNMP v3 user:

Step 1  Select SNMP > V3 > User.
The Find, Add, Delete, Edit V3 Users window lists the available SNMP users, sorted by name, 10 at a time.

Step 2  Click Add New.
The SNMP V3 User Configuration window opens to the Configuration tab.
Step 3 Fill in the username and verify that the default values for other fields are correct.

Step 4 Select the Devices tab and assign the user to a device.

Step 5 Click Save to save the settings in the Operations Console database. Click Save & Deploy to save and apply the change to the selected devices.

---

**Edit SNMP v3 User**

**Related Topics**

- SNMP v3 User Settings, on page 243
- Assign SNMP Entity to Device, on page 237
- Find SNMP v3 User, on page 242

**Procedure**

You can change the access privileges, authentication and privacy information for an SNMP V3 user.

---

**Step 1** Select SNMP > V3 > User.

The Find, Add, Delete, Edit Users window lists the available SNMP users, sorted by name, 10 at a time.

**Step 2** Select the SNMP user name to edit by selecting the check box preceding it or highlighting the user name and then clicking Edit.

The SNMP User Configuration window opens to the Configuration tab.

**Step 3** Make the desired changes to SNMP V3 users settings. You cannot change the username for the SNMP V3 user.

**Step 4** Select the Devices tab and change the assignment of the user to a device.

**Step 5** Click Save to save the settings in the Operations Console database. Click Save & Deploy to save and apply the change to the selected devices.

---

**SNMP v3 User Settings**

The following table describes the fields that you can change to configure an SNMP v3 user.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>Enter the SNMP v3 user name. You cannot change this name when editing an SNMP v3 user.</td>
<td>None</td>
<td>Letters in the alphabet, the numbers 0 through 9, and a dash</td>
<td>No</td>
</tr>
</tbody>
</table>
## SNMP v3 User 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>Access Privileges</td>
<td>Select the appropriate access level from the following list:</td>
<td>ReadOnly</td>
<td>ReadOnly, ReadWrite</td>
<td>No</td>
</tr>
<tr>
<td>Access Privileges:</td>
<td>Access Privileges:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>ReadOnly</strong></td>
<td>The community string can only read the values of MIB objects.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>ReadWrite</strong></td>
<td>The community string can read and write the values of MIB objects.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host IP Addresses Information</td>
<td>Accept SNMP Packets From any Host or Accept SNMP Packets Only from these Hosts</td>
<td>Accept SNMP Packets From Any Host</td>
<td>From any host or from only these hosts</td>
<td>No</td>
</tr>
<tr>
<td>Host IP Address</td>
<td>Enter the IP address of an SNMP management station from which SNMP agents accept SNMP packets. Enter the IP address and click <strong>Add</strong> to include the IP address in the list of Host IP Addresses. To remove an IP address from the list, select the IP address and click <strong>Remove</strong>.</td>
<td>None</td>
<td>Valid IP address</td>
<td>No</td>
</tr>
<tr>
<td>Authentication Information</td>
<td>Select to require authentication for this user. This offers an additional level of security not provided with SNMP v1 and v2c. The SNMP user only gains access to the device when using both a valid user name and password. If authentication is not required, security is no better with v3 than it would be for SNMP v1/v2c using community strings.</td>
<td>Disabled</td>
<td>Enabled or Disabled</td>
<td>No</td>
</tr>
<tr>
<td>Authentication Required</td>
<td>Password for the SNMP Version 3 user. This password is required to accept incoming SNMP v3 packets.</td>
<td>None</td>
<td>Any text that follows the Secure Password Requirements.</td>
<td>No</td>
</tr>
</tbody>
</table>

SNMP Agent Setup

SNMP v3 User Settings
### Delete SNMP v3 User

#### Procedure

To delete one or more SNMP users:

**Step 1**  
Select SNMP > V3 > User.  
The Find, Add, Delete, Edit window lists the available users, sorted by name, 10 at a time.

**Step 2**  
Select the SNMP users to delete by selecting the check box preceding it or highlighting the user name, and then clicking **Delete**.

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

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Re-enter Password</td>
<td>Retype the password for this user account to verify that you typed the password correctly.</td>
<td>None</td>
<td>The same text that was entered in the Password field.</td>
<td>No</td>
</tr>
<tr>
<td>Protocol</td>
<td>Choose MD5 or SHA-1 protocols to encrypt the password.</td>
<td>None</td>
<td>MD5 or SHA-1</td>
<td>No</td>
</tr>
<tr>
<td>Privacy Information</td>
<td>Select to require privacy for the SNMP user. Enabling privacy causes the SNMP message data to be encrypted during transmission. This provides an additional level of security over authentication (only) in that it protects the data, rendering it unreadable by would-be snoopers while traveling over the wire.</td>
<td>Disabled</td>
<td>Enabled or disabled.</td>
<td>No</td>
</tr>
<tr>
<td>Privacy Required</td>
<td>Select to require privacy for the SNMP user. Enabling privacy causes the SNMP message data to be encrypted during transmission. This provides an additional level of security over authentication (only) in that it protects the data, rendering it unreadable by would-be snoopers while traveling over the wire.</td>
<td>Disabled</td>
<td>Enabled or disabled.</td>
<td>No</td>
</tr>
<tr>
<td>Password</td>
<td>Password the SNMP user must enter.</td>
<td>None</td>
<td>Any text that follows the Secure Password Requirements.</td>
<td>No</td>
</tr>
<tr>
<td>Re-enter Password</td>
<td>Re-type the same text entered in the Password field.</td>
<td>None</td>
<td>The same text entered in the Password field.</td>
<td>No</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocol to encrypt the user password.</td>
<td>None</td>
<td>3DES, AES-192 , AES-256</td>
<td>No</td>
</tr>
</tbody>
</table>
SNMP v3 Notification Destination Setup

A notification destination identifies the target host and port to receive SNMP notifications sent by the Unified CVP SNMP agent on the devices you specify. You can specify an SNMP v3 user and associated authorization for an SNMP v3 notification destination.

Add SNMP v3 Notification Destination

Procedure

To add an SNMP V3 notification destination:

Step 1 Select SNMP > V3 > Notification Destination.
The Find, Add, Delete, Edit window lists the available SNMP notification destinations, sorted by name, 10 at a time.

Step 2 Click Add New.
The SNMP Notification Destination Configuration window opens to the Configuration tab.

Step 3 Fill in the name of the SNMP V3 notification destination.

Step 4 Select the Devices tab and assign the SNMP notification destination to a device.

Step 5 Click Save to save the settings in the Operations Console database. Click Save & Deploy to save the change and apply them to the selected devices.

Edit SNMP v3 Notification Destination

Procedure

To change an SNMP v3 notification destination:

Step 1 Select SNMP > V3 > Notification Destination.
The Find, Add, Delete, Edit window lists the available SNMP notification destinations, sorted by name, 10 at a time.

Step 2 Click Edit.
The SNMP Notification Destination Configuration window opens to the Configuration tab.

**Step 3** Change the desired notification destination configuration settings. You cannot change the name of the notification destination.

**Step 4** Select the **Devices** tab and add or remove devices to this notification destination.

**Step 5** Click **Save** to save the settings in the Operations Console database, or click **Save & Deploy** to save the change and apply them to the selected devices.

---

### SNMP v3 Notification Destination Settings

The following table describes the fields that you can change to configure the host and port to receive SNMP notifications.

<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>Notification Destination Information</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notification Destination Name</td>
<td>Name for the notification destination. You cannot change this name when editing a notification destination.</td>
<td>None</td>
<td>Letters in the alphabet, the numbers 0 through 9, and a dash</td>
<td>No</td>
</tr>
<tr>
<td><strong>Host IP Addresses Information</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host IP Address</td>
<td>IP address of host to receive SNMP notifications.</td>
<td>None</td>
<td>Valid IP address</td>
<td>No</td>
</tr>
<tr>
<td>Port Number</td>
<td>Port number to receive SNMP notifications.</td>
<td>162</td>
<td>Any available port number. Valid port numbers are integers between 1 and 65535</td>
<td>No</td>
</tr>
<tr>
<td><strong>User Information</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>Select a user from the drop-down list.</td>
<td>None</td>
<td>None</td>
<td>No</td>
</tr>
</tbody>
</table>

### Find SNMP v3 Notification Destination

As you probably have several SNMP notification destinations in your network, the Operations Console lets you locate specific destination notifications on the basis of specific criteria. Use the following procedure to locate an SNMP notification destination.

**Procedure**

To find an SNMP V3 notification destination:

**Step 1** Select **SNMP > V3 > Notification Destination**.
The Find, Add, Delete, Edit window lists the available SNMP notification destinations, 10 at a time, sorted by name.

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

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

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

---

**Delete SNMP v3 Notification Destination**

**Procedure**

To delete one or more SNMP V3 notification destinations:

**Step 1** Select SNMP > V3 > Notification Destination.

**Step 2** Select the SNMP notification destination to delete by selecting the check box preceding it or highlighting the notification destination and then clicking Delete.

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

**Related Topics**

Find SNMP v1/v2C Notification Destination, on page 241

---

**SNMP MIB2 System Group Setup**

The Operations Console allows you to change the system contact and system location information in the SNMP MIB-II system group, and to assign that system group to a device. For example, you could enter Administrator, 555-121-6633, for the system contact and San Jose, Bldg 23, 2nd floor, for the system location.

You can perform the following tasks:

**Add SNMP MIB2 System Group**

**Procedure**

To add an SNMP MIB2 system group:

**Step 1** Select SNMP > System Group > MIB2 System Group.
The Find, Add, Delete, Edit MIB2 System Groups window lists the available SNMP MIB2 system groups, sorted by name, 10 at a time. Each device can only be associated with one system group. Only devices that are not associated with other system groups are displayed in the available system groups.

**Step 2**
Click **Add New**.
The MIB2 System Group Configuration window opens to the Configuration tab.

**Step 3**
In the **System Contact** field, enter a person to notify when problems occur.

**Step 4**
In the **System Location** field, enter the location of the person that is identified as the system contact.

**Step 5**
Select the **Devices** tab and assign the devices to this system group.

**Step 6**
Click **Save** to save the configuration to the Operations Console database, or click **Save & Deploy** to save the changes and apply them to the selected devices.

---

**Edit SNMP MIB2 System Group**

**Procedure**

To change SNMP MIB2 system group information:

**Step 1**
Select **SNMP > System Group > MIB2 System Group**.
The Find, Add, Delete, Edit window lists the available SNMP MIB2 system groups, sorted by name, 10 at a time.

**Step 2**
Click **Edit**.
The MIB2 System Group Configuration window opens to the Configuration tab.

**Step 3**
In the **System Contact** field, change the name of the person to notify when problems occur.

**Step 4**
Select the **Devices** tab and add or remove devices to this system group.

**Step 5**
Click **Save** to save the configuration to the Operations Console database, or click **Save & Deploy** to save the changes and apply them to the selected devices.

---

**Delete SNMP MIB2 System Group**

**Procedure**

To delete one or more SNMP MIB2 system groups:

**Step 1**
Select **SNMP > System Group > MIB2 System Group**.
The Find, Add, Delete, Edit window lists the available SNMP MIB2 system groups, sorted by name, 10 at a time.

**Step 2**
Select the SNMP MIB2 system group to delete by selecting the check box preceding it and then clicking **Delete**.
Step 3 When prompted to confirm the delete operation, click **OK** or click **Cancel**.

---

**Related Topics**

[Find SNMP MIB2 System Group](#), on page 250

---

**Find SNMP MIB2 System Group**

**Procedure**

To find an SNMP MIB2 system group:

**Step 1** Select **SNMP > System Group > MIB2 System Group**.

The Find, Add, Delete, Edit window lists the available SNMP MIB2 system groups, sorted by name, 10 at a time.

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

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

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

---

**Syslog**

**Set Up Syslog Server**

The instructions below describe how to adjust syslog settings for a Unified CVP Call Server, Unified CVP VXML Server, and/or Unified CVP Reporting Server using the Operations Console.

**Step 1** Open the Operations Console.

**Step 2** Select the server where you want to configure syslog.

**Step 3** Click **Edit**.

**Step 4** Click **Infrastructure** tab.

**Step 5** Edit the fields for backup servers and port numbers for secondary syslog server.

**Step 6** Click **Save**.

Unified CVP allows you to configure primary and backup syslog servers. However, it is important to note that failover from primary to backup server is not guaranteed. When the primary syslog server goes down (the entire machine not just the syslog receiver application), Unified CVP relies on the host operating system and the Java Runtime Environment for notification that the destination is not reachable. As this notification does not guarantee delivery, Unified CVP cannot guarantee failover.
Unified CVP allows you to configure secondary set of syslog and backup servers. CVP sends the syslog messages to both primary syslog and secondary syslog server on the ports specified.

See the *Configuration Guide for Cisco Unified Customer Voice Portal* for additional information about Syslog Server settings.
Launch Tools

- Launch SNMP Monitor, on page 253
- Links to Tools, on page 253

Launch SNMP Monitor

You can use any standard SNMP-based monitoring tool to view details of the health of the Unified CVP solution network. All Unified CVP product components issue SNMP events, which can be delivered to the network monitoring tool. To specify a SNMP-based monitoring tool as the destination for SNMP traps and statistics, you must edit the Log Messages XML file on the Unified CVP Server for each event that the server generates. For information on editing the Log Message XML file to send SNMP events to an SNMP monitoring tool, see Edit Log Messages XML File, on page 166.

You can launch the administration web page for an external SNMP monitoring tool from the Tools menu in the Operations Console.

Before you begin

Before you can launch an SNMP monitor, you must first specify the URL of the SNMP monitor web page to launch. For information on configuring the URL external tools, see the Links to Tools, on page 253 topic.

To Launch SNMP Monitor, choose Tools > SNMP Monitor from the Operations Console.

Links to Tools

You can store URLs for the tools available from the Tools menu. Once configured, you can launch the administrative web page for each tool by selecting the tool from the Operations Console Tools menu bar.

Add URL to Tools Menu

Procedure

To add a URL link to a tool:
Remove URL From Tools Menu

Procedure

To remove a URL link for a tool:

Step 1  Choose **Tools > Configure** from the Operations Console.
The Configure Tools window opens, listing the current URL for each tool.

Step 2  In the Enter New URL text box for the tool you want to configure, delete the URL from the text box, and click **Save**.
The URL for that tool is removed from the Operations Console, which means that no URL is configured for that tool.

Modify URL on Tools Menu

Procedure

To modify a URL link for a tool:

Step 1  Select **Tools > Configure** from the Operations Console.
The Configure Tools window opens, listing the current URL for each tool.

Step 2  In the Enter New URL text box for the tool you want to configure, modify the URL and click **Save**.
This modifies the URL for the selected tool. The web page indicated by this URL is launched when you select the tool from the Tools menu.
Documentation Search

The Documentation search feature searches for a term in the Unified CVP documents hosted on cisco.com. You can refine your search results by clicking on the tabs at the top of the page (for example, Configuration or Troubleshooting).

Note

The Operations Console must be able to access both google.com and cisco.com for the documentation search to function. If the Operations Console is firewalled for port 80, then you cannot use the documentation search feature.

To use the search documentation feature from within the Operations Console, click the Documentation Search link on the top right of the page.
A
adding locations 53
  Location 53

B
backups 146
cancelling for Reporting Server 146
running for Reporting Server 146
Basic Video 111
call flow model 111
before you begin tasks 4, 124, 137, 170, 222, 253
adding a Unified CVP Reporting Server 137
adding a Unified CVP VXML Server 153
adding a Unified CVP VXML Server (standalone) 170
creating a user account 222
IVR Service configuration 124
launching SNMP monitor 253
logging into the Operations Console 4
Bulk Administration menu 7
call statistics 25, 28, 30
file transfer 7
overview 7
bulk file transfer 227
license files 227
script files 227

C
call director call flow model 110
  overview 110
call flow models 110, 111, 169
  Basic Video 111
call director using SIP 110
Unified CVP VXML Server (standalone) 111, 169
Unified CVP VXML Server with ICM lookup 111
VRU-only 110
call control services 108
configuration 108
configuration settings 135
configuring ICM Service 112
configuring IVR Service 124
configuring SIP Service 115
downloading Log Messages XML file 165

Call Server (continued)
  ICM Service configuration settings 113
  IVR Service prerequisites 124
  license thresholds 132
  uploading Log Messages XML file 168
call statistics 25, 28, 30
  ICM Service 25
  IVR service 28
  SIP Service 30
Call Studio scripts 153
elements in reporting data 153
Communications Manager 193, 198
call statistics 25, 28, 30
configuration tasks 193
deleting 198
finding 198
comprehensive call flow model overview 110
configuration settings 5, 46, 62, 64, 69, 72, 113, 116, 125, 128, 135, 175, 178, 183, 185, 188, 190, 220, 236, 239, 243, 247
Call Server 135
  Dialed Number Pattern 69, 72
gateway 175, 178
general user information 5, 220
  ICM Service 113
  infrastructure 128
  IVR Service 125
  Location 46
  media server 188, 190
  SIP server groups 62, 64
  SIP Service 116
  SNMP V1/V2C community strings 236
  SNMP V1/V2C notification destinations 239
  SNMP v3 notification destinations 247
  SNMP v3 users 243
  speech server 183, 185
configuration tabs 5, 113, 116, 125, 128, 135, 138, 140, 156, 157, 188, 190, 220, 236, 239, 243, 247
Call Server 135
  ICM Service 113
  infrastructure 128
  IVR Service 125
  media server 188, 190
  Reporting Server Infrastructure Tab 140
  Reporting Server reporting properties 140
  SIP Service 116
configuration tabs (continued)
  SNMP V1/V2C community strings 236
  SNMP V1/V2C notification destination configuration settings 239
  SNMP v3 notification destination settings 247
  SNMP v3 user settings 243
  Unified CVP Reporting Server general information 138
  Unified CVP VXML Server 157
  Unified CVP VXML Server properties 156
  user information settings 5, 220

configuring 76
  Web Services 76
configuring courtesy callback system-level 92

Control Center 14, 15, 16, 21, 22, 36, 39, 40
  editing a device configuration 39
  restarting a server 40
  shutting down a server 40
  sorting servers 39
  using 14
  viewing device statistics 21, 36
  viewing device status 16
  viewing devices by device pool 16
  viewing devices by type 15
  viewing infrastructure statistics 22

creating a user account 222
  prerequisites 222

CVLogMessages.properties file 166
CVLogMessages.xml file 166
  editing 166

D

data retention 148
  default number of days 148
database 149
  viewing details 149
default device pool 41
deleting 54
  Location 54
  deploying 51, 94
  Location 51
  Realtime Database 94
deployment states 12
  reasons for failure 12
deployment status 77
  Web Services 77
device 36, 105
  finding 105
  viewing device statistics 36

Device Management menu (continued)
  overview 7
  Recording Server option 7
  Reporting Server option 7
  SIP Proxy option 7
  Speech Server option 7
  Unified CM option 7
  VXML Server (standalone) option 7
  VXML Server option 7
device pool 36
  viewing device statistics 36
device pools 41, 42, 43, 44, 192
  adding 42
  adding or removing a device 43
  adding or removing a media server 192
  default 41
  deleting 43
  description 41
  editing 42
  finding 44
device statistics 21, 150, 181
  gateway 181
  Reporting Server 150
  viewing 21
device status 16
  down 16
  not reachable 16
  partial 16
  up 16
  viewing 16
device versions 212
  viewing 212
device views 103
devices 15, 16, 21, 22, 39, 40, 103, 104, 108, 134, 237
  adding a Unified CVP Call Server 108
  assigning SNMP community string 237
  editing configuration 39
  offline view 104
  online view 104
  restarting a server 40
  shutting down a server 40
  sorting servers 39
  viewing 21
  viewing by device pool 16
  viewing by type 15
  viewing infrastructure statistics 22
  viewing properties 103
  viewing status 16
  viewing Unified CVP Call Server statistics 134

Dialed Number Pattern 69, 72
  configuration settings 69, 72
disaster recovery 44, 45
  exporting system configuration 45
  importing system configuration 44
<table>
<thead>
<tr>
<th><strong>E</strong></th>
<th><strong>F</strong></th>
<th><strong>G</strong></th>
<th><strong>H</strong></th>
<th><strong>I</strong></th>
<th><strong>M</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>editing locations 54</td>
<td>features and benefits 2</td>
<td>gateway 14, 174, 175, 178, 180, 181, 182</td>
<td>Help menu</td>
<td>IC Server 210</td>
<td>main Cisco Unified Customer Voice Portal page 6</td>
</tr>
<tr>
<td>Location 54</td>
<td>Unified CVP 2</td>
<td>adding 175</td>
<td>about 7</td>
<td>finding 210</td>
<td>Operations Console 6</td>
</tr>
<tr>
<td>error handling 14</td>
<td>file transfer 14, 151, 227</td>
<td>configuration settings 175, 178</td>
<td>contents 7</td>
<td>ICM Server 199, 200, 202</td>
<td>media server 187, 188, 190, 192</td>
</tr>
<tr>
<td>events 167</td>
<td>license 151</td>
<td>configuring 174</td>
<td>this page 7</td>
<td>adding 199</td>
<td>adding 188</td>
</tr>
<tr>
<td>severity levels for 167</td>
<td>single script file at a time 14</td>
<td>deleting 178</td>
<td><strong>INDEX</strong></td>
<td>configuring 199</td>
<td><strong>Administration Guide for Cisco Unified Customer Voice Portal, Release 12.0(1)</strong></td>
</tr>
<tr>
<td>exporting 45</td>
<td>Unified CVP VXML Server 161</td>
<td>executing IOS commands 182</td>
<td></td>
<td>deleting 200</td>
<td></td>
</tr>
</tbody>
</table>
media server (continued)
  adding and removing from a device pool 192
  configuration settings 188, 190
  finding 192
  using with Unified CVP 187

menu options 7
  for Operations Console 7

MIB2 system group 248
  configuring 248

My Account screen 4

not reachable device status 16

notification destinations 247
  SNMP v3 configuration settings 247

offline device view 104
  online device view 104

Operations Console 3, 4, 6, 7, 12, 14
  Control Center 14
  logging in 4
  logging out 12
  main Cisco Unified Customer Voice Portal page 6
  menu options 7
  overview 3

passwords 143
  changing reporting database user 143
  past device configuration 211, 212
    applying 212
    finding 211
    viewing 211
  pool statistics tab 38
  device pool 38
  port licensing 107
  purging 148
    number of days to retain data 148
  purging data 147

reporting 137
  configuring Reporting Server 137
  reporting database 143
  changing user passwords 143
  reporting filters 157
  for Unified CVP VXML Server 157

Reporting Server 37, 137, 140, 143, 144, 145, 146, 147, 149, 150, 151, 152, 165, 168
  adding reporting users 144

reporting Server (continued)
  applying a license 151
  cancelling backups 146
  changing a reporting user's password 145
  changing reporting database user password 143
  configuring 137
  configuring properties 140
  deleting 151
  downloading Log Messages XML file 165
  editing 143
  finding 152
  infrastructure settings 140
  removing reporting users 145
  running backups 146
  running purge 147
  statistics 37
  uploading Log Messages XML file 168
  viewing database details 149
  viewing statistics 150

reporting users 144, 145
  adding 144
  changing passwords 145
  removing 145

resource properties file 166
  restart 40
  call server, reporting server, Unified CVP VXML Server 40

Scripts files 227
  transferring multiple files 227

scripts 14
  transferring to devices 14

severity 166, 167
  log messages 166
  of events 167

shutdown 40

Call Server, Reporting Server, Unified CVP VXML Server 40

SIP Proxy Server 203, 205, 206
  configuring for Unified CVP 203
  deleting 206
  editing 205
  finding 206
  qualified server 203

SIP server groups 62, 64
  configuration settings 62, 64

SIP Service 115, 116, 130, 131
  configuration settings 116
  configuring on Call Server 115
  load balancing 131
  tradeoffs between UDP and TCP 130
  valid dialed number patterns 131

SIP Service call statistics 30

SNMP 233, 235, 236, 237, 238, 239, 240, 241, 248, 249
  adding MIB2 system groups 248
  adding V1/V2C community string 235
SNMP (continued)
adding V1/V2C notification destination 239
deleting a V1/V2C community string 238
deleting SNMP MIB2 system groups 249
deleting SNMPv3 notification destination 248
deleting V1/V2C notification destination 240
editing a V1/V2C community string 235
editing a V1/V2C notification destination 240
editing MIB2 system groups 249
finding V1/V2C community string 237
finding V1/V2C notification destination 241
importing previously configured Windows SNMP V1 community strings 233
MIB2 system group 248
V1/V2C community strings configuration settings 236
V1/V2C notification destination settings 239

SNMP menu 7
overview 7
system group option 7
v1/v2 option 7
v3 option 7

SNMP MIB2 system group 248, 249, 250
adding 248
deleting 249
editing 249
finding 250

SNMP monitor 253
launching 253
prerequisites for launching 253

SNMP V1/V2c 234
overview 234

SNMP V1/V2C 234
configuring community strings 234
SNMP V1/V2c community strings 234
configuring 234

SNMP V1/V2C community strings 235, 237, 238
adding 235
assigning to devices 237
deleting 238
editing 235
finding 237

SNMP V1/V2C notification destination 240, 241
deleting 240
editing 240
finding 241

SNMP V1/V2C notification destinations 238, 239
adding 239
configuration settings 239
overview 238

SNMP v3 241, 242, 243, 245, 246, 247
adding notification destination 246
adding user 242
agent overview 241
deleting user 245
editing notification destination 246
editing user 243

SNMP v3 (continued)
finding notification destination 247
finding user 242
notification destination configuration settings 247
user configuration 242
user configuration settings 243

SNMP v3 agent 241
SNMP v3 notification destinations 246, 247, 248
adding 246
configuration settings 247
deleting 248
editing 246
finding 247

SNMP v3 users 242, 243, 245
adding 242
configuration settings 243
deleting 245
editing 243
finding 242

speech server 182, 183, 184, 185, 186
adding 183
applying a license 186
configuration settings 183, 185
configuring for Unified CVP 182
deleting 184
editing 183, 185
finding 186

statistics 23, 25, 28, 30, 33, 36, 37, 38, 134
device pool 38
gateway 33
ICM service 25
infrastructure 23
IVR Service 28
licensing 23
Reporting Server 37
SIP Service 30
thread pool 23
Unified CVP Call Server 134
VXML (Standalone) Server 36
VXML Server 33

synchronizing 55
Location 55

System 44, 45
exporting configuration 45
importing a configuration 44

System menu 7
control center option 7
device pool option 7
export system configuration option 7
import system configuration option 7
Location 7
overview 7
Realtime Database 7
service advertisement framework 7
SIP server groups 7
web services 7
system statistics 23
licensing 23
thread pool 23

T

TCP 130
versus UDP in SIP deployments 130
thread pool statistics 23
tools 253
configuring links 253
Tools menu 7, 253, 254
adding links 253
configure option 7
Diagnostic Portal option 7
modifying links 254
overview 7
removing links 254
SNMP monitor 7
transferring files 180
gateway 180

Unified Customer Voice Portal (continued)
downloading Log Messages XML file 165
editing 154
example filter wildcards 163
example reporting filters 163
filters for reporting 161
finding 169
general configuration settings 156
prerequisites for adding 153
rules for reporting filters 162
transferring Log Messages XML file 168
uploading Log Messages XML file 168
Unified Customer Voice Portal (standalone) 111, 169, 170, 171, 172, 173, 174
adding 170
applying license 174
call flow model 111
configuring 169
deleting 171
editing 172
finding 173
prerequisites for adding 170
Unified Customer Voice Portal with ICM Lookup overview 111
Uniform Resource Locators (URLs) 253, 254
adding links to the Tools menu 253
modifying links to the Tools menu 254
removing links to the Tools menu 254
URL 253
adding links to Tools menu 253
user accounts 5, 220, 222, 223, 224
configuring user information 5, 220
creating 222
deleting 223
finding 224
user groups 215, 217, 218, 219, 225
adding 217
adding or removing a user 225
assigning roles 218
defined 217
deleting 219
editing 218
finding 215, 219
User Management menu 7
overview 7
user groups option 7
user roles option 7
users option 7
user roles 214, 215, 216, 218
adding 214
assigning access criteria 215
assigning to a user group 218
defined 214
deleting 216
editing 215
users 144
  adding reporting 144
using 76
  Web Services 76

V
viewing 50
  Location 50
viewing status 57
  Location 57
VoiceXML filters 162, 163
  example inclusive and exclusive 163
VoiceXML filters (continued)
  example wildcards 163
  rules 162
VoiceXML platform 2
  features and benefits 2
VRU-only call flow model 110
  overview 110
VXML 152
  configuring Unified CVP VXML Server 152
VXML (Standalone) Server 36
  statistics 36
VXML Server 14, 33
  statistics 33
  transferring script files 14