



Cisco Packaged Contact Center Enterprise Administration and Configuration Guide, Release 12.0(1)

First Published: 2019-01-11

Last Modified: 2023-08-21

Americas Headquarters

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

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 NON-INFRINGEMENT 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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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)

© 1994–2019 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface	xxi
Change History	xxi
About This Guide	xxiii
Audience	xxiv
Related Documents	xxiv
Communications, Services, and Additional Information	xxv
Field Notice	xxv
Documentation Feedback	xxvi
Conventions	xxvi

CHAPTER 1

Post Installation Configuration	1
Packaged CCE 2000 Agents Deployment	1
Configure CCE Component	2
Configure SQL Server for CCE Components	2
Set up Organizational Units	2
Initialize the Packaged CCE 2000 Agents Deployment Type	5
Configure Cisco Unified Contact Center Enterprise PG	20
Cisco SNMP Setup	21
Configure Cisco Unified Customer Voice Portal	24
Configure Cisco Unified Communications Manager	24
Configure Fully Qualified Domain Name	25
Configure Cisco Unified Communications Manager Groups	25
Configure Conference Bridges	26
Configure Media Termination Points	26
Transcoder Configuration in Unified CM and IOS Gateway	27
Configure Media Resource Groups	27

Configure and Associate Media Resource Group List	28
Configure CTI Route Point	28
Configure Ingress Gateways for Locations-based Call Admission Control	29
Add a SIP Profile in Unified CM	29
Configure Trunk	30
Configure Route Group	30
Configure Route List	31
Configure Route Pattern	31
Configure Cisco Unified Intelligence Center	31
Configure Unified Intelligence Center Data Sources for External HDS	32
Download Report Bundles	33
Import Reports	33
Configure Unified Intelligence Center Administration	35
Configure Cisco Finesse	36
Configure Contact Center Agents and Routing for Live Data Reports	36
Live Data Reports	37
Configure Cisco Unified Customer Voice Portal Reporting Server	39
Obtain Cisco Unified Customer Voice Portal Report Templates	40
Create Data Source for Cisco Unified CVP Report Data	40
Import Unified CVP Report Templates in Unified Intelligence Center	42
Configure VVB	43
Configure Cisco IOS Enterprise Voice Gateway	43
About Ingress and VXML Gateway Configuration	43
Common Configuration for the Ingress Gateway and VXML Gateway	43
Configure Ingress Gateway	44
Configure VXML Gateway	47
File Transfer to Gateway	49
Configure Codec for Ingress and VXML Gateways	49
Configure IPv6	50
IPv6 Configuration	51
Set Up IPv6 for VOS-Based Contact Center Applications	51
Configure NAT64 for IPv6-Enabled Deployment	52
Configure IPv6 on Unified CVP Call Server	54
Configure Gateways to Support IPv6	55

Configure IPv6 on Unified Communications Manager	56
Packaged CCE 4000 Agents Deployment	58
Configure CCE Component	59
Configure Rogger	60
Configure AW-HDS-DDS	64
Configure Packaged CCE Deployment Type	67
System Inventory for Packaged CCE 4000 Agents and 12000 Agents Deployment	74
Configure Cisco Unified Contact Center Enterprise PG	77
Configure Cisco Unified Customer Voice Portal	81
Configure SNMP	82
License Management	84
Configure Cisco Unified Communications Manager	85
Set Up Device Pool	85
Set Up Application User	86
Configure A-Law Codec	86
Configure SNMP	87
Configure Agent Desk Settings	88
Configure Cisco Unified Intelligence Center	89
Configure Cisco Finesse	90
Restart the Cisco Tomcat Service	90
Configure Cisco Finesse Administration	90
Configure Live Data	98
Initial Setup for Live Data	98
Configure Live Data with AW	98
Configure Live Data Machine Services	99
Configure Live Data for Unified Intelligence Center Data Sources	100
Restart Live Data	101
Set Up Certificates for Live Data	101
Configure Cisco Identity Service	101
Configure an Identity Provider (IdP)	102
Configure the Cisco Identity Service	108
Register Components and Set Single Sign-On Mode	110
Packaged CCE 12000 Agents Deployment	111
Configure CCE Component	112

- Configure Logger 112
- Configure Router 113
- Configure HDS-DDS 113
- Configure AW-HDS 113
- Packaged CCE Lab Only Deployments 115
 - Packaged CCE Lab Only Deployment Components 116
 - Simplex Mode 116
 - Duplex Mode 117
 - Initialize the Packaged CCE Lab Mode Deployment 119
 - Enable System Inventory, Log Collection, and Live Data Using the Inventory Content File 120
 - Inventory Content File 121

CHAPTER 2

Optional Configurations 123

- Optional Configuration for Packaged CCE 2000 Agents Deployment 123
 - Add and Maintain Remote Sites 123
 - Add Remote Site 124
 - Reconfigure Remote Site 126
 - Delete Remote Site 126
 - Add and Maintain External Machines 127
 - Add External Machines 127
 - Add Media Server as External Machine 128
 - Edit External Machines 129
 - Add PIMs to the Media Routing Peripheral Gateway 130
 - Add Multichannel PIM to 2000 Agent Deployment 131
 - Configure Email and Chat 132
- Optional Configuration for Packaged CCE 4000/12000 Agents Deployment 133
 - Remote Site 133
 - Add and Maintain Remote Site 133
 - Delete Remote Site 136
 - Machines 136
 - Add and Maintain Machines 136
 - Edit Machines 139
 - Delete Machine 140
 - Add PIMs to the Media Routing Peripheral Gateway 141

Add Multichannel PIM to Packaged CCE 4000/12000 Agents Deployment	142
Peripheral Set	143
Add and Maintain Peripheral Set	143
Delete Peripheral Set	145
Avaya Configurations	145
Add Users to Local Security Group	146
Configure and Setup Avaya Peripheral Gateway	147
Restart Live Data for Avaya PG	148
ICM-to-ICM Gateway Configurations	148
Remote ICM type application gateway global settings	149
Optional Configuration for Packaged CCE Lab deployment	150
Remote Sites in Lab Mode	150

CHAPTER 3
Packaged CCE Administration 151

Getting Started	151
Sign In	151
Single Sign-On Log Out	152
System Interface	152
Lists	153
Add Objects	154
Update Objects	154
Delete Objects	157
Popup Windows	159
Keyboard Shortcuts	159
System and Device Sync Alerts	159
System Alerts	159
Device Out of Sync Alerts	159
Infrastructure Settings	160
Smart Licensing	160
Smart Licensing Overview	160
Smart Licensing Task Flow	163
Smart Licensing Tasks	170
Smart Licensing Configurations	173
Manage Devices	174

CVP Server Services Setup	174
Configure CVP Reporting Server	203
Cisco Virtualized Voice Browser (VVB) Setup	209
Finesse	216
Single Sign-On	222
Application Gateway	225
Peripheral Gateways	226
Log Collection	226
Command Execution Pane	227
User Setup	229
Manage Agents	229
Agents	229
Add and Maintain Agents	230
Add an Agent by Copying an Existing Agent Record	234
Search for Agents	235
Manage Agent Expertise	236
Agent Reskilling	236
Edit Skill Group Membership for Multiple Agents	237
Edit Description, Desk Settings, and Teams for Multiple Agents	238
Manage Supervisors	239
Supervisor Access and Permissions	239
Add Supervisor Status to an Agent	241
Manage Roles	241
Roles	241
Manage Administrators	243
Add and Maintain Administrators	244
Administrators and System Access	245
Changing Authorization Modes of Administrators	248
Organization Setup	249
Manage Teams	249
Teams	249
Manage Skills	255
Skill Groups	256
Attributes	259

Precision Queues	261
Manage Departments	269
Departments	269
Manage Campaigns	272
Add and Maintain Agent Based Campaigns	272
Add and Maintain IVR Based Campaigns	278
Edit Contacts	283
Edit Status and Schedule	284
Save File Path of Do Not Call List Import File	284
Business Hours	285
Business Hours	285
Search for Business Hours	285
Add and Maintain Business Hours	286
Add Status Reasons	287
Edit Status for Multiple Business Hours	288
Edit Schedule for Multiple Business Hours	288
Desktop Settings	288
Resources	288
Resources	288
Manage Call Variables Layout	289
Manage Desktop Layouts	292
Manage Phone Books	306
Manage Workflows	310
Reason Labels	318
Reason Labels	318
Desk Settings	322
Desk Settings	322
Agent Trace	324
Agent Trace	324
Call Settings	325
Route Settings	325
Media Routing Domains	325
Dialed Number	327
Routing Pattern	334

- Location Configuration 335
- SIP Server Group 338
- Call Type 342
- Expanded Call Variables 344
- IVR Settings 349
 - Network VRU Scripts 349
 - File Transfers 356
- Bucket Intervals 358
 - Add and Maintain Bucket Intervals 359
- Miscellaneous 360
 - Global 360
 - Main Site 362
 - Remote Sites 363
- Feature Setup 363
 - Manage Features 363
 - Courtesy Callback 363
 - Context Service 366
 - Set up Single Sign-On 368
 - Third-party Integration 369
- Email and Chat 376
 - Email and Chat 376
- Bulk Imports 377
 - Manage Bulk Jobs 377
 - Download Bulk Job Content File Template 377
 - Add and Maintain Bulk Jobs 391
 - Review Bulk Job Details 391
- Capacity 392
 - Capacity Info 392

PART I

CHAPTER 4

- Using Configuration Manager 395**
- Configuration Manager 397**
 - Permanent Deletion 397
 - Packaged CCE 4000 and 12000 Agent Supported Tools 398

Packaged CCE 2000 Supported Tools 402

PART II

Routing and Scripting 405

CHAPTER 5

Script Editor and Internet Script Editor 407

Script Editor and Internet Script Editor 407

Administrator Privileges in Internet Script Editor 407

Install Internet Script Editor 408

Start Internet Script Editor 408

Upgrade Internet Script Editor 409

CHAPTER 6

Common Tasks 411

Common Tasks 411

The Palette 412

General Tab 412

Routing Tab 412

Targets Tab 412

Queue Tab 413

Create Routing Script 413

Add Comments to a Node 414

Specify a Connection Label Location for a Node 414

Validate Scripts 415

Open Script Explorer 415

Schedule Routing Script 416

Viewing Modes 418

Making Packaged CCE Work with Unified CVP 418

CHAPTER 7

Call Types, Contact Data, and Scripting 421

Call Types 421

Default Call Types 421

Relation Between Call Types and Scripts 421

Call Type Qualifiers 422

 Dialed Number (DN) 422

Association of Contacts with Call Types 422

Determination of Call Type for Voice Contact 422
 Determination of Call Type for ECE Web Request 423
 Determination of Call Type for a Task Routing Task 423

CHAPTER 8

Contact Categorization 425

Contact Categorization 425
 Categorization and Call Type 425
 Categorization Through Scheduling Scripts by Call Type 425
 Change Call Type to Static 425
 Change Call Type to Dynamic 426
 Change Call Type and Run a New Script 427
 Categorization by Call Type Qualifiers 428
 Categorize Contact by Dialed Number 429
 Categorization by Time and Date 430
 Categorize Contact by Date and Time 430
 Categorize Contact by the Day of Week 432
 Categorization by Branching 433
 Run a Different Script 433
 Direct Script Execution to Different Branches by Percentage 434
 Categorize Contact Based on a Condition 436
 Categorize a Contact Based on Its Media Routing Domain 436
 Categorize by External Applications 437

CHAPTER 9

Routing Target Selection 441

Routing Targets 441
 Agent Routing Nodes 441
 Transfer Calls from Agents to Agents 441
 Nodes Used to Receive Contacts 443
 Define Set of Enterprise Skill Groups to Receive the Contact 443
 Define Set of Enterprise Services to Receive the Contact 445
 Define Set of Services to Receive the Contact 446
 Send Call to a VRU with Translation Route to VRU 447
 Nodes Used to Stop Script Processing 450
 End Node 450

Release Call Node	450
Service Requested	450
ServiceRequested Variable	451
Target Requery	451
Target Requery Functionality	451
Test of the RequeryStatus Variable	452
Nodes That Support Target Requery	453
Use Target Requery	453

CHAPTER 10**Network VRUs 455**

VRU Functionality	455
Access to VRU Scripts in Packaged CCE Routing Scripts	455
Send Call to a VRU with Send to VRU Node	455
Run External Scripts	456
VRU Errors	458
Call Queuing at VRUs	459
Place a Call in Queue	460
Precision Queue Script Node	462
Precision Queue Properties Dialog Box - Static Precision Queue	463
Precision Queue Properties Dialog Box - Dynamic Precision Queue	464
Queuing Behavior of the Precision Queue Node	465
Adjust Priority of a Call in a Queue	465
Remove Call from a Queue	466
Temporarily Halt Script Execution	467

CHAPTER 11**Multichannel Routing 469**

Overview of Multichannel Services	469
Enterprise Chat and Email	469
Supported Route Requests for Enterprise Chat and Email	469
Application Request Routing with Enterprise Chat and Email	470
Synchronized Agents and Skill Groups for ECE	470
Independent Media Queues for ECE	470
Task Routing	470
Media Routing Domains	471

Media Routing Domains and Interruptibility	471
Use Media Routing Domains to Categorize Contacts	471
Pick / Pull Node	472
Skill Group and Precision Queue Routing for Nonvoice Tasks	473
Queue to Agent Node	474
Change Queue to Agent Type	474
Specify an Agent Directly	475
Select an Agent by an Expression	476
RONA and Transfer Scripting for Task Routing	478
Estimated Wait Time Scripting for Task Routing	478
Example Universal Queue Scripts	479
Selection of Agents from Skill Groups	479
Categorization by Media Routing Domain with Skill Groups	480
Categorization by Media Routing Domain with Precision Queues	481
Script That Queues to Agents	481
RONA and Transfer Script	482
Estimated Wait Time Script	483
Example Enterprise Chat and Email Scripts	485

CHAPTER 12
Use of Formulas 487

Formula Usage	487
Formula Example	487
Variables	487
Variable Syntax	488
Single-Target Variables	488
Multiple-Target Variables	488
Call Control Variables	488
Expanded Call Variables	490
ECC Payloads	490
Persistent vs. Non-persistent Call Variables	492
User Variables	492
Set Variable Node Usage	493
SkillGroup.Avail and SkillGroup.ICMAvailable Variables	494
SkillGroup.ICMAvailable Variable	494

SkillGroup.Avail Variable	494
Closed Variables	495
Operators	496
Operator Precedence	496
Prefix Operators	497
Arithmetic Operators	497
Equality Operators	497
Relational Operators	497
Logical Operators	498
Bitwise Operators	498
Miscellaneous Operators	498
Built-in Functions	499
Date and Time Functions	499
Mathematical Functions	500
Miscellaneous Functions	501
Custom Functions	502
Add Custom Functions	503
Import Custom Functions	503
Export Custom Functions	504
<hr/>	
CHAPTER 13	Scripting Specifics in a Packaged CCE Environment 505
Call Priority	505
Check for Available Agents	505
Scripts for Precision Queues	505
Precision Queue Script Node	506
Configure a Static Precision Queue	506
Configure a Dynamic Precision Queue	507
Queuing Behavior of the Precision Queue Node	507
Cancel Queuing Node	508
End Node	508
Agent to Agent Node	508
Unified CVP as a queue point	509
Interruptible vs. Non-interruptible	509

CHAPTER 14	Utility Nodes	511
	Start Node	511
	Comment Node	511
	Line Connector Node	512

CHAPTER 15	Unified CVP Scripting	515
	Writing Scripts for Unified CVP	515
	Before You Begin	515
	Scripts to Access Unified CVP from Packaged CCE	516
	Invoke Unified CVP Micro-applications Through Routing Scripts	516
	Unified CVP Call Studio Scripting	516
	Scripting for Unified CVP with Packaged CCE	517
	Micro-applications	517
	Simple Example Script: Welcome to XYZ Corporation	518
	Packaged CCE Unified CVP Micro-app Connection	519
	Information Exchange Between Packaged CCE and Unified CVP	521
	Packaged CCE Data Handling	521
	Unified CVP Script Error Checking	521
	Writing Packaged CCE Applications for Unified CVP	526
	Run External Script Node That Accesses a Unified CVP Micro-application	526
	Unified CVP Micro-applications	526
	Dynamic Audio File Support for Micro-applications	527
	Default Media Server for Micro-applications	527
	Capture Micro-application	528
	Play Media Micro-application	529
	Configure Network VRU Script for Play Media	529
	Configure Play Media Micro-application to Use Streaming Audio	531
	Play Media Examples: Play Welcome Message	534
	Play Data Micro-application	535
	Play Data and Data Storage	536
	Configure Network VRU Script Settings for Play Data Micro-application	536
	Play Back Types for Voice Data	538
	Play Data Configuration Examples	556

Get Digits Micro-application	557
Configure Network VRU Script Settings for Get Digits Micro-application	557
Get Digits Configuration Examples	560
Get Digits and Digit Entry Completion	561
Menu Micro-application	562
Configure Network VRU Script Settings for the Menu Micro-application	562
Menu Configuration Examples	564
Menu and Digit Entry Completion	565
Get Speech Micro-application	566
Configure Network VRU Script Settings for the Get Speech Micro-application	566
Passing Information to the Call Studio Scripts Executing on VXML Server	567
Passing Data Back to Packaged CCE from the VXML Server	568
Scripting for Unified CVP with Call Studio	568
High-Level Configuration Instructions	569
Call Studio ReqICMLabel Element to Pass Data	569
Integrate Call Studio Scripts with Unified CCE Scripts - Traditional Method	571
Integrate Call Studio Scripts with Packaged CCE Scripts	572
Call Studio Scripts in Unified CVP	572
Deploy Call Studio Scripts Using Call Studio	572

CHAPTER 16 **Outbound Option Scripting** 575

Outbound Option Scripting	575
---------------------------	-----

PART III **Database Administration** 577

CHAPTER 17 **Database Administration** 579

Unified CCE Database Administration	579
Historical Data	580
Database Statistics	581
Database Administration Tool	581
Create Database with Configured Components	582
Create Database Without Configured Components	583
Delete a Database	584
Expand a Database	585

Recreate a Database	586
View Database Properties	586
View Table Properties	587
Import and Export Data	587
Synchronize Database Data	587
Configure a Database Server	588
Increase the size of the disk space for an existing virtual machine	589
Database Sizing Estimator Tool	590
Start Database Sizing Estimator	591
Estimate Database Size	592
Administration and Data Server with Historical Data Server Setup	592
Set Up HDS and Add Instance	592
Set Up HDS from Added Instance	593
Database Size Monitoring	593
System Response When Database Nears Capacity	594
Allocation of More Database Space	595
Initialize Local Database (AWDB)	595
General Database Administration	595
Logger Events	596
Database Networking Support	596
Database Backup and Restore	596
Database Recovery Models	597
Database Comparison	597
Database Resynchronization	597
Synchronize Configuration Data between Loggers from Command Window	598

APPENDIX A
Troubleshooting 599

Packaged CCE Logs	599
Character Sets	601
System Performance During Database Updates	602

APPENDIX B
Reference 603

Security Certificates	603
Certificates for Live Data	603

Add Self-Signed Certificates for Live Data	604
Obtain and Upload CA Certificate for Live Data from a Third Party Vendor	604
Setup CA in Windows	605
Set up Microsoft Certificate Server for Windows 2008 R2	605
Set up Microsoft Certificate Server for Windows Server	605
Generate and Import CA Signed Certificate in AW Machine	606
Generate and Import Self-signed Certificate in AW Machine	607
Generate Self-Signed Certificate in ECE Web Server	608
Change Java Truststore Password	608
	609
Import WSM CA Certificate into CVP	609
Import CA Certificate into AW Machines	610
Add Solution Components Self-Signed Certificate to AW Machine	611
Add Finesse Certificate to AW Machine	611
Add IdS Certificate to AW Machine	612
Add ECE Web Server Certificate to AW Machine	613
Import WSM Certificate into AW Machines	613
Import VVB Self-Signed Certificate into AW Machines	615
Graceful Shutdown of Call Server or Reporting Server	616
Unified CVP Statistics	616
Call Server	616
Unified ICM Service Call Statistics	616
SIP Service Call Statistics	618
Infrastructure Statistics	621
VXML Server	624
Unified CVP VXML Server Statistics	624
Infrastructure Statistics	626
IVR Service Call Statistics	626
Unified CVP Reporting Statistics	628
Reporting Statistics	628
Infrastructure Statistics	629



Preface

- [Change History](#), on page [xxi](#)
- [About This Guide](#), on page [xxiii](#)
- [Audience](#), on page [xxiv](#)
- [Related Documents](#), on page [xxiv](#)
- [Communications, Services, and Additional Information](#), on page [xxv](#)
- [Field Notice](#), on page [xxv](#)
- [Documentation Feedback](#), on page [xxvi](#)
- [Conventions](#), on page [xxvi](#)

Change History

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

Change	See	Date
Edge Chromium (Microsoft Edge) updates	Set Up CA Certificate for Chrome and Edge Chromium (Microsoft Edge) Browsers , on page 94 Accept Security Certificates , on page 94	Dec, 2020

Change	See	Date
Added Media Server and FTP configuration details.	Add Media Server as External Machine , on page 128 Edit External Machines , on page 129 Add and Maintain Main Site in 4000 Agents or 12000 Agents Deployment Type , on page 68 Add and Maintain Remote Site , on page 133 Add and Maintain Machines , on page 136 Edit Machines , on page 139 Delete Machine , on page 140 Add and Maintain Peripheral Set , on page 143 Remote Sites in Lab Mode , on page 150 System Inventory for Packaged CCE 2000 Agents Deployment , on page 9 Initialize the Packaged CCE Lab Mode Deployment , on page 119 Simplex Mode , on page 116 Duplex Mode , on page 117	July 2019
Added information on the new Third-party Integration feature.	Third-party Integration , on page 369	
Added configuration details for Avaya.	Avaya Configurations , on page 145	
Added configuration details for ICM-to-ICM Gateway.	ICM-to-ICM Gateway Configurations , on page 148	
Appended the list of tools and added Avaya, ICM-to-ICM Gateway information.	Packaged CCE 4000 and 12000 Agent Supported Tools , on page 398	
Added additional nodes in Script Editor and information to route contacts.	Nodes Used to Receive Contacts Send Call to a VRU with Translation Route to VRU , on page 447	

Change	See	Date
Added CVP and CVP Reporting statistics.	Unified CVP Statistics Unified CVP Reporting Statistics, on page 628	May 2019
Updated the table with CVP and CVP Reporting Statistics information.	System Inventory for Packaged CCE 2000 Agents Deployment, on page 9 System Inventory for Packaged CCE 4000 Agents and 12000 Agents Deployment, on page 74	
Initial Release of Document for Release 12.0(1)		January 2019
Added post installation components configuration sections for 2000, 4000, and 12000 agents deployments.	Post Installation Configuration, on page 1	
Restructured sections as per the new Unified CCE Administration interface.	Packaged CCE Administration, on page 151	
Support for Packaged CCE 4000 and 12000 Agents deployment has been added in the CCE administration		
Added Business Hours, Email and Chat, Device Configuration, SIP Server Group, Campaigns, Routing Pattern, Location Configuration, Courtesy Callback, Resources, File Transfer features.	Business Hours, on page 285 Email and Chat, on page 376 Manage Devices, on page 174 SIP Server Group, on page 338 Manage Campaigns, on page 272 Routing Pattern, on page 334 Location Configuration, on page 335 Courtesy Callback, on page 363 Resources , on page 288 File Transfers, on page 356	
Added CA and Self-Signed certification and CVP Graceful Shutdown sections.	Security Certificates, on page 603 Graceful Shutdown of Call Server or Reporting Server, on page 616	

About This Guide

Unified CCE Administration is a set of web-based tools for creating, configuring, and maintaining objects, such as agents, teams, skill groups, and call types, that are used to operate contact centers. This guide explains the complete set of Unified CCE Administration tools that are available in a Packaged CCE deployment for

an Administrator who has the System Administrator role. Administrators with other roles, Supervisors, and those who sign in with other deployment types may not have access to all of tools documented in this guide.

Audience

This guide is prepared for:

- Contact center administrators who configure and run the contact center, manage agents and supervisors, and address operational issues.
- Contact center supervisors, who lead agent teams and are responsible for team performance.

This guide is written with the understanding that your system has been deployed by a partner or service provider who has validated the deployment type, virtual machines, and database and has verified that your contact center can receive and send calls.

Related Documents

Document or resource	Link
<i>Reporting Concepts for Cisco Unified ICM/Contact Center Enterprise</i>	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html
<i>Cisco Packaged Contact Center Enterprise Documentation Guide</i>	https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-documentation-roadmaps-list.html
Cisco.com site for Packaged CCE documentation	https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html
<i>Solution Design Guide for Cisco Packaged Contact Center Enterprise</i>	https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html
<i>Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide</i>	https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-installation-guides-list.html
<i>Cisco Packaged Contact Center Enterprise Features Guide</i>	https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html
<i>Cisco Unified Contact Center Enterprise</i>	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/tsd-products-support-series-home.html
<i>Cisco Unified Communications Manager</i>	https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

Document or resource	Link
<i>Cisco Unified Intelligence Center</i>	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/tsd-products-support-series-home.html
<i>Cisco Finesse</i>	https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/tsd-products-support-series-home.html
<i>Cisco Unified Customer Voice Portal</i>	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html
<i>Cisco Enterprise Chat and Email</i>	https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/tsd-products-support-series-home.html

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.

Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround, or other user action. For more information, see *Product Field Notice Summary* at <https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html>.

You can create custom subscriptions for Cisco products, series, or software to receive email alerts or consume RSS feeds when new announcements are released for the following notices:

- Cisco Security Advisories
- Field Notices
- End-of-Sale or Support Announcements
- Software Updates
- Updates to Known Bugs

For more information on creating custom subscriptions, see *My Notifications* at <https://cway.cisco.com/mynotifications>.

Documentation Feedback

To provide comments about this document, send an email message to the following address:
contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	<p>Boldface font is used to indicate commands, such as user entries, keys, buttons, folder names, and submenu names.</p> <p>For example:</p> <ul style="list-style-type: none"> • Choose Edit > Find. • Click Finish.
<i>italic font</i>	<p>Italic font is used to indicate the following:</p> <ul style="list-style-type: none"> • To introduce a new term. Example: A <i>skill group</i> is a collection of agents who share similar skills. • A syntax value that the user must replace. Example: IF (<i>condition, true-value, false-value</i>) • A book title. Example: See the <i>Cisco Unified Contact Center Enterprise Installation and Upgrade Guide</i>.
window font	<p>Window font, such as Courier, is used for the following:</p> <ul style="list-style-type: none"> • Text as it appears in code or that the window displays. Example: <code><html><title>Cisco Systems, Inc. </title></html></code>
< >	<p>Angle brackets are used to indicate the following:</p> <ul style="list-style-type: none"> • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.



CHAPTER 1

Post Installation Configuration

- [Packaged CCE 2000 Agents Deployment, on page 1](#)
- [Packaged CCE 4000 Agents Deployment, on page 58](#)
- [Packaged CCE 12000 Agents Deployment, on page 111](#)
- [Packaged CCE Lab Only Deployments, on page 115](#)

Packaged CCE 2000 Agents Deployment

Follow this sequence to configure components for Packaged CCE 2000 Agents deployment.

Sequence	Task
1	Configure CCE Component, on page 2
2	Configure Cisco Unified Customer Voice Portal, on page 24
3	If Media Server is external, Configure Media Server, on page 202
4	Configure Cisco Unified Communications Manager, on page 24
5	Configure Cisco Unified Intelligence Center, on page 31
6	Configure Cisco Finesse, on page 36
7	Configure Cisco Identity Service, on page 101
8	Configure Cisco Unified Customer Voice Portal Reporting Server, on page 39 (optional)
9	Configure VVB, on page 43 (optional)
10	Configure Cisco IOS Enterprise Voice Gateway, on page 43
11	Configure IPv6, on page 50
12	Configure Enterprise Chat and Email (ECE) (optional) Email and Chat, on page 376

Configure CCE Component

Follow this sequence to configure the core CCE components.

Sequence	Task
1	Configure SQL Server for CCE Components, on page 2
2	Set up Organizational Units, on page 2
3	Initialize the Packaged CCE 2000 Agents Deployment Type, on page 5
4	Add PIMs to the Media Routing Peripheral Gateway, on page 130 (optional)
5	Cisco SNMP Setup, on page 21 (optional)
6	For details on CA certificate, see Generate and Import CA Signed Certificate in AW Machine, on page 606
7	For details on self-signed certificate, see Generate and Import Self-signed Certificate in AW Machine, on page 607

Configure SQL Server for CCE Components

The following procedure must be done in Logger, Rogger, and AW Machines.

Procedure

-
- Step 1** Open **Microsoft SQL Server Management Studio**.
- Step 2** Log in.
- Step 3** Expand **Security** and then **Logins**.
- Step 4** If the BUILTIN\Administrators group is not listed:
- Right-click **Logins** and select **New Login**.
 - Click **Search** and then **Locations** to locate BUILTIN in the domain tree.
 - Type **Administrators** and click **Check Name** and then **OK**.
 - Double-click **BUILTIN\Administrators**.
 - Choose **Server Roles**.
 - Ensure that **public** and **sysadmin** are both checked.
-

Set up Organizational Units

Add a Domain

Use the Domain Manager tool to add a domain. Perform the following steps only once on the AW server.

Procedure

- Step 1** Log in with a Domain Administrator privilege.
- Step 2** Open the **Domain Manager** Tool from Unified CCE Tools shortcut on your desktop.
- Step 3** Click **Select.** under **Domains.**
- Step 4** You can add domains through the **Select Domains** dialog box, or you can add a domain manually if the target domain cannot be detected automatically.

To add domains by using the controls in the Select Domains dialog box:

- a) In the left pane under Choose domains, select one or more domains.
- b) Click **Add** to add the selected domains, or click **Add All** to add all the domains.

To add a domain manually:

- a) In the field under Enter domain name, enter the fully qualified domain name to add.
 - b) Click **Add.**
 - c) Click **OK.**
-

Add Organizational Units

Use the Domain Manager tool to create the Cisco root Organizational Unit (OU) for a domain, and then create the facility and instance OUs.

The system software always uses the root OU named Cisco_ICM. You can place the Cisco_ICM OU at any level within the domain where the Unified ICM Central Controller is installed. The system software components locate the root OU by searching for this name.

The user who creates the Cisco Root OU automatically becomes a member of the Setup Security Group for the Cisco Root OU. In effect, this user is granted privileges to all Unified CCE tasks in the domain.

Procedure

- Step 1** Log in with a domain administrator privilege and open the **Domain Manager** Tool from Unified CCE Tools shortcut on the desktop.
- Step 2** Choose the domain.
- Step 3** If this OU is the first instance, then perform the following steps to add the Cisco_ICM root:
- a) Under Cisco root, click **Add.**
 - b) Select the OU under which you want to create the Cisco root OU, then click **OK.**

When you return to the Domain Manager dialog box, the Cisco root OU appears either at the domain root or under the OU you selected. You can now add the facility.

- Step 4** Add the facility OU:
- a) Select the Cisco Root OU under which you want to create the facility OU.
 - b) In the right pane, under Facility, click **Add.**
 - c) Enter the name for the Facility, and click **OK.**

- Step 5** Add the instance OU:

- a) Navigate to and select the facility OU under which you want to create the instance OU.
- b) In the right pane, under Instance, click **Add**.
- c) Enter the instance name and click **OK**.

Step 6 Click **Close**.

Add Users to Security Groups

To add a domain user to a security group, use this procedure. The user is then granted the user privileges to the functions that are controlled by that security group.

Procedure

- Step 1** Open the Domain Manager tool and select the Security Group (**Config** or **Setup**) you want to add a user to.
 - Step 2** Under Security group, click **Members**.
 - Step 3** Under Users, click **Add**.
 - Step 4** Select the domain of the user you want to add.
 - Step 5** (Optional) In the **Optional Filter** field, choose to further filter by the Name or User Logon Name, apply the search condition, and enter the search value.
 - Step 6** Click **Search**.
 - Step 7** Select the member you want to add to the Security Group from the search results.
 - Step 8** Click **OK**.
-

Add Users to Local Administrators Group

Repeat the following steps for all the Unified CCE servers, to add the domain user or domain group to the local Administrators group.



Note You can add a domain group to local Administrators group of the server to provide users in domain group administrative permission on the server, provided the users are immediate members of the domain group.

Procedure

- Step 1** Click **Server Manager > Tools > Computer Management**.
- Step 2** Select **Local Users and Groups**.
- Step 3** Double-click **Groups**.
- Step 4** Right-click **Administrators**. Select **Properties**.
- Step 5** Click **Add** and enter the user name or domain group name in the **Edit the Object names to select** check box.
- Step 6** Select **Check Names** to validate the names.
- Step 7** After the name is successfully validated, click **OK**.
- Step 8** Click **Apply** and **OK** in the **Properties** dialog box.

Step 9 Close the **Computer Management** and **Server Manager** windows.

Initialize the Packaged CCE 2000 Agents Deployment Type

Initialize the Packaged CCE deployment using Unified CCE Administration.

When you sign into Unified CCE Administration for the first time, you are prompted to enter information and credentials for the components in your deployment. Packaged CCE uses this information to configure the components and build the System Inventory.

If you are in the process of upgrading from an earlier release, Packaged CCE prompts you only for missing information and credentials; you may not need to perform each step.



Note After a Packaged CCE deployment is initialized, you cannot switch to another deployment type.



Note The system does not support IP address change. This is applicable for all the **Hostname/ IP Address** fields.

Procedure

Step 1 Sign into **Unified CCE Administration** using the Active Directory username (*user@domain*) and password (<https://<IP Address>/cceadmin>, where <IP Address> is the address of the Side A Unified CCE AW-HDS-DDS).

The **Configure your deployment** popup window opens automatically.

Step 2 On the **Deployment Type** page, select a **Deployment Type** and an **Instance** from the respective drop-down lists. You must be a member of the Setup security group for the instance you select. Click **Next**.

Step 3 On the **VM Host** page, enter the IP address, Username, and Password for the VMware hosts for Side A and Side B.

The VMware hosts are the two servers on which ESXi is installed. The username and password fields are the host login names and passwords configured in ESXi.

- If you do not want to use the "root" user credentials. You can create user with the following permissions:

Users must have *Read* and *Reboot* permissions on the hosts. To enable these permissions in the VMware Host Client, set the following in **Manage Permissions**:

- *Anonymous*, *View*, and *Read* in **Root > System** (enabled by default).
- *Reset* in **Root > VirtualMachine > Interact**.

Note If you update the ESXi root password in Packaged CCE 2000 agent deployment, be sure to reinitialize the deployment in the Inventory page.

Step 4 Select the hardware layout type as **M3/M4 Tested Reference Configuration** or **M5 Tested Reference Configuration / Specification Based Configuration** and click **Next**.

Packaged CCE validates the hosts in your deployment.

- If you select **M3/M4 Tested Reference Configuration**, the system checks if the hardware is supported UCS hardware and verifies if the VMs are configured as per the reference design. If the validation is successful, the **Credentials** page opens.
- If you select **M5 Tested Reference Configuration / Specification Based Configuration**, the system validates the hardware specifications of the VMware host and verifies if the VMs are configured as per the reference design. If the validation is successful, click **Next** to open the **Credentials** page. See the *Virtualization for Cisco Packaged CCE* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html for hardware specifications.

- Note**
- Datastores used by Cisco VMs should not be shared or used by other third-party VMs.
 - Packaged CCE core components include:
 - Unified CCE Rogger
 - Unified CCE AW/HDS/DDS
 - Unified CCE PG
 - Unified CVP Server
 - Unified Intelligence Center Publisher (with coresident Live Data and IdS)
 - Finesse

VM annotations are used to identify Packaged CCE core component VMs. Do not change the default annotations of any of the core component VMs. The following terms are reserved for core component annotations: Cisco, Finesse, CUIC, and CVP. Do not use these reserved terms in the annotations of any of the non-core component VMs.

- Core components must be on-box, all other components have to be added as external machines. For more information, see the *Add External Machines* topic in the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide, Release 11.6(1)* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html>
 - All other non-core components are required to be added as an external machine in the Packaged CCE Inventory.
- If the validation fails, click **Update Hosts** to go back to the **VM Hosts** page and edit the values. Click **Retry** to run the validation with existing values.

- Step 5** On the **Credentials** page, enter the specified information for each component in your deployment. After entering information for a component, click **Next**.
- The system validates the credentials you entered before prompting you for the next component's information.

Component	Information Required
Unified CM	<p>Either:</p> <ul style="list-style-type: none"> The Unified CM Publisher for an on-box Unified Communications Manager deployment. The Unified CM Publisher Name and IP address for an external Unified Communications Manager deployment. <p>Note</p> <ul style="list-style-type: none"> Only a single Unified CM cluster can be integrated to a single site of Packaged CCE deployment. For M3/M4 Tested Reference Configuration, Unified CM 12.5 installation must be off-box. <p>AXL username and password.</p>
Unified CVP	<p>Unified CVP Server (Side A) Windows Administration Username and Password.</p> <p>Unified CVP Server (Side B) Windows Administration Username and Password.</p>
Unified CCE AW-HDS-DDS	<p>Unified CCE Diagnostic Framework Portico domain, username, and password.</p> <p>These credentials must be of a domain user who is a local administrator on all the CCE servers and valid on all Unified CCE components in your deployment (the Side A and Side B Unified CCE Rogers, PGs, and AW-HDS-DDSs).</p> <p>Note Every time the Active Directory credentials are updated, the credentials configured here must be updated as well.</p>
Unified Intelligence Center	<p>Unified Intelligence Center Administration application username and password.</p> <p>Identity Service Administration username and password.</p>
Finesse	<p>Finesse Administration username and password.</p>
CVP Reporting	<p>Note This tab is available only if Unified CVP Reporting server is on-box for M3/M4 Tested Reference Configuration.</p> <p>Unified CVP Reporting Server Windows Administration Username and Password used during server installation.</p>

Step 6 On the **Settings** page, select the following:

- Select the codec used for Mobile Agent calls from the **Mobile Agent Codec** drop-down menu. The codec you select must match the codec specified on the voice gateways.
- If you have an external Unified Communications Manager, select the Unified CM Subscribers to which the Side A and Side B Unified CCE PGs connect from the **Side A Connection** and **Side B Connection** drop-down menus.
- Enter the username and password for an existing Active Directory user in the same domain as the Packaged CCE servers. This account will be added to the Service group.

Click **Next**.

The deployment is initialized. The **Details** dialog box displays the status of the automated initialization tasks. See [Automated Initialization Tasks for Components, on page 8](#) for more information.

Step 7

After the automated initialization tasks complete, click **Done**.

If one of the automated initialization tasks fails, correct the errors and then click **Retry**.

If the retry is successful, the automated initialization continues.

For some task failures, all completed tasks must be reverted before the task can be retried. You see a message informing you that the system needs to be reverted to a clean state.

Click **OK**, and then after the system is in a clean state, click **Start Over**.



Note The System Inventory displays alerts for some machines when it opens after initialization completes and you click **Done**. These alerts will be cleared after you configure Unified Communications Manager.

What to do next

After you have configured the deployment, you can specify system-level settings. For example, you can enter labels for Unified Communications Manager, Unified CVP, and outbound calls. See [Miscellaneous, on page 360](#).

Automated Initialization Tasks for Components

Packaged CCE performs the following tasks during initialization.

Component	Automated Initialization Tasks
Unified CCE Rogger	<ul style="list-style-type: none"> • Creates the Logger. • Creates the Router.
Unified CCE PG	<ul style="list-style-type: none"> • Downloads JTAPI from the Unified Communications Manager, and installs it on the Unified CCE PG. • Creates the CUCM Peripheral Gateway (PG) with the CUCM PIM. • Creates the Media Routing PG (MR PG). • Creates the VRU PG with two VRU PIMs. • Creates the CTI Server.
Unified CCE AW-HDS-DDS	<ul style="list-style-type: none"> • Creates the AW-HDS-DDS. • Creates the Cisco Unified Intelligence Center SQL user account that is used for Unified Intelligence Center data sources. • Creates the Cisco Finesse SQL user account that is used for Cisco Finesse data sources.

Component	Automated Initialization Tasks
Unified Communications Manager	<ul style="list-style-type: none"> Creates the Application User that is used to configure the Unified CCE PG.
Unified Customer Voice Portal	<ul style="list-style-type: none"> Configures the Unified CVP Call Server. Configures the Unified CVP VXML Server. Configures the Unified CVP Media Server.
Unified CVP Reporting Server	<ul style="list-style-type: none"> Initializes the Unified CVP Reporting Server.
Unified Intelligence Center	<ul style="list-style-type: none"> Updates the historical and real-time data sources. Disables the AW database synchronization
Cisco Finesse	<ul style="list-style-type: none"> Configures the CTI Server settings. Configures the connection to the AW database. Disables the Reasons gadget in Finesse Administration.

System Inventory for Packaged CCE 2000 Agents Deployment



Note The System Inventory shows IPv4 addresses only.

The System Inventory is a visual display of the machines in your deployment, including: Virtual Machine Hosts (ESXi servers), Virtual Machines (VMs) on Side A, VMs on Side B, External Machines, Gateways, and Cisco Virtualized Voice Browsers (VVB). You can access the System Inventory after you have completed the change to a Packaged CCE deployment.

Access the System Inventory by navigating to **Unified CCE Administration > Infrastructure > Inventory**.

System Inventory contents are updated when you select or change the deployment type and after regular system scans. If a system scan detects VMs that do not conform to Packaged CCE requirements, the **Configure your deployment** pop-up window opens automatically, detailing the errors. You can access the System Inventory again after you have corrected the errors and completed the **Configure your deployment** pop-up window.

For more details about the Packaged CCE requirements, see **Server Status** pop-up window, see [Monitor Server Status Rules for Packaged CCE 2000 Agents Deployment, on page 19](#).

Table 1: System Inventory Layout and Actions

Item	Notes	Actions
Validate	If a system scan detects an error or warning for validation rules, correct the error, and then click Validate to run an immediate scan and verify that you corrected the problem.	Click Validate .

Item	Notes	Actions
Side A	This panel shows all VMs on Side A.	

Item	Notes	Actions
		<p>The System Inventory displays read-only information for the following VMs:</p> <ul style="list-style-type: none"> • Unified CCE Rogger • Unified CCE PG • Unified CM Subscriber 1(if on-box) <p>The following VMs are editable. Click the VM pencil icon to edit the following fields:</p> <p>Note If you change the password of any of the Packaged CCE components, you must update the password in the respective VM in the system inventory.</p> <ul style="list-style-type: none"> • Unified CCE AW-HDS-DDS—Diagnostic Framework Service Domain, Username, and Password. • Unified CM Publisher(if on-box)—AXL Username and Password. These are the credentials for connecting to the Unified CM Publisher. • CUIC-LD-IdS Publisher—Username and Password for Unified Intelligence Center Administration. Username and Password for Identity Service Administration. • Unified CVP Server— Unified CVP Server Windows credentials. Configure FTP. <p>For more information on the FTP attributes, see FTP Section in the Add Media Server as External Machine, on page 128.</p> <ul style="list-style-type: none"> • Finesse Primary—Username and Password for Cisco Finesse Administration. <p>You can launch the administration tool for these VMs by clicking the VM arrow icon:</p> <ul style="list-style-type: none"> • CUIC-LD-IdS Publisher • Unified CM Publisher <p>You can perform the full synchronization or differential synchronization of the configurations of various components. For more information on the machines that support data synchronization, see Device Out of Sync Alerts, on page 159.</p> <p>Note To enable CVP Statistics feature in Packaged CCE 12.0(1), install the ICM12.0(1) ES</p>

Item	Notes	Actions
		<p>patch. For more information, see <i>Release Notes for Packaged Contact Center Enterprise</i> at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html.</p> <p>You can launch statistics for the following VMs by clicking the Statistics icon:</p> <ul style="list-style-type: none">• Unified CVP• Unified CVP Reporting <p>For more information, see Unified CVP Statistics, on page 616 and Unified CVP Reporting Statistics, on page 628.</p>

Item	Notes	Actions
Side B	This panel shows all VMs on Side B.	

Item	Notes	Actions
		<p>The System Inventory displays read-only information for the following VMs:</p> <ul style="list-style-type: none"> • Unified CCE Rogger • Unified CCE PG • Unified CCE AW-HDS-DDS • Unified CM Subscriber 2(if on-box) • CUIC-LD-IdS Subscriber • Finesse Secondary • ECE Data Server <p>The following VMs are editable. Click the VM pencil icon to edit the following fields:</p> <p>Note If you change the password of any of the Packaged CCE components, you must update the password in the respective VM in the system inventory.</p> <ul style="list-style-type: none"> • Unified CVP - Unified CVP Server Windows credentials. Configure FTP. <p>For more information on the FTP attributes, see FTP Section in the Add Media Server as External Machine, on page 128.</p> <ul style="list-style-type: none"> • Unified CVP Reporting - Cisco Unified CVP Reporting Server Windows credentials. <p>If the CVP Reporting server VM is re-imaged or re-installed, you need to initialize the CVP Reporting server.</p> <p>To initialize the CVP Reporting Server , click the Initialize icon and then click Yes to confirm.</p> <p>Note Initialization removes existing call server association and Courtesy Callback configuration.</p> <p>To re-associate call servers with CVP Reporting server, navigate to Overview > Infrastructure Settings > Device Configuration > Device Configuration.</p> <p>To reconfigure Courtesy Callback, navigate to Overview > Features > Courtesy Callback.</p> <p>You can perform the full synchronization or differential</p>

Item	Notes	Actions
		<p>synchronization of the configurations of various components. For more information on the machines that support data synchronization, see Device Out of Sync Alerts, on page 159.</p> <p>You can launch statistics for the following VMs by clicking the Statistics icon:</p> <ul style="list-style-type: none">• Unified CVP• Unified CVP Reporting <p>For more information, see Unified CVP Statistics, on page 616 and Unified CVP Reporting Statistics, on page 628.</p>

Item	Notes	Actions
External Machines		<p>To add or update the external machines, see Add External Machines, on page 127.</p> <p>You can perform the full synchronization or differential synchronization of the configurations of various components. For more information on the machines that support data synchronization, see Device Out of Sync Alerts, on page 159.</p> <p>Note If you change the password of any of the Packaged CCE components, you must update the password in the respective VM in the system inventory.</p> <p>Note If you edit the Unified CM Publisher, the Unified CM Subscribers associated with the publisher are updated automatically. You cannot edit Unified CM Subscribers from the System Inventory.</p> <p>To associate the external HDS with a default Cisco Identity Service (IdS) for single sign-on:</p> <ol style="list-style-type: none"> 1. Click the pencil icon on the external HDS. 2. Click the Search icon next to Default Identity Service. 3. Enter the machine name for the Cisco IdS in the Search field or choose the Cisco IdS from the list. 4. Click Save. <p>To delete, click the x on the machine. Confirm the deletion.</p> <p>You can open the administration tool for these external machines by clicking the arrow icon in the machine box:</p> <ul style="list-style-type: none"> • Unified CM Publisher • SocialMiner • MediaSense

Item	Notes	Actions
	<p>This section shows all external machines in the deployment, and can include any of the following:</p> <ul style="list-style-type: none"> • HDS • Unified CM Publisher • Unified CM Subscriber • SocialMiner • ECE Data Server (refers to ECE Data Server VM for 400 agents and Services Server VM for ECE 1500 agents) • ECE Web Server • 3rd Party Multichannel • Unified CVP Reporting • MediaSense • Unified SIP Proxy • Virtualized Voice Browser • Gateway • Media Server <p>Note</p> <ul style="list-style-type: none"> • Unified CM Subscriber machines are dedicated to the contact center. When you configure an external Unified CM Publisher, its Unified CM Subscribers are added to the System Inventory automatically. 	

Monitor Server Status Rules for Packaged CCE 2000 Agents Deployment

In Packaged CCE 2000 Agents deployment, the Inventory displays the total number of alerts for machines with validation rules. Click the alert count to open the **Server Status** popup window, which lists all of the rules for that machine and indicates which have warnings and errors. Rules are grouped by these categories:

Server Status Category	Description	Example Rules
Configuration	<p>Rules for installation and configuration of a component.</p> <p>These rules identify problems with mismatched configuration between components, missing services, and incorrectly configured services.</p>	<p>Unified CCE Rogger: The trace level must be set to normal to ensure performance.</p> <p>Unified CVP: The names of the SIP Server Groups on CVP containing Communications Manager addresses must match the Communications Manager Cluster Fully Qualified Domain Name.</p>
Operations	<p>Rules for the runtime status of a component.</p> <p>These rules identify services and processes that cannot be reached, are not running, or are not in the expected state.</p>	<p>Unified CCE Rogger: The central controller agent process (ccagent.exe) must be in service for both PGs.</p> <p>Note Webex Experience Management and Call Transcript should be reachable on Network.</p>
System Health	<p>Metrics to monitor the CPU, memory, and disk usage of a component's Virtual Machine (VM) as reported by ESXi over the last 10 minutes. The memory and CPU usage may differ slightly from system tools reported by the VM itself. For VM Hosts, these metrics also include datastore performance information.</p> <p>For VM Hosts under M5 Tested Reference Configuration / Specification Based Configuration, these metrics include CPU reservation, CPU oversubscription, memory reservation and datastore utilization information.</p>	<p>All: Memory usage as reported by ESXi - 17%</p> <p>For VM Hosts under M5 Tested Reference Configuration / Specification Based Configuration:</p> <ul style="list-style-type: none"> • Maximum CPU Reservation - 65% • Maximum CPU Oversubscription - 200% • Maximum Memory Reservation - 80% • Maximum Storage Usage per Datastore - 80%
VM	VM requirements for a component.	All: VMware Tools must be up to date

Server Status Category	Description	Example Rules
System Validation	<p>Rules for Unified CCE database and configuration settings.</p> <p>These rules identify whether the configuration of objects in your deployment match the requirements and limits for Packaged Contact Center Enterprise.</p> <p>Note The System Validation category is available only for the Side A Unified CCE AW-HDS-DDS.</p>	<p>Side A Unified CCE AW-HDS-DDS: Agent Desk Settings: Ring No Answer Times must not be set.</p> <p>Side A Unified CCE AW-HDS-DDS: Application Gateway</p> <p>Side A Unified CCE AW-HDS-DDS: Application Instance: Up to 12 Application Instances can be defined.</p>

VM Validation

The validation for the Packaged CCE: 2000 Agents deployment type makes the following checks to ensure hardware compliance and conformance with the Cisco-provided OVA files.

- For Hosts:
 - BIOS
 - Minimum number of CPU cores
 - Minimum memory
 - Data store size
- For VMs:
 - Number of virtual CPU cores
 - Number of configured networks
 - Virtual network card driver (except for Unified CM)
 - VM is powered on
 - CPU reservation
 - Exact memory
 - Exact disk size
 - Exact number of disks
 - VMware tools

Configure Cisco Unified Contact Center Enterprise PG

The following table outlines the configuration task for Media Routing Peripheral Gateway for the Packaged CCE 2000 Agents deployment.

Configuration Task

[Add PIMs to the Media Routing Peripheral Gateway, on page 130](#) (optional)

Cisco SNMP Setup

Complete the following procedures to configure Cisco SNMP:

- [Add Cisco SNMP Agent Management Snap-In, on page 21](#)
- [Save Cisco SNMP Agent Management Snap-In View, on page 21](#)
- [Set Up Community Names for SNMP V1 and V2c , on page 22](#)
- [Set Up SNMP User Names for SNMP V3 , on page 22](#)
- [Set Up SNMP Trap Destinations , on page 23](#)
- [Set Up SNMP Syslog Destinations , on page 23](#)

Add Cisco SNMP Agent Management Snap-In

You can configure Cisco SNMP Agent Management settings using a Windows Management Console snap-in. Complete the following procedure to add the snap-in and change Cisco SNMP Management settings.

Procedure

-
- Step 1** From the Start menu, enter **mmc.exe /32**.
 - Step 2** From the Console, choose **File > Add or Remove Snap-ins**.
 - Step 3** In the Add or Remove Snap-ins dialog box, choose **Cisco SNMP Agent Management** from the list of available snap-ins. Click **Add**.
 - Step 4** In the Selected snap-ins pane, double-click **Cisco SNMP Agent Management**.
 - Step 5** In the Extentions for Cisco SNMP Agent Management dialog box, select **Always enable all available extentions**. Click **OK**.
 - Step 6** In the Add/Remove Snap-in window, click **OK**. The Cisco SNMP Agent Management Snap-in is now loaded into the console.
-

Save Cisco SNMP Agent Management Snap-In View

After you load the Cisco SNMP Agent Management MMC snap-in, you can save the console view to a file with a .MSC file extension. You can launch the file directly from Administrative Tools.

Complete the following procedure to save the Cisco SNMP Agent Management snap-in view.

Procedure

-
- Step 1** Choose **File > Save**.
 - Step 2** In the Filename field, enter **Cisco SNMP Agent Management**.

- Step 3** In the Save As type field, choose a file name to map to the administrative tools such as **Microsoft Management Console Files (*.msc)**.
- Step 4** Click **Save**.
-

Set Up Community Names for SNMP V1 and V2c

If you use SNMP v1 or v2c you must configure a community name so that Network Management Systems (NMSs) can access the data your server provides. Use SNMP community names to authenticate data exchange of SNMP information. An NMS can exchange SNMP information only with servers that use the same community name.

Complete the following procedure to configure the community name for SNMP v1 and v2c.

Before you begin

Ensure Cisco SNMP is added and saved using the procedures [Add Cisco SNMP Agent Management Snap-In, on page 21](#) and [Save Cisco SNMP Agent Management Snap-In View, on page 21](#).

Procedure

- Step 1** Choose **Start > All Programs > Administrative tools > Cisco SNMP Agent Management**.
- Step 2** Right-click **Cisco SNMP Agent Management** and choose **Run as administrator**.
- Step 3** The Cisco SNMP Agent Management screen lists some of the configurations that require SNMP for traps and system logs.
- Step 4** Right-click **Community Names (SNMP v1/v2c)** and choose **Properties**.
- Step 5** In the Community Names (SNMP v1/v2c) Properties dialog box, click **Add New Community**.
- Step 6** In the Community Name field, enter a community name.
- Step 7** In the Host Address List, enter the host IP address.
- Step 8** Click **Apply** and click **OK**.
-

Set Up SNMP User Names for SNMP V3

If you use SNMP v3 you must configure a user name so that NMSs can access the data your server provides.

Complete the following procedure to configure a user name for SNMP v3.

Before you begin

Ensure Cisco SNMP is added and saved using the procedures [Add Cisco SNMP Agent Management Snap-In, on page 21](#) and [Save Cisco SNMP Agent Management Snap-In View, on page 21](#).

Procedure

- Step 1** From the Console Root, choose **Cisco SNMP Agent Management > User Names (SNMP v3) > Properties**.
- Step 2** Click **Add New User**.
- Step 3** In the User Name field, enter a username.

- Step 4** Click **Save**.
 - Step 5** The username appears in the Configured Users pane at the top of the dialog box.
 - Step 6** Click **Apply** and click **OK**.
-

Set Up SNMP Trap Destinations

You can configure SNMP Trap Destinations for SNMP v1, SNMP v2c, and SNMP v3. A Trap is a notification that the SNMP agent uses to inform the NMS of a certain event.

Complete the following procedure to configure the trap destinations.

Before you begin

Ensure Cisco SNMP is added and saved using the procedures [Add Cisco SNMP Agent Management Snap-In, on page 21](#) and [Save Cisco SNMP Agent Management Snap-In View, on page 21](#).

Procedure

- Step 1** From the Console Root, choose **Cisco SNMP Agent Management > Trap Destinations > Properties**.
 - Step 2** Click **Add Trap Entity**.
 - Step 3** Click the SNMP version that your NMS uses.
 - Step 4** In the Trap Entity Name field, enter a name for the trap entity.
 - Step 5** Choose the User Name/Community Name that you want to associate with this trap. This list is auto-populated with existing configured users/community names.
 - Step 6** Enter one or more IP addresses in the IP Address entry field. Click **Insert** to define the destinations for the traps.
 - Step 7** Click **Apply** and click **Save** to save the new trap destination.
The trap entity name appears in the Trap Entities section at the top of the dialog box.
 - Step 8** Click **OK**.
-

Set Up SNMP Syslog Destinations

You can configure Syslog destinations for SNMP from the Cisco SNMP Agent Management Snap-in.

Complete the following procedure to configure Syslog destinations.

Procedure

- Step 1** From the Console Root, choose **Cisco SNMP Agent Management > Syslog Destinations > Properties**.
- Step 2** Choose an Instance from the list box.
- Step 3** Check **Enable Feed**.
- Step 4** Enter an IP address or host name in the Collector Address field.
- Step 5** Click **Save**.

Step 6 Click **OK** and restart the logger.

Configure Cisco Unified Customer Voice Portal

The following table outlines the Cisco Unified Customer Voice Portal (CVP) configuration tasks for Packaged 2000 Agents deployment.



Note The CVP configurations are site specific. Side A and Side B configurations per site must be the same.

Configuration Tasks

To secure communication between Call Server and ICM, see [Secure GED 125 Communication between Call Server and ICM, on page 183](#).

For more information about securing CVP communication, see [Unified CVP Security, on page 183](#)

For web secure communication, see [, on page 609](#)

To change the default settings, see [CVP Server Services Setup, on page 174](#)

[Configure Media Server, on page 202](#)

[Configure SNMP, on page 82](#)

Configure Cisco Unified Communications Manager

The following table outlines the Cisco Unified Communications Manager configuration tasks for Packaged CCE 2000 Agents deployment.

Configuration Tasks

For details on CA and self-signed certificate, see [Secure Communication on CUCM, on page 192](#)

[Configure Fully Qualified Domain Name, on page 25](#)

[Configure Cisco Unified Communications Manager Groups, on page 25](#)

[Configure Conference Bridges, on page 26](#)

[Configure Media Termination Points, on page 26](#)

[Transcoder Configuration in Unified CM and IOS Gateway, on page 27](#)

[Configure Media Resource Groups, on page 27](#)

[Configure and Associate Media Resource Group List, on page 28](#)

[Configure CTI Route Point, on page 28](#)

[Configure Ingress Gateways for Locations-based Call Admission Control, on page 29](#)

Configuration Tasks[Add a SIP Profile in Unified CM, on page 29](#)[Configure Trunk, on page 30](#)[Configure Route Group, on page 30](#)[Configure Route List, on page 31](#)[Configure Route Pattern, on page 31](#)

Configure Fully Qualified Domain Name

Procedure

-
- Step 1** Open Cisco Unified Communications Manager and log in.
- Step 2** Navigate to **System > Enterprise Parameters**.
- Step 3** Fill in **Clusterwide Domain Configuration > Cluster Fully Qualified Domain Name** with the Fully Qualified Domain Name of your cluster.

Example:

ccm.hcsec.icm

Note The Cluster Fully Qualified Domain Name is the name of the Unified Communications Manager Server Group defined in Unified CVP.

- Step 4** Click **Save**.
-

Configure Cisco Unified Communications Manager Groups

Complete the following procedure to add a Cisco Unified Communications Manager to the Unified Communications Manager Group.

Procedure

-
- Step 1** Select Cisco Unified CM Administrator from the **Navigation** menu and click **Go**.
- Step 2** Select **System > Cisco Unified CM Group**.
- Step 3** Click **Find**. Then click **Default**.
- Step 4** Move the two subscribers from the Available panel to the Selected panel.
- Step 5** Click **Save**.
- Step 6** Click **Reset**.
- Step 7** On the **Device Reset** popup, click **Reset**.
- Step 8** Click **Close**.
-

Configure Conference Bridges

Perform this procedure for each gateway in the deployment.

Procedure

- Step 1** Select **Media Resources > Conference bridge**.
- Step 2** Click **Add New**.
- Step 3** Select Conference Bridge Type of **Cisco IOS Conference Bridge**.
- Step 4** In the **Conference Bridge name** field, enter a unique identifier for the conference bridge name that matches the configuration on the gateway.
- In the example, this is gw70conf.
- ```
Add a SCCP group for each of the hardware resource types
sccp ccm group 1
associate ccm 1 priority 1
associate profile 2 register gw70mtp
associate profile 1 register gw70conf
associate profile 3 register gw70xcode
```
- Step 5** Select a Device Pool.
- Step 6** Click **Save**.
- Step 7** Click **Apply Config**.
- 

## Configure Media Termination Points

Complete this procedure for each gateway in the deployment.

### Procedure

---

- Step 1** Select **Media Resources > Media Termination Point**.
- Step 2** Click **Add New**.
- Step 3** In the Media Termination Point Name field, enter a unique identifier for the media termination that coincides with the configuration on the gateway.
- In the example, this is gw70mtp.
- ```
# Add a SCCP group for each of the hardware resource types
sccp ccm group 1
associate ccm 1 priority 1
associate profile 2 register gw70mtp
associate profile 1 register gw70conf
associate profile 3 register gw70xcode
```
- Step 4** Select a Device Pool.
- Step 5** Click **Save**.
- Step 6** Click **Apply Config**.
-

Transcoder Configuration in Unified CM and IOS Gateway

A transcoder is required for multicodec scenarios to convert a stream from a G.711 codec to a G.729 codec.

For more information about transcoder configuration in Unified Communications Manager and gateway, see the section "Configure Transcoders and Media Termination Points" in the *System Configuration Guide for Cisco Unified Communications Manager* at <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>.

Configure Transcoders

Perform this procedure for each gateway in the deployment.

Procedure

- Step 1** In Unified Communications Manager Administration, select **Media Resources > Transcoder**.
- Step 2** Click **Add New**.
- Step 3** For Transcoder Type, select **Cisco IOS enhanced media termination point**.
- Step 4** In the **Device Name** field, enter a unique identifier for the transcoder name that coincides with the configuration on the gateway.

In the following example, this is gw70xcode.

```
# Add a SCCP group for each of the hardware resource types
sccp ccm group 1
associate ccm 1 priority 1
associate profile 2 register gw70mtp
associate profile 1 register gw70conf
associate profile 3 register gw70xcode
```

- Step 5** In the **Device Pool** field, select the appropriate device pool.
 - Step 6** Click **Save**.
 - Step 7** Click **Apply Config**.
-

Configure the CVP Call Server Dial Peers in Ingress Gateway

The Ingress Gateway to Unified CVP outbound dial peer configuration uses the IPv4 address of Unified CVP as the session target.

Configure Media Resource Groups

Procedure

- Step 1** Select **Media Resources > Media Resource Group**.
- Step 2** Add a Media Resource Group for Conference Bridges.
 - a) Click **Add New**.
 - b) Enter a Name.
 - c) From the Available list, select all the Cisco IOS conference bridge resources configured for each ingress/VXML combination gateway in the deployment and add them to the group.

d) Click **Save**.

Step 3 Add a Media Resource Group for Media Termination Point.

a) Click **Add New**.

b) Enter a Name.

c) From the Available list, select all the hardware media termination points configured and add them to the group.

d) Click **Save**.

Step 4 Add a Media Resource Group for Transcoder.

a) Click **Add New**.

b) Enter a Name.

c) From the Available list, select all the transcoders configured and add them to the group.

d) Click **Save**.

Step 5 Click **Save**.

Configure and Associate Media Resource Group List

Procedure

Step 1 Select **Media Resources > Media Resource Group List**.

Step 2 Click **Add New** and enter a Name.

Step 3 Add a Media Resource Group list and associate all of the media resource groups. Click **Save**.

Step 4 Select **System > Device Pool**. Click **Find**. Select the appropriate device pool.

Step 5 From the Media Resource Group List drop-down list, choose the media resource group list added in Step 2.

Step 6 Click **Save**. Click **Reset**.

Configure CTI Route Point

Complete the following procedure to add a computer telephony integration (CTI) route point for agents to use for transfers and conferences.

Procedure

Step 1 In Cisco Unified CM Administration, select **Device > CTI Route Point**.

Step 2 Click **Add New**.

Step 3 Set a device name; for example, **PCCEInternalDNs**.

Step 4 For Device Pool, select **Default**.

Step 5 Select a Media Resource Group List from the list.

Step 6 Click **Save**.

Step 7 Click on Line [1] to configure the directory number associated with this route point.

This directory number will be a pattern that is intended to match any of the internal Dialed Numbers you configure in Packaged CCE for internally routed calls. (For instance, for Transfers and Conferences).

Important Define a pattern that is flexible enough to match all your internal dialed numbers yet restrictive enough not to inadvertently intercept calls intended for other Route Patterns you may have defined for other parts of your dial plan. Use a unique prefix for internal calls. For example, if you have internal dialed numbers 1230000 and 1231111, then an appropriate line number to enter for the cti route point would be 123XXXX.

- Step 8** Select **User Management** > **Application User**.
- Step 9** Select *pguser* created during Packaged CCE automated initialization.
- Step 10** Select the CTI Route Point from the list of **Available Devices**, and add it to the list of **Controlled Devices**.
- Step 11** Click **Save**.

Configure Ingress Gateways for Locations-based Call Admission Control

Locations-based call admission control (CAC) is used in the Unified CCE branch-office call flow model (also known as the Centralized Model). This means that all servers (Unified CVP, Unified CCE, Unified Communications Manager, and SIP Proxy server) are centralized in one or two data centers, and each branch office.

Configure Unified Communications Manager to use the Ingress gateway instead of Unified CVP as the originating location of the call. This configuration ensures that CAC can be properly adjusted based on the locations of the calling endpoint and the phone.



Important Do not define Unified CVP as a gateway device in Unified Communications Manager.

Procedure

In Cisco Unified CM Administration, define the Ingress gateways as gateway devices. Assign the correct location to the devices.

Add a SIP Profile in Unified CM

This option allows a dual-stack SIP trunk to offer both IPv4 and IPv6 media. Perform this procedure for IPv6-enabled deployments only.

Procedure

-
- Step 1** From **Cisco Unified CM Administration**, choose **Device** > **Device Settings** > **SIP Profile**.
 - Step 2** Click **Add New** and enter the name of the SIP profile.
 - Step 3** Check the **Enable ANAT** check box on the SIP Profile.

Step 4 Save your changes.

Configure Trunk

There are two Unified CVP Servers and each must be associated with a SIP trunk in Unified Communications Manager. The following procedure explains how to configure the SIP trunks, each targeting a different Unified CVP Server.

Actual site topology may necessitate the use of alternate SIP trunk plans, which are supported as long as both Unified CVP Servers are targeted by the configured SIP trunks.

Procedure

Step 1 In Unified Cisco CM Administration, select **Device > Trunk**.

Step 2 Click **Add New**.

Step 3 From the Trunk Type drop-down list, choose **SIP Trunk**, and then click **Next**.

Step 4 Enter the following in the **Device Information** section:

- a) In the **Device Name** field, enter a name for the SIP trunk, for example, **sipTrunkCVPA**.
- b) In the **Device Pool** drop-down list, select the device pool that the customer has defined.
- c) Select a Media Resource Group List from the list.
- d) Make sure that the **Media Termination Point Required** check box is not checked.

Step 5 Scroll down to the **SIP Information** section:

- a) In Row 1 of the **Destination** table, enter the IP address of a CVP server. Accept the default destination port of 5060.
- b) In the **SIP Trunk Security Profile** drop-down list, select **Non Secure SIP Trunk Profile**.
- c) In the **SIP Profile** drop-down list, select **Standard SIP Profile**.

Note If you are using an IPv6-enabled deployment, use the SIP Profile created in [Add a SIP Profile in Unified CM, on page 29](#).

- d) In the **DTMF Signaling Method** drop-down list, select **RFC 2833**.

Step 6 Click **Save**.

Step 7 Click **Reset**.

Step 8 Repeat for all the remaining Unified CVP servers in the deployment.

Configure Route Group

Complete the following procedure to create a route group.

Procedure

Step 1 In Unified Communications Manager, select **Call Routing > Route Hunt > Route Group**.

Step 2 Click **Add New**.

- Step 3** Enter a name for the route group; for example, **CVP Route Group**.
 - Step 4** Using the Add to Route Group button, add all CVP Trunks as Selected Devices.
 - Step 5** Click **Save**.
-

Configure Route List

Complete the following procedure to add a route list to the route group.

Procedure

- Step 1** In Unified Communications Manager, select **Call Routing > Route Hunt > Route List**.
 - Step 2** Click **Add New**.
 - Step 3** Enter a name for the route list; for example, **CVP Route List**.
 - Step 4** Select a Cisco Unified Communications Manager Group.
 - Step 5** Add the route group you created.
 - Step 6** Click **Save**.
-

Configure Route Pattern

Complete the following procedure to add a route pattern to the route list.

Procedure

- Step 1** In Unified Communications Manager, select **Call Routing > Route Hunt > Route Pattern**.
 - Step 2** Click **Add New**.
 - Step 3** Enter a route pattern of **88811111000xxxx**.
 - Step 4** Select the route list that you created.
 - Step 5** Keep all defaults in all panels
 - Step 6** Click **Save**.
 - Step 7** Click **OK** at the message about the Forced Authorization Code. You do not want a Forced Authorization Code.
-

Configure Cisco Unified Intelligence Center

Follow this sequence to configure the Cisco Unified Intelligence Center for Packaged CCE 2000 Agentsdeployment

Sequence	Task
1	For details on security certificate, see <i>Cisco Unified Intelligence Center User Guide</i> at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-user-guide-list.html
2	For details on self-signed certificate, see Add IdS Certificate to AW Machine, on page 612
3	Download Report Bundles, on page 33
4	Import Reports, on page 33
5	Configure Unified Intelligence Center Administration, on page 35

Configure Unified Intelligence Center Data Sources for External HDS

Perform this procedure only if your deployment includes an external HDS and you wish to have a longer retention period.

Before you begin

Configure the Unified Intelligence Center SQL user for the External HDS databases before configuring the data sources (applicable for 4000 Agents and 12000 Agents). For more information, refer the Configure Unified Intelligence Center SQL User Account on the External HDS section in the Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-installation-guides-list.html>

Procedure

-
- Step 1** Sign in to Unified Intelligence Center with your Cisco Intelligence Center administrator account (<https://<hostname/ IP address of CUIC Publisher>:8444/cuicui>).
- Step 2** Select **Configure > Data Sources**.
- Step 3** Click **Data Sources** in the left panel.
- Step 4** Select the **UCCE Historical** data source. Click **Edit**.
- In the **Datasource Host** field, enter the IP Address of the external HDS server.
 - In the **Port** field, enter the AW SQL server port number. The default is **1433**.
 - In the **Database Name** field, enter **{instance}_awdb**.
 - Leave the **Instance** field blank.
 - Select the **Timezone**.
 - In the **Database User ID**, enter the user name that you configured for the Cisco Unified Intelligence Center SQL Server user account.
 - Enter and confirm the SQL Server User **password**.
 - Select the **Charset** based on the collation of SQL Server installation.
 - Click **Test Connection**.
 - Click **Save**.
- Step 5** Click the **Secondary** tab to configure Unified CCE Historical Data Source.
- Check the **Failover Enabled** checkbox.

- b) In the **Datasource Host** field, enter the IP address of the second external HDS server.
- c) In the **Port** field, enter **1433**.
- d) In the **Database Name** field, enter **{instance}_awdb**.
- e) Complete other fields as in the Primary tab.
- f) Click **Test Connection**.
- g) Click **Save**.

Step 6 Repeat this procedure for the **UCCE Realtime** datasource for 4000 or 12000 Agents deployment. The **Database Name** for the Realtime Data Source is **{instance}_awdb**.

Download Report Bundles

The following Cisco Unified Intelligence Center report bundles are available as downloads from Cisco.com <https://software.cisco.com/download/type.html?mdfid=282163829&catid=null>. Click the **Intelligence Center Reports** link to view all available report bundles:

- Realtime and Historical Transitional templates - Introductory templates designed for new users. These templates are simplified versions of the All Fields templates, and are similar to templates available in other contact center solutions.
- Realtime and Historical All Fields templates - Templates that provide data from all fields in a database. These templates are most useful as a basis for creating custom report templates.
- Live Data templates - Templates that provide up to the moment data for contact center activity.
- Realtime and Historical Outbound templates - Templates for reporting on Outbound Option activity. Import these templates if your deployment includes Outbound Option.
- Realtime and Historical SocialMiner templates - Templates for reporting on SocialMiner activity. Import these templates if your deployment includes SocialMiner.
- Cisco Unified Intelligence Center Admin Security templates - Templates to report on Cisco Unified Intelligence Server audit trails, permissions, and template ownership.

Some of the templates in these bundles are not applicable in Cisco Packaged CCE deployment. See the *Cisco Packaged Contact Center Enterprise Reporting User Guide* at https://www.cisco.com/en/US/products/ps12586/tsd_products_support_series_home.html for more information about the templates used in Packaged CCE deployments.

Additionally, sample custom report templates are available from Cisco DevNet (<https://developer.cisco.com/site/reporting/documentation/>) and include templates for:

- Enterprise Chat and Email
- Cisco Unified Customer Voice Portal (Unified CVP)

When downloading report template bundles, select bundles for the version of software deployed in your contact center.

Import Reports

You can import the Unified Intelligence Center report, which is in either .xml or .zip file format.

The imported report retrieves data for the following entities:

- Report
- Report Definition
- Value Lists
- Views
- Thresholds
- Drilldowns
- Template Help



Note Each report template help folder has a size limit of 3 MB. If the folder size exceeds this limit, the system does not load the help content.



Note You cannot import Report Filters and Collections.

To import reports, perform the following steps:

Procedure

- Step 1** In the left navigation pane, choose **Reports**.
- Step 2** In the **Reports** listing page, click **Import**.
- Step 3** Click **Browse** to select the file (.xml or .zip format) to be imported.
Note Maximum file size for .zip file format is 60 MB and for .xml file format is 3 MB.
- Step 4** Select the required file and click **Open**.
- Step 5** Select the file location from the **Save to Folder** list to save the file.
- Step 6** Click **Upload**.
 Once the file is successfully uploaded, the table gets populated with the corresponding report template, current available version, and incoming version of the files being imported.
- Step 7** Select a Data Source for the Report Definition only if the Report Definition for the report being imported is not defined in Unified Intelligence Center.
- Step 8** Select a Data Source for the Value List that is defined in the Report Definition.
Note Selection of a Data Source for the Value List is mandatory:
 - If the Value List does not use the same Data Source as the Report Definition.
 - For Real Time Streaming Report Definitions.
- Step 9** Select the files to import or overwrite.

- Overwrite—If the report being imported exists in the Unified Intelligence Center.
- Import—If the report being imported is the new set of report files.

Step 10 Click **Import**.

- Note**
- Importing a report to a different version of Unified Intelligence Center is not supported. However, when you upgrade Unified Intelligence Center, report templates continue to work in the upgraded version.
 - Importing manually edited XMLs is not supported.

Configure Unified Intelligence Center Administration

Procedure

Step 1 Sign in to the **Cisco Unified Intelligence Center Administration Console**

(<https://<hostname>:8443/oamp>).

Step 2 Configure the Active Directory tab under **Cluster Configuration > Reporting Configuration**.

- Enter the Host Address for the Primary Active Directory Server.
- Leave the default value for Port.
- Complete the **Manager Distinguished Name** fields.
- Enter and confirm the password with which the Manager accesses the domain controller.
- For User Search Base, specify the Distinguished Name or Organization Unit of the domain you want to search.
- For Attribute for User ID, select the required option.

Note If the Windows domain name and the NETBIOS names are different, do the following: in the **Cisco Unified Intelligence Center Administration Console**, under **Active Directory Settings**, in the field **Attribute for User ID**, ensure to select *sAMAccountName*, and add the *NETBIOS* value to set it as default value.

- Add at least one domain for the UserName Identifier. Do not type the @ sign before the domain name.
- Set a domain as the default.
- Click **Test Connection**.
- Click **Save**.

Note For more details, see the online help.

Step 3 Configure syslog for all devices.

- Choose **Device Management > Logs and Traces Settings**.
- For each host address:
 - Select the associated servers and click the arrow to expand.
 - Select the server name.

- In the **Edit Serviceability Settings** screen **Syslog Settings** pane, configure the Primary and Backup Host. Click **Save**.

- Step 4** Configure SNMP for all devices, if used.
- Select **Network Management > SNMP**.
 - Navigate to SNMP and for each server add the following:
 - V1/V2c Community Strings.
 - Notification Destination.

Configure Cisco Finesse

Follow this sequence to configure the Cisco Finesse for Packaged CCE 2000 Agents deployment

Sequence	Task
1	For details on CA certificate, see <i>Cisco Finesse Administration Guide</i> at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html
2	For details on self-signed certificate, see Add Finesse Certificate to AW Machine, on page 611
3	Configure Contact Center Agents and Routing for Live Data Reports, on page 36
4	Live Data Reports, on page 37

Configure Contact Center Agents and Routing for Live Data Reports

In order to test the Live Data reports in the Finesse desktops, configure the following in Unified CCE Administration(<https://<Side A/B Unified CCE AW-HDS-DDS IP address>/cceadmin>):

- Agents
- Skill groups or precision queues
- Call types
- Dialed numbers
- Network VRU scripts
- Routing scripts



Note Routing scripts are configured in Script Editor, which you can open from Unified CCE Administration Tools.

Live Data Reports

Cisco Unified Intelligence Center provides Live Data real-time reports that you can add to the Finesse desktop.

Add Live Data Reports to Finesse

The following sections describe how to add the Live Data reports to the Finesse desktop. The procedure that you follow depends on several factors, described in the following table.

Procedure	When to use
Add Live Data reports to default desktop layout	Use this procedure if you want to add Live Data reports to the Finesse desktop after a fresh installation or after an upgrade if you have not customized the default desktop layout.
Add Live Data reports to custom desktop layout	Use this procedure if you have customized the Finesse desktop layout.
Add Live Data reports to team layout	Use this procedure if you want to add Live Data reports to the desktop layout for specific teams only.

Add Live Data Reports to Default Desktop Layout

The Finesse default layout XML contains commented XML code for the Live Data report gadgets available for the Finesse desktop. The gadgets are divided into two categories: HTTPS version of Live Data gadgets and HTTP version of Live Data gadgets.

This procedure explains how to add the Live Data report gadgets to the default desktop layout. Use this procedure after a fresh installation of Finesse. If you upgraded Finesse but do not have a custom desktop layout, click **Restore Default Layout** on the Manage Desktop Layout gadget and then follow the steps in this procedure. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.

Procedure

- Step 1** In **Unified CCE Administration**, navigate to **Desktop > Resources**.
- Step 2** Click the **Desktop Layout** tab.
- Step 3** Remove the comment characters (<!-- and -->) from each report that you want to add to the desktop layout. Make sure you choose the reports that match the method your agents use to access the Finesse desktop (HTTP or HTTPS).
- Step 4** Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.
- Step 5** Optionally, change the gadget height.

Example:

The height specified in the Live Data gadget URLs is 310 pixels. If you want to change the height, change the gadgetHeight parameter in the URL to the desired value. For example, if you want the gadget height to be 400 pixels, change the code as follows, replacing 310 with 400:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
  gadgetHeight=400&viewId_1=99E6C8E210000141000000D80A0006C4&
  filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
```

```
filterId_2=agent.id=CL%20teamName
</gadget>
```

To maintain the optimal display of the gadget with scroll bars, set the value for the gadget height to a minimum of 200 pixels. If the report does not require scroll bars, for example a one-row report, you can set a smaller gadget height (for example, 100 pixels). If you do not specify anything for the gadget height (if you remove the 310 from the URL), it defaults to 170 pixels.

Step 6 Click **Save**.

Add Live Data Reports to Custom Desktop Layout

The Finesse default layout XML contains commented XML code for the Live Data report gadgets available for the Finesse desktop. The gadgets are divided into two categories: HTTPS version of Live Data gadgets and HTTP version of Live Data gadgets.

This procedure explains how to add the Live Data report gadgets to a custom desktop layout. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.

Procedure

Step 1 In **Unified CCE Administration**, navigate to **Desktop > Resources**.

Step 2 Click the **Desktop Layout** tab.

Step 3 Click **Finesse Default Layout XML** to show the default layout XML.

Step 4 Copy the XML code for the report you want to add from the Finesse default layout XML.

Example:

To add the Agent Report for HTTPS, copy the following:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
  gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&
  filterId_1=agent.id=CL%20teamName&
  viewId_2=9AB7848B10000141000001C50A0006C4&
  filterId_2=agent.id=CL%20teamName
</gadget>
```

Step 5 Paste the XML within the tab tags where you want it to appear.

Example:

To add the report to the home tab of the agent desktop:

```
<layout>
  <role>Agent</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
  </page>
  <tabs>
    <tab>
      <id>home</id>
      <label>finesse.container.tabs.agent.homeLabel</label>
      <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
        gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&
        filterId_1=agent.id=CL%20teamName&
        viewId_2=9AB7848B10000141000001C50A0006C4&
```



```

        filterId_2=agent.id=CL%20teamName
    </gadget>
</tab>
<tab>
    <id>manageCall</id>
    <label>finesse.container.tabs.agent.manageCallLabel</label>
</tab>
</tabs>
</layout>

```

Step 6 Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

Step 7 Optionally, change the gadget height.

Example:

The height specified in the Live Data gadget URLs is 310 pixels. If you want to change the height, change the gadgetHeight parameter in the URL to the desired value. For example, if you want the gadget height to be 400 pixels, change the code as follows:

```

<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
    gadgetHeight=400&viewId_1=99E6C8E210000141000000D80A0006C4&
    filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
    filterId_2=agent.id=CL%20teamName
</gadget>

```

To maintain the optimal display of the gadget with scroll bars, set the value for the gadget height to a minimum of 200 pixels. If the report does not require scroll bars, for example a one-row report, you can set a smaller gadget height (for example, 100 pixels). If you do not specify anything for the gadget height (if you remove the 310 from the URL), it defaults to 170 pixels.

Step 8 Click **Save**.

Note After you add a gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with a large number of rows, you may want to adjust the gadget height or the screen resolution on the computer used to access the desktop to make the report easier to read or make more rows appear on the screen without needing to scroll down.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.

Configure Cisco Unified Customer Voice Portal Reporting Server

Follow this sequence to configure the Cisco Unified Customer Voice Portal Reporting Server for Packaged CCE deployment



Note The Unified CVP Reporting VM is required for customers who use Courtesy Callback and who want to run Unified CVP call and application reports.

Sequence	Task
1	Import WSM CA Certificate into CVP, on page 609

Sequence	Task
2	For details on self-signed, see Import WSM Certificate into AW Machines, on page 613
3	Obtain Cisco Unified Customer Voice Portal Report Templates, on page 40
4	Create Data Source for Cisco Unified CVP Report Data, on page 40
5	Import Unified CVP Report Templates in Unified Intelligence Center, on page 42

Obtain Cisco Unified Customer Voice Portal Report Templates

To import Unified CVP report templates complete the following:

Procedure

-
- Step 1** On the Unified CVP Reporting Server, click **Start**.
 - Step 2** In the search box, type `%CVP_HOME%\CVP_Reporting_Templates` and press **Enter**.
 - Step 3** Compress the reports into a zip folder and copy it to the system from which you will run Unified Intelligence Center Administration.
-

Create Data Source for Cisco Unified CVP Report Data

Perform the following procedure to create a data source.

Procedure

-
- Step 1** Log in to the Unified Intelligence Center at `https://<hostname/ IP address of CUIC Publisher>:8444/cuicui`.
 - Step 2** Select the **Data Sources** drawer to open the **Data Sources** page.
 - Step 3** Click **New** to open **New Data Source** page.
 - Step 4** Complete fields on this page as follows:

Field	Value
Name	Enter the name of this data source. Report Designers and Report Definition Designers do not have access to the Data Sources page but can see the list of Data Sources when they create custom reports. To benefit those users, give a new Data Source a meaningful name.
Description	Enter a description for this data source.

Field	Value
Data Source Type	Choose Informix . Note Type is disabled in Edit mode.
Host Settings	
Database Host	Enter the IP address or hostname for the Unified CVP Reporting server.
Port	Enter the port number. Typically, the port is 1526. You may have to open this port in the CVP Reporting Server firewall (Windows Firewall > Advanced Settings > Inbound rules > new rule).
Database Name	Enter the name of the reporting database on the Unified CVP reporting server. The database name can be <code>cvp_data</code> or <code>callback</code> .
Instance	Specify the instance name of the desired database. By default, this is <code>cvp</code> .
Timezone	Choose the correct time zone for the data stored in the database. In locations that change from Standard Time to Daylight Savings Time, this time zone is updated automatically. Note Set CVP datasource timezone configuration to UTC on CUIC.
Authentication Settings	
Database User ID	Enter the user ID of the Reporting User to access the Unified CVP reporting database. (The <code>cvp_dbuser</code> account is created automatically during Unified CVP Reporting server installation.)
Password and Confirm Password	Enter and confirm the password for the database user.
Charset	Choose UTF-8.
Default Permissions	View or edit the permissions for this datasource for My Group and for the All Users group.
Max Pool Size	Select the maximum pool size. Value ranges from 5-200. The default Max Pool Size value is 100 and is common for both the primary and secondary data source tabs.

Step 5 Click **Test Connection**.

If the status is not Online, review the error message to determine the cause and edit the data source accordingly.

- Step 6** Click **Save** to close the Add Data Source window.
The new data source appears on the Data Sources list.

Import Unified CVP Report Templates in Unified Intelligence Center

You can import a report (XML) and the associated template help file (ZIP format) into Cisco Unified Intelligence Center.

Procedure

- Step 1** Launch the Unified Intelligence Center web application at `https://<Hostname/IP Address of CUIC Publisher>:8444/cuic`
- Step 2** From the left navigation pane, click **Reports**.
- Step 3** On the Reports toolbar, click **New > Import**.
You will be redirected to the legacy interface.
- Step 4** Navigate to the folder where you want to import the report.
- Note** If you are importing a stock report bundle from Cisco.com, it must be placed at the Reports folder level.
- Step 5** Click **Import Report**.
- Step 6** In the **File Name (XML or ZIP file)** field, click **Choose File**.
- Step 7** Browse to and select the XML or the compressed report file, and click **Open**.
- Step 8** From the **Data source for ReportDefinition** drop-down list, select a data source used by the report definition.
- Note** This field appears only if the Report Definition for the report being imported is not currently defined in Unified Intelligence Center.
- Step 9** From the **Data Source for ValueList** drop-down list, select the data source used by the value lists defined in the report definition.
- Note** You have to select a data source for the value list only if it does not use the same data source as the Report Definition. For Report Definitions of Real Time Streaming, it is mandatory to select a data source for the Value Lists.
- Step 10** In the **Save To** field, browse to the folder where you want to place the imported report. Use the arrow keys to expand the folders.
- Step 11** Click **Import**.



- Note** Importing a report to a different version of Unified Intelligence Center is not supported. However, when you upgrade Unified Intelligence Center, report templates continue to work in the upgraded version.

Configure VVB



- Note**
- If you have configured VXML Gateway, it is not mandatory to configure Virtualized Voice Browser (VVB). You may configure either VVB or VXML Gateway, or configure both.
 - The Cisco VVB configurations are site specific. All the VVBs in a site must have the same configurations.

To configure Cisco VVB for all deployments:

- Add VVB as an external machine. For more information, see [Add External Machines, on page 127](#).
- Change the default configuration (Optional). For more information, see [Cisco Virtualized Voice Browser \(VVB\) Setup, on page 209](#).
- Configure SNMP (Optional). For more information, see [Configure SNMP, on page 87](#).

Configure Cisco IOS Enterprise Voice Gateway

Tasks to configure the Cisco IOS Enterprise Voice Gateway for Packaged CCE deployment

Task
Common Configuration for the Ingress Gateway and VXML Gateway, on page 43
Configure Ingress Gateway, on page 44
Configure VXML Gateway, on page 47 (optional)
Configure Codec for Ingress and VXML Gateways, on page 49

About Ingress and VXML Gateway Configuration

Complete the following procedures to configure the Ingress Gateway and VXML Gateway. Instructions are applicable to both TDM and Cisco Unified Border Element (CUBE) Voice gateways, unless otherwise noted.

You can add all Gateways as an external machine. For more information, see [Add External Machines, on page 127](#).



- Note** Complete all configuration steps in **enable > configuration terminal** mode.

Common Configuration for the Ingress Gateway and VXML Gateway

```
logging buffered 2000000 debugging
no logging console
service timestamps debug datetime msec localtime
ip routing
ip cef
ip source-route
```

```

interface GigabitEthernet0/0
  ip route-cache same-interface
  duplex auto
  speed auto
  no keepalive
  no cdp enable

voice service voip
  ip address trusted list
  ipv4 0.0.0.0 0.0.0.0 # OR an explicit Source IP Address Trust List
  allow-connections sip to sip
  signaling forward unconditional

```

Configure Ingress Gateway

Procedure

Step 1 Configure global settings.

```

voice service voip
  allow-connections sip to sip
  signaling forward unconditional
  # If this gateway is being licensed as a Cisco UBE the following lines are also required
  mode border-element
  ip address trusted list
  ipv4 0.0.0.0 0.0.0.0 # Or an explicit Source IP Address Trust List
  sip
  rel1xx disable
  header-passing
  options-ping 60
  midcall-signaling passthru

```

Step 2 Configure voice codec preference:

```

voice class codec 1
  codec preference 1 g711ulaw
  codec preference 2 g711alaw
  codec preference 3 g729r8

```

Step 3 Configure default services:

To download and transfer the `survivability.tcl` file to the Ingress Gateway, see [File Transfer to Gateway, on page 49](#).

```

#Default Services
application
  service survivability flash:survivability.tcl

```

Step 4 Configure gateway and sip-ua timers:

```

gateway
  media-inactivity-criteria all
  timer receive-rtp 1200

sip-ua
  retry invite 2
  retry bye 1
  timers expires 60000
  timers connect 1000
  reason-header override

```

Step 5 Configure POTS dial-peers:

```
# Configure Unified CVP survivability
dial-peer voice 1 pots
  description CVP TDM dial-peer
  service survivability
  incoming called-number .T
  direct-inward-dial
```

Note This is required for TDM gateways only.

Step 6 Configure the switch leg:

```
#Configure the Switch leg where
# preference is used to distinguish between sides.
# max-conn is used prevent overloading of Unified CVP
# options-keepalive is used to handle failover
# Note: the example below is for gateways located on the A-side of a geographically
#distributed deployment
# Note: Ensure that you configure switch dial-peers for each Unified CVP server.

dial-peer voice 70021 voip
  description Used for Switch leg SIP Direct
  preference 1
  max-conn 225
  destination-pattern xxxx..... #Customer specific destination pattern
  session protocol sipv2
  session target ipv4:###.###.###.### #IP Address for Unified CVP, SideA
  session transport tcp
  voice-class codec 1
  voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
  dtmf-relay rtp-nte
  no vad

dial-peer voice 70022 voip
  description Used for Switch leg SIP Direct
  preference 2
  max-conn 225
  destination-pattern xxxx..... #Customer specific destination pattern
  session protocol sipv2
  session target ipv4:###.###.###.### #IP Address for Unified CVP, SideB
  session transport tcp
  voice-class codec 1
  voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
  dtmf-relay rtp-nte
  no vad
```

Step 7 Configure the hardware resources (transcoder, conference bridge, and MTP):

Note This configuration section is unnecessary for virtual CUBE or CSR 1000v Gateways. They do not have physical DSP resources.

```
#For gateways with physical DSP resources, configure Hardware resources using
#Unified Communications Domain Manager.

# Configure the voice-cards share the DSP resources located in Slot0
voice-card 0
  dspfarm
  dsp services dspfarm
voice-card 1
  dspfarm
  dsp services dspfarm
voice-card 2
  dspfarm
```

```

    dsp services dspfarm
voice-card 3
    dspfarm
    dsp services dspfarm
voice-card 4
    dspfarm
    dsp services dspfarm

# Point to the contact center call manager
sccp local GigabitEthernet0/0
    sccp ccm ###.###.###.### identifier 1 priority 1 version 7.0 # Cisco Unified CM sub 1
    sccp ccm ###.###.###.### identifier 2 priority 2 version 7.0 # Cisco Unified CM sub 2

# Add a SCCP group for each of the hardware resource types
sccp ccm group 1
    associate ccm 1 priority 1
    associate profile 2 register <gatewaynametmp>
    associate profile 1 register <gatewaynameconf>
    associate profile 3 register <gatewaynamecode>

# Configure DSPFarms for Conference, MTP and Transcoder

dspfarm profile 1 conference
    codec g711ulaw
    codec g711alaw
    codec g729r8
    maximum sessions 24
    associate application SCCP

dspfarm profile 2 mtp
    codec g711ulaw
    codec g711alaw
    codec g729r8
    maximum sessions software 500
    associate application SCCP

dspfarm profile 3 transcode universal
    codec g711ulaw
    codec g711alaw
    codec g729r8
    maximum sessions 52
    associate application SCCP

```

Step 8 Optional, configure the SIP Trunking:

```

# Configure the resources to be monitored
voice class resource-group 1
    resource cpu 1-min-avg threshold high 80 low 60
    resource ds0
    resource dsp
    resource mem total-mem
    periodic-report interval 30

# Configure one rai target for each CVP Server
sip-ua
    rai target ipv4:###.###.###.### resource-group1 # CVPA
    rai target ipv4:###.###.###.### resource-group1 # CVPB
    permit hostname dns:%Requires manual replacement - ServerGroup Name defined in
CVP.System.SIP Server Groups%

```

Step 9 Configure incoming PSTN SIP trunk dial peer:

```

dial-peer voice 70000 voip
    description Incoming Call From PSTN SIP Trunk

```



```

service survivability
incoming called-number xxxx..... # Customer specific incoming called-number pattern
voice-class sip rellxx disable
dtmf-relay rtp-nte
session protocol sipv2
voice-class codec 1
no vad

```

Note This is required for CUBE only.

Configure VXML Gateway

Before you begin



Note If you have configured VVB, it is not mandatory to configure VXML Gateway. You may configure either VVB or VXML Gateway, or configure both.

Procedure

Step 1 Configure global settings:

```

voice service voip
  allow-connections sip to sip
  signaling forward unconditional
  # If this gateway is being licensed as a Cisco UBE the following lines are also required
  mode border-element
  ip address trusted list
    ipv4 0.0.0.0 0.0.0.0 # Or an explicit Source IP Address Trust List
  sip
    rellxx disable
    header-passing
    options-ping 60
    midcall-signaling passthru

```

Step 2 Configure default Unified CVP services:

To download and transfer the following files to VXML Gateway, see [File Transfer to Gateway](#), on page 49.

```

#Default Unified CVP Services
application
  service new-call flash:bootstrap.vxml
  service CVPSelfService flash:CVPSelfServiceBootstrap.vxml
  service ringtone flash:ringtone.tcl
  service cvperror flash:cvperror.tcl
  service bootstrap flash:bootstrap.tcl
  service handoff flash:handoff.tcl

```

Step 3 Configure dial-peers:

Note While configuring VXML gateway voice class codec must not be used. G711ulaw may be used in general for the dial-peers, but still depending on the implementation the other codec may be used.

```
# Configure Unified CVP Ringtone
dial-peer voice 919191 voip
  description CVP SIP ringtone dial-peer
  service ringtone
  incoming called-number 9191T
  voice-class sip rellxx disable
  dtmf-relay rtp-nte
  codec g711ulaw
  no vad

# Configure Unified CVP Error
dial-peer voice 929292 voip
  description CVP SIP error dial-peer
  service cvperror
  incoming called-number 9292T
  voice-class sip rellxx disable
  dtmf-relay rtp-nte
  codec g711ulaw
  no vad
```

Step 4 Configure default Unified CVP HTTP, ivr, rtsp, mrpc and vxml settings:

```
http client cache memory pool 15000
http client cache memory file 1000
http client cache refresh 864000
no http client connection persistent
http client connection timeout 60
http client connection idle timeout 10
http client response timeout 30
ivr prompt memory 15000

vxml tree memory 500
vxml audioerror
vxml version 2.0
```

Step 5 Configure VXML leg where the incoming called-number matches the Network VRU Label:

```
dial-peer voice 7777 voip
  description Used for VRU leg
  service bootstrap
  incoming called-number 777T
  dtmf-relay rtp-nte
  codec g711ulaw
  no vad
```

Step 6 Exit configuration mode and use the Cisco IOS CLI command **call application voice load <service_Name>** to load the transferred Unified CVP files into the Cisco IOS memory for each Unified CVP service:

- call application voice load new-call
- call application voice load CVPSelfService
- call application voice load ringtone
- call application voice load cvperror
- call application voice load bootstrap
- call application voice load handoff

File Transfer to Gateway

This procedure explains how to download and transfer files to the Gateway.

Procedure

-
- Step 1** Download the GWDdownloads_12.0.zip from [https://software.cisco.com/download/home/270563413/type/280840592/release/12.0\(1\)](https://software.cisco.com/download/home/270563413/type/280840592/release/12.0(1)) and extract it.
 - Step 2** Fetch the required .tcl files and save it to a location in any server.
 - Step 3** Transfer the .tcl files to the flash memory of the Gateway using FTP.
-

Configure Codec for Ingress and VXML Gateways

Configure Ingress Gateway

Procedure

-
- Step 1** Add the voice class codec 1 to set the codec preference in dial-peer:

Example:

```
voice class codec 1
  codec preference 1 g729r8
  codec preference 2 g711alaw
  codec preference 3 g711ulaw

dial-peer voice 70021 voip
  description Used for Switch leg SIP Direct
  preference 1
  max-conn 225
  destination-pattern xxxx..... # Customer specific destination
  session protocol sipv2
  session target ipv4:###.###.###.### # IP Address for Unified CVP
  session transport tcp
  voice class codec 1
  voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
  dtmf-relay rtp-nte
  no vad
```

- Step 2** Modify the dial-peer to specify the codec explicitly for a dial-peer:

```
dial-peer voice 9 voip
  description For Outbound Call for Customer
  destination-pattern <Customer Phone Number Pattern>
  session protocol sipv2
  session target ipv4:<Customer SIP Cloud IP Address>
  session transport tcp
  voice-class sip rel1xx supported "100rel"
  voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
  dtmf-relay rtp-nte
  codec g711alaw
  no vad

dial-peer voice 10 voip
  description ***To CUCM Agent Extension For Outbound***
```

```

destination-pattern <Agent Extension Pattern to CUCM>
session protocol sipv2
session target ipv4:<CUCM IP Address>
voice-class sip rel1xx supported "100rel"
dtmf-relay rtp-nte
codec g711alaw

```

Configure VXML Gateway

Procedure

Modify the following dial-peer to specify the codec explicitly for a dial-peer:

```

dial-peer voice 919191 voip
  description Unified CVP SIP ringtone dial-peer
  service ringtone
  incoming called-number 9191T
  voice-class sip rel1xx disable
  dtmf-relay rtp-nte
  codec g711alaw
  no vad

dial-peer voice 929292 voip
  description CVP SIP error dial-peer
  service cvperror
  incoming called-number 9292T
  voice-class sip rel1xx disable
  dtmf-relay rtp-nte
  codec g711alaw
  no vad

dial-peer voice 7777 voip
  description Used for VRU leg #Configure VXML leg where the incoming called
  service bootstrap
  incoming called-number 7777T
  dtmf-relay rtp-nte
  codec g711alaw
  no vad

```

Configure IPv6

Tasks to configure IPv6 for Packaged CCE deployment

Task
Set Up IPv6 for VOS-Based Contact Center Applications, on page 51
Configure NAT64 for IPv6-Enabled Deployment, on page 52
Configure IPv6 on Unified CVP Call Server, on page 54
Configure Gateways to Support IPv6, on page 55

Task

[Configure IPv6 on Unified Communications Manager, on page 56](#)

IPv6 Configuration

Packaged CCE can support IPv6 connections for agent and supervisor Finesse desktops and phones. An IPv6-enabled deployment can use either all IPv6 endpoints or a mix of IPv4 and IPv6 endpoints. Servers that communicate with these endpoints can accept both IPv4 and IPv6 connections. Communication between servers continues to use IPv4 connections.

This chapter contains the configuration procedures that you perform for IPv6-enabled deployments.

Set Up IPv6 for VOS-Based Contact Center Applications

By default, only IPv4 is enabled for Unified Communications Manager, Cisco Finesse, and Unified Intelligence Center.

If you choose to enable IPv6 on these applications, you must enable it on both the publisher/primary nodes and subscriber/secondary nodes for those applications.

You can use Cisco Unified Operating System Administration or the CLI to enable IPv6.

See the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html> for more information about IPv6 support in Packaged CCE deployments.

Set Up IPv6 Using Cisco Unified Operating System Administration

To set up IPv6 using Cisco Unified Operating System Administration, perform the following procedure on the primary and secondary VOS servers.

Procedure

-
- Step 1** Sign into Cisco Unified Operating System Administration on the Publisher/Primary node:
- Unified Communications Manager and Unified Intelligence Center: `https://<host or IP address of the Publisher or Primary node>/cmplatform`
 - Finesse: `https://FQDN of the Primary node:8443/cmplatform`
- Step 2** Navigate to **Settings > IP > Ethernet IPv6**.
- Step 3** Check the **Enable IPv6** check box.
- Step 4** Enter values for **IPv6Address**, **Prefix Length**, and **Default Gateway**.
- Step 5** Check the **Update with Reboot** check box.
- Step 6** Click **Save**.
The server restarts.
- Step 7** Repeat this procedure on the subscriber/secondary node.
-

Set Up IPv6 for VOS-Based Applications Using the CLI

To set up IPv6 using the CLI, perform the following procedure on both the primary and secondary VOS servers.

Procedure

-
- Step 1** Access the CLI on the VOS server.
- Step 2** To enable or disable IPv6, enter:
set network ipv6 service {enable | disable}
- Step 3** Set the IPv6 address and prefix length:
set network ipv6 static_address *addr mask*
- Example:**
- ```
set network ipv6 static_address 2001:db8:2::a 64
```
- Step 4** Set the default gateway:  
**set network ipv6 gateway *addr***
- Step 5** Restart the system for the changes to take effect.  
**utils system restart**
- Step 6** To display the IPv6 settings, enter:  
**show network ipv6 settings**
- 

## Configure NAT64 for IPv6-Enabled Deployment

NAT64 allows communication between IPv6 and IPv4 networks. For IPv6-enabled deployments, you must set up NAT64 so that supervisors on an IPv6 network can access Unified CCE Administration web tools on an IPv4 network. You can use either Stateful and Stateless NAT64.

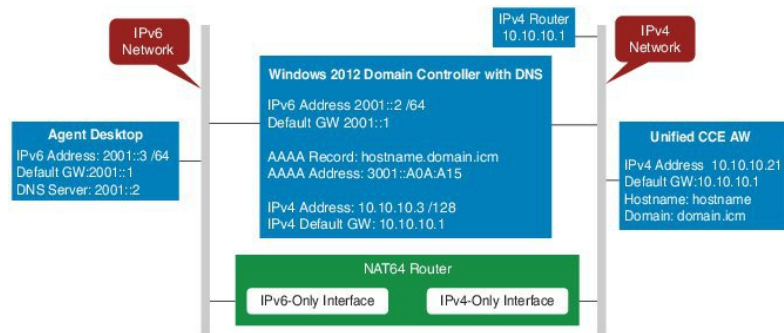
To read more about which translation type is the most appropriate for your deployment see Table 2. Comparison Between Stateless and Stateful NAT64 here: [https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white\\_paper\\_c11-676278.html](https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html)



**Note** NAT64 is NOT supported on M train IOS. T train is required.

For more information, see the Compatibility Matrix for Packaged Contact Center Enterprise at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html>.

The following example network diagram and interface configuration demonstrates Stateful NAT64 translation between an IPv6 network and an IPv4 network.



```

interface GigabitEthernet0/0
description ipv4-only interface
 ip address 10.10.10.81 255.255.255.128
 duplex auto
 speed auto
 nat64 enable
 no mop enabled

interface GigabitEthernet0/1
description ipv6-only interface
 no ip address
 duplex auto
 speed auto
 nat64 enable
 ipv6 address 2001::1/64
 ipv6 enable

ipv6 unicast-routing
ipv6 cef
!
nat64 prefix stateful 3001::/96
nat64 v4 pool POOL1 10.10.10.129 10.10.10.250
nat64 v6v4 list V6ACL1 pool POOL1 overload
ipv6 router rip RIPv6
!
ipv6 router rip RIP

!
ipv6 access-list V6ACL1
 permit ipv6 2001::/64 any

```

## Configure DNS for IPv6

To meet the requirement that Unified CCE Administration be accessed by FQDN, a Forward lookup AAAA record for the Unified CCE AW-HDS-DDS servers and any External HDS servers must be created in DNS.

The steps in this procedure are for a Windows DNS server.

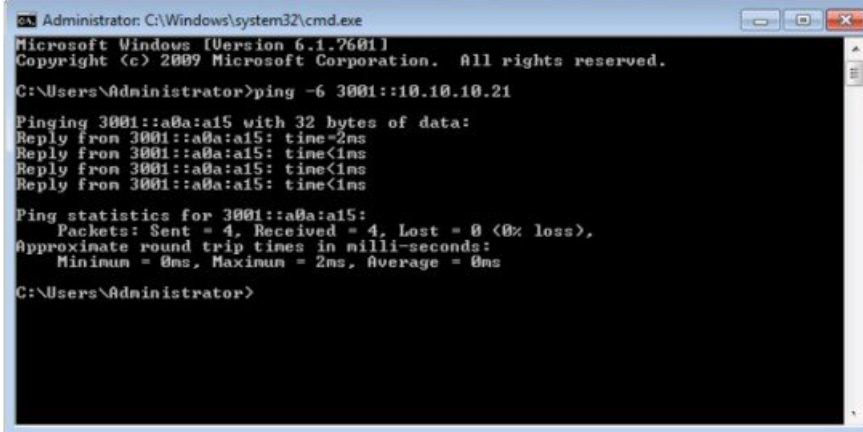
### Procedure

- Step 1** In Windows, navigate to **Administrative Tools > DNS**. This opens the DNS Manager.
- Step 2** In the Forward lookup zone, navigate to your deployment's domain name.
- Step 3** Right-click the domain name and select **New Host (A or AAAA)**.

- Step 4** In the New Host dialog box, enter the computer name and IP address of the Unified CCE AW-HDS-DDS servers and any External HDS servers. Click **Add Host**.

### Determine IPv6 Translation of IPv4 Address for DNS Entry

You can determine the IPv6 address needed for the AAAA DNS record by running a ping command on any Windows machine using mixed notation. Type “ping -6” followed by your IPv6 Nat64 Prefix, two colons, and then the IPv4 address.



```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping -6 3001::10.10.10.21

Pinging 3001::a0a:a15 with 32 bytes of data:
Reply from 3001::a0a:a15: time=2ms
Reply from 3001::a0a:a15: time<1ms
Reply from 3001::a0a:a15: time<1ms
Reply from 3001::a0a:a15: time<1ms

Ping statistics for 3001::a0a:a15:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\Administrator>

```

In the ping response, the IPv4 address is converted to the hexadecimal equivalent. Use this address in your static AAAA record.



- Note** Optionally, DNS64 can be used in place of static DNS entries. Use of DNS64 helps facilitate translation between IPv6 and IPv4 networks by synthesizing AAAA resource records from A resource records.

The *NAT64 Technology: Connecting IPv6 and IPv4 Networks* technical paper gives an overview of DNS64 and how it is used with IPv6: [https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white\\_paper\\_c11-676278.html](https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html).

## Configure IPv6 on Unified CVP Call Server

For IPv6-enabled deployments, you must add an IPv6 address to your Unified CVP Call Server's existing network interface.

Perform this procedure only if you have an IPv6-enabled environment.

### Procedure

- Step 1** On the Unified CVP Call Server, navigate to **Control Panel > Network and Sharing**.
- Step 2** Click **Ethernet**.
- Step 3** From the **Ethernet Status** window, select **Properties**.
- Step 4** Check the **Internet Protocol Version 6 (TCP/IPv6)** check box, and choose **Properties**.



- Step 5** Choose **Use the following IPv6 address** radio button.
  - Step 6** Enter values in the **IPv6 address**, **Subnet prefix length**, and **Default gateway** fields.
  - Step 7** Click **OK** and restart Windows when prompted.
- 

## Configure Gateways to Support IPv6

For IPv6-enabled deployments, you must configure your Ingress and VXML gateways to enable IPv6 addressing.

### Configure an Interface to Support IPv6 Protocol Stack

This procedure applies to both the Ingress and the VXML gateway.

#### Procedure

---

Configure the following on the Gateway:

```
>Enable
>configure terminal
>interface type number
>ipv6 address{ ipv6-address / prefix-length | prefix-name sub-bits / prefix-length}
>ipv6 enable
```

---

### Enable ANAT in Ingress Gateway

#### Procedure

---

Configure the following on the Gateway:

```
>conf t
>voice service voip
>SIP
>ANAT
>bind control source-interface GigabitEthernet0/2
>bind media source-interface GigabitEthernet0/2
```

---

### Enable Dual Stack in the Ingress Gateway

#### Procedure

---

Configure the following on the Gateway:

```
>conf t
```

```
>sip-ua
>protocol mode dual-stack preference ipv6
```

---

## Configure IPv6 on Unified Communications Manager

In an IPv6-enabled environment, you must perform the procedures in this section to configure IPv6 on Unified Communications Manager.

### Cluster-Wide Configuration in Unified CM Administration

Perform the following procedure to set IPv6 as the addressing mode preference for media and signaling cluster-wide.

#### Procedure

---

- Step 1** From **Cisco Unified CM Administration**, choose **System > Enterprise Parameters > IPv6 Configuration Modes** to configure the cluster-wide IPv6 settings for each Unified Communications Manager server.
  - Step 2** From the **Enable IPv6** drop-down list, choose **True**.
  - Step 3** From the **IP Addressing Mode Preference for Media** drop-down list, choose **IPv6**.
  - Step 4** From the **IP Addressing Mode Preference for Signaling** drop-down list, choose **IPv6**.
  - Step 5** From the **Allow Auto-configuration for Phones** drop-down list, choose **Off**.
  - Step 6** Save your changes.
- 

### Transcoding

In an IPv6-enabled environment, a transcoder is required for the following scenarios:

- An agent logged in to an IPv6 endpoint needs to send or receive transfers from an agent logged in to an IPv4 endpoint.
- An agent logged in to an IPv6 endpoint needs to connect to a VXML Gateway for self service.

### Add a Common Device Configuration Profile in Unified Communications Manager

In an IPv6-enabled environment, you may have both IPv4 and IPv6 devices.

Perform the following procedure to add an IPv4, IPv6, or dual stack common device configuration profile in Unified Communications Manager.

#### Procedure

---

- Step 1** From **Cisco Unified CM Administration**, choose **Device > Device Settings > Common Device Configuration**.
- Step 2** Click **Add New** and enter the name of the new common device configuration profile.
- Step 3** From the **IP Addressing Mode** drop-down list:

- To add an IPv6 common device configuration profile in Unified Communications Manager, choose **IPv6 only**.
- To add an IPv4 common device configuration profile in Unified Communications Manager, choose **IPv4 only**.
- To add a dual stack common device configuration profile in Unified Communications Manager, choose **IPv4 and IPv6**. Then choose **IPv4** from the **IP Addressing Mode Preference for Signaling** drop-down list.

**Step 4** Save your changes.

---

### Associate the Common Device Configuration Profile with Gateway Trunk

Perform the following procedure to associate the common device configuration profile with the Gateway trunk. This procedure applies to the Ingress Gateway.

#### Procedure

---

**Step 1** From **Cisco Unified CM Administration**, choose **Device > Trunk**.

**Step 2** Click **Find**.  
Choose the trunk profile that you want to view.

**Step 3** From the **Common Device Configuration** drop-down list:

- To associate the IPv6 common device configuration profile with the Gateway trunk, choose the IPv6 common device configuration profile.
- To associate the IPv4 common device configuration profile with the Gateway trunk, choose the IPv4 common device configuration profile.

**Note** Unified CM gateway trunk supports only an IPv4 or IPv6 trunk. You cannot associate a dual stack common device configuration profile to a Unified CM gateway trunk.

**Step 4** Enter the IPv6 address in the **Destination Address IPv6** field.

**Note** Unified CM to Gateway trunk supports only standard SIP Profile and does not support ANAT enabled dual-stack SIP trunk.

**Step 5** Save your changes.

---

### Associate the Common Device Configuration Profile with an IPv4 or IPv6 Phone

#### Procedure

---

**Step 1** From **Cisco Unified CM Administration**, choose **Device > Phone**.

**Step 2** Click **Find**.  
Choose the trunk profile that you want to view.

**Step 3** From the **Common Device Configuration** drop-down list: choose the IPv6 common device configuration profile.

- To associate the IPv6 common device configuration profile to an IPv6 phone, choose the IPv6 common device configuration profile.
- To associate the IPv4 common device configuration profile to an IPv4 phone, choose the IPv4 common device configuration profile.

**Step 4** Save your changes.

---

### Associate a SIP Profile in Unified CM

In an IPv6-enabled deployment, you must associate a SIP profile with the trunk you configured for Unified CVP.

#### Procedure

---

**Step 1** From **Cisco Unified CM Administration**, choose **Device > Trunk**.

**Step 2** Click **Find**. Choose the trunk profile that you want to view.

**Step 3** From the **SIP Profile** drop-down list, choose the SIP Profile you created.

**Note** For more information on how to create a SIP Profile, see

Add a SIP Profile in Unified CM section in the Cisco Packaged Contact Center Enterprise Administration and Configuration Guide at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html>.

**Step 4** Save your change.

---

### Associate the Dual Stack Common Device Configuration Profile with SIP Trunk

#### Procedure

---

**Step 1** From **Cisco Unified CM Administration**, choose **Device > Trunk**.

**Step 2** Click **Find**. Choose the trunk profile that you want to view.

**Step 3** From the **Common Device Configuration** drop-down list, choose the Dual Stack Common Device Configuration Profile.

**Note** For more information on how to add a Dual Stack Common Device Configuration Profile, see [Add a Common Device Configuration Profile in Unified Communications Manager, on page 56](#).

**Step 4** Save your change.

---

## Packaged CCE 4000 Agents Deployment

Follow this sequence to configure components for Packaged CCE 4000 Agents deployment.

| Sequence | Task                                                                                                  |
|----------|-------------------------------------------------------------------------------------------------------|
| 1        | <a href="#">Configure CCE Component, on page 59</a>                                                   |
| 2        | <a href="#">Configure Cisco Unified Customer Voice Portal, on page 81</a>                             |
| 3        | If Media Server is external, <a href="#">Configure Media Server, on page 202</a>                      |
| 4        | <a href="#">Configure Cisco Unified Communications Manager, on page 85</a>                            |
| 5        | <a href="#">Configure Cisco Unified Intelligence Center, on page 89</a>                               |
| 6        | <a href="#">Configure Cisco Finesse, on page 90</a>                                                   |
| 7        | <a href="#">Configure Live Data, on page 98</a>                                                       |
| 8        | <a href="#">Configure Cisco Identity Service, on page 101</a>                                         |
| 9        | <a href="#">Configure Cisco Unified Customer Voice Portal Reporting Server, on page 39 (optional)</a> |
| 10       | <a href="#">Configure VVB, on page 43 (optional)</a>                                                  |
| 11       | <a href="#">Configure Cisco IOS Enterprise Voice Gateway, on page 43</a>                              |
| 12       | <a href="#">Configure IPv6, on page 50</a>                                                            |
| 13       | <a href="#">Configure Enterprise Chat and Email (ECE) (optional) Email and Chat, on page 376</a>      |

## Configure CCE Component

Follow this sequence to configure components for Packaged CCE 4000 Agents deployment.

| Sequence | Task                                                                                             |
|----------|--------------------------------------------------------------------------------------------------|
| 1        | <a href="#">Configure SQL Server for CCE Components, on page 2</a>                               |
| 2        | <a href="#">Set up Organizational Units, on page 2</a>                                           |
| 3        | <a href="#">Configure Rogger, on page 60</a>                                                     |
| 4        | <a href="#">Configure AW-HDS-DDS, on page 64</a>                                                 |
| 5        | <a href="#">Start Unified CCE Services, on page 64</a>                                           |
| 6        | If you have PG VMs installed, <a href="#">Add Unified CCE Instance, on page 76</a> on all PG VMs |
| 7        | <a href="#">Configure Packaged CCE Deployment Type, on page 67</a>                               |
| 8        | <a href="#">Configure Cisco Unified Contact Center Enterprise PG, on page 77</a>                 |

| Sequence | Task                                                                                                                                |
|----------|-------------------------------------------------------------------------------------------------------------------------------------|
| 9        | For configuration using Configuration Manager, see <a href="#">Packaged CCE 4000 and 12000 Agent Supported Tools</a> , on page 398  |
| 10       | For details on CA certificate, see <a href="#">Generate and Import CA Signed Certificate in AW Machine</a> , on page 606            |
| 11       | For details on self-signed certificate, see <a href="#">Generate and Import Self-signed Certificate in AW Machine</a> , on page 607 |

## Configure Rogger

Follow this sequence to configure Rogger for Packaged CCE 4000 Agents deployment.

| Sequence | Task                                                                                     |
|----------|------------------------------------------------------------------------------------------|
| 1        | <a href="#">Add Unified CCE Instance</a> , on page 76                                    |
| 2        | <a href="#">Create Logger Database</a> , on page 60                                      |
| 3        | To use Outbound Option, see <a href="#">Create Outbound Option Database</a> , on page 61 |
| 4        | <a href="#">Add Logger Component to Instance</a> , on page 62                            |
| 5        | <a href="#">Add Router Component to Instance</a> , on page 63                            |
| 6        | <a href="#">Cisco SNMP Setup</a> , on page 21 (optional)                                 |

### Create Logger Database

Perform this procedure on the Side A and Side B Logger/Rogger VM.

#### Procedure

- 
- Step 1** From Unified CCE Tools, open the ICMDBA tool, and click **Yes** at any warnings that display.
- Step 2** Navigate to **Server > Instances**.
- Step 3** Right-click the instance name and choose **Create** to create the logger database.
- Step 4** In the Select Component dialog box, choose the logger you are working on (Logger A or Logger B). Click **OK**.
- Step 5** At the prompt, “SQL Server is not configured properly. Do you want to configure it now?”, click **Yes**.
- Step 6** On the Configure page, in the SQL Server Configurations pane check **Memory (MB)** and **Recovery Interval**. Click **OK**.
- Step 7** On the Stop Server page, click **Yes** to stop the services.
- Step 8** In the Select Logger Type dialog box, choose **Enterprise**. Click **OK** to open the Create Database dialog box.
- Step 9** Create the Logger database and log as follows:
- In the DB Type field, choose the Side (A or B).
  - In the region field, choose your region.

- c) In the Create Database dialog box, click **Add** to open the Add Device dialog box.
- d) Click **Data**.
- e) Choose the drive on which you want to create the database, for example, the E drive.
- f) For the **Size** field, consider whether to choose the default (which is 1.4GB, a fairly minimal size) or calculate a value appropriate for your deployment by using the Database Size Estimator Tool. If you calculate the value, enter it here.

**Note** You can use the Database Size Estimator Tool only after the database is created.

- a) Click **OK** to return to the Create Database dialog box.
- b) Click **Add** again.
- c) In the Add Device dialog box, click **Log**.
- d) Choose the drive where you created the database.
- e) In the **Size** field, choose the default setting or, if you have calculated an appropriate size for your deployment, enter that value.
- f) Click **OK** to return to the Create Database dialog box.

**Step 10** In the Create Database dialog box, click **Create**, then click **Start**.

**Step 11** When you see the successful creation message, click **OK** and then **Close**.

## Create Outbound Option Database

Outbound Option uses its own SQL database on the Logger. Perform the following procedure on the Side A Logger only.

### Procedure

- Step 1** Open the ICMDBA tool and click **Yes** to any warnings.
- Step 2** Navigate to **Servers > <Logger Server> > Instances > <Unified CCE instance> > LoggerA**. Right-click the instance name and select **Database > Create**.
- Step 3** On the Stop Server message, click **Yes** to stop the services.
- Step 4** In the Create Database dialog box, click **Add** to open the Add Device dialog box.
- Step 5** Click **Data**, and choose the drive on which you want to create the database, for example, the E drive. In the database size field, you can choose to retain the default value or enter a required value.
- Step 6** Click **OK** to return to the Create Database dialog box.
- Step 7** In the Add Device dialog box, click **Log**. Choose the desired drive. Retain the default value in the log size field and click **OK** to return to the Create Database dialog box.
- Step 8** In the Create Database dialog box, click **Create**, and then click **Start**. When you see the successful creation message, click **OK** and then click **Close**.

For more information about configuring Outbound Options, see the *Outbound Option Guide for Unified Contact Center Enterprise* guide at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html>

## Add Logger Component to Instance

Perform this procedure on the Side A and Side B Loggers.

### Procedure

- 
- Step 1** Open the Web Setup tool.
- Step 2** Choose **Component Management > Loggers**. Click **Add**, and then choose the instance.
- Step 3** On the Deployment page, select the Logger (A or B). Click **Duplexed**, and then click **Next**.
- Step 4** On the Central Controller Connectivity page, enter the host names for Sides A and B for the **Router Private Interface** and **Logger Private Interface**. Then, click **Next**.
- Step 5** Check **Enable Historical/Detail Data Replication**.
- Step 6** On the Additional Options page, click **Display Database Purge Configuration Steps**.
- Step 7** Click the **Enable Outbound Option** check box.
- Note** If this Logger is being added for a Rogger server, where there are two IP addresses that are configured on the public Network Interface Card (for IP-based prioritization), uncheck "Register this connection's addresses in DNS" for the public ethernet card. In addition, ensure that there is only one A-record entry in the DNS server corresponding to the host name of the server, which maps to the general priority IP address. This is necessary for processes like the campaign manager and replication running as part of the Logger service, to listen on the right interface IP address for client connections.
- Step 8** If you enable High Availability, enter the **Active Directory Account Name** that the opposite side logger runs under or a security group that includes that account. For example, if you are running Websetup on the logger on Side A, enter the name of the Active Directory account (or security group) that is run on Side B logger.
- Step 9** Select the **Syslog** box to enable the Syslog event feed process (cw2kfeed.exe).
- Note** The event feed is processed and sent to the Syslog collector only if the Syslog collector is configured. For more information about the Syslog event feed process, see the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise* at <http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html>.
- Step 10** Click **Next**.
- Step 11** On the Data Retention page, modify the Database Retention Configuration table:
- a) For these tables, set the retention period to 40 days:
- Application\_Event
  - Event
  - Network\_Event
  - Route\_Call\_Detail
  - Route\_Call\_Variable
  - Termination\_Call\_Detail
  - Termination\_Call\_Variable



- b) Accept the default settings for all other tables. If your contact center requires access to any of that data for a longer period, enter an appropriate value.

**Step 12** Click **Next**.

**Step 13** On the Data Purge page, configure purges for a day of the week and a time when there is low demand on the system.

**Step 14** Accept the default **Automatic Purge at Percent Full**.

**Step 15** Click **Next**.

**Step 16** In the **Summary** window select the **Create Service Account** option, complete the following steps:

- a) Enter the domain user.

Verify that the user is created in the specified domain.

- b) Enter the valid password.

- c) Review the Summary and click **Finish**.

**Caution** Use the same domain user account for all the distributor and logger services. If you want to use different domain accounts for the logger and the distributor, ensure that the distributor service user account is added to the local logger `UcceService` groups on Side A and Side B.

---

## Add Router Component to Instance

Perform this procedure for Side A and Side B Routers.

### Procedure

---

**Step 1** In the Web Setup tool, select **Component Management > Routers**.

**Step 2** Click **Add**.

**Step 3** On the **Deployment** page, choose the current instance.

**Step 4** In the **Deployment** dialog, select the appropriate side.

**Step 5** Click **Duplexed**, and then click **Next**.

**Step 6** In the **Router Connectivity** dialog, configure the Private Interface and Public Interfaces. Click **Next**.

**Note** For the address input fields, use Fully Qualified Domain Names instead of IP addresses.

When there are two IP addresses configured on the public Network Interface Card (for IP-based prioritization), manually add two A-records on the DNS server. One A-record is for the high priority IP address and the other one is for the general priority IP address. The host part of the two DNS entries should be different from the hostname of Windows server. Use the new DNS entries to configure the interfaces. This note applies to the Router and to all PG machines.

**Step 7** Leave the **Enable Peripheral Gateways** field blank, and click **Next**.

**Step 8** In the **Router Options** dialog, the **Enable Quality of Service (QoS)** is enabled by default. Click **Next**.

On the Router Quality of Service page, you see preconfigured values for the Router QoS for the Private Network. These values only appear if you selected a Side A Router. You can change the values in the DSCP fields if necessary.

Keep QoS enabled for all Unified CCE Private network traffic. For most deployments, disable QoS for the public network traffic. For more details, refer to the appropriate section in the *Solution Design Guide for Cisco Packaged Contact Center Enterprise*, at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html>.

**Step 9** In the **Router Quality of Service** dialog, click **Next**.

**Step 10** In the **Summary** dialog, make sure that the Router summary is correct, then click **Finish**.

## Start Unified CCE Services

The Unified CCE components run as a Windows service on the host computer. You can start, stop, or cycle these services from the **Unified CCE Service Control tool** on the desktop.



**Note** This procedure is required for activating Unified CCE services. However, you must postpone this task until you install Unified CCE components in all virtual machines given in the deployment model.

### Procedure

**Step 1** On each Unified CCE Server machine, open **Unified CCE Service Control**.

**Step 2** Start the **Unified CCE component** services.

## Configure AW-HDS-DDS

Follow this sequence to configure AW-HDS-DDS for Packaged CCE 4000 Agents deployment.

| Sequence | Task                                                                                 |
|----------|--------------------------------------------------------------------------------------|
| 1        | <a href="#">Configure SQL Server for CCE Components, on page 2</a>                   |
| 2        | <a href="#">Add Unified CCE Instance, on page 76</a>                                 |
| 3        | <a href="#">Create HDS Database, on page 64</a>                                      |
| 4        | <a href="#">Add Administration and Data Server Component to Instance, on page 65</a> |
| 5        | <a href="#">Configure ICM Database Lookup, on page 114 (optional)</a>                |
| 6        | <a href="#">Cisco SNMP Setup, on page 21 (optional)</a>                              |

### Create HDS Database

Perform this procedure on the Administration & Data Server on which you want to create the HDS database.

## Procedure

---

- Step 1** Open the ICMDBA tool, and click **Yes** at any warnings that display.
- Step 2** Navigate to **Servers > Instances**.
- Step 3** Right-click the instance name and choose **Create**.
- Step 4** In the Select Component dialog box, choose **Administration & Data Server**. Click **OK**.
- Step 5** At the prompt “SQL Server is not configured properly. Do you want to configure it now?”, click **Yes**.
- Step 6** On the Configure dialog box, click **OK**.
- Step 7** On the Select AW Type dialog box, choose **Enterprise**. Click **OK** to open the Create Database dialog box.
- Step 8** Create the HDS database as follows:
- From the DB Type drop-down list, choose **HDS**.
  - Click **Add**.
  - On the Add Device dialog box, select **Data**.
  - From the Available Drives list, choose the drive on which you want to install the database.
  - In the Size field, you can leave the default value or enter an appropriate size for your deployment.
- Note** You can use the Database Size Estimator Tool to calculate the appropriate size for your deployment.
- Click **OK** to return to the Create Database dialog box.
  - Click **Add**.
  - On the Add Device dialog box, select **Log**.
  - From the Available Drives list, choose the drive on which you created the database.
  - In the Size field, you can leave the default value or enter an appropriate size for your deployment.
  - Click **OK** to return to the Create Database dialog box.
- Step 9** On the Create Database dialog box, click **Create** and then click **Start**.
- Step 10** When you see the successful creation message, click **OK** and then click **Close**.
- 

## Add Administration and Data Server Component to Instance

### Procedure

---

- Step 1** Open the Web Setup tool.
- Step 2** Select **Component Management > Administration & Data Servers**. Click **Add**.
- Step 3** On the **Deployment** page, choose the current instance.
- Step 4** On the **Add Administration & Data Servers** page, configure as follows:
- Click **Enterprise**.
  - Select the deployment size:
  - Click **Next**.
- Step 5** Select the radio button for your deployment size (either Small to Medium or Large).
- Note** For deployment size definitions and guidelines, see the *Solution Design Guide for Cisco Unified Contact Center Enterprise*.

**Step 6** Click **Next**.

**Step 7** In a Small to Medium Deployment page, select the radio button for your preferred option.

The three options from which to select are:

- Administration Server, Real-time and Historical Data Server and Detail Data Server (AW-HDS-DDS)
- Administration Server and Real-time Data Server (AW)
- Configuration-Only Administration Server

**Note** If you select AW-HDS-DDS, you must also specify Enable Historical Detail Data Replication during Logger setup.

**Note** Before you select a role that includes Historical Database Server (HDS), you must deploy an HDS database on this instance by running the Cisco Unified Intelligent Contact Management Database Administration Tool (ICMDBA) on the local machine.

**Step 8** Click **Next**.

**Step 9** On the Server Role in a Large Deployment page, select the radio button for your preferred option.

The four options from which to select are:

- Administration Server and Real-time and Historical Data Server (AW-HDS)
- Historical Data Server and Detail Data Server (HDS-DDS)
- Administration Server and Real-time Data Server (AW)
- Configuration-Only Administration Server

**Note** If you select AW-HDS or HDS-DDS, you must also specify Enable Historical Detail Data Replication during Logger setup.

**Note** Before you select a role that includes Historical Database Server (HDS), you must deploy an HDS database on this instance by running ICMDBA on the local machine.

**Step 10** Click **Next**.

**Step 11** On the next page of the wizard, enter connectivity information between Primary and Secondary Administration and Data servers.

**Note** Each site has at least one and usually two Administration & Data Servers that serve as real-time data Administration & Data Servers for the site. The primary Administration & Data Server maintains an active connection to the real-time server through which it receives real-time data. If the site has two Administration & Data Servers, Administration Clients are configured to automatically switch to a secondary Administration & Data Server if the first Administration & Data Server becomes non-functional for any reason. The secondary Administration & Data Server also maintains connections to the real-time server; however, these connections remain idle until needed. The secondary Administration & Data Server uses the primary Administration & Data Server, as their source for the real-time feed.

Indicate whether the server being setup is the Primary or Secondary Administration & Data Server at the site, by clicking on the radio button.

Next enter the host name or IP address of the Primary and Secondary Administration and Data Server at the site. The Secondary Administration and Data Server field is mandatory. If there is no secondary Administration

and Data Server being deployed at the site, then the same host name as that of the primary needs to be provided in this field.

Each primary and secondary pair must have its own Site Name, and the Site Name must be exactly the same on both Administration & Data Servers for them to be logically viewed as one.

**Step 12** On the Database and Options page, configure as follows:

- a) In the **Create Database(s) on Drive** field, choose C.
- b) Uncheck the **Configuration Management Service (CMS) Node** check box.
- c) Check the **Internet Script Editor (ISE) Server** (optional) check box.
- d) Click **Next**.

**Step 13** On the Central Controller Connectivity page, configure as follows:

**Note** For Packaged CCE 4000 Agents deployment, the IP address of Router and Logger is same.

- a) For **Router Side A**, enter the Router Side A IP address.
- b) For **Router Side B**, enter the Router Side B IP address.
- c) For **Logger Side A**, enter the Logger Side A IP address.
- d) For **Logger Side B**, enter the Logger Side B IP address.
- e) Enter the **Central Controller Domain Name**.
- f) Based on the Reference Design of your deployment type, distribute your AW-HDS and HDS-DDS VMs on Side A or Side B by selecting **Central Controller Side A Preferred** or **Central Controller Side B Preferred**. For details on the Reference Designs, see the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html>.
- g) Click **Next**.

**Step 14** In the **Summary** window select the Create Service Account option, and complete the following steps:

- a) Create a domain user account. Enter the created domain user.
- b) Enter the valid password.
- c) Review the Summary and click **Finish**.

**Caution** Use the same domain user account for all the distributor and logger services. If you want to use different domain accounts for the logger and the distributor, ensure that the distributor service user account is added to the local logger `UcceService` groups on Side A and Side B.

---

## Configure Packaged CCE Deployment Type

When you configure the Packaged CCE 4000 Agents and 12000 Agents deployment types, you must add a main site. A main or remote site can have zero or more peripheral sets associated with it. Peripheral set is a collection of all components (like Finesse, CVP, and so on) that are dependent on peripheral gateway (including the peripheral gateway itself). For information on how to add peripheral sets, see [Add and Maintain Peripheral Set, on page 143](#).

## Add and Maintain Main Site in 4000 Agents or 12000 Agents Deployment Type

### Procedure

- 
- Step 1** Navigate to the **Unified CCE Administration > Overview > Infrastructure Settings > Deployment Settings**.
- Step 2** Click the gear icon in the **Deployment Type**.  
The **Configure your deployment** wizard opens.
- Step 3** Select the deployment type as *Packaged CCE: 4000 Agents* or *Packaged CCE: 12000 Agents* from the drop-down list.
- Step 4** Use the **Download Template** to get the CSV template for the selected deployment type.
- Step 5** Fill the particulars in the file and save it.

**Table 2: CSV Template Details**

| Column | Description                       | Required? | Permissible Values                                                                                                                                         |
|--------|-----------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| name   | Unique identifier for the machine | Yes       | Name must start with an alphabet. Maximum length is limited to 128 characters. Valid characters are a-z, A-Z, 0-9, dot (.), underscore (_), or hyphen (-). |

| Column      | Description              | Required? | Permissible Values |
|-------------|--------------------------|-----------|--------------------|
| machineType | MachineType<br>Enum name | Yes       |                    |

| Column | Description | Required? | Permissible Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|-------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        |             |           | <p>Mandatory machines are:</p> <ul style="list-style-type: none"> <li>• CCE_ROGGER (applicable for 4000 Agents deployment)</li> <li>• CCE_ROUTER (applicable for 12000 Agents deployment)</li> <li>• CCE_LOGGER (applicable for 12000 Agents deployment)</li> <li>• CCE_AW</li> <li>• CUIC_PUBLISHER</li> <li>• CUIC_SUBSCRIBER</li> <li>• LIVE_DATA</li> <li>• IDS_PUBLISHER</li> <li>• IDS_SUBSCRIBER</li> </ul> <p>Optional machines:</p> <ul style="list-style-type: none"> <li>• CCE_PG</li> <li>• CVP</li> <li>• FINESSE_PRIMARY</li> <li>• FINESSE_SECONDARY</li> <li>• CM_PUBLISHER</li> <li>• CM_SUBSCRIBER</li> <li>• HDS</li> <li>• ECE (refers to ECE Data Server VM for ECE 400 agents and Services Server VM for ECE 1500 agents)</li> <li>• ECE_WEB_SERVER</li> <li>• CVP_REPORTING</li> <li>• GATEWAYS</li> <li>• CVVB</li> <li>• CUSP</li> <li>• SOCIAL_MINER</li> <li>• THIRD_PARTY_MULTICHANNEL</li> <li>• MEDIA_SERVER</li> </ul> |



| Column        | Description    | Required? | Permissible Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|----------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                |           | <ul style="list-style-type: none"> <li>•</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>•</li> </ul> <p>To enable addition of Media Servers in Packaged CCE 12.0(1), install the ICM12.0(1) ES and CVP ES patch. For more information, see <i>Release Notes for Packaged Contact Center Enterprise</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html</a>.</p> |
| publicAddress | Public address | Yes       | Valid IP address or hostname                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Column            | Description                           | Required?                                                                                                   | Permissible Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|---------------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| connectionInfo    | Connection information of the machine | Required for CM_PUBLISHER, FINESSE_PRIMARY, ECE_WEB_SERVER, CVP, CVP_REPORTING, CUSP, GATEWAY and LIVE_DATA | <p>Enter the username and password in the following format:</p> <pre>userName=&lt;user&gt;&amp;password=&lt;password&gt;</pre> <p>For more information on the credentials of each component, see <a href="#">Table 7: Machine Credentials, on page 139</a>.</p> <p>ConnectionInfo is optional if you are configuring FTP for CVP (Media Server).</p> <p><b>Note</b> To enable FTP configuration for CVP in Packaged CCE 12.0(1), install the ICM12.0(1) ES and CVP ES patch. For more information, see <i>Release Notes for Packaged Contact Center Enterprise</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html</a>.</p> <p>Append the FTP attributes to the username and password in the following format:</p> <pre>userName=&lt;user&gt;&amp;password=&lt;password&gt;; ftpEnabled=&lt;true or false&gt; &amp;ftpUserName=&lt;ftp_username&gt; &amp;ftpPassword=&lt;ftp_password&gt; &amp;ftpPort=&lt;ftp_portnumber&gt;</pre> <p>For more information on the FTP attributes, see FTP Section in the <a href="#">Add Media Server as External Machine, on page 128</a>.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Replace Ampersand (&amp;) or equal sign (=) in usernames or passwords with their respective URL encoded values "%26" or "%3D".</li> <li>• Semicolon (;) delimits the Windows Administration credentials from FTP credentials.</li> </ul> |
| privateAddress    | Private address                       | Required for ROgger, ROUTER, LOGGER, and PG                                                                 | Valid IP address                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| peripheralSetName | Peripheral set name                   | Required for PG, CUCM, Finesse, CVP                                                                         | Name can start with an alphabet. Maximum length is limited to 10 characters. Valid characters are a-z, A-Z, 0-9, dot (.), or an underscore (_).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Column | Description      | Required? | Permissible Values |
|--------|------------------|-----------|--------------------|
| side   | Side information | Yes       | sideA<br>sideB     |

**Step 6** Upload the file and click **Next**.

**Step 7** Wait for validation to be completed.

During the validation, tasks are performed depending on the components defined in the CSV template. For more information about the tasks, see [Automated Initialization Tasks for 4000 and 12000 Agent Deployments, on page 73](#).

**Note** • If any of the performed tasks fails, then all the tasks are reverted.

If validation fails, then click **Back** to fix the issues in the file and upload the file again, else click **Done**.

The main site that is thus created is added to the Inventory page.

*Automated Initialization Tasks for 4000 and 12000 Agent Deployments*

Packaged CCE performs the following tasks during initialization.

| Component      | Automated Initialization Tasks                                                                                                                                                                                                                                                                                                                                                                                                                                      | Other Dependent Components                                    |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Unified CCE PG | Creates the Agent Peripheral Gateway (PG) and PIMs                                                                                                                                                                                                                                                                                                                                                                                                                  | Cisco Unified Communications Manager (CUCM) and Cisco Finesse |
|                | Creates the Media Routing PG (MR PG), without PIMs                                                                                                                                                                                                                                                                                                                                                                                                                  | None                                                          |
|                | Creates the VRU PG and PIMs                                                                                                                                                                                                                                                                                                                                                                                                                                         | Unified Customer Voice Portal                                 |
|                | Creates the routing client for each peripheral<br><b>Note</b> <ul style="list-style-type: none"> <li>Depending on your call flow requirements, create Network VRU labels in the Label list option using the <i>Configuration Manager Tool</i>.</li> <li>Network VRU Type 10 and Type 2 must be created in the Network VRU Explorer using the Configuration Manager Tool. For more information, see the <i>online help in Configuration Manager Tool</i>.</li> </ul> | None                                                          |

| Component                     | Automated Initialization Tasks                                                                                                                                                                                                   | Other Dependent Components |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| Unified Customer Voice Portal | <ul style="list-style-type: none"> <li>• Configures the Unified CVP Call Server components</li> <li>• Configures the Unified CVP VXML Server components</li> <li>• Configures the Unified CVP Media Server components</li> </ul> | None                       |
| Unified CVP Reporting Server  | Configures the Unified CVP Reporting Server components (not applicable for peripheral set)                                                                                                                                       | None                       |
| Live Data                     | Redeploys Lives data                                                                                                                                                                                                             | CUCM and Cisco Finesse     |

## System Inventory for Packaged CCE 4000 Agents and 12000 Agents Deployment

You can access the Inventory after you have completed the change to a Packaged CCE deployment.

Access the Inventory by navigating to the **Unified CCE Administration > Infrastructure > Inventory**.

System Inventory contents are updated when you select or change the deployment type and after regular system scans. If a system scan detects VMs that do not conform to Packaged CCE requirements, the **Configure your deployment** pop-up window opens automatically, detailing the errors. You can access the Inventory again after you have corrected the errors and completed the **Configure your deployment** popup window.

For more details on **Server Status** rules, see the [Monitor Server Status Rules for Packaged CCE 4000 and 12000 Agents Deployments, on page 77](#).




---

**Note** After a Packaged CCE deployment is initialized, you cannot switch to another deployment type.

---

Table 3: System Inventory Layout and Actions

| Item                 | Notes                                              | Actions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Set the Principal AW | Only one AW machine can be Principal AW at a time. | <p>Specifying the Principal AW is required. The first SideA AW machine in the CSV file is the principal AW.</p> <p>The Principal AW (Admin Workstation) is responsible for managing background tasks that are run periodically to sync configuration with other solution components, such as SSO management, Smart Licensing, etc.</p> <p>The Principal AW is used by the following features:</p> <ul style="list-style-type: none"> <li>• File Transfer</li> <li>• Context Service Registration</li> <li>• SSO Registration and Enablement</li> <li>• Differential Sync</li> </ul> <p>You can change the Principal AW by selecting a different AW in the Inventory. Set the AW on which you make most of your configuration changes as the Principal AW.</p> <p><b>To set the Principal AW:</b></p> <ol style="list-style-type: none"> <li>1. Click the AW to open the Edit CCE AW window.</li> <li>2. Check the <b>PrincipalAW</b> check box.</li> <li>3. Unified CCE Diagnostic Framework Portico domain, username, and password.</li> </ol> <p>These credentials must be of a domain user who is a local administrator on all the CCE servers and valid on all Unified CCE components in your deployment (the Side A and Side B Unified CCE Roggers, PGs, and AW-HDS-DDSs).</p> <p><b>Note</b> Every time the Active Directory credentials are updated, the credentials configured here must be updated as well.</p> <ol style="list-style-type: none"> <li>4. Click <b>Save</b>.</li> </ol> |

| Item            | Notes                                | Actions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| View Statistics | Unified CVP and CVP Reporting Server | <p><b>Note</b> To enable CVP Statistics feature in Packaged CCE 12.0(1), install the ICM12.0(1) ES patch. For more information, see <i>Release Notes for Packaged Contact Center Enterprise</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html</a>.</p> <p>You can launch statistics by hovering over the following VMs and clicking the <b>Statistics</b> icon:</p> <ul style="list-style-type: none"> <li>• <b>Unified CVP</b></li> <li>• <b>Unified CVP Reporting</b></li> </ul> <p>For more information, see <a href="#">Unified CVP Statistics, on page 616</a> and <a href="#">Unified CVP Reporting Statistics, on page 628</a>.</p> |



**Note** If you change the password of any of the Packaged CCE components, you must update the password in the respective VM in the system inventory.

## Add Unified CCE Instance

### Procedure

- Step 1** Open the Unified CCE Web Setup tool from shortcut on your desktop.
- Step 2** Sign in as a domain user with local administrator rights.
- Step 3** Click **Instance Management**, and then click **Add**.
- Step 4** On the **Add Instance** page, from the drop-down list, choose the customer **Facility and Instance**.
- Step 5** Enter an instance number.

The same instance name can occur more than once in a domain, so the instance number provides the uniqueness. The instance number must be between 0 and 24. The instance number must match for the same instance across your entire deployment. For an Enterprise (single instance) deployment, select 0 unless there are reasons to select another value.

- Step 6** Click **Save**.

**Note** These steps of adding instance must be repeated on each Windows Server VM that hosts the Unified ICM component(s).

## Monitor Server Status Rules for Packaged CCE 4000 and 12000 Agents Deployments

In Packaged CCE 4000 and 12000 Agents deployments, the Inventory table displays an alerts icon for the Principal AW machine. Hover over the alert icon to view status of the machine.



**Note** If any machine in the Inventory is updated, it can take approximately three minutes for the status to appear.

## Configure Cisco Unified Contact Center Enterprise PG



**Note** Repeat the following tasks each time you add the Peripheral Set to the Main Site or Remote Site. See [Add and Maintain Peripheral Set, on page 143](#) for information on Peripheral Set.

### Configuration Tasks

If the Peripheral Set contains CUCM PG:

[Install Cisco JTAPI Client on PG, on page 77](#)

[Install Cisco JTAPI Client on PG, on page 78](#)

[Set up CTI Server, on page 79](#)

If the peripheral set contains VRU PG, manually restart the CVP Servers.

If the peripheral set contains MR PG, [Add PIMs to the Media Routing Peripheral Gateway, on page 130](#)

## Install Cisco JTAPI Client on PG

After setting up the Cisco Unified Communications Manager (CUCM) PG, you must install the Cisco JTAPI client. PG uses Cisco JTAPI to communicate with CUCM. Install the Cisco JTAPI client from CUCM Administration.



**Note** Continue with the steps provided in this section if you are installing the JTAPI client for CUCM version earlier than Release 12.5.

To install the JTAPI client for CUCM, Release 12.5 and above, see [Install Cisco JTAPI Client on PG, on page 78](#).

### Before you begin

Before you install the JTAPI client, ensure that the previous version is uninstalled.

### Procedure

**Step 1** Open a browser window on the PG machine.

- Step 2** Enter the URL for the Unified Communications Manager Administration utility: `http://<Unified Communications Manager machine name>/ccmadmin`.
- Step 3** Enter the username and password that you created while installing and configuring the Unified Communications Manager.
- Step 4** Choose **Application > Plugins**. Click **Find**.
- Step 5** Click the link next to **Download Cisco JTAPI for Windows**. We recommend you to download the 64 bit version. However, if you have already downloaded the 32 bit version, you can proceed to step 7.  
Download the JTAPI plugin file.
- Step 6** Choose **Save** and save the plugin file to a location of your choice.
- Step 7** Open the installer.
- Step 8** In the Security Warning box, click **Yes** to install.
- Step 9** Choose **Next** or **Continue** through the remaining Setup screens. Accept the default installation path.
- Step 10** When prompted for the TFTP Server IP address, enter the CUCM IP address.
- Step 11** Click **Finish**.
- Step 12** Reboot the machine.
- 

### Install Cisco JTAPI Client on PG

Complete the following procedure only if you are installing JTAPI client to connect to Cisco Unified Communications Manager, Release 12.5 and above.

#### Before you begin

Before you install the JTAPI client, ensure that the previous version is uninstalled.

#### Procedure

---

- Step 1** Open a browser window on the PG machine.
- Step 2** Enter the URL for the Unified Communications Manager Administration utility: `http://<Unified Communications Manager machine name>/ccmadmin`.
- Step 3** Enter the username and password that you created while installing and configuring the Unified Communications Manager.
- Step 4** Choose **Application > Plugins**. Click **Find**.
- Step 5** Click the link next to **Download Cisco JTAPI Client for Windows 64 bit** or **Download Cisco JTAPI Client for Windows 32 bit**.  
Download the JTAPI plugin file.
- Step 6** Choose **Save** and save the plugin file to a location of your choice.
- Step 7** Unzip the JTAPI plugin zip file to the default location or a location of your choice.  
There are two folders in the unzipped folder `CiscoJTAPIx64` and `CiscoJTAPIx32`.
- Step 8** Run the `install64.bat` file in the `CiscoJTAPIx64` folder or run the `install32.bat` file in the `CiscoJTAPIx32` folder.



The default install path for JTAPI client is `C:\Program Files\JTAPITools`.

- Step 9** To accept the default installation path, click **Enter** and proceed.  
Follow the instructions. Click **Enter** whenever necessary as per the instructions.  
The JTAPI client installation completes at the default location. The following message is displayed:

```
Installation Complete.
```

- Step 10** Reboot the machine.

### What to do next



- Note** The default location, where the JTAPI client is installed, also contains the `uninstall64.bat` and `uninstall32.bat` file. Use this file to uninstall this version of the client, if necessary.

## Set up CTI Server

Use the PG Setup tool to set up a CTI Server.



- Note** Only users who are part of the local Administrators group can run Peripheral Gateway setup.

## Add CTI Server Component

### Procedure

- Step 1** Open Peripheral Gateway Setup tool from **Unified CCE Tools** on the desktop.
- Step 2** Click **Add** in the Instance Components section.  
The ICM Component Selection dialog box opens.
- Step 3** Click **CTI Server**, and click **OK**.  
The CTI Server Properties dialog box opens.

## Set CTI Server Properties

### Procedure

- Step 1** In the CTI Server Properties dialog box, check **Production mode** and **Auto start at system startup** unless your Unified CCE support provider tells you otherwise. These settings set the CTI Server Service startup type to Automatic, so the CTI Server starts automatically when the machine starts up.

- Step 2** Check the **Duplexed CTI Server** option if you are configuring redundant CTI Server machines.
- Step 3** In the CG Node Properties section, the numeric portion of the CG node **ID** must match the PG node ID (for example, CG 1 and PG 1).
- Step 4** The **ICM system ID** is the Device Management Protocol (DMP) number of the PG associated with the CTI Gateway. Generally this number is the number associated with the CG ID in step 3.
- Step 5** If the CTI Server you add is duplexed, specify which **Side** you are setting up: Side A or Side B. If the CTI Server is simplex, choose Side A.
- Step 6** Click **Next**.
- The CTI Server Component Properties dialog box opens.

### Set CTI Server Component Properties

The CTI Server Component Properties dialog box supports the following modes of connections:

- **Secured and Non-Secured Connection (Mixed-mode):** Allows secured and non-secured connection between the CTI Server and the CTI clients.
- **Secured-Only Connection:** Allows secured connection between the CTI Server and the CTI clients.



**Important** Non-Secured only mode is not supported.



**Note** To enable secured connection between the components, ensure to complete the security certificate management process.

For more information, see the chapter *Certificate Management for Secured Connections* in *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html>.

In the CTI Server Component Properties dialog box, setup automatically displays the default **Secured Connection Port** and the **Non-Secured Connection Port** values. Use these values or change them to the required port numbers. CTI clients use these ports to connect to the CTI Server.

If you have multiple CTI servers running on a single machine, each CTI server must use a different port number set for *Secured connection* and *Mixed-mode connection*.

### Procedure

- Step 1** Select the appropriate connection type.
- For *Secured Connection*, check the **Enable Secure-Only Mode** check box.  
This option disables the **Non-Secured Connection Port** field.
  - For *Mixed-mode connection*, ensure that the **Enable Secure-Only Mode** check box is unchecked.

This is the default connection mode.

- Step 2** To ensure that an agent is logged in to the client before the client receives events from the CTI Server, check the **Agent Login Required for Client Events** check box. This ensures that the clients are prevented from accessing data for other agents.
- Step 3** Click **Next**.
- The CTI Server Network Interface Properties dialog box opens.
- 

### Set CTI Server Network Interface Properties

#### Procedure

---

- Step 1** In the CTI Server Network Interface Properties dialog box, in the **PG public interfaces** section, enter the public network addresses for the PGs associated with the CTI Server.
- Step 2** In the **CG private interfaces** section, enter the private network addresses of the CTI Server.
- Step 3** In the **CG visible interfaces** section, enter the public network addresses of the CTI Server.
- Step 4** Click **Next**.
- The Check Setup Information window opens.
- 

### Complete CTI Server Setup

#### Procedure

---

- Step 1** In the Check Setup Information window, ensure that the settings displayed are as you intended. If you want to modify any settings before proceeding, use the **Back** button.
- Step 2** When the settings are correct, click **Next**.
- Step 3** The final screen displays and asks whether you want to start the Node Manager now.
- Step 4** Click **Finish** to exit setup (and optionally start the Node Manager).
- If you choose to start it, the Node Manager automatically starts the other Unified CCE processes on the CTI Server.
- 

## Configure Cisco Unified Customer Voice Portal

The following table outlines the Cisco Unified Customer Voice Portal (CVP) configuration tasks for Packaged 4000 Agents deployment or 12000 Agents deployment.



**Note** The CVP configurations are site specific. Side A and Side B configurations per site must be the same.

---

| Configuration Tasks                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------|
| To secure communication between Call Server and ICM, see <a href="#">Secure GED 125 Communication between Call Server and ICM, on page 183</a> . |
| For more information about securing CVP communication, see <a href="#">Unified CVP Security, on page 183</a>                                     |
| For web secure communication, see <a href="#">, on page 609</a>                                                                                  |
| <a href="#">CVP Server Services Setup, on page 174</a>                                                                                           |
| <a href="#">Configure Media Server, on page 202</a>                                                                                              |
| <a href="#">Configure SNMP, on page 82</a>                                                                                                       |

## Configure SNMP

Use the Simple Network Management Protocol (SNMP) configuration to receive SNMP traps from the Cisco Customer Voice Portal (CVP) server. You can do this configuration in the CVP server using a configuration file.

### Procedure

- Step 1** Log in to the CVP server using Administrator credentials.
- Step 2** Navigate to C:\Cisco\CVP\conf\SNMPD.CNF.
- Step 3** Complete the following parameters to do the SNMP configuration:

**Note** Ensure to enter the parameter values in a single line, without a break.

*Table 4: SNMP configuration parameters*

| Parameter                | Description                                                                                                                                                                                                                               | Format                                                                                                                                                                                                                                                                                                                           |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| snmpCommunityEntry       | 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 and associate community strings with the device. | <pre>snmpCommunityEntry &lt;snmpCommunityIndex&gt; &lt;snmpCommunityName&gt; &lt;snmpCommunitySecurityName&gt; &lt;snmpCommunityContextEngineID&gt; &lt;snmpCommunityContextName&gt; &lt;snmpCommunityTransportTag&gt; &lt;snmpCommunityStorageType&gt;</pre> <p>Example:</p> <pre>v2ccvp cvp cvp localSnmpID - - readOnly</pre> |
| vacmSecurityToGroupEntry | Configure authentication group for V1/V2C SNMP protocol.                                                                                                                                                                                  | <pre>vacmSecurityToGroupEntry &lt;vacmSecurityModel&gt; &lt;vacmSecurityName&gt; &lt;vacmGroupName&gt; &lt;vacmSecurityToGroupStorageType&gt;</pre> <p>Example:</p> <pre>vacmSecurityToGroupEntry snmpv2c cvp v2cNoAuthNoPrivGroup nonVolatile</pre>                                                                             |

| Parameter       | Description                                                                                                                                                                                                                               | Format                                                                                                                                                                                                                                                                                                                 |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| snmpNotifyEntry | 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; configure a destination to receive SNMP notifications from an SNMP management station.        | <pre>snmpNotifyEntry &lt;snmpNotifyName&gt; &lt;snmpNotifyTag&gt; &lt;snmpNotifyType&gt; &lt;snmpNotifyStorageType&gt;</pre> <p><b>Example:</b></p> <pre>snmpNotifyEntry Descvp Descvp-TrapTag trap readOnly</pre>                                                                                                     |
| usmUserEntry    | 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 and associate SNMP users with devices. | <pre>usmUserEntry &lt;usmUserEngineID&gt; &lt;usmUserName&gt; &lt;usmUserAuthProtocol&gt; &lt;usmUserPrivProtocol&gt; &lt;usmUserStorageType&gt; &lt;usmTargetTag&gt; &lt;AuthKey&gt; &lt;PrivKey&gt;</pre> <p><b>Example:</b></p> <pre>usmUserEntry localSnmID cvp usmNoAuthProtocol usmNoPrivProtocol readOnly</pre> |
| snmpNotifyEntry | Configure the SNMP agent that runs on the Unified CVP device to use the V3 SNMP protocol to communicate with an SNMP management station; configure a destination to receive SNMP notifications from an SNMP management station.           | <pre>snmpNotifyEntry &lt;snmpNotifyName&gt; &lt;snmpNotifyTag&gt; &lt;snmpNotifyType&gt; &lt;snmpNotifyStorageType&gt;</pre> <p><b>Example:</b></p> <pre>snmpNotifyEntry Descvp Descvp-TrapTag trap readOnly</pre>                                                                                                     |
| sysLocation     | Configure the MIB2 System Group system location settings, and associate the MIB2 System Group with devices.                                                                                                                               | <pre>&lt;octetString&gt;</pre> <p><b>Example:</b></p> <pre>MIBLoc</pre>                                                                                                                                                                                                                                                |
| sysContact      | Configure the MIB2 System Group system contact and associate the MIB2 System Group with devices.                                                                                                                                          | <pre>&lt;octetString&gt;</pre> <p><b>For example:</b></p> <pre>MIBContact</pre>                                                                                                                                                                                                                                        |

| Parameter             | Description                                                      | Format                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| snmpTargetAddrEntry   | Configure SNMP trap receiver target IP.                          | <pre>snmpTargetAddrEntry &lt;snmpTargetAddrName&gt; &lt;snmpTargetAddrTDomain&gt; &lt;snmpTargetAddrTAddress&gt; &lt;snmpTargetAddrTimeout&gt; &lt;snmpTargetAddrRetryCount&gt; &lt;snmpTargetAddrTagList&gt; &lt;snmpTargetAddrParams&gt; &lt;snmpTargetAddrStorageType&gt; &lt;snmpTargetAddrTMask&gt; &lt;snmpTargetAddrMMS&gt;</pre> <p><b>Example:</b></p> <pre>snmpTargetAddrEntry targetDesV2-Addr1 snmpUDPDomain 10.100.10.100:0 0 0 \ targetDesV2-TrapTag targetDesV2-TrapParams readOnly 255.255.255.255:0 2048</pre> |
| snmpTargetParamsEntry | Configure the parameters to be used while sending notifications. | <pre>snmpTargetParamsEntry &lt;snmpTargetParamsName&gt; &lt;snmpTargetParamsMPModel&gt; &lt;snmpTargetParamsSecurityModel&gt; &lt;snmpTargetParamsSecurityName&gt; &lt;snmpTargetParamsSecurityLevel&gt; &lt;snmpTargetParamsStorageType&gt;</pre> <p><b>Example:</b></p> <pre>snmpTargetParamsEntry params1 0 snmpv1 principal noAuthNoPriv nonVolatile</pre>                                                                                                                                                                  |

**Step 4** Save the changes.

**Step 5** Go to Services and restart Cisco CVP SNMP Management.

## License Management

Complete the following procedure to configure license in the CVP server (Call Server or Reporting Server).

### Procedure

**Step 1** Log in to the CVP server (Call Server or Reporting Server).

**Step 2** Copy the license file into C:\Cisco\CVP\conf\license location.

**Note** The license file must be named as cvp.license.

**Step 3** Restart the respective server.

## Configure Cisco Unified Communications Manager

The following table outlines the Cisco Unified Communications Manager configuration tasks for Packaged CCE 4000 Agents deployment or 12000 Agents deployment.

| Task                                                                                                         |
|--------------------------------------------------------------------------------------------------------------|
| For details on CA and self-signed certificate, see <a href="#">Secure Communication on CUCM, on page 192</a> |
| <a href="#">Set Up Application User</a>                                                                      |
| <a href="#">Configure Fully Qualified Domain Name, on page 25</a>                                            |
| <a href="#">Configure Cisco Unified Communications Manager Groups, on page 25</a>                            |
| <a href="#">Set Up Device Pool</a>                                                                           |
| <a href="#">Configure Conference Bridges, on page 26</a>                                                     |
| <a href="#">Configure Media Termination Points, on page 26</a>                                               |
| <a href="#">Transcoder Configuration in Unified CM and IOS Gateway, on page 27</a>                           |
| <a href="#">Configure Media Resource Groups, on page 27</a>                                                  |
| <a href="#">Configure and Associate Media Resource Group List, on page 28</a>                                |
| <a href="#">Configure CTI Route Point, on page 28</a>                                                        |
| <a href="#">Configure Ingress Gateways for Locations-based Call Admission Control, on page 29</a>            |
| <a href="#">Add a SIP Profile in Unified CM, on page 29</a>                                                  |
| <a href="#">Configure Trunk, on page 30</a>                                                                  |
| <a href="#">Configure Route Group, on page 30</a>                                                            |
| <a href="#">Configure Route List, on page 31</a>                                                             |
| <a href="#">Configure Route Pattern, on page 31</a>                                                          |
| <a href="#">Configure A-Law Codec</a>                                                                        |
| <a href="#">Configure SNMP, on page 87</a>                                                                   |
| <a href="#">Configure Agent Desk Settings, on page 88</a>                                                    |

### Set Up Device Pool

Complete the following procedure to configure a device pool.

### Procedure

---

- Step 1** Choose **System** > **device pool**.
  - Step 2** Click **Add new**.
  - Step 3** Provide an appropriate device pool name in **Device Pool Name**.
  - Step 4** Select a corresponding Call manager group in **Cisco Unified Communications Manager group**.
  - Step 5** Select appropriate **Date/Time Group** and **Region**.
  - Step 6** Select an appropriate Media resource group list in **Media Resource Group List**.
  - Step 7** Click **Save**.
- 

## Set Up Application User

### Procedure

---

- Step 1** In Unified Communications Manager, Choose **User Management** > **Application User**.
  - Step 2** In the Application User Configuration window, click **Add New**.
  - Step 3** Enter the User ID that is set in the Peripheral Gateway Setup.  
**Note** The <site>\_<peripheralsetname>\_pguser is set on the PIM when the Peripheral Set is created.
  - Step 4** Enter a password of your choice.
  - Step 5** You must enter the same password set in the Peripheral Gateway Setup for CUCM PIM.
  - Step 6** Add the application user to the Standard CTI Enabled Group and Role:
    - a) Click **Add to Access Control Group**.
    - b) Select the **Standard CTI Enabled** group.
    - c) Select the **Standard CTI Allow Control of Phones supporting Connected Xfer and conf** group.
    - d) Select the **Standard CTI Allow Control of Phones supporting Rollover Mode** group.
    - e) Click **Add Selected**.
    - f) Click **Save**.
  - Step 7** Associate the CTI route points and the phones with the application user.
  - Step 8** Click **Save**.
- 

## Configure A-Law Codec

Complete the following procedure to configure Unified Communications Manager.

### Procedure

---

- Step 1** Click the **System**.
- Step 2** Select **Service Parameters**.



- Step 3** Select a Server.
- Step 4** Select the service as **Cisco Call Manager(Active)**.
- Step 5** Under Clusterwide Parameters (system-location and region), ensure the following:
- **G.711 A-law Codec Enabled** is **Enabled**.
  - **G7.11 mu-law Codec Enabled** to **Disabled**.
- Step 6** Click **Save**.
- 

## Configure SNMP

### Procedure

---

- Step 1** Log in to the Cisco Unified Serviceability (*https://hostname of primary server:8443/ccmservice*) using administrator credentials.
- Step 2** Select **SNMP > V1/V2c > Community String**.
- Step 3** From **Server** drop-down list, select the server for which you want to configure a community string and click **Find**.
- Step 4** Click **Add New** to add new community string.
- a) Enter **Community String**.  
**Example:**  
public.
  - b) In **Host IP Addresses Information** field, choose **Accept SNMP Packets from any host**.
  - c) From **Access Privileges** drop-down list, select **ReadWriteNotify** option.
  - d) Check **Apply to All Nodes** check box to apply community string to all nodes in the cluster. Information message will be displayed.
  - e) Click **OK**.
  - f) Click **Save**.  
A message is displayed, that indicates that changes will not take effect until you restart the SNMP primary agent. To continue the configuration without restarting the SNMP primary agent, click **Cancel**. To restart the SNMP primary agent service, click **OK**.
  - g) Click **OK**.
- Step 5** Select **SNMP > V1/V2c > Notification Destination**.
- Step 6** From **Server** drop-down list, select the server for which you want to configure a notification destination and click **Find**.
- Step 7** Click **Add New** button to add new notification destination.
- a) From **Host IP Addresses** drop-down list, select **Add New**.
  - b) In **Host IP Address** field, enter the Prime Collaboration server IP address .
  - c) In the **Port Number** field, enter the notification receiving port number.  
**Note** Default port number is 162.
  - d) In **SNMP Version Information** field, select the SNMP Version V2C.

- e) In **Notification Type Information** field; from **Notification Type** drop-down list, select **Trap**.
  - f) In **Community String Information** field; from **Community String** drop-down list, select Community String created in Step 4 from the drop-down list.
  - g) Check the **Apply to All Nodes** check box to apply community string to all nodes. Information message will be displayed.
  - h) Click **OK**.
  - i) Click **Insert**.  
A message is displayed, that indicates that changes will not take effect until you restart the SNMP primary agent. To continue the configuration without restarting the SNMP primary agent, click **Cancel**. To restart the SNMP primary agent service, click **OK**.
  - j) Click **OK**.
- 

## Configure Agent Desk Settings

### Procedure

---

**Step 1** From the AW server, open Configuration Manager, choose **Configure ICM > Enterprise > Agent Desk Settings > Agent Desk Settings List**. The Agent Desk Settings List dialog box opens.

**Step 2** Click **Retrieve** and then Click **Add**.

**Step 3** Fill in the Attributes tab information:

**Name.** Enter a name for the agent desk settings that is unique within the enterprise.

**Ring No Answer Time.** Enter the number of seconds (between 1 and 120) that a call may ring at the agent's station. If you are deploying the Unified CVP, make sure this number is less than the number set for the No Answer Timeout for Router Requery that you set in the Unified CVP.

If you configure this timer, you do not need to configure the Unified Communications Manager Call Forward on No Answer for agent extensions in the Unified Communications Manager, unless you want them to be used when the agent is not logged in. If you set the Unified Communications Manager Call Forward No Answer time, enter a value at least 3 seconds higher than the Ring No Answer Time on each Unified Communications Manager node.

**Ring no answer dialed number.** Enter the Unified CCE DN associated with the routing script that you want to use to reroute a call that an agent has not answered. If you are deploying the Unified CVP, leave this field blank.

**Logout non-activity Time.** Enter the number of seconds (between 10 and 7200) in which the agent can remain in Not Ready state before Unified CCE automatically logs out the agent.

**Work Mode on Incoming.** Select whether wrap-up is required following an incoming call. Select an option from the drop-down list.

**Work Mode on Outgoing.** Select whether wrap-up is required following an outgoing call. Select an option from the drop-down list.

**Wrap Up Time.** Enter the amount of time, in seconds, allocated to an agent to wrap up a call.

**Assist Call Method.** Select whether Unified CCE creates a consultative call or a blind conference call for a supervisor assistance request.

**Emergency Alert Method.** Select whether the Unified CCE creates a consultative call or a blind conference call for an emergency call request.

Blind conference is not supported if the call may queue on a VRU.

**Description.** Enter additional optional information about the agent desk settings.

**Step 4** Use the following boxes to select or de-select miscellaneous settings:

**Auto-answer.** Indicates whether calls to the agent are automatically answered. The agent is not required to take any action to answer the call. If a second call comes in while a call is in progress, the call is not automatically answered. This is the same behavior as with Unified Communications Manager.

If you enable auto-answer, you must also configure the agent phone in Unified Communications Manager to turn the speakerphone or headset (or both) to ON. If you turn *only* the headset to ON, the agent must also turn the phone headset button to ON.

In a multi-line enabled environment with auto-answer selected, if you are on a call on your non-ACD line, the call will *not* auto-answer. However, if you turn on Unified Communications Manager Auto Answer, the call *will* answer.

**Idle Reason Required.** Indicates whether an agent is required to enter a reason before entering the Idle state.

**Logout Reason Required.** Indicates whether an agent is required to enter a reason before logging out.

**Auto Record on Emergency.** Indicates in a record request is automatically sent when an emergency call request starts.

**Cisco Unified Mobile Agent** (check box). Enables the Unified Mobile Agent feature so that the agent can log in remotely and take calls from any phone. For more information about the Unified Mobile Agent, see the *Cisco Unified Contact Center Enterprise Features Guide* at [https://www.cisco.com/en/US/products/sw/custcosw/ps1844/products\\_feature\\_guides\\_list.html](https://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_feature_guides_list.html).

**Step 5** Click **Save** and then click **Close**.

**Note** For any change, you perform in the **Agent Desk Settings** to take effect, log out and then log in to the Finesse Agent Desktop.

## Configure Cisco Unified Intelligence Center

Follow this sequence to configure the Cisco Unified Intelligence Center for Packaged CCE 4000 and 12000 Agents deployment

| Sequence | Task                                                                                                                                                                                                                                                                                                                                                        |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | For details on security certificate, see <i>Cisco Unified Intelligence Center User Guide</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-user-guide-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-user-guide-list.html</a> |
| 3        | <a href="#">Configure Unified Intelligence Center Data Sources for External HDS, on page 32</a>                                                                                                                                                                                                                                                             |
| 3        | <a href="#">Download Report Bundles, on page 33</a>                                                                                                                                                                                                                                                                                                         |
| 4        | <a href="#">Import Reports, on page 33</a>                                                                                                                                                                                                                                                                                                                  |

| Sequence | Task                                                                             |
|----------|----------------------------------------------------------------------------------|
| 5        | <a href="#">Configure Unified Intelligence Center Administration, on page 35</a> |

## Configure Cisco Finesse

Follow this sequence to configure the Cisco Finesse for Packaged CCE 4000 Agents deployment or 12000 Agents deployment

| Sequence | Task                                                                                                                                                                                                                                                                                                                                                                                  |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | For details on CA certificate, refer the <i>Cisco Finesse Administration Guide</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html</a>                                                             |
| 2        | For details on self-signed certificate, see <a href="#">Add Finesse Certificate to AW Machine, on page 611</a>                                                                                                                                                                                                                                                                        |
| 3        | Navigate to <b>Infrastructure Settings &gt; Device Configuration &gt; Finesse</b> to configure, and then select the <b>Site</b> and <b>Peripheral Set</b> of the Finesse server.<br><a href="#">Configure Contact Center Enterprise Administration and Data Server Settings, on page 221</a><br><a href="#">Configure Contact Center Enterprise CTI Server Settings , on page 219</a> |
| 4        | <a href="#">Configure Contact Center Agents and Routing for Live Data Reports, on page 36</a>                                                                                                                                                                                                                                                                                         |
| 5        | <a href="#">Restart the Cisco Tomcat Service, on page 90</a>                                                                                                                                                                                                                                                                                                                          |
| 6        | <a href="#">Live Data Reports, on page 37</a>                                                                                                                                                                                                                                                                                                                                         |
| 7        | <a href="#">Configure SNMP, on page 87</a>                                                                                                                                                                                                                                                                                                                                            |

## Restart the Cisco Tomcat Service

After you change and save any value on Unified CCE Administration server settings, you must restart the Cisco Tomcat Service on the primary Cisco Finesse server.

### Procedure

- 
- Step 1** Enter `utils service stop Cisco Tomcat` command, to stop the Cisco Tomcat service.
- Step 2** Enter `utils service start Cisco Tomcat` command, to start the Cisco Tomcat service.
- 

## Configure Cisco Finesse Administration

- [Obtain and Upload a CA Certificate, on page 91](#)
- [Accept Security Certificates, on page 94](#)

## Obtain and Upload a CA Certificate



**Note** This procedure applies only if you are using HTTPS.

This procedure is optional. If you are using HTTPS, you can choose to obtain and upload a CA certificate or you can choose to use the self-signed certificate provided with Cisco Finesse.

To open Cisco Unified Operating System Administration, enter the following URL in your browser:  
`https://FQDN of primary Finesse server:8443/cmplatform.`

Sign in using the username and password for the application user account created during Cisco Finesse installation.

### Procedure

- Step 1** Generate a CSR as follows.
  - a) Select **Security > Certificate Management > Generate CSR**.
  - b) From the certificate name drop-down list, select **tomcat**.
  - c) Click **Generate CSR**.
- Step 2** Download the CSR.
  - a) Select **Security > Certificate Management > Download CSR**.
  - b) From the certificate name drop-down list, select **tomcat**.
  - c) Click **Download CSR**.
- Step 3** Use the CSR to obtain the signed application certificate and the CA root certificate from the Certificate Authority.
- Step 4** When you receive the certificates, select **Security > Certificate Management > Upload Certificate**.
- Step 5** Upload the root certificate.
  - a) Choose **tomcat-trust** from **Certificate Name** drop-down list.
  - b) Click **Browse** and open the root certificate file, in **Upload File** field.
  - c) Click **Upload File**.
- Step 6** Upload the application certificate.
  - a) Choose **tomcat** from **Certificate Name** drop-down list.
  - b) Enter the name of the CA root certificate in the **Root Certificate** field.
  - c) Click **Browse** and open the root certificate file, in **Upload File** field.
  - d) Click **Upload File**.
- Step 7** After the upload is complete, sign out from Cisco Finesse.
- Step 8** Access the CLI on the primary Cisco Finesse server.
- Step 9** Enter **utils service restart Cisco Finesse Notification Service** command to restart the Cisco Finesse Notification service.
- Step 10** Enter **utils service restart Cisco Tomcat** command to restart the Cisco Tomcat service.
- Step 11** Upload the root certificate and application certificate to the secondary Cisco Finesse server.

**Note** Enter the following URL in browser: `https://FQDN of secondary Finesse server:8433/cmplatform`, to open **Cisco Unified Operating System Administration** for the secondary server.

**Step 12** Access the CLI on the secondary Cisco Finesse server and restart the Cisco Finesse Notification Service and the Cisco Tomcat Service.

---

## Deploy Certificate in Browsers

### Download CA certificate

This procedure assumes that you are using the Windows Certificate Services. Perform the following steps to retrieve the root CA certificate from the certificate authority. After you retrieve the root certificate, each user must install it in the browser used to access Finesse.

#### Procedure

---

- Step 1** On the Windows domain controller, run the CLI command `certutil -ca.cert ca_name.cert`, in which `ca_name` is the name of your certificate.
- Step 2** Save the file. Note where you saved the file so you can retrieve it later.
- 

### Set Up CA Certificate for Internet Explorer Browser

After obtaining and uploading the CA certificates, either the certificate must be automatically installed via group policy or all users must accept the certificate.

In environments where users do not log directly in to a domain or group policies are not utilized, every Internet Explorer user in the system must perform the following steps once to accept the certificate.

#### Procedure

---

- Step 1** In Windows Explorer, double-click the `ca_name.cert` file (in which `ca_name` is the name of your certificate) and then click **Open**.
- Step 2** Click **Install Certificate > Next > Place all certificates in the following store**.
- Step 3** Click **Browse** and select **Trusted Root Certification Authorities**.
- Step 4** Click **OK**.
- Step 5** Click **Next**.
- Step 6** Click **Finish**.
- A message appears that states you are about to install a certificate from a certification authority (CA).
- Step 7** Click **Yes**.
- A message appears that states the import was successful.
- Step 8** To verify the certificate was installed, open Internet Explorer. From the browser menu, select **Tools > Internet Options**.

- Step 9** Click the **Content** tab.
- Step 10** Click **Certificates**.
- Step 11** Click the **Trusted Root Certification Authorities** tab.
- Step 12** Ensure that the new certificate appears in the list.
- Step 13** Restart the browser for certificate installation to take effect.

**Note** If using Internet Explorer 11, you may receive a prompt to accept the certificate even if signed by private CA.

---

### Set Up CA Certificate for Firefox Browser

Every Firefox user in the system must perform the following steps once to accept the certificate.



**Note** To avoid certificate warnings, each user must use the fully-qualified domain name (FQDN) of the Finesse server to access the desktop.

---

#### Procedure

---

- Step 1** From the Firefox browser menu, select **Options**.
  - Step 2** Click **Advanced**.
  - Step 3** Click the **Certificates** tab.
  - Step 4** Click **View Certificates**.
  - Step 5** Click **Authorities**.
  - Step 6** Click **Import** and browse to the *ca\_name.cer* file (in which *ca\_name* is the name of your certificate).
  - Step 7** Check the **Validate Identical Certificates** check box.
  - Step 8** Restart the browser for certificate installation to take effect.
- 

### Deploy Root Certificate for Browsers

In environments where group policies are enforced via the Active Directory domain, the root certificate can be added automatically to each user's browser. Adding the certificate automatically simplifies user requirements for configuration.



**Note** To avoid certificate warnings, each user must use the fully-qualified domain name (FQDN) of the Finesse server to access the desktop.

---

#### Procedure

---

- Step 1** On the Windows domain controller, navigate to **Administrative Tools > Group Policy Management**.

**Note** Users who have strict Group Policy defined on the Finesse Agent Desktop are required to disable **Cross Document Messaging** from **Group Policy Management** to ensure proper functioning of Finesse on browser.

- Step 2** Right-click Default Domain Policy and select **Edit**.
- Step 3** In the Group Policy Management Console, go to **Computer Configuration > Policies > Window Settings > Security Settings > Public Key Policies**.
- Step 4** Right-click Trusted Root Certification Authorities and select **Import**.
- Step 5** Import the *ca\_name.cer* file.
- Step 6** Go to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Certificate Services Client - Auto-Enrollment**.
- Step 7** From the Configuration Model list, select **Enabled**.
- Step 8** Sign in as a user on a computer that is part of the domain and open browser.
- Step 9** If the user does not have the certificate, run the command **gpupdate.exe /target:computer /force** on the user's computer.

---

### Set Up CA Certificate for Chrome and Edge Chromium (Microsoft Edge) Browsers

#### Procedure

- Step 1** In the browser, go to **Settings**.
- Step 2** In the Chrome browser, select **Advanced Settings > Privacy and Security**, click **Manage Certificates**.
- Step 3** In the Microsoft Edge browser, select **Privacy, search, and services**. Under **Security**, click **Manage Certificates**.
- Step 4** Click **Trusted Root Certification Authorities** tab.
- Step 5** Click **Import** and browse to the *ca\_name.cer* file.  
In the **Trusted Root Certification Authorities** tab, ensure that the new certificate appears in the list.
- Step 6** Restart the browser for the certificate to install.

### Accept Security Certificates

Ensure that the pop-ups are enabled for the Finesse desktop.

After you enter the Finesse desktop URL in your browser, the procedure to add a certificate is as follows:

#### Install certificates on Windows operating system:

The procedure to add a certificate varies for each browser. The procedure for each browser is as follows:

#### Internet Explorer





---

**Note** If you are using a Windows client, signed in as a Windows user, you must run Internet Explorer as an administrator to install the security certificates. In your Start menu, right-click Internet Explorer and select Run as administrator.

Contact your administrator if you do not have the required permissions to install the security certificates.

---

1. A page appears that states there is a problem with the website's security certificate. Click **Continue to this website (not recommended)** link to open the Finesse sign in page. The Finesse sign in screen appears with a certificate error in the address bar.
2. Click on the certificate error that appears in the address bar and then click **View Certificates**.
3. In the **Certificate** dialog box, click **Install Certificate** to open the **Certificate Import Wizard**.
4. Select **Current User** to install the certificate for the current user only, or select **Local Machine** to install the certificate for all Windows users.
5. On the **Certificate Import Wizard**, click **Next**.
6. Select **Place all certificates in the following store** and click **Browse**.
7. Select **Trusted Root Certification Authorities** and click **OK**.
8. Click **Next** and then click **Finish**. A **Security Warning** dialog box appears.
9. Click **Yes** to install the certificate. The **Certificate Import** dialog box appears.
10. Click **OK** and close the **Certificate Import** dialog box.
11. Close the browser tab. The accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box.

Repeat the preceding steps for all the certificate links. After you accept all the certificates, the sign-in process is complete.



---

**Note** To remove the certificate error from the desktop, you must close and reopen your browser.

---

### Firefox

1. On **Your connection is not secure** page, click **Advanced > Add Exception**.



---

**Note** Ensure that the **Permanently store this exception** box is checked.

---

2. Click **Confirm Security Exception**.
3. On and click **Sign In**.
4. In the **SSL Certificate Not Accepted** dialog box, click the certificate link. A browser tab opens for the certificate that you must accept.

5. On the browser tab, click **I Understand the Risks > Add Exception**. Ensure that the **Permanently store this exception** box is checked.
6. Click **Confirm Security Exception**. The browser tab closes after you accept the certificate and the accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box. Close the browser tab if it does not automatically close.

Repeat the preceding steps for all the certificate links. After you accept all the certificates, the sign-in process is complete.

#### Chrome and Edge Chromium (Microsoft Edge)

1. A page appears that states your connection is not private. To open the Finesse sign in page,
  - In Chrome, click **Advanced > Proceed to <Hostname> (unsafe)**.
  - In Microsoft Edge, click **Advanced > Continue to <Hostname> (unsafe)**.
2. Enter your agent ID or username, password, and extension, and then click **Sign In**.
3. In the **SSL Certificate Not Accepted** dialog box, click the certificate link. A browser tab opens for the certificate that you must accept.
4. On the browser tab,
  - In Chrome, click **Advanced > Proceed to <Hostname> (unsafe)**.
  - In Microsoft Edge, click **Advanced > Continue to <Hostname> (unsafe)**.

The browser tab closes after you accept the certificate and the accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box. Close the browser tab if it does not automatically close.




---

**Note** If you click the certificate link and do not accept it, the certificate link stays enabled in the **SSL Certificate Not Accepted** dialog box. The certificate error appears every time you sign in. The procedure to permanently accept the certificate is as follows.

---

5. Click on the certificate error that appears in the address bar and then,
  - In Chrome, select **Certificate (Invalid)**.
  - In Microsoft Edge, select **Certificate (not valid)**.
 The **Certificate** dialog box appears.
6. In the **Details** tab, click **Copy to File**. The **Certificate Export Wizard** appears.
7. Click **Next**.
8. Keep the default selection **DER encoded binary X.509 (.CER)** and click **Next**.
9. Click **Browse** and select the folder in which you want to save the certificate, enter a recognizable file name and click **Save**.
10. Browse to the folder where you have saved the certificate (.cer file), right-click on the file, and click **Install Certificate**. The **Certificate Import Wizard** appears.
11. Keep the default selection **Current User** and click **Next**.

12. Select **Place all certificates in the following store** and click **Browse**. The **Select Certificate Store** dialog box appears.
13. Select **Trusted Root Certification Authorities** and click **OK**.
14. Click **Next** and then click **Finish**. A **Security Warning** dialog box appears that asks if you want to install the certificate.
15. Click **Yes**. A **Certificate Import** dialog box that states the import was successful appears.

Close the browser and sign in to Finesse. The security error does not appear in the address bar.

### Install certificates on macOS:

The procedure to download a certificate varies for each browser. The procedure for each browser is as follows:

#### Chrome and Edge Chromium (Microsoft Edge)

1. A warning page appears which states that your connection is not private. To open the Finesse Console sign in page,
  - In Chrome, click **Advanced > Proceed to <Hostname> (unsafe)**.
  - In Microsoft Edge, click **Advanced > Continue to <Hostname> (unsafe)**.
2. Click on the certificate error that appears in the address bar and then,
  - In Chrome, select **Certificate (Invalid)**.
  - In Microsoft Edge, select **Certificate (Not Valid)**.A certificate dialog box appears with the certificate details.
3. Drag the **Certificate** icon to the desktop.
4. Double-click the certificate. The **Keychain Access** application opens.
5. In the right pane of Keychains dialog, browse to the certificate, right-click on the certificate, and select **Get Info** from the options that are listed. A dialog appears with more information about the certificate.
6. Expand **Trust**. From the **When using this certificate** drop-down, select **Always Trust**.
7. Close the dialog box that has more information about the certificate. A confirmation dialog box appears.
8. Authenticate the modification of Keychains by providing a password.
9. The certificate is now trusted, and the certificate error does not appear on the address bar.

#### Firefox

1. In your Firefox browser, enter the Finesse desktop URL. A warning page appears which states that there is a security risk.
2. Click **Advanced** and then click **View Certificate** link. The **Certificate Viewer** dialog box appears.
3. Click **Details** and then click **Export**. Save the certificate (**.crt** file) in a local folder.



---

**Note** If **.crt** file option is not available, select **.der** option to save the certificate.

---

4. From the menu, select **Firefox > Preferences**. The **Preferences** page is displayed.
5. In the left pane, select **Privacy & Security**.
6. Scroll to the **Certificates** section and click **View Certificates ...**. The **Certificate Manager** window is displayed.
7. Click **Import** and select the certificate.
8. The certificate is now authorized, and the certificate error does not appear on the address bar.

## Configure Live Data

| Sequence | Task                                                                                          |
|----------|-----------------------------------------------------------------------------------------------|
| 1        | <a href="#">Initial Setup for Live Data, on page 98</a>                                       |
| 2        | <a href="#">Configure Live Data with AW, on page 98</a>                                       |
| 3        | <a href="#">Configure Live Data Machine Services, on page 99</a>                              |
| 4        | <a href="#">Configure Live Data for Unified Intelligence Center Data Sources, on page 100</a> |
| 6        | <a href="#">Restart Live Data, on page 101</a>                                                |

### Initial Setup for Live Data

For Live Data to work on Packaged CCE 4000 and 12000 Agents deployment, do the following on both Side A and Side B Logger:

#### Procedure

- 
- Step 1** Launch **Microsoft SQL Server Management Studio** and select the Logger database (Side A or Side B appropriately).
- Step 2** Run the queries in the file `C:\icm\install\LiveDataMachineServiceCorrection.sql`.
- Note** From AW Machine, run the Initialize Local Database tool.
- 

### Configure Live Data with AW

Configure Live Data with AW to access the primary AW DB and the secondary AW DB. The command also automatically tests the connection from Live Data to the primary or secondary AW, checks to see if you (as the configured user) have appropriate AW DB access, and reports the results.

You can use the optional skip-test parameter if you do not want to perform the test. When you include the skip-test parameter, the command does not check if you (as the configured user) have appropriate AW DB access and does not report results.




---

**Note** You do not need to configure the AW DB on both the Publisher and the Subscriber. The configuration is replicated between the Publisher and Subscriber.

---

### Before you begin

Before you can configure Live Data, you must first configure a SQL user (with special permissions) to work with Live Data.

The SQL administrative user "sa" or a user with sysadmin privileges must then run the following SQL queries on the primary system database for the SQL user who is configured to work with Live Data:

```
USE master
GO
GRANT CONTROL ON CERTIFICATE :: UCCESymmetricKeyCertificate TO "<user>"
GRANT VIEW DEFINITION ON SYMMETRIC KEY :: UCCESymmetricKey TO "<user>"
```

### Procedure

---

- Step 1** Log in to your Live Data server.
- Step 2** Run the following command to configure Live Data with the primary AW DB. The command automatically tests the connection from Live Data, checks the user permission, and displays results.
- The skip-test parameter is optional. Include it only if you do not want to perform the test.
- ```
set live-data aw-access primary addr port db user [skip-test]
```
- Step 3** Run the following command to configure Live Data with the secondary AW DB. The command automatically tests the connection from Live Data, checks the user permission, and displays results.
- The skip-test parameter is optional. Include it only if you do not want to perform the test.
- ```
set live-data aw-access secondary addr port db user [skip-test]
```
- You can also optionally run the following command at any time to show and test the AW configuration that you set from Live Data to the primary and secondary AW DBs.
- The skip-test parameter is optional. Include it only if you do not want to perform the test.
- ```
show live-data aw-access [skip-test]
```
-

Configure Live Data Machine Services

This command tells the AW where your Live Data machine services are located.



-
- Note**
- Whenever you run set live-data machine-services, be sure to also run set live-data cuic-datasource to reconfigure the Live Data data sources for the Unified Intelligence Center. See [Configure Live Data for Unified Intelligence Center Data Sources, on page 100](#).
-

Procedure

Step 1 Log in to your Live Data server.

Step 2 Run the following command to configure the Live Data machine services:

```
set live-data machine-services awdb-user
```

Use the `user@domain` format to specify the AW database domain user with write-access permission. The domain is a fully qualified domain name (FQDN), and the username is a user principal name. You must be authorized to change Unified CCE configuration.

- Note**
- The Router and Peripheral Gateway (PG) TIP and TOS connection information is automatically populated for Unified CCE deployments that support Live Data.
 - Cisco Unified Communications Manager (CUCM) PG, generic PGs with CUCM peripherals, Unified CCE Gateway PGs, and Avaya PGs are supported for Live Data.

Note Once you have updated the host name of Live Data Server, you need to re-run the below set of commands, otherwise new host name will not be accepted.

```
set live-data machine-services awdb-user
```

```
set live-data cuic-datasource cuic-addr cuic-port cuic-user
```

Verify that the show machine-services display changed hostname.

It is necessary for you to re-run the set of commands, otherwise Live data machine services will not be updated with the new host name.

Configure Live Data for Unified Intelligence Center Data Sources

This command tells Unified Intelligence Center how to access Live Data.



Note If you are using any certificates that are unapproved by Cisco, ensure to import the CUIC certificate into the Live Data server before you run `set live-data machine-services`.

Procedure

Step 1 Log in to your Live Data server.

Step 2 Run the following command to configure your Live Data Unified Intelligence Center data sources:

```
set live-data cuic-datasource cuic-addr cuic-port cuic-user
```

Restart Live Data

After you complete the configuration procedures for the AW, the Live Data Machine Services, and the Unified Intelligence Center data source, restart the Live Data system to enable the changes.

Procedure

Access the Live Data CLI and run the following command:

```
utils system restart
```

Note Whenever a new peripheral gateway that supports Live Data gets deployed and started, its feed will not be available to Live Data server automatically. Restart the Live Data server to start the feed from the newly deployed Peripheral Gateway.

Set Up Certificates for Live Data

For secure Cisco Finesse, Cisco Unified Intelligence Center, and Live Data server-to-server communication, perform any of the following:

- Use the self-signed certificates provided with Live Data.



Note When using self-signed certificates, agents must accept the Live Data certificates in the Finesse desktop when they sign in before they can use the Live Data gadget.

- Produce a Certification Authority (CA) certificate internally.
- Obtain and install a Certification Authority (CA) certificate from a third-party vendor.

For complete information, see [Certificates for Live Data, on page 603](#).

Configure Cisco Identity Service

The following table outlines the Cisco Identity Service configuration task for Packaged 2000 Agent deployments to 12000 Agent deployments.

Task
Add IdS Certificate to AW Machine, on page 612
Configure an Identity Provider (IdP), on page 102
Configure SAML Certificate Secure Hash Algorithm from SHA-1 to SHA-256, on page 102
Configure the Cisco Identity Service, on page 108
Set Up the External HDS for Single Sign-On, on page 223

Task
Register Components and Set Single Sign-On Mode, on page 110 For more information about configuring the Single Sign-On feature, see <i>Cisco Packaged Contact Center Enterprise Features Guide</i> at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html .
Cisco SNMP Setup, on page 21 (optional)

Configure an Identity Provider (IdP)

To support SSO for the contact center solution, configure an Identity Provider (IdP) that is compliant with the Security Assertion Markup Language 2.0 (SAML v2) Oasis standard. The IdP stores user profiles and provides authentication services to the contact center solution.



Note For a current list of supported Identity Provider products and versions, see the [Contact Center Enterprise Compatibility Matrix](#).

This section provides sample configuration information for Microsoft AD FS.

Follow this sequence of tasks to configure the Identity Provider.

Sequence	Task
1	Install and Configure Active Directory Federation Services, on page 103
2	Set Authentication Type. See Authentication Types, on page 103 .
3	Configure an Identity Provider (IdP), on page 102
4	Enable Signed SAML Assertions, on page 106
5	Optionally Customize the AD FS Sign-In Page in Windows Server to Allow User ID, on page 107

Configure SAML Certificate Secure Hash Algorithm from SHA-1 to SHA-256

This procedure is useful for upgrades from version 11.x where the only Secure Hash Algorithm supported was SHA-1.

Perform this procedure after the upgrade has completed successfully.

Procedure

-
- Step 1** From browser in AD FS Server, login to Cisco IdS admin interface <https://<Cisco IdS server address>:8553/idsadmin>.
- Step 2** Click **Settings**.
- Step 3** Click **Security** tab.

Step 4 Click **Keys and Certificates**.

Note After this step, Single Sign On will stop working until you complete Step 8.

Step 5 Regenerate SAML Certificate with SHA-256 Secure Hash Algorithm. In the SAML Certificate section, change Secure Hash algorithm dropdown menu to SHA-256 and then click **Regenerate** button

Step 6 Download new metadata file. Click on **IdS Trust** tab and then click download button.

Step 7 Change Secure Hash Algorithm in AD FS Relaying Party Trust configuration. In AD FS server, open AD FS Management. Go to **ADFS ->Trust Relationships->Relying Party Trusts**, right click on existing Relying Party Trust for Cisco IdS and then click on Properties. In the Advanced Tab, change the Secure Hash Algorithm to **SHA-256**. Click **Apply**.

Step 8 Update Relying party trust on AD FS. From AD FS Server, run the following Powershell command:

```
Update-AdfsRelyingPartyTrust -MetadataFile <path to Step 6 new MetaData File> -TargetName
<Relying Party Trust Display Name>
```

Install and Configure Active Directory Federation Services

Follow Microsoft instructions and guidelines to install Microsoft Active Directory Federation Services (AD FS).

For example, see *Active Directory Federation Services Overview* at [https://technet.microsoft.com/en-us/library/hh831502\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh831502(v=ws.11).aspx)

- For AD FS 2.0, see *AD FS Content Map* at <http://aka.ms/adfscontentmap>.



Note Cisco IdS does not support AD FS Automatic Certificate Rollover. If the AD FS certificate gets rolled over, then re-establish the trust relationship between the IdS and AD FS.



Note The Secure Hash Algorithm (SHA) used for signature verification between:

- IdP and Cisco IdS: SHA-1, SHA-256
- Cisco IdS and the application browsers: SHA-256

Authentication Types

Cisco Identity Service supports form-based authentication of the Identity Provider.

For information on enabling form-based authentication in ADFS, see Microsoft documentation:

- For ADFS 2.0 see <https://social.technet.microsoft.com/wiki/contents/articles/1600.ad-fs-2-0-how-to-change-the-local-authentication-type.aspx>
- For ADFS 3.0 see <https://blogs.msdn.microsoft.com/josrod/2014/10/15/enabled-forms-based-authentication-in-adfs-3-0/>

For Kerberos authentication to work, ensure to disable the form-based authentication and follow the steps provided in *Kerberos Authentication (Integrated Windows Authentication)*.

- In AD FS on Windows Server, set the Authentication Type to Forms-based authentication (FBA). Refer to the following Microsoft TechNet article, <http://social.technet.microsoft.com/wiki/contents/articles/1600.ad-fs-2-0-how-to-change-the-local-authentication-type.aspx>
- In AD FS on Windows Server, set the Authentication Policy to Forms Authentication. Refer to the following Microsoft TechNet article, <https://blogs.msdn.microsoft.com/josrod/2014/10/15/enabled-forms-based-authentication-in-adfs-3-0/>

Integrate Cisco IdS to the Shared Management AD FS

Procedure

-
- Step 1** In AD FS, be sure that the default Authentication Type is set to Forms. (Cisco Identity Service requires the Identity Provider to provide form-based authentication.) See the Microsoft AD FS documentation for details.
- Step 2** In AD FS server, open **AD FS Management**.
- Step 3** Right-click **AD FS** -> **Trust Relationships** -> **Relying Party Trust**.
- Step 4** From the menu, choose **Add Relying Party Trust** to launch the **Add Relying Party Trust Wizard**.
- Step 5** In the **Select Data Source** step, choose the option **Import data about the relying party from a file**.
- Step 6** **Browse** to the `sp.xml` file that you downloaded from Cisco Identity Server and complete the import to establish the relying party trust.
- Step 7** Select the step **Specify Display Name**, and add a significant name you can use to identify the Relying Party Trust.
- Step 8** For AD FS in Windows Server, select the option **I do not want to configure multi-factor authentication settings for the relying party at this time** in the Step **Configure Multi-factor Authentication Now**.
This step does not appear in AD FS 2.0 or 2.1. Continue with the next step.
- Step 9** In the Step Choose Issuance Authorization Rules, select the option **Permit all users to access this relying party** and click **Next**.
- Step 10** Click **Next** again to finish adding the relying party.
- Step 11** Right-click on the **Relying Party Trust** and click **Properties**. Select the **Identifiers** tab.
- Step 12** On the Identifiers tab, Set **Display name** to the name you specified when creating the Relying Party Trust, and set the **Relying party identifier** to the **fully qualified hostname** of the Cisco Identity Server from which `sp.xml` was downloaded.
- Step 13** Still in **Properties**, select the **Advanced** tab.
- Step 14** Select **secure hash algorithm** as **SHA-1** and then click **OK**.

Note In the following steps, you configure two claim rules to specify the claims that are sent from AD FS to Cisco Identity Service as part of a successful SAML assertion:

- A claim rule with the following custom claims, as AttributeStatements, in the assertion:
 - **uid** - Identifies the authenticated user in the claim sent to the applications.
 - **user_principal** - Identifies the authentication realm of the user in the assertion sent to Cisco Identity Service.
- A second claim rule that is a NameID custom claim rule specifying the fully qualified domain name of the AD FS server and the Cisco IdS server.

Follow the steps to configure these rules.

Step 15 In **Relying Party Trusts**, right-click on the Relying Party Trust you created, and click **Edit Claim Rules**.

Step 16 Follow these steps to add a rule with **Send LDAP Attributes as Claims** as the Claim rule template.

- a) In the **Issuance Transform Rules** tab, click **Add Rule**.
- b) In the Step **Choose Rule Type**, select the claim rule template **Send LDAP Attributes as Claims** and click **Next**.
- c) In the **Configure Claim Rule** step, in the **Claim rule name** field, enter **NameID**.
- d) Set the **Attribute store** drop-down to **Active Directory**.
- e) Set the table **Mapping of LDAP attributes to outgoing claim types** to the appropriate **LDAP Attributes** and the corresponding **Outgoing Claim Type** for the type of user identifier you are using:
 - When the identifier is stored as a **SAM-Account-Name** attribute:
 1. Select an **LDAP Attribute** of **SAM-Account-Name**, and set the corresponding **Outgoing Claim Type** to **uid** (lowercase).
 2. Select a second **LDAP Attribute** of **User-Principal-Name** and set the corresponding **Outgoing Claim Type** to **user_principal** (lowercase).
 - When the identifier is a UPN:
 1. Select an **LDAP Attribute** of **User-Principal-Name**, and set the corresponding **Outgoing Claim Type** to **uid** (lowercase).
 2. Select a second **LDAP Attribute** of **User-Principal-Name** and set the corresponding **Outgoing Claim Type** to **user_principal** (lowercase).

Note The SAM-Account-Name or UPN choice is based on the User ID configured in the AW.

Step 17 Follow these steps to add a second rule with the template **custom claim rule**.

- a) Select **Add Rule** on the **Edit Claim Rules** window.
- b) Select **Send Claims Using Custom Rule**.
- c) Set the name of rule to the **fully qualified domain name (FQDN)** of the Cisco Identity Server publisher (primary) node.
- d) Add the following rule text:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
```

```

    Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
    Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
    "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",

    Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
    =
    "http://<AD FS Server FQDN>/adfs/services/trust",

    Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"]
    =
    "<fully qualified domain name of Cisco IdS>";

```

e) Edit the script as follows:

- Replace <ADFS Server FQDN> to match exactly (including case) the ADFS server FQDN (fully qualified domain name.)
- Replace <Cisco IdS server FQDN> to match exactly (including case) the Cisco Identity Server FQDN.

Step 18 Click **OK**.

Enable Signed SAML Assertions

Enable Signed SAML Assertions for the Relying Party Trust (Cisco Identity Service).

Procedure

Step 1 Click **Start** and type **powershell** in the Search field to display the Windows Powershell icon.

Step 2 Right-click on the Windows Powershell program icon and select **Run as administrator**

Note All PowerShell commands in this procedure must be run in Administrator mode.

Step 3 Run the command, **Set-ADFSRelyingPartyTrust -TargetName <Relying Party Trust Display Name> -SamlResponseSignature "MessageAndAssertion"**.

Note Set <Relying Party Trust Display Name> to exactly match (including case) the Identifier tab of the Relying Party Trust properties.

For example:

```

Set-ADFSRelyingPartyTrust -TargetName CUICPub.PCCERCDN.cisco.com
-SamlResponseSignature "MessageAndAssertion" .

```

Step 4 Navigate back to the Cisco Identity Service Management window.

Step 5 Click **Settings**.
By default **IdS Trust** tab is displayed.

Step 6 On the Download SAML SP Metadata and Upload IdP Metadata windows, click **Next** as you have already established trust relationship between IdP and IdS.

Step 7 On the AD FS authentication window, provide the login credentials.

Step 8 On successful SSO setup, the message "SSO Configuration is tested successfully" is displayed.

- Note** If you receive the error message "An error occurred", ensure that the claim you created on the AD FS is enabled.
- If you receive the error message "IdP configuration error: SAML processing failed", ensure that the rule has the correct names for Ids and AD FS.

Optionally Customize the AD FS Sign-In Page in Windows Server to Allow User ID

By default, the sign-in page presented to SSO users by AD FS in Windows Server requires a username that is a UPN. Usually this is an email format, for example, user@cisco.com. If your contact center solution is in a single domain, you can modify the sign-in page to allow your users to provide a simple User ID that does not include a domain name as part of the user name.

There are several methods you can use to customize the AD FS sign-in page. Look in the Microsoft AD FS in Windows Server documentation for details and procedures to configure alternate login IDs and customize the AD FS sign-in pages.

The following procedure is an example of one solution.

Procedure

- Step 1** In the AD FS **Relying Party Trust**, change the NameID claim rule to map the chosen LDAP attribute to **uid**.
- Step 2** Click the Windows **Start** control and type **powershell** in the Search field to display the Windows Powershell icon.
- Step 3** Right-click on the Windows Powershell program icon and select **Run as administrator**
- All PowerShell commands in this procedure must be run in Administrator mode.
- Step 4** To allow sign-ins to AD FS using the sAMAccountName, run the following Powershell command:
- ```
Set-AdfsClaimsProviderTrust -TargetIdentifier "AD AUTHORITY" -AlternateLoginID sAMAccountName
-LookupForests myDomain.com
```
- In the LookupForests parameter, replace myDomain.com with the forest DNS that your users belong to.
- Step 5** Run the following commands to export a theme:
- ```
mkdir C:\themeExport-AdfsWebTheme -Name default -DirectoryPath c:\theme
```
- Step 6** Edit onload.js in C:\theme\script and add the following code at the bottom of the file. This code changes the theme so that the AD FS sign-in page does not require a domain name or an ampersand, "@", in the username.
- ```
// Update the placeholder text to not include the domain
var userNameInput = document.getElementById("userNameInput");
if (userNameInput) {
 userNameInput.setAttribute("placeholder", "Username");
}

// Override submitLoginRequest to not have the "@" check
Login.submitLoginRequest = function () {
 var u = new InputUtil();
 var e = new LoginErrors();
 var userName = document.getElementById(Login.userNameInput);
 var password = document.getElementById(Login.passwordInput);
```

```

if (!userName.value) {
 u.setError(userName, e.userNameFormatError);
 return false;
}
if (!password.value) {
 u.setError(password, e.passwordEmpty);
 return false;
}
document.forms['loginForm'].submit();
return false;
};

```

**Step 7** In Windows PowerShell, run the following commands to update the theme and make it active:

```

Set-AdfsWebTheme -TargetName custom -AdditionalFileResource
@{Uri='/adfs/portal/script/onload.js';path="c:\theme\script\onload.js"}

Set-AdfsWebConfig -ActiveThemeName custom

```

## Configure the Cisco Identity Service

The Cisco Identity Service (Cisco IdS) provides authorization between the Identity Provider (IdP) and applications.

When you configure the Cisco IdS, you set up a metadata exchange between the Cisco IdS and the IdP. This exchange establishes a trust relationship that then allows applications to use the Cisco IdS for single sign-on. You establish the trust relationship by downloading a metadata file from the Cisco IdS and uploading it to the IdP. You can then select settings that are related to security, identify clients of the Cisco IdS service, and set log levels. If desired, enable Syslog format.



**Note** In Packaged CCE 4000 or 12000 Agent deployments:

- Unified CCE AW, Unified Intelligence Center, Finesse, and external HDS gets automatically associated with a default Cisco Identity Service (Cisco IdS).
- Make sure that the Principal AW is configured, and is functional before using the Single Sign-On tool in the Unified CCE Administration. Also, add the SSO-capable machines to the Inventory.

In Packaged CCE 2000 Agent deployments, you must manually associate an external HDS with a default Cisco Identity Service (Cisco IdS). For more information, see [Set Up the External HDS for Single Sign-On, on page 223](#).

### Procedure

**Step 1** In the Unified CCE Administration, choose **Overview > Infrastructure Settings > Device Configuration > Single Sign-On Setup**.

**Note** Use a log in name in the format *username@FQDN* to log in to the Unified CCE Administration.

The **Identity Service Nodes**, **Identity Service Settings**, and **Identity Service Clients** tabs appear.

**Step 2** Click **Identity Service Nodes**.

You can view the overall Node level and identify which nodes are in service. You can also view the **SAML Certificate Expiry** details for each node, indicating when the certificate is due to expire. The node **Status** options are **Not Configured**, **In Service**, **Partial Service**, and **Out of Service**. Click a status to see more information. The star to the right of one of the Node names identifies the node that is the primary publisher.

**Step 3** Click **Identity Service Settings**.

**Step 4** Click **Security**.

**Step 5** Click **Tokens**.

Enter the duration for the following settings:

- **Refresh Token Expiry** -- Refresh token is used to get new Access tokens. This parameter specifies the duration after which the Refresh token expires. The default value is 10 hours. The minimum value is 2 hours. The maximum is 24 hours.
- **Authorization Code Expiry** -- Authorization code is used to get Access tokens from Cisco IdS. This parameter specifies the duration after which the Authorization code expires. The default value is 1 minute, which is also the minimum. The maximum is 10 minutes.
- **Access Token Expiry** -- Access token contains security credentials used to authorize clients for accessing resource server. This parameter specifies the duration after which the Access token expires. The default value is 60 minutes. The minimum value is 5 minutes. The maximum is 120 minutes.

**Step 6** Set the **Encrypt Token** (optional); the default setting is **On**. Use this configuration to secure the tokens as Cisco IdS issues tokens in both plain text or encrypted formats.

**Step 7** Click **Save**.

**Step 8** Click **Keys and Certificates**.

The **Generate Keys and SAML Certificate** page opens and allows you to:

- Regenerate the **Encryption/Signature key** by clicking **Regenerate**. A message appears to say that the Token Registration is successful and advises you to restart the system to complete the configuration. An Administrator regenerates the Encryption/Signature key when it is exposed or compromised.
- Regenerate the **SAML Certificate** by clicking **Regenerate**. A message appears to say that the SAML certificate regeneration is successful. SAML certificate is regenerated when it expires or when IdS relying party trust configuration on IdP is deleted.

**Note** Establish the trust relationship again whenever the Encryption keys or SAML certificates are regenerated.

**Step 9** Click **Save**.

**Step 10** Click **Identity Service Clients**.

On the **Identity Service Clients** tab, you can view the existing Cisco IdS clients, with the client name, client ID, and a redirect URL. To search for a particular client, click the Search icon above the list of names and type the name of client.

**Step 11** To add a client on the **Identity Service Clients** tab:

- a) Click **New**.
- b) Enter the name of client.
- c) Enter the Redirect URL. To add more than one URL, click the plus icon.
- d) Click **Add** (or click **Clear** and then click the X to close the page without adding the client).

**Step 12** To edit or delete a client, highlight the client row and click the ellipses under **Actions**. Then:

- Click **Edit** to edit the client's name, ID, or redirect URL. On the **Edit Client** page, make changes and click **Save** (or click **Clear** and then click the X to close the page without saving edits).
- Click **Delete** to delete the client.

**Step 13** Click **Identity Service Settings**.

**Step 14** Click **Troubleshooting** to perform some optional troubleshooting.

**Step 15** From the **Log Level** drop-down list, set the local log level by choosing **Error**, **Warning**, **Info** (the default), **Debug**, or **Trace**.

**Step 16** To receive errors in Syslog format, enter the name of the Remote Syslog Server in the **Host** (Optional) field.

**Step 17** Click **Save**.

---

You can now:

- Register components with the Cisco IdS.
- Enable (or disable) SSO for the entire deployment.

## Register Components and Set Single Sign-On Mode

If you add any SSO-compatible machines to the System Inventory after you register components with the Cisco IdS, those machines are registered automatically.

### Before you begin

- Configure the Cisco Identity Service (Cisco IdS).
- Disable popup blockers. It enables viewing all test results correctly.
- If you are using Internet Explorer, verify that:
  - It is not in the Compatibility Mode.
  - You are using the fully qualified domain name of AW to access the CCE Administration (for example, <https://<FQDN>/cceadmin>).

### Procedure

---

**Step 1** In the Unified CCE Administration, navigate to **Features > Single Sign-On Overview > Infrastructure Settings > Device Configuration > Single Sign-On Setup**.

**Step 2** Click the **Register** button to register all SSO-compatible components with the Cisco IdS.

The component status table displays the registration status of each component.

If a component fails to register, correct the error and click **Retry**.

**Step 3** Click the **Test** button. When the new browser tab opens, you may be prompted to accept a certificate. In order for the page to load, accept any certificates. Then, when presented with a log in dialog, log in as a user with SSO credentials.



The test process verifies that each component has been configured correctly to reach the Identity Provider, and that the Cisco IdS successfully generates access tokens. Each component that you are setting up for SSO is tested.

The component status table displays the status of testing each component.

If a test is unsuccessful, correct the error, and then click **Test** again.

Test results are not saved. If you refresh the page, run the test again before enabling SSO.

**Step 4** Select the SSO mode for the system from the **Set Mode** drop-down menu:

- Non-SSO: This mode disables SSO for all agents and supervisors. Users log in using existing Active Directory-based local authentication.
- Hybrid: This mode allows you to enable agents and supervisors selectively for SSO.
- SSO: This mode enables SSO for all agents and supervisors.

The component status table displays the status of setting the SSO mode on each component.

If the SSO mode fails to be set on a component, correct the error, and then select the mode again.

## Packaged CCE 12000 Agents Deployment

Follow this sequence to configure components for Packaged CCE 12000 Agents deployment.

| Sequence | Task                                                                                                  |
|----------|-------------------------------------------------------------------------------------------------------|
| 1        | <a href="#">Configure CCE Component, on page 112</a>                                                  |
| 2        | <a href="#">Configure Cisco Unified Customer Voice Portal, on page 81</a>                             |
| 3        | If Media Server is external, <a href="#">Configure Media Server, on page 202</a>                      |
| 4        | <a href="#">Configure Cisco Unified Communications Manager, on page 85</a>                            |
| 5        | <a href="#">Configure Cisco Unified Intelligence Center, on page 89</a>                               |
| 6        | <a href="#">Configure Cisco Finesse, on page 90</a>                                                   |
| 7        | <a href="#">Configure Live Data, on page 98</a>                                                       |
| 8        | <a href="#">Configure Cisco Identity Service, on page 101</a>                                         |
| 9        | <a href="#">Configure Cisco Unified Customer Voice Portal Reporting Server, on page 39 (optional)</a> |
| 10       | <a href="#">Configure VVB, on page 43 (optional)</a>                                                  |
| 11       | <a href="#">Configure Cisco IOS Enterprise Voice Gateway, on page 43</a>                              |
| 12       | <a href="#">Configure IPv6, on page 50</a>                                                            |

| Sequence | Task                                                                                                |
|----------|-----------------------------------------------------------------------------------------------------|
| 13       | Configure Enterprise Chat and Email (ECE) (optional)<br><a href="#">Email and Chat, on page 376</a> |

## Configure CCE Component

Follow this sequence to configure components for Packaged CCE 12000 Agents deployment.

| Sequence | Task                                                                                                                               |
|----------|------------------------------------------------------------------------------------------------------------------------------------|
| 1        | <a href="#">Configure SQL Server for CCE Components, on page 2</a>                                                                 |
| 2        | <a href="#">Set up Organizational Units, on page 2</a>                                                                             |
| 3        | <a href="#">Configure Logger, on page 112</a>                                                                                      |
| 4        | <a href="#">Configure Router, on page 113</a>                                                                                      |
| 5        | <a href="#">Configure AW-HDS, on page 113</a>                                                                                      |
| 6        | <a href="#">Configure HDS-DDS, on page 113</a>                                                                                     |
| 7        | <a href="#">Start Unified CCE Services, on page 64</a>                                                                             |
| 8        | If you have PG VMs installed , <a href="#">Add Unified CCE Instance, on page 76</a> on all PG VMs                                  |
| 9        | <a href="#">Configure Packaged CCE Deployment Type, on page 67</a>                                                                 |
| 10       | <a href="#">Configure Cisco Unified Contact Center Enterprise PG, on page 77</a>                                                   |
| 11       | For configuration using Configuration Manager, see <a href="#">Packaged CCE 4000 and 12000 Agent Supported Tools, on page 398</a>  |
| 12       | For details on CA signed certificate, see <i>Generate and Import CA Signed Certificate in AW Machine</i>                           |
| 13       | For details on self-signed certificate, see <a href="#">Generate and Import Self-signed Certificate in AW Machine, on page 607</a> |

## Configure Logger

Follow this sequence to configure Logger for Packaged CCE 12000 Agents deployment.

| Sequence | Task                                                                                    |
|----------|-----------------------------------------------------------------------------------------|
| 1        | <a href="#">Add Unified CCE Instance, on page 76</a>                                    |
| 2        | <a href="#">Create Logger Database, on page 60</a>                                      |
| 3        | To use Outbound Option, see <a href="#">Create Outbound Option Database, on page 61</a> |

| Sequence | Task                                                         |
|----------|--------------------------------------------------------------|
| 4        | <a href="#">Add Logger Component to Instance, on page 62</a> |
| 5        | <a href="#">Cisco SNMP Setup, on page 21 (optional)</a>      |

## Configure Router

Follow this sequence to configure Router for Packaged CCE 12000 Agents deployment.

| Sequence | Task                                                         |
|----------|--------------------------------------------------------------|
| 1        | <a href="#">Add Unified CCE Instance, on page 76</a>         |
| 2        | <a href="#">Add Router Component to Instance, on page 63</a> |
| 3        | <a href="#">Cisco SNMP Setup, on page 21 (optional)</a>      |

## Configure HDS-DDS

Follow this sequence to configure HDS-DDS for Packaged CCE 12000 Agents deployment.

| Sequence | Task                                                                                 |
|----------|--------------------------------------------------------------------------------------|
| 1        | <a href="#">Configure SQL Server for CCE Components, on page 2</a>                   |
| 2        | <a href="#">Add Unified CCE Instance, on page 76</a>                                 |
| 3        | <a href="#">Create HDS Database, on page 64</a>                                      |
| 4        | <a href="#">Add Administration and Data Server Component to Instance, on page 65</a> |
| 5        | <a href="#">Cisco SNMP Setup, on page 21 (optional)</a>                              |

## Configure AW-HDS

Follow this sequence to configure AW-HDS for Packaged CCE 12000 Agents deployment.

| Sequence | Task                                                                                 |
|----------|--------------------------------------------------------------------------------------|
| 1        | <a href="#">Configure SQL Server for CCE Components, on page 2</a>                   |
| 2        | <a href="#">Add Unified CCE Instance, on page 76</a>                                 |
| 3        | <a href="#">Create HDS Database, on page 64</a>                                      |
| 4        | <a href="#">Add Administration and Data Server Component to Instance, on page 65</a> |
| 5        | <a href="#">Configure ICM Database Lookup, on page 114 (optional)</a>                |
| 6        | <a href="#">Cisco SNMP Setup, on page 21 (optional)</a>                              |

## Configure ICM Database Lookup

You can use Database Lookup Explorer tool in Configuration Manager to view, define, delete, or edit script table from an external database.

Complete the following procedure to configure ICM Database Lookup.

### Procedure

- 
- Step 1** Launch the Unified CCE Web Setup tool.
- Step 2** In the Router Options window, select **Enable Database Routing**.
- Step 3** Configure Database Lookup explorer:
- Click **Start > All programs > Cisco Unified CCE Tools > Administration Tools > Configuration Manager**.
  - Open **Tools > Explorer Tools > Database Lookup Explorer**.
  - Configure Script Table and Script Table Column as shown in the following example:
 

Script Table:

```
Name: AccountInfo
Side A: \\dblookup1\DBLookup.AccountInfo
Side B: <Update Side B of database here>
Description: <Provide description here>
```

dblookup1 is external database server name, DBLookup is external database name, and AccountInfo is the table name.

Script Table Column:

```
Column name: AccountNo
Description: <Provide description here>
```
- Step 4** Configure the following to change the registry settings in Unified CCE:
- Navigate to **HKEY\_LOCAL\_MACHINE > SOFTWARE > Cisco Systems, Inc. > ICM > <Instance Name> > RouterA > Router > CurrentVersion > Configuration > Database registry**.
 

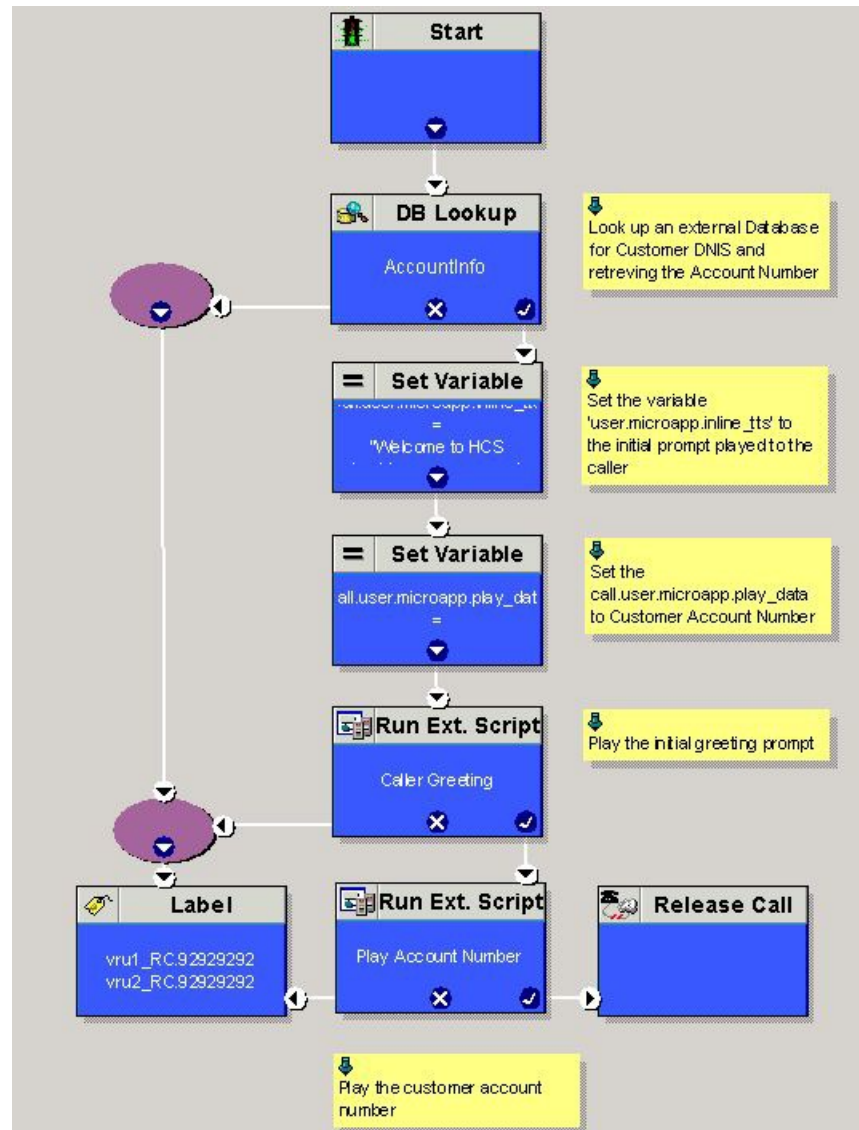
**Instance Name** is the name of the Instance that is configured.
  - Set the SQLLogin registry key as shown in the following example:
 

**Example:**

```
\\dblookup1\DBLookup=(sa,sa)
```

Where DBLookup is the external database name and (sa,sa) are the SQL server authentication.
- Step 5** Create the ICM script with the database lookup node with the respective table and lookup value. The following figure shows AccountInfo as the table name and Call.CallingLineID as the lookup value.

Figure 1: Example ICM Database Look Up



## Packaged CCE Lab Only Deployments

Packaged CCE Lab Mode allows you to install Packaged CCE for demonstration and lab use. You can use all the features in a limited capacity without the need to install a full Packaged CCE deployment on supported hardware. If you exceed the capacity limit of an attribute, you are alerted with error messages that are displayed in **Unified CCE Administration**.

For procedures to configure and manage contact center operations using the Unified CCE Administration web-based tool, see [Packaged CCE Administration, on page 151](#).

The following Unified CCE Administration features are not initially available when you change into the Packaged CCE Lab deployment:

- System Inventory, available on the **Inventory** page
- Log Collection
- Live Data
- Single sign-on

## Packaged CCE Lab Only Deployment Components

Packaged CCE Lab Mode allows you to install Packaged CCE for demonstration and lab use. You can use all the features in a limited capacity without the need to install a full Packaged CCE deployment on supported hardware. If you exceed the capacity limit of an attribute, you are alerted with error messages that are displayed in the **Unified CCE Administration** interface.

Packaged CCE Lab Only deployments can be configured as simplex systems or duplex systems only in 2000 Agents deployment. In a simplex system, all components are installed on Side A and there is no Side B. In a duplex system, components are installed on Side A and Side B.

### Simplex Mode

The Lab Only simplex deployment must consist of the following components:

- 1 Unified CCE Rogger
- 1 Unified CCE AW-HDS-DDS
- 1 Unified CCE PG
- 1 Cisco Unified CM, functioning as a combined Publisher and Subscriber
- 1 Cisco Unified Intelligence Center, functioning as a combined Publisher and Subscriber
- 1 Cisco Finesse, functioning as both a Publisher and Subscriber
- Gateways
- SocialMiner
- Cisco MediaSense
- Cisco Enterprise Chat and Email
- Third-Party Multichannel



---

**Note** In the System Inventory, the status rules that apply to machines outside of the Packaged Contact Center Enterprise Simplex Lab Only deployment returns a status of blocked. Status rules which require ESXi host return a status of blocked.

---

For main site and remote site, you can add the following external machines:

- Cisco Virtualized Voice Browser

- Cisco Unified SIP Proxy
- Gateways
- MediaSense




---

**Note** You can add MediaSense only for the main site.

---

- Cisco Unified CVP Reporting




---

**Note** Adding a CVP Reporting Server via Inventory CSV is not supported. It can only be added as an external server after a successful initialization of inventory.

---

- Cisco Enterprise Chat and Email
- Third-Party Multichannel
- Media Server




---

**Note** SocialMiner can be added as an external machine only in the main site.

---

For more information on the configuration limits for external machines, see the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html>.

## Duplex Mode

The Lab Only duplex mode consists of the following components.




---

**Note** In Lab Mode, Packaged CCE does not validate the ESXi host.

---

### Side A

Side A must have the following:

- 1 Unified CCE Rogger
- 1 Unified CCE AW-HDS-DDS
- 1 Unified CCE PG
- 1 Cisco Unified CVP Server
- 1 Unified Communications Manager Publisher
- 1 Unified Communications Manager Subscriber

- 1 Unified Intelligence Center Publisher
- 1 Finesse Primary

### Side B

Side B must have the following:

- 1 Unified CCE Rogger
- 1 Unified CCE AW-HDS-DDS
- 1 Unified CCE PG
- 1 Cisco Unified CVP Server
- 1 Unified Communications Manager Subscriber
- 1 Unified Intelligence Center Subscriber
- 1 Finesse Secondary

### External

The Lab Only duplex mode can have the following external machines:

- Gateways
- Cisco Virtualized Voice Browsers
- Cisco Unified SIP Proxy
- SocialMiner
- Enterprise Chat and Email
- Unified CVP Reporting
- MediaSense
- third Party Multichannel
- Media Server



---

**Note** Status rules which require ESXi host returns a status of blocked.

---

For remote site, you can add the following external machines:

- Cisco Unified CVP Reporting
- Cisco Enterprise Chat and Email
- Third-Party Multichannel
- Media Server





**Note** SocialMiner can be added as an external machine only in the main site.

For more information on the configuration limits for external machines, see the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html>.

## Initialize the Packaged CCE Lab Mode Deployment

When you sign into Unified CCE Administration for the first time, you are prompted to supply information and credentials for the components in your deployment. Packaged CCE uses this information to configure the components and build the System Inventory.

### Procedure

**Step 1** On the **Inventory** page, select **Packaged CCE: Lab Mode** from the **Deployment Type** drop-down list, then select an instance from the **Instance** drop-down list that has been created using Domain Manager. Click **Next**.

**Step 2** Select one of the following options from the **Template** drop-down list:

- Simplex Inventory for Simplex Lab Mode deployment
- Duplex Inventory for Duplex Lab Mode deployment

Click **Download** to download the Inventory Content File Template. Fill out and save the template to your computer. In the required **Content File** field, browse to the content file you have completed. The content file is validated before the inventory is created. Click **Next**.

For more information on completing the Inventory Content File Template, see [Inventory Content File](#), on page 121.

**Step 3** On the **Settings** page do the following:

- Select the codec used for Mobile Agent calls from the **Mobile Agent Codec** drop-down list. The **Side A Connection** and **Side B Connection** drop-down lists are disabled in Lab Only deployment.
- For the **Automatically create service accounts** check box, either:
  - Uncheck the check box if you want to use an existing Active Directory account. Enter the username and password for an existing Active Directory user in the same domain as the Packaged CCE servers. This account will be added to the Service group.

Click **Next**.

The deployment is initialized. The **Details** dialog box displays the status of the automated initialization tasks.

**Step 4** After the automated initialization tasks complete, click **Done**.

If one of the automated initialization tasks fails, correct the errors and then click **Retry**.

If the retry is successful, the automated initialization continues.

For some task failures, all completed tasks must be reverted before the task can be retried. You see a message informing you that the system needs to be reverted to a clean state.

Click **OK**, and then after the system is in a clean state, click **Start Over**.

**Note** You should restart the Unified CVP Server.

After you initiate Simplex or Duplex Lab Mode deployment, you can also add the following external machines for the main site on the **Inventory** page:

- Unified CM Publisher
- Unified CVP Reporting Server
- Unified SIP Proxy
- Virtualized Voice Browser
- Gateway
- SocialMiner
- MediaSense
- Enterprise Chat and Email
- Third-party Multichannel
- Media Server

To add, edit or delete the external machines on the main site, see [System Inventory for Packaged CCE 2000 Agents Deployment, on page 9](#).

---

## Enable System Inventory, Log Collection, and Live Data Using the Inventory Content File

To use the following Unified CCE Administration features for demonstration purposes, you must provide Packaged CCE with information and credentials for the machines in your deployment:

- System Inventory (available under **Inventory** page)
- Log Collection
- Live Data
- Single Sign-on

You provide this information using the Inventory Content File.

If you are configuring the Packaged CCE Lab Only deployment in Unified CCE Administration as part of the installation process, you are prompted to complete and upload the Inventory Content File.

If you switch into Packaged CCE Lab Only deployment from a different deployment, you complete and upload the Content Inventory file in Unified CCE Administration from the Bulk Import tool.

To complete and upload the Content Inventory file in Bulk Import:

## Procedure

- 
- Step 1** In the Unified CCE Web Administration, click the **Bulk Import** card on the **Overview** page. Download the Inventory content file template.
  - Step 2** Open the file in Microsoft Excel and populate the content file fields as described in Inventory Content File.
  - Step 3** Save your changes.
  - Step 4** Create a new bulk job in **Bulk Jobs**. In the **Content File** field, select the Inventory content file you created and click **Save**.

## Related Topics

[Manage Bulk Jobs](#)

## Inventory Content File

The Inventory content file template contains the following fields:



- 
- Note** If a username and/or password contains the "=" or "&" characters, use the encoded value of "%3D" or "%26" respectively.
- 

| Field         | Description                                                                            |
|---------------|----------------------------------------------------------------------------------------|
| operation     | The default is CREATE; do not change the operation.                                    |
| name          | Do not change the machine name.<br><b>Note</b> This field applies only to duplex mode. |
| machineType   | Do not change the machine type.                                                        |
| publicAddress | Enter the public IP address or hostname for each machine.                              |

| Field                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| publicAddressServices | <p><b>CCE_ROGGER</b> - Do not change this field.</p> <p><b>CCE_PG</b> - This field specifies services that are required for the Unified CCE PG. If the Logical Controller ID for the UCM PG is not the default of 5000, change the pairing value for the TIP_PG and TIP_PG_TOS services to match the Logical Controller ID. (The Logical Controller ID can be found on the Peripheral Gateways tab of System &gt; Information.)</p> <p><b>CCE_AW</b> -</p> <p>Unified CCE Diagnostic Framework Portico domain, username, and password.</p> <p>These credentials must be of a domain user who is a local administrator on all the CCE servers and valid on all Unified CCE components in your deployment (the Side A and Side B Unified CCE Roggers, PGs, and AW-HDS-DDSs).</p> <p><b>Note</b> Every time the Active Directory credentials are updated, the credentials configured here must be updated as well.</p> <p><b>CVP</b> - Unified CVP Server Windows credentials</p> <p><b>CM_PUBLISHER</b> - This field specifies AXL credentials. Replace user and password with the correct credentials.</p> <p><b>CUIC_PUBLISHER</b> - This field specifies the services for Unified Intelligence Center. For the Administration credentials and Cisco Identity Service credentials, replace user and password with the correct credentials. For all other services, do not change the default values.</p> <p><b>FINESSE</b> - This field specifies Finesse Administration credentials. Replace user and password with the correct credentials.</p> |
| privateAddress        | Enter the private IP address for the <b>CCE_PG</b> and <b>CCE_ROGGER</b> . Leave this field blank for all other machines.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| side                  | Enter sideA or sideB.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |



## CHAPTER 2

# Optional Configurations

- [Optional Configuration for Packaged CCE 2000 Agents Deployment, on page 123](#)
- [Optional Configuration for Packaged CCE 4000/12000 Agents Deployment, on page 133](#)
- [Optional Configuration for Packaged CCE Lab deployment, on page 150](#)

## Optional Configuration for Packaged CCE 2000 Agents Deployment

To configure optional components for Packaged CCE 2000 Agents deployment.

| Task                                                                                       |
|--------------------------------------------------------------------------------------------|
| <a href="#">Add and Maintain Remote Sites, on page 123</a>                                 |
| <a href="#">Add and Maintain External Machines, on page 127</a>                            |
| <a href="#">Add PIMs to the Media Routing Peripheral Gateway, on page 130</a>              |
| <a href="#">Add Multichannel PIM to 2000 Agent Deployment, on page 131</a>                 |
| <a href="#">Configure Email and Chat, on page 132</a>                                      |
| <a href="#">Configure Cisco Unified Customer Voice Portal Reporting Server, on page 39</a> |
| <a href="#">Configure VVB, on page 43</a>                                                  |

### Add and Maintain Remote Sites

You can add new remote sites to the 2000 Agents deployment type. Each remote site added appears as a separate tab. Click the + icon to open the **Add Remote Site** pop-up window. See [Add Remote Site, on page 124](#) for more information.

## Add Remote Site

### Procedure

**Step 1** Navigate to **Unified CCE Administration > Infrastructure > Inventory**.

**Step 2** Click the + icon to open the **Add Remote Site** page.

**Step 3** On the **CCE PG** screen, enter the remote site information in the following fields:

| Field                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                                | Enter a name for the site. Maximum length is ten characters. Valid characters are alphanumeric, period (.), and underscore (_). The first character must be alphanumeric.<br><br><b>Note</b> You cannot use the system reserved terms like core, main, and site.                                                                                                                                                |
| <b>Side A PG Hostname/ IP Address</b>      | Enter the hostname, IP address, or fully qualified domain name (FQDN) for Side A.                                                                                                                                                                                                                                                                                                                               |
| <b>Side B PG Hostname/ IP Address</b>      | Enter the hostname, IP address, or fully qualified domain name (FQDN) for Side B.                                                                                                                                                                                                                                                                                                                               |
| <b>Select PG Client Types to Configure</b> | Select the required peripheral gateway client types. The subsequent screens appear as per the selected options. <ul style="list-style-type: none"> <li>• If you select <b>Agent</b>, the <b>Unified CM</b> and <b>Finesse</b> screens appear.</li> <li>• If you select <b>VRU</b>, the <b>CVP</b> screen appears.</li> <li>• If you select <b>Multichannel</b>, the <b>Configure</b> screen appears.</li> </ul> |

**Note** The system does not support IP address change. Use the hostname if you foresee a change in IP address. This is applicable for all the **Hostname/ IP Address** fields.

**Step 4** Click **Next**. The subsequent screens appear as per the selected PG client types.

**Step 5** On the **Unified CM** page, you can either select an existing publisher or add a new one. If you select a publisher, the associated subscribers appear and you can select the subscriber details. To add a new publisher,

- Select **Add a new CM Publisher**.
- Enter the Hostname, Username, and Password.
- Click **Save**.

**Note** You can add only one CM Publisher while creating a remote site.

**Step 6** On the **Subscribers** section, select the following connection settings for the agent peripheral:

- Side A Connection
- Side B Connection
- Mobile Agent Codec

**Step 7** Click **Next**.

**Step 8** On the **Finesse** page, enter the Hostname, Username, and Password for the Finesse primary server.

**Step 9** Click **Next**.

**Step 10** On the **CVP** page, enter the Hostname/IP Address, Username, and Password of the Side A and Side B CVP Servers.

**Step 11** Click **Next**.

The system performs the following Configuration tasks.

| Component                      | Automated Configuration Tasks                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unified CCE PG                 | <p><b>Agent</b></p> <ul style="list-style-type: none"> <li>• Downloads JTAPI from the Unified Communications Manager, and installs it on the Unified CCE PG.</li> <li>• Creates the CUCM Peripheral Gateway (PG) with the CUCM PIM.</li> <li>• Creates the CTI Server.</li> </ul> <p><b>VRU</b> - Creates the VRU PG with two VRU PIMs.</p> <p><b>Multichannel</b> - Creates the Multichannel PG.</p> |
| Unified CCE Rogger             | Updates the router configuration with the new PGs that are created as a part of the site.                                                                                                                                                                                                                                                                                                             |
| Unified Communications Manager | <ul style="list-style-type: none"> <li>• Creates the Application User that is used to configure the Agent PG.</li> </ul>                                                                                                                                                                                                                                                                              |
| Finesse                        | <ul style="list-style-type: none"> <li>• Configures the CTI Server settings.</li> <li>• Configures the connection to the AW database.</li> </ul>                                                                                                                                                                                                                                                      |
| Unified Customer Voice Portal  | <ul style="list-style-type: none"> <li>• Configures the Unified CVP Call Server components and adds them to the Main site Reporting Server.</li> <li>• Configures the Unified CVP VXML Server components.</li> <li>• Configures the Unified CVP Media Server components.</li> </ul>                                                                                                                   |

**Note** If one of the automated initialization tasks fail, the system reverts all the completed tasks.

**Step 12** Click **Done** when all the tasks are complete. If there are configuration errors, you can click **Back** to edit the previous pages.

**Step 13** For the configuration to take effect, do the following:

- Restart the router service.
- If you have selected the PG client type as VRU, restart the two newly configured CVP Call Servers .

### What to do next



---

**Note** For all remote sites configured with Agent PG, you must add the Finesse Self Signed Certificate (if the solution does not have the CA certificate) to the AW Machine. For more information on how to add Finesse certificate to AW Machine, see [Add Finesse Certificate to AW Machine, on page 611](#).

---

### Related Topics

[Import VOS Components Certificate](#)

## Reconfigure Remote Site

### Procedure

---

**Step 1** Navigate to **Unified CCE Administration > Infrastructure > Inventory**.

**Step 2** Click the site you want to reconfigure.

**Step 3** Click **Reconfigure** to open the **CCE PG** page.

**Note** You can only add PG client types.

**Step 4** Click **Next** and proceed the same way as you add a new remote site.  
Refer to [Add Remote Site, on page 124](#) for more information.

---

## Delete Remote Site

You can delete a remote site if the following are not associated to the remote site:

- Agents
- Teams
- Dialed Numbers
- Skill groups
- Routing Pattern
- SIP Server Groups
- Locations
- Script
- Dialer



---

**Note** Before deleting a remote site, you must stop all the services and processes running on the Cisco Finesse server of the remote site manually.

---



If remote sites has CVPs configured, make sure the following tasks are completed before deleting remote site:

- Dissociate CVP Server from CVP Reporting Server.
- If a site specific Reporting Server is used in Courtesy Call Back, replace the Reporting Server with another.



---

**Note** Post deletion of remote site, delete the Packaged CCE ID from the ORM.properties file.

---

### Procedure

---

**Step 1** Navigate to **Unified CCE Administration > Infrastructure > Inventory**.

**Step 2** Click the remote site you want to delete.

**Step 3** Click **Delete**.

A message appears asking if you are sure to delete the remote site.

**Step 4** Click **Yes** to confirm.

The remote site disappears from the **Inventory** page.

**Note** The delete operation does not remove the remote site objects permanently from the database. If you want to recreate a site with same name, you must permanently delete these objects from **Configuration Manager > Tools > Miscellaneous Tools > Deleted Objects**.

---

## Add and Maintain External Machines

### Add External Machines

You can add the following external machines based on PG types configured on:

- Agent: None
- VRU: Unified CVP Reporting Server, Virtualized Voice Browser, Gateways, Media Server, and Unified SIP Proxy



---

**Note** For detailed steps on how to add a Media Server as an external machine, see [Add Media Server as External Machine, on page 128](#)

---

- Multichannel: Third-Party Multichannel, ECE Data Server (refers to ECE Data Server VM for 400 agents and Services Server VM for ECE 1500 agents), ECE Web Server, and SocialMiner

If you are using any Multichannel applications (SocialMiner, Enterprise Chat and Email, and Third-Party Multichannel), add them to the System Inventory external machines.

### Procedure

---

- Step 1** On the **Inventory** page, select the main site or remote site and in the **External Machines** section, click the + icon.
- Step 2** Choose the machine type from the **Type** drop-down list.
- Step 3** In the **Host Name** field, enter the hostname, IP address, or fully qualified domain name (FQDN) for the selected machine type.

**Note** The system attempts to convert the value you enter to FQDN.

The system does not support IP address change. Use the hostname if you foresee a change in IP address.

- Step 4** In the machine's **Administration** section, enter the administration username and password for the selected machine type.
- Step 5** Click **Save**.

**Note** • **Email and Chat:**

- In Configuration Manager Tool, application instance and application path are to be created and associated to CUCM PG.
- LDAP configuration needs to be done using Single Sign-On (for Partition Administrators) in the ECE Administration Web interface. For more information, see *Enterprise Chat and Email Administrator's Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html>.
- **VVB:**When you add VVB, the system will mark the machine as Out of Sync. Either wait for auto synchronization (which happens every 10 mins) or do manual synchronization.
- **SocialMiner:**If you add SocialMiner, the system automatically creates a SocialMiner Task feed for Task Routing, including the associated campaign and Connection to CCE notification.

## Add Media Server as External Machine

### Procedure

---

- Step 1** In Unified CCE Administration, select **Infrastructure Settings > Inventory**.
- Step 2** Select the main site or the remote site and in the **External Machines** section, click the + icon.
- Step 3** In the **Add Machine** dialog box, complete the following fields:

**Note** To enable addition of Media Servers and perform FTP configuration in Packaged CCE 12.0(1), install the ICM12.0(1) ES and CVP ES patch. For more information, see *Release Notes for Packaged Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html>.

| Field                 | Required? | Description                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type                  | Yes       | From the drop-down list, choose "Media Server".                                                                                                                                                                                                                                                                                                                                                                                                         |
| Host Name/IP Address  | Yes       | Enter the hostname, IP address, or fully qualified domain name (FQDN) for the selected machine type.<br><br><b>Note</b> The system attempts to convert the value you enter to FQDN.<br><br>The system does not support IP address change. Use the hostname if you foresee a change in IP address.                                                                                                                                                       |
| FTP Section           |           | Configure FTP during off-peak hours. Do not do the configuration during heavy call load.                                                                                                                                                                                                                                                                                                                                                                |
| FTP Enabled           | No        | Indicates whether a Media Server has FTP enabled.<br><br>A Media Server, which has FTP enabled, is automatically populated as a session variable to the VXMLServer. The (default) Agent Greeting recording application automatically uses the Media Servers in the inventory that have FTP enabled for the recording.<br><br>If Microsoft FTP Service is not enabled in Windows Services Control Panel, then set it to Automatic and start the service. |
| Anonymous Access      | No        | Indicates that this Media Server uses anonymous FTP access. In this case, the user name is specified as anonymous by default. The password field is not editable if you chose anonymous access.                                                                                                                                                                                                                                                         |
| Username and Password | No        | These fields apply only if the FTP field is enabled and if the Anonymous Access field is disabled. In this case, enter the username and password.                                                                                                                                                                                                                                                                                                       |
| Port                  | Yes       | Enter a new port number or use the default port number (21).                                                                                                                                                                                                                                                                                                                                                                                            |

**Step 4** Click **Save**.

**Note** • When a Media Server is added, configurations are propagated to all CVPs across sites.

## Edit External Machines

On the **Inventory** page, select the main site or a remote site and click the pencil icon to edit the following machines:

| Machine              | Editable Field            |
|----------------------|---------------------------|
| Unified CM Publisher | AXL Username and Password |

| Machine                                              | Editable Field                                                                                                                                                                                                              |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SocialMiner                                          | Administration Username and Password                                                                                                                                                                                        |
| Enterprise Chat and Email and 3rd Party Multichannel | <ul style="list-style-type: none"> <li>• Web Server: edit partition Administration User name and Password.</li> <li>• Data Server: none</li> </ul>                                                                          |
| Virtualized Voice Browser                            | Administration Username and Password                                                                                                                                                                                        |
| Unified SIP Proxy                                    | Administration Username and Password                                                                                                                                                                                        |
| Gateway                                              | Administration Username and Password                                                                                                                                                                                        |
| Unified CVP Reporting                                | Windows Administration credentials                                                                                                                                                                                          |
| Media Server                                         | FTP Enabled, Anonymous Access, FTP Credentials, and Port<br><br><b>Note</b> <ul style="list-style-type: none"> <li>• When a Media Server is updated, configurations are propagated to all CVPs and across sites.</li> </ul> |

To delete an external machine on the main site or a remote site, click the **x** on the machine. Confirm the deletion.


**Note**

- You cannot delete the Virtualized Voice Browser and Unified SIP Proxy external machines if they are associated with a SIP Server Group. To delete these external machines, you must disassociate them from the SIP Server Group.
- You cannot delete the Gateway external machine if it is associated with Location. To delete this external machine, you must disassociate the Gateway from the Location.
- If you delete the Unified CM Publisher, the Unified CM Subscribers are also deleted automatically, and the Configure Deployment pop-up window opens. Enter the name, IP address, AXL username, and AXL password for the Unified CM Publisher in your deployment.
- When a Media Server is deleted, configurations are propagated to all CVPs across sites.

## Add PIMs to the Media Routing Peripheral Gateway

The Media Routing Peripheral Gateway (MR PG) is created during automated initialization.

Creating PIMs for the MR PG is optional. You can create the following PIMs on the Media Routing Peripheral Gateway:

- Outbound PIM
- Multichannel PIM for SocialMiner

- Multichannel PIM for Enterprise Chat and Email (ECE)
- Multichannel PIM for a third-party multichannel application
- Multichannel PIM for Digital Routing

To create Dialed Numbers associated with the Multichannel PIMs, first do the following:

- Create the PIM using Peripheral Gateway Setup.
- Add an external machine in the Solution Inventory using the Unified CCE Administration System. Navigate to **Overview > Infrastructure > Inventory**. Scroll down and click **Add External Machine**.




---

**Note** If ECE Data Server is deployed on box, you do not need to create a Dialed Number associated with the PIM.

---




---

**Note** Refer to the *Cisco Packaged Contact Center Enterprise Features Guide* at [https://www.cisco.com/en/US/products/ps12586/prod\\_maintenance\\_guides\\_list.html](https://www.cisco.com/en/US/products/ps12586/prod_maintenance_guides_list.html) for directions on adding the Outbound PIM and the Multichannel PIMs.

Refer to the *Enterprise Chat and Email Installation Guide (for Packaged Contact Center Enterprise)* at <https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html>.

---

## Add Multichannel PIM to 2000 Agent Deployment




---

**Caution** Before performing the step to enable the secured connection between the components, ensure that the security certificate management process is completed.

---

### Before you begin

Only users who are part of the local Administrators group can run Peripheral Gateway setup.

### Procedure

---

- Step 1** In the **Peripheral Gateway Component Properties** window, click **Add**.
- Step 2** From the **Client Type** drop-down list, select **Media Routing**.
- Step 3** From the **Available PIMS** list, select **MR PIM1**, then click **OK**.
- Step 4** In the **Configuration** dialog box, check the **Enabled** check box.
- Step 5** In the **Peripheral name** field, enter the peripheral name.
- Step 6** In the **Peripheral ID** field, enter the logical controller ID of the Unified CCE component you are adding. The following are the names by which the Unified CCE components are represented in the database. Refer *Peripheral Gateway* page in CCE Admin to get the peripheral ID of the corresponding PIM.
  - Name of Outbound is *Outbound*

- Name of ECE is *Multichannel*
- Name of CCP is *Multichannel2*
- Name of THIRD\_PARTY\_MULTICHANNEL is *MutliChannel3*
- Name of Digital Routing is *DigitalRouting*

**Example:**

If you are adding ECE, find the component of the name *Multichannel* in the database. Enter the logical controller ID of that component in the **Peripheral ID** field.

**Step 7** In the **Application Hostname (1)** field, enter the hostname or the IP address of the ECE services server.

**Step 8** In the **Application connection port (1)** field, enter the port number.

**Note** Use the port number that is on the ECE services server that PIM uses to communicate with the application. The default port is 38001.

**Step 9** In the **Application Hostname (2)** field, leave the field blank.

**Step 10** In the **Application connection port (2)** field, leave the field blank.

**Step 11** In the **Heartbeat interval (sec)** field, enter **5**.

**Step 12** In the **Reconnect interval (sec)** field, enter **10**.

**Step 13** Check the **Enable Secured Connection** option.

This establishes a secured connection between the MR PIM and the application server.

Ensure that you provide the correct information in the application hostname(1) and Application Connection Port(1) fields.

**Step 14** Click **OK**.

## Configure Email and Chat

For the ECE configuration page to appear on the Unified CCE Administration, do the following:

### Procedure

**Step 1** Configure LDAP in the **ECE Administration** Web Interface.

For more information, see Single Sign-On (for Partition Administrators) in the *Enterprise Chat and Email Administrator's Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html>.

**Step 2** Accept the certificate in the **Unified CCE Administration**. Do the following:

- Enter *https://<fqdn of ecewebserver>* in the address bar of the web browser.
- Accept the certificate.
- Reload the **Unified CCE Administration** page.

# Optional Configuration for Packaged CCE 4000/12000 Agents Deployment

To configure optional components for Packaged CCE 4000 or 12000 Agents deployment.

| Task                                                                                           |
|------------------------------------------------------------------------------------------------|
| <a href="#">Remote Site, on page 133</a>                                                       |
| <a href="#">Machines, on page 136</a>                                                          |
| <a href="#">Peripheral Set, on page 143</a>                                                    |
| <a href="#">Add PIMs to the Media Routing Peripheral Gateway, on page 130</a>                  |
| <a href="#">Add Multichannel PIM to Packaged CCE 4000/12000 Agents Deployment, on page 142</a> |
| <a href="#">Configure Email and Chat, on page 132</a>                                          |
| <a href="#">Configure Cisco Unified Customer Voice Portal Reporting Server, on page 39</a>     |
| <a href="#">Configure VVB, on page 43</a>                                                      |
| <a href="#">Packaged CCE 4000 and 12000 Agent Supported Tools, on page 398</a>                 |
| <a href="#">Avaya Configurations, on page 145</a>                                              |
| <a href="#">ICM-to-ICM Gateway Configurations, on page 148</a>                                 |

## Remote Site

A remote site must have at least one peripheral set. Each remote site added appears as a separate tab.

### Add and Maintain Remote Site

#### Procedure

- 
- Step 1** Navigate to the **Unified CCE Administration > Infrastructure > Inventory**.
  - Step 2** Click the + icon to add a remote site.
  - Step 3** Enter the remote site name.
  - Step 4** Click **Download Template**.
  - Step 5** Fill the particulars in the file and save it.

Table 5: CSV Template Details

| Column        | Description                       | Required? | Permissible Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------|-----------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| name          | Unique identifier for the machine | Yes       | Name must start with an alphabet. Maximum length is limited to 128 characters. Valid characters are a-z, A-Z, 0-9, dot (.), underscore (_), or hyphen (-).                                                                                                                                                                                                                                                                                                                                                                                                     |
| machineType   | MachineType Enum name             | Yes       | <p>Mandatory machines are:</p> <ul style="list-style-type: none"> <li>• CVP</li> <li>• FINESSE_PRIMARY</li> <li>• FINESSE_SECONDARY</li> <li>• CM_PUBLISHER</li> <li>• CM_SUBSCRIBER</li> <li>• CCE_PG</li> </ul> <p>Optional machines:</p> <ul style="list-style-type: none"> <li>• ECE (refers to ECE Data Server VM for 400 agents and Services Server VM for ECE 1500 agents)</li> <li>• ECE_WEB_SERVER</li> <li>• CVP_REPORTING</li> <li>• GATEWAY</li> <li>• CVVB</li> <li>• CUSP</li> <li>• THIRD_PARTY_MULTICHANNEL</li> <li>• MEDIA_SERVER</li> </ul> |
| publicAddress | Public address                    | Yes       | Valid IP address or hostname                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |



| Column            | Description                           | Required?                                                                                     | Permissible Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------|---------------------------------------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| connectionInfo    | Connection information of the machine | Required for CM_PUBLISHER, FINESSE_PRIMARY, ECE_WEB_SERVER, CVP, CVP_REPORTING, CUSP, GATEWAY | <p>Enter the username and password in the following format:</p> <pre>userName=&lt;user&gt;&amp;password=&lt;password&gt;</pre> <p>ConnectionInfo is optional if you are configuring FTP for CVP (Media Server).</p> <p>Append the FTP attributes to the username and password in the following format:UserName=&lt;user&gt;&amp;password=&lt;password&gt;;ftpEnabled=&lt;true or false&gt;&amp;ftpUserName=&lt;ftp_username&gt;&amp;ftpPassword=&lt;ftp_password&gt;&amp;ftpPort=&lt;ftp_portnumber&gt; For more information on the FTP attributes, see FTP Section in the <a href="#">Add Media Server as External Machine, on page 128</a>.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Replace Ampersand (&amp;) or equal sign (=) in usernames or passwords with their respective URL encoded values "%26" or "%3D".</li> <li>• Semicolon (;) delimits the Windows Administration credentials from FTP credentials.</li> </ul> |
| privateAddress    | Private address                       | Required for CCE_PG                                                                           | Valid IP address                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| peripheralSetName | Peripheral set name                   | Required for PG, CUCM, Finesse, CVP                                                           | Name can start with an alphabet. Maximum length is limited to 10 characters. Valid characters are a-z, A-Z, 0-9, dot (.), or an underscore (_).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| side              | Side information                      | Yes                                                                                           | sideA<br>sideB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

**Step 6** Upload the file and click **Next**.

**Step 7** Wait for validation to be completed and click **Done**.

During the validation, tasks are performed depending on the components defined in the CSV template.

If validation fails, then click **Back** to fix the issues in the file and upload it again.

The remote site that is created appears as a tab on the Inventory page.

- Note**
- Agent PG and PIMs are created only when Finesse and CUCM are present.
  - Multichannel PGs are created. For adding PIMs, see the section "Add Multichannel PIM to Packaged CCE 4000/12000 Agents Deployment".
  - VRU PG and PIMs are created only when CVP is present.
  - Only one peripheral set must be created at a time.
  - Live Data Configuration Services, TIP\_PG and TIP\_PG\_TOS will be added in Machine\_Service table only for Agent PG.

---

**Related Topics**

[Add Multichannel PIM to Packaged CCE 4000/12000 Agents Deployment](#), on page 142

## Delete Remote Site

**Before you begin**

To delete a remote site, you must:

- Delete all the SIP server groups, routing patterns, and locations associated with the remote site.
- Delete the peripheral sets associated with the remote site.
- Disassociate CVP Reporting Server from CVP Server and courtesy callback.

**Procedure**

---

- Step 1** Navigate to **Unified CCE Administration > Infrastructure > Inventory**.
- Step 2** Select the remote site you want to delete and click **Delete > Current Site**.  
The remote site is deleted from the inventory.
- 

## Machines

You can configure machines for the main sites and remote sites in the 4000 Agents and 12000 Agents deployment type.

### Add and Maintain Machines

**Procedure**

---

- Step 1** Navigate to the **Unified CCE Administration > Infrastructure > Inventory**.
- Step 2** Go to **Import > Device** to add a machine.
- Step 3** Click **Download Template**.

**Step 4** Fill the particulars in the file and save it.

**Table 6: CSV Template Details**

| Column      | Description                       | Required? | Permissible Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------|-----------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| name        | Unique identifier for the machine | Yes       | Name must start with an alphabet. Maximum length is limited to 128 characters.<br><br>Valid characters are a-z, A-Z, 0-9, dot (.), underscore (_), or hyphen (-).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| machineType | MachineType Enum name             | Yes       | Mandatory machines are: <ul style="list-style-type: none"> <li>• AW</li> <li>• HDS</li> <li>• ECE (refers to ECE Data Server VM for ECE 400 agents and Services Server VM for ECE 1500 agents)</li> <li>• ECE_WEB_SERVER</li> <li>• CVP</li> <li>• CVP_REPORTING</li> <li>• CM_PUBLISHER</li> <li>• CM_SUBSCRIBER</li> <li>• FINESSE</li> <li>• FINESSE_PRIMARY</li> <li>• FINESSE_SECONDARY</li> <li>• GATEWAY</li> <li>• CVVB</li> <li>• CUSP</li> <li>• SOCIAL_MINER</li> <li>• THIRD_PARTY_MULTICHANNEL</li> <li>• MEDIA_SERVER</li> <li>•</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• HDS, AW, CUIC_SUBSCRIBER are only applicable for the main site.</li> <li>• Add FINESSE and CM together.</li> </ul> |

| Column            | Description                           | Required?                                                                                     | Permissible Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------|---------------------------------------|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| publicAddress     | Public address                        | Yes                                                                                           | Valid IP address or hostname                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| connectionInfo    | Connection information of the machine | Required for CM_PUBLISHER, FINESSE_PRIMARY, ECE_WEB_SERVER, CVP, CVP_REPORTING, CUSP, GATEWAY | <p>Enter the username and password in the following format:</p> <pre>userName=&lt;user&gt;&amp;password=&lt;password&gt;</pre> <p>For more information on the credentials of each component, see <a href="#">Table 7: Machine Credentials, on page 139</a>.</p> <p>ConnectionInfo is optional if you are configuring FTP for CVP (Media Server).</p> <p>Append the FTP attributes to the username and password in the following format:</p> <pre>UserName=&lt;user&gt;&amp;password=&lt;password&gt;; ftpEnabled=&lt;true or false&gt; &amp;ftpUserName=&lt;ftp_username&gt; &amp;ftpPassword=&lt;ftp_password&gt; &amp;ftpPort=&lt;ftp_portnumber&gt;</pre> <p>For more information on the FTP attributes, see FTP Section in the <a href="#">Add Media Server as External Machine, on page 128</a>.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Replace Ampersand (&amp;) or equal sign (=) in usernames or passwords with their respective URL encoded values "%26" or "%3D".</li> <li>• Semicolon (;) delimits the Windows Administration credentials from FTP credentials.</li> </ul> |
| privateAddress    | Private address                       | Required for CCE_PG                                                                           | Valid IP address                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| peripheralSetName | Peripheral set name                   | Required for CUCM, Finesse, CVP                                                               | Name can start with an alphabet. Maximum length is limited to 10 characters. Valid characters are a-z, A-Z, 0-9, dot (.), or an underscore (_).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| side              | Side information                      | Yes                                                                                           | sideA<br>sideB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

**Step 5** Upload the file and click **Next**.

**Step 6** Wait for validation to be completed and click **Done**.

During the validation, tasks are performed depending on the components defined in the CSV template. For more information about the tasks, see [Automated Initialization Tasks for 4000 and 12000 Agent Deployments, on page 73](#).

If validation fails, then click **Back** to fix the issues in the file and upload it again.

## Edit Machines

You can edit the credentials of any machine using this procedure.

### Procedure

**Step 1** On the **Inventory** page, click the main site or a remote site to edit the following machines:

**Table 7: Machine Credentials**

| Machine                   | Editable Field                                                                                                                                                                                                                                             |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AW                        | Diagnostic Framework Service Domain, Username, and Password<br><br>You can also set a Principal AW machine in 4000 and 12000 Agent deployments.<br><br>The credentials must be the same for all CCE machines.                                              |
| Live Data                 | Administration Username and Password                                                                                                                                                                                                                       |
| Finesse                   | Administration Username and Password                                                                                                                                                                                                                       |
| SocialMiner               | Administration Username and Password                                                                                                                                                                                                                       |
| ECE Web Server            | Application Instance, Partition Administration Username, and Password                                                                                                                                                                                      |
| Virtualized Voice Browser | Administration Username and Password                                                                                                                                                                                                                       |
| CUSP                      | Administration Username and Password                                                                                                                                                                                                                       |
| CUIC Publisher            | Administration Username and Password                                                                                                                                                                                                                       |
| CVP                       | Windows Administration Username and Password, FTP Enabled, Anonymous Access, FTP Credentials, and Port<br><br><b>Note</b> When a CVP (which acts as a Media Server) is updated, Media Server configurations are propagated to all other CVPs across sites. |
| Gateway                   | Administration Username and Password                                                                                                                                                                                                                       |

| Machine              | Editable Field                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVP Reporting        | <p>Windows Administration Username and Password</p> <p>The <b>Deploy</b> check box initializes the CVP Reporting Server configuration. Initialization removes the existing call server association and Courtesy Callback configuration.</p> <p>To reassociate the call servers with the CVP Reporting server, see <a href="#">Configure CVP Reporting Server</a> , on page 203.</p> <p>To reconfigure Courtesy Callback, see <a href="#">Courtesy Callback</a>, on page 363.</p> |
| IDS Publisher        | Administration Username and Password                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Media Server         | <p>FTP Enabled, Anonymous Access, FTP Credentials, and Port</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• When a Media Server is updated, configurations are propagated to all CVPs across sites.</li> </ul>                                                                                                                                                                                                                                                   |
| Unified CM Publisher | AXL Username and Password                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Step 2** Edit the credentials.

If successful, you can see the message on the **Inventory** page; else, fix the errors that are shown before clicking **Save**.

## Delete Machine

You can delete the following machine types:

- CCE\_AW
- HDS
- CVP\_REPORTING
- CUIC\_SUBSCRIBER
- CUSP
- GATEWAY
- CVVB
- EXTERNAL\_THIRD\_PARTY\_MULTICHANNEL
- DC\_EXTERNAL\_THIRD\_PARTY\_MULTICHANNEL
- MEDIA\_SERVER



- 
- Note**
- When a Media Server is deleted, configurations are propagated to all CVPs across sites.
- 

### Procedure

---

- Step 1** To delete a machine individually, select that particular row and click **Delete (X)** icon at the end of the row.
- Step 2** Click **Yes**.  
If the deletion is successful, then a message is displayed that the machine was deleted successfully. If the deletion fails, then check the error message and resolve the issue before attempting to delete again.
- 

## Add PIMs to the Media Routing Peripheral Gateway

The Media Routing Peripheral Gateway (MR PG) is created during automated initialization.

Creating PIMs for the MR PG is optional. You can create the following PIMs on the Media Routing Peripheral Gateway:

- Outbound PIM
- Multichannel PIM for SocialMiner
- Multichannel PIM for Enterprise Chat and Email (ECE)
- Multichannel PIM for a third-party multichannel application
- Multichannel PIM for Digital Routing

To create Dialed Numbers associated with the Multichannel PIMs, first do the following:

- Create the PIM using Peripheral Gateway Setup.
- Add an external machine in the Solution Inventory using the Unified CCE Administration System. Navigate to **Overview > Infrastructure > Inventory**. Scroll down and click **Add External Machine**.



- 
- Note** If ECE Data Server is deployed on box, you do not need to create a Dialed Number associated with the PIM.
- 



- 
- Note** Refer to the *Cisco Packaged Contact Center Enterprise Features Guide* at [https://www.cisco.com/en/US/products/ps12586/prod\\_maintenance\\_guides\\_list.html](https://www.cisco.com/en/US/products/ps12586/prod_maintenance_guides_list.html) for directions on adding the Outbound PIM and the Multichannel PIMs.

Refer to the *Enterprise Chat and Email Installation Guide (for Packaged Contact Center Enterprise)* at <https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html>.

---

# Add Multichannel PIM to Packaged CCE 4000/12000 Agents Deployment



**Caution** Before performing the step to enable the secured connection between the components, ensure that the security certificate management process is completed.

## Before you begin

Only users who are part of the local Administrators group can run Peripheral Gateway setup.

## Procedure

- 
- Step 1** In the **Peripheral Gateway Component Properties** window, click **Add**.
- Step 2** From the **Client Type** drop-down list, select **Media Routing**.
- Step 3** From the **Available PIMS** list, select **MR PIM1**, then click **OK**.
- Step 4** In the **Configuration** dialog box, check the **Enabled** check box.
- Step 5** In the **Peripheral name** field, enter the peripheral name.
- Step 6** In the **Peripheral ID** field, enter the logical controller ID of the Unified CCE component you are adding. The following are the names by which the Unified CCE components are represented in the database. Refer PG explorer tool using Configuration Manager to get the Peripheral ID of the corresponding PIM.
- Name of Outbound is *Outbound*
  - Name of ECE is *MR1*
  - Name of CCP is *MR2*
  - Name of THIRD\_PARTY\_MULTICHANNEL is *MR3*
  - Name of Digital Routing is *MR4*
- Example:**
- If you are adding ECE, find the component of the name *MR1* in the database. Enter the logical controller ID of that component in the **Peripheral ID** field.
- Step 7** In the **Application Hostname (1)** field, enter the hostname or the IP address of ECE services server.
- Step 8** In the **Application connection port (1)** field, enter the port number.
- Note** Use the port number that is on the ECE services server that PIM uses to communicate with the application. The default port is 38001.
- Step 9** In the **Application Hostname (2)** field, leave the field blank.
- Step 10** In the **Application connection port (2)** field, leave the field blank.
- Step 11** In the **Heartbeat interval (sec)** field, enter **5**.
- Step 12** In the **Reconnect interval (sec)** field, enter **10**.
- Step 13** Check the **Enable Secured Connection** option.

This establishes a secured connection between the MR PIM and the application server.



Ensure that you provide the correct information in the **Application Hostname(1)** and **Application Connection Port(1)** fields.

**Step 14** Click **OK**.

## Peripheral Set

Peripheral set is a collection of all components that are dependent on the peripheral gateway (including the peripheral gateway itself).

For example, Cisco Finesse, CVP. A main or remote site can have zero or more peripheral sets that are associated with it.

## Add and Maintain Peripheral Set

### Procedure

**Step 1** Navigate to the **Unified CCE Administration > Infrastructure > Inventory**.

**Step 2** Go to **Import > Peripheral Set** to add a peripheral set.  
The **New Peripheral Set** wizard opens.

**Step 3** Click **Download Template**.

**Step 4** Fill the particulars in the file and save it.

**Table 8: CSV Template Details**

| Column        | Description                       | Required? | Permissible Values                                                                                                                                                                                                                             |
|---------------|-----------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| name          | Unique identifier for the machine | Yes       | Name must start with an alphabet. Maximum length is limited to 128 characters. Valid characters are a-z, A-Z, 0-9, dot (.), underscore (_), or hyphen (-).                                                                                     |
| machineType   | MachineType Enum name             | Yes       | Mandatory machine is CCE_PG<br>Optional machines are: <ul style="list-style-type: none"> <li>• CVP</li> <li>• FINESSE_PRIMARY</li> <li>• FINESSE_SECONDARY</li> <li>• CM_PUBLISHER</li> <li>• CM_SUBSCRIBER</li> <li>• MEDIA_SERVER</li> </ul> |
| publicAddress | Public address                    | Yes       | Valid IP address or hostname                                                                                                                                                                                                                   |

| Column            | Description                           | Required?                                                                                     | Permissible Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|---------------------------------------|-----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| connectionInfo    | Connection information of the machine | Required for CM_PUBLISHER, FINESSE_PRIMARY, ECE_WEB_SERVER, CVP, CVP_REPORTING, CUSP, GATEWAY | <p>Enter the username and password in the following format:</p> <pre>userName=&lt;user&gt;&amp;password=&lt;password&gt;</pre> <p>ConnectionInfo is optional if you are configuring FTP for CVP (Media Server).</p> <p>Append the FTP attributes to the username and password in the following format:</p> <pre>userName=&lt;user&gt;&amp;password=&lt;password&gt;; ftpEnabled=&lt;true or false&gt; &amp;ftpUserName=&lt;ftp_username&gt; &amp;ftpPassword=&lt;ftp_password&gt; &amp;ftpPort=&lt;ftp_portnumber&gt;</pre> <p>For more information on the FTP attributes, see FTP Section in the <a href="#">Add Media Server as External Machine</a>, on page 128.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Replace Ampersand (&amp;) or equal sign (=) in usernames or passwords with their respective URL encoded values "%26" or "%3D".</li> <li>• Semicolon (;) delimits the Windows Administration credentials from FTP credentials.</li> </ul> |
| privateAddress    | Private address                       | Optional                                                                                      | Valid IP address                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| peripheralSetName | Peripheral set name                   | Required for PG, CUCM, Finesse, CVP                                                           | <p>Name can start with an alphabet. Maximum length is limited to 10 characters. Valid characters are a-z, A-Z, 0-9, dot (.), or an underscore (_).</p> <p><b>Note</b> Name must be unique. It cannot be reused even after that peripheral set is deleted.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| side              | Side information                      | Yes                                                                                           | sideA<br>sideB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

**Step 5** Upload the file and click **Next**.

**Step 6** Wait for validation to be completed and click **Done**.

During the validation, tasks are performed depending on the components defined in the CSV template.

If validation fails, then click **Back** to fix the issues in the file and upload it again.

- Note**
- Agent PG and PIMs are created only when Finesse and CUCM are present.
  - Multichannel PGs are created. For adding PIMs, see the section "Add Multichannel PIM to Packaged CCE 4000/12000 Agents Deployment".
  - VRU PG and PIMs are created only when CVP is present.
  - Only one peripheral set must be created at a time.
  - Live Data Configuration Services, TIP\_PG and TIP\_PG\_TOS will be added in Machine\_Service table only for Agent PG.

### What to do next

Perform the PG configuration. See [Configure Cisco Unified Contact Center Enterprise PG, on page 77](#)

### Related Topics

[Add Multichannel PIM to Packaged CCE 4000/12000 Agents Deployment](#), on page 142

## Delete Peripheral Set

You can delete peripheral sets associated with the main site or remote sites.

### Before you begin

To delete a peripheral set, you must delete agents, skill groups, teams, and dialed numbers associated with it.

### Procedure

- Step 1** Navigate to **Unified CCE Administration > Infrastructure > Inventory**.
- Step 2** Select the peripheral set from main or remote site that you want to delete and click **Delete > Peripheral Set**. The **Delete Peripheral Set from <site name>** popup window appears.
- Step 3** Select a peripheral set from the **Peripheral Set** drop-down list.
- Step 4** Click **Delete**.
- Step 5** Click **Back** to delete another peripheral set. Else, click **Done** to return to the Inventory page.

## Avaya Configurations



- Note**
- To enable this feature in Packaged CCE 12.0(1), install the ICM12.0(1) ES patch. For more information, see *Release Notes for Packaged Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html>.

The following table outlines the Avaya configuration tasks in Packaged CCE 4000 and 12000 Agent deployments.

| Sequence | Avaya Configuration Tasks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | In the PG Explorer tool, add Avaya Peripheral Gateway (with Avaya (Definity)) as the client type.<br><br>For more information, see the section <i>Peripherals and Trunk Groups</i> in the <i>Configuration Guide for Cisco Unified ICM/Contact Center Enterprise</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html</a> . |
| 2        | <a href="#">Configure and Setup Avaya Peripheral Gateway, on page 147</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 3        | <a href="#">Set up CTI Server, on page 79</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 4        | Set up CTI OS Server and CTI Desktop Client<br><br>For information, see sections <i>CTI OS Server Installation</i> and <i>CTI Toolkit Desktop Client Installation</i> in the <i>CTI OS System Manager Guide for Cisco Unified ICM/Contact Center Enterprise</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html</a> .                                          |
| 5        | <a href="#">Restart Live Data for Avaya PG, on page 148</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |



**Note** For detailed information about the required Avaya configurations, see chapter *Unified ICM Software Configuration* in the *Cisco Unified ICM ACD Supplement for Avaya Communication Manager Guide* at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cust\\_contact/contact\\_center/icm\\_enterprise/icm\\_enterprise\\_12\\_0\\_1/Reference/Guide/ucce\\_b\\_cisco-unified-icm-acd-supplement-1201.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_0_1/Reference/Guide/ucce_b_cisco-unified-icm-acd-supplement-1201.html).

#### Related Topics

[Routing Target Selection](#), on page 441

[Packaged CCE 4000 and 12000 Agent Supported Tools](#), on page 398

## Add Users to Local Security Group

### Before you begin

Only Packaged CCE configuration users who have been added to the UcceConfig group in all the local distributors can access the Configuration Manager.

### Procedure

---

- Step 1** Click **Server Manager > Tools > Computer Management**.
  - Step 2** Select **Local Users and Groups**.
  - Step 3** Double-click **Groups**.
  - Step 4** Right-click **UcceConfig**. Select **Properties**.
  - Step 5** Click **Add** and enter the user name in the **Edit the object names to select** text box. Click **Check Names** to validate the user name.
  - Step 6** After the user name is successfully validated, click **OK**.
  - Step 7** Click **Apply** and **OK** in the **Properties** dialog box.
  - Step 8** Close the **Computer Management** and **Server Manager** windows.
- 

## Configure and Setup Avaya Peripheral Gateway

### Before you begin

Only users who are part of the local Administrators group can run Peripheral Gateway setup.

### Procedure

---

- Step 1** Open the **Peripheral Gateway Setup** tool from Unified CCE Tools on the desktop.
- Step 2** Click **Add** in the **Instance Components** section.
- Step 3** Click **Peripheral Gateway**.
- Step 4** Complete the following steps in the Peripheral Gateway Properties dialog box.
  - a) Choose **Production Mode**. Do not set the Auto Start feature until after the installation is complete.
  - b) Specify whether the PG is part of a duplexed pair.
  - c) In the ID field, select from the drop-down list the PG device number as enabled in the Router.
  - d) If the PG is duplexed, specify whether you are installing Side A or Side B. If the PG is simplex, select Side A.
  - e) In the **Client Type Selection** section of the window, select the client type:
    - For an Avaya PG: Avaya (Definity)
- Step 5** Click **Add**, and then click **Next**.
- Step 6** Enter the Logical Controller ID generated while configuring the PG in the **PG Explorer** tool. Click **Add** and select **PIM 1** from the list. Click **OK**.
- Step 7** Configure PIM.

For more information, see *Cisco Unified ICM ACD Supplement for Avaya Communication Manager* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-technical-reference-list.html>.
- Step 8** Click **OK**.
- Step 9** From the **Peripheral Gateway Component Properties** window, click **Next**. The **Device Management Protocol Properties** window appears.

- a) Enter the appropriate settings and click **Next**. The **Peripheral Gateway Network Interfaces** window appears.
- b) Configure the Private Interface and Public interfaces and click **Next**.

**Note:**

For the address input fields, use Fully Qualified Domain Names instead of IP addresses.

When there are two IP addresses configured on the public Network Interface Card (for IP-based prioritization), manually add two A-records on the DNS server. One A-record is for the high priority IP address and the other one is for the general priority IP address. The host part of the two DNS entries should be different from the hostname of Windows server. Use the new DNS entries to configure the public interfaces. This note applies to the Router and to all PG machines.

**Step 10** In the **Check Setup Information** window, verify the setup information and click **Next**.

**Step 11** When the **Setup Complete** window appears, click **Finish**.

**Note** When you add new PG, ensure that the PG ID is provided in the Router configuration. Provide the number that is assigned to the PG in the Enable Peripheral Gateway field in Web Setup

---

## Restart Live Data for Avaya PG

When a new peripheral gateway that supports Live Data is deployed and started, its feed will not be available to the Live Data server automatically. Restart the Live Data server to start the feed from the newly deployed Peripheral Gateway.

**Procedure**

Access the Live Data CLI and run the following command:

```
utils system restart
```

**Note** Restarting Live Data server impacts all CCE components.

---

## ICM-to-ICM Gateway Configurations



**Note** To enable this feature in Packaged CCE 12.0(1), install the ICM12.0(1) ES patch. For more information, see *Release Notes for Packaged Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html>.

The following table outlines the ICM-to-ICM Gateway configuration tasks in Packaged CCE 4000 and 12000 Agent deployments.

| Sequence | ICM-to-ICM Gateway Configuration Tasks                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | Configure ICM-to-ICM Gateway<br>For more information, see <i>ICM to ICM Gateway User Guide for Unified CCE</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html</a> |
| 2        | <a href="#">Remote ICM type application gateway global settings, on page 149</a>                                                                                                                                                                                                                                                                                                                                                                |

**Related Topics**

[Routing Target Selection](#), on page 441

[Packaged CCE 4000 and 12000 Agent Supported Tools](#), on page 398

**Remote ICM type application gateway global settings**

The configuration for Remote ICM Type Application Gateway can be performed by using **Configuration Manager > List Tools > Application Gateway List >** .

Following are the Remote ICM type Application Gateway global settings.

**Table 9: Remote ICM type Application Gateway Global Setting**

| Name                   | Value |
|------------------------|-------|
| Abandon Timeout.       | 5000  |
| ApplicationGatewayType | 1     |
| DateTimeStamp          | NULL  |
| ChangeStamp            | 0     |
| ErrorThreshold         | 10    |
| HeartbeatLimit         | 2     |
| HeartbeatRetry         | 200   |
| HeartbeatTimeout       | 300   |
| HeartbeatInterval      | 15000 |
| ID                     | 2     |
| LateTimeout            | 400   |
| LinkTestThreshold      | 2     |
| OpenTimeout            | 500   |
| RequestTimeout         | 500   |

| Name              | Value |
|-------------------|-------|
| SessionRetry      | 30000 |
| SessionRetryLimit | 0     |

## Optional Configuration for Packaged CCE Lab deployment

### Remote Sites in Lab Mode

You can create remote sites in lab mode deployment. If you initiate your lab mode in simplex, you can create remote sites only with Side A machines.

To add a remote site in lab mode deployment, see [Add and Maintain Remote Sites, on page 123](#).

When you configure the simplex or duplex lab mode deployment, you can also add the following external machines for a remote site:

- Unified CM Publisher
- Unified CVP Reporting Server
- Unified SIP Proxy
- Virtualized Voice Browser
- Gateway
- MediaSense
- Enterprise Chat and Email
- Third-party Multichannel
- Media Server



---

**Note** You can add SocialMiner, and MediaSense only in the main site.

---

To add, edit or delete the external machines on the remote site, see [Add External Machines, on page 127](#) and [Edit External Machines, on page 129](#) sections.

For more information on the configuration limits for external machines, see the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html>.





## CHAPTER 3

# Packaged CCE Administration

---

- [Getting Started](#), on page 151
- [Infrastructure Settings](#), on page 160
- [User Setup](#), on page 229
- [Organization Setup](#), on page 249
- [Desktop Settings](#), on page 288
- [Call Settings](#), on page 325
- [Feature Setup](#), on page 363
- [Email and Chat](#), on page 376
- [Bulk Imports](#), on page 377
- [Capacity](#), on page 392

## Getting Started

### Sign In

You must do post installation configurations to sign in to the Unified CCE Administration. For more information, see [Post Installation Configuration, on page 1](#).

Sign in to Unified CCE Administration at `https://<IP Address>/cceedmin`. <IP Address> is the address of the Side A or B Unified CCE AW or optional external HDS.



---

**Note** Users are logged out of the Unified CCE Administration console automatically after 30 minutes of inactivity.

---

#### Administrators

Administrators sign in using their Active Directory credentials. For **username**, use the `user@domain.com` format.

#### Supervisors

Supervisors on an IPv6 network sign in to Unified CCE Administration at `https://<FQDN>/cceedmin`. <FQDN> is the fully qualified domain name of the Side A or B CCE AW or optional external HDS.

Supervisors sign in using their Active Directory (*user@domain.com*) or single sign-on credentials. If supervisors are enabled for single sign-on, after entering their username they are redirected to the Identity Provider sign-in screen to enter their credentials. Supervisors are redirected to Unified CCE Administration after successfully signing in.

### Languages

If the Language Pack is installed, the Sign-In window includes a Language drop-down menu, showing more than a dozen languages. English is the initial and the default language. Select any other language to see the user interface and the online help in that language. The system retains your choice for subsequent sign-ins until you change it again.

## Single Sign-On Log Out

For a complete logout from all applications, sign out of the applications and close the browser window. In a Windows desktop, log out of the Windows account. In a Mac desktop, quit the browser application.



---

**Note** Users enabled for single sign-on are at risk of having their accounts misused by others if the browser is not closed completely. If the browser is left open, a different user can access the application from the browser page without entering credentials.

---

## System Interface

Packaged CCE user interface enables you to configure the application through one window. The landing page has a left navigation bar and a card view which contains all the configuration options. What you see after a successful sign-in depends on your role.

The left navigation bar consists of the following menus:

- Overview
- Infrastructure
- Organization
- Users
- Desktop
- Capacity

The following menus appear as cards:

- Infrastructure Settings
- Call Settings
- User Setup
- Organization Setup
- Bulk Import

- Desktop Settings
- Features
- Email and Chat

(Available only when ECE Web Server is added to the **Infrastructure** > **Inventory** page on the Unified CCE Administration.)



**Note** The Unified CCE Administration interface also provides access to HTML-based online help for users and administrators. Click on the help button (?) on any page (except the Overview page) in the Unified CCE Administration interface and the online help specific to that page is displayed in a pop-over window. You can navigate to the previous or next page in the online help using the following keys:

- MAC - **Command + left arrow** or **Command + right arrow**
- Windows - **Alt+ right arrow** or **Alt + left arrow**

## Lists

### List Windows

Most tools open to a List window that has rows for all currently configured objects. For example, the Teams tool has a list with a row for each team, and the Call Types tool has a list with a row for each call type. List windows allow you to search, sort, edit, and delete from the list.

Permissions on List windows vary for administrators and supervisors and are noted in the topic for each tool.

### Search a List

There is a Search field on the List window for most tools. The search interface is similar, with small variations, depending on the tool.

### Search and Administrators

If you sign in as a global administrator, a search returns all objects.

If you sign in as a departmental administrator, a search returns all objects in the departments you administer, as well as all global objects (objects that are in no departments).

### Basic Search

Some tools offer a basic search on the **Name** (or name-equivalent) and **Description** fields.

Enter all or part of either value to find matches. Clear the search by deleting text from the Search field.

### Search for Tools with Department IDs

For objects that can be associated with a department, you can click the + icon to the right of the Search field to open a popup window, where you can:

- Enter a name or description ( for call types and precision queues add **id**).
- Select departments, with options for **Globals and Departments**, **Globals only**, or **Departments only**.

Selecting **Globals and Departments** or **Departments only** enables an input field where you can enter a space-separated list of department names. (Departments is an OR search.)




---

**Note** Search by department is enabled only when departments are configured.

---

### Agent Advanced Search

The Search field in the Agents tool offers an advanced and flexible search.

Click the + icon at the far right of the Search field to open a popup window, where you can:

- Select to search for agents only, supervisors only, or both.
- Enter a username, agent ID, first or last name, or description to search for that string.
- Enter one or more team names separated by spaces. (Team is an OR search--the agent or supervisor must be a member of one of the teams.)
- Enter one or more attribute names separated by spaces. (Attributes is an AND search--the agent or supervisor must have all attributes.)
- Enter one or more skill group names separated by spaces. (Skill Groups is an AND search.)
- Select departments, with options for **Globals and Departments**, **Globals only**, or **Departments only**.

Selecting **Globals and Departments** or **Departments only** enables an input field where you can enter a space-separated list of department names. (Departments is an OR search.)

### Related Topics

[Departments](#), on page 269

### Sort a List

If a column in a List window has an arrow icon in the column header, click the **arrow** to sort in ascending or descending order.

### Add Objects

Click **New** in a List window to open an Add window where you can complete fields to create and save a new object.

### Update Objects

To edit an object in a List window, click in the row for that object. This opens a window where you can make and save modifications. This table explains which fields are editable for each tool.

In the List window for the Agent tool, you can edit descriptions, desk settings, and teams for multiple agents at once (see [Edit Description, Desk Settings, and Teams for Multiple Agents](#), on page 238).

In the List window of the Dialed Number tool, you can edit the ringtone media file for multiple Dialed Numbers at once (see [Add and Update Ringtone Media File for Multiple Dialed Numbers](#), on page 333).



**Remember** Not all tools are available for all Deployment Types.

| Tool             | Editable Fields                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrators   | All fields                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Agents           | <p>All fields except <b>Site</b> and <b>Peripheral Set</b>.</p> <p>If an agent is not enabled for single sign-on, you can check <b>Change Password</b> to reset the agent's password.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• When you change the team association for an agent record in Packaged CCE, the same change is updated in the corresponding collection in Unified Intelligence Center.</li> <li>• When you change the username for a supervisor's record in Packaged CCE, the same is updated in the corresponding user account in Unified Intelligence Center.</li> <li>• For an existing supervisor's record, if you uncheck the <b>Is Supervisor</b> check box, the corresponding user account is deleted from Unified Intelligence Center.</li> </ul> |
| Attributes       | All fields except <b>Type</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Bucket Intervals | <p><b>Name</b></p> <p>You cannot edit the built-in bucket interval.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Bulk Jobs        | No fields                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Business Hours   | <p><b>General</b> tab: All fields.</p> <p><b>Regular Hours</b> tab: All fields.</p> <p><b>Special Hours &amp; Holidays</b> tab: All fields.</p> <p><b>Status Reasons</b>: The <b>Status Reason</b> field is editable.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Call Types       | All fields except the system-generated ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Campaigns        | <p><b>General</b> tab: All fields except <b>Type</b> field.</p> <p><b>Skill Group</b> tab: You can add and delete the Skill Groups using <b>Add</b> and <b>Delete</b> buttons.</p> <p><b>Advanced</b> tab: All fields.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| <b>Tool</b>             | <b>Editable Fields</b>                                                                                                                                                                                                                                                                                           |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Desk Settings           | All fields                                                                                                                                                                                                                                                                                                       |
| Dialed Numbers          | All fields except <b>Site</b> , <b>Routing Type</b> , <b>Peripheral Set</b> and <b>Media Routing Domain</b> .                                                                                                                                                                                                    |
| Expanded Call Variables | For user-defined array and scalar expanded call variables, <b>Name</b> , <b>Description</b> , <b>Maximum Length</b> , <b>Enabled</b> , and <b>Persistent</b> are editable.<br><br>For built-in expanded call variables, <b>Enabled</b> and <b>Persistent</b> are the only editable fields.                       |
| Media Routing Domains   | All fields<br><br>You cannot edit the built-in Cisco_Voice MRD or Multichannel MRDs for Enterprise Chat and Email.                                                                                                                                                                                               |
| Network VRU Scripts     | All fields                                                                                                                                                                                                                                                                                                       |
| Precision Queues        | All fields                                                                                                                                                                                                                                                                                                       |
| Reason Labels           | <b>Label</b> , <b>Description</b> , <b>Global</b> , and <b>Team Specific</b>                                                                                                                                                                                                                                     |
| Roles                   | For custom roles, except for the <b>Administrators</b> , <b>Departments</b> and <b>Roles</b> fields in the <b>Access</b> category, all fields on both tabs are editable.<br><br>You cannot edit the built-in roles.                                                                                              |
| Routing Pattern         | All fields except <b>Routing Pattern</b> , <b>Site</b> and <b>Pattern Type</b> .                                                                                                                                                                                                                                 |
| Location                | All fields except <b>Location Name</b> .                                                                                                                                                                                                                                                                         |
| SIP Server Group        | All fields except <b>Domain Name FQDN</b> , <b>Site</b> , and <b>Type</b> .                                                                                                                                                                                                                                      |
| Teams                   | All fields except <b>Site</b> and <b>Peripheral Set</b> .<br><br><b>Note</b> When you update an existing team record in Packaged CCE, the same changes are also updated in the corresponding collection in Unified Intelligence Center.                                                                          |
| Skill Groups            | All fields except <b>Site</b> , <b>Media Routing Domain</b> , <b>Peripheral Set</b> and <b>Peripheral Number</b> .<br><br><b>Note</b> The <b>Peripheral Number</b> field is generated automatically when you add and save a new skill group. It shows the number of the skill group, as known on the peripheral. |

## Delete Objects

To delete an object from a List window, hover over the row for that object to see the **x** icon at the end of the row. Click the **x** icon and confirm your intention to delete.

Departmental administrators cannot delete global objects. Objects are identified as global in the Department column in the List window.

When you delete an object from Unified CCE Administration, the system does one of the following:

- Immediately deletes the object.
- Marks the object for deletion and enables permanent deletion. (You delete the object permanently using the Deleted Objects tool in Configuration Manager.)
- Shows an error message explaining why the object cannot be deleted in its current state.

You cannot delete certain objects, including:

- Objects set as system defaults, such as the default desk settings.
- Objects referenced by other objects, such as a call type that is referenced by a dialed number.
- Most built-in objects, such as built-in expanded call variables.

This table lists the delete types for all Unified CCE Administration objects. Available objects depend on your role and deployment type.

| Tool             | Delete Type | Notes                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrators   | Permanent   | —                                                                                                                                                                                                                                                                                                                                                                                         |
| Agents           | Marked      | <p><b>Note</b> When you delete an agent for which <b>Is Supervisor</b> check box is selected, the corresponding user account in Unified Intelligence Center is also deleted.</p> <p>When you delete an agent, the association with team is also removed and same is updated in the corresponding collection in Unified Intelligence Center.</p>                                           |
| Attributes       | Marked      | —                                                                                                                                                                                                                                                                                                                                                                                         |
| Bucket Intervals | Marked      | —                                                                                                                                                                                                                                                                                                                                                                                         |
| Bulk Jobs        | Permanent   | <p>Deletes the bulk job, its content file, and its log file from the host computer that created it.</p> <p>You can delete a bulk job that is in queue, has completed, or has failed.</p> <p>You cannot delete a bulk job that is in process.</p> <p>If your deployment includes two AW server hosts, you must delete a bulk job from the Unified CCE AW host on which it was created.</p> |

| Tool                    | Delete Type | Notes                                                                                                                                                                                       |
|-------------------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Business Hours          | Permanent   | You cannot delete a business hour associated with a script. You must first dissociate the business hour from the script.                                                                    |
| Status Reasons          | Permanent   | —                                                                                                                                                                                           |
| Call Types              | Marked      | —                                                                                                                                                                                           |
| Campaigns               | Marked      | —                                                                                                                                                                                           |
| Desk Settings           | Permanent   | —                                                                                                                                                                                           |
| Dialed Numbers          | Marked      | —                                                                                                                                                                                           |
| SIP Server Group        | Permanent   | You cannot delete the SIP Server Group associated with a Routing Pattern. You must first remove the SIP Server Group from the Routing Pattern.                                              |
| Expanded Call Variables | Marked      | —                                                                                                                                                                                           |
| Media Routing Domains   | Permanent   | You cannot delete the built-in Cisco_Voice MRD or Multichannel MRDs for Enterprise Chat and Email (ECE).                                                                                    |
| Network VRU Scripts     | Permanent   | —                                                                                                                                                                                           |
| File Transfer Job       | Permanent   | Deletes the file transfer job, its job details file, and its log file from the host computer where it is created.<br><br>You cannot delete a file transfer job that is in processing state. |
| Precision Queues        | Marked      | Depends on whether the precision queue is referenced statically or dynamically in a script. .                                                                                               |
| Reason Labels           | Marked      | —                                                                                                                                                                                           |
| Roles                   | Permanent   | —                                                                                                                                                                                           |
| Routing Pattern         | Permanent   | —                                                                                                                                                                                           |
| Location                | Permanent   | —                                                                                                                                                                                           |
| Teams                   | Permanent   | <b>Note</b> When you delete a team in Packaged CCE, the corresponding collection is also deleted in Unified Intelligence Center.                                                            |
| Skill Groups            | Marked      | —                                                                                                                                                                                           |

**Related Topics**

[Permanent Deletion](#), on page 397



## Popup Windows

### Popup window selection

Many Add and Edit windows have popup windows for searching and choosing objects that are relevant to that tool.

Some popup windows allow you to choose one object. Other popup windows allow you to select multiple objects. For example, because an agent can be on only one team, the popup window for adding an agent to a team allows only one selection, while the Skill Group Members popup window allows you to select one or more agents to add to the skill group.

Click the + icon to open the popup window, where you can locate and select items that are configured.

## Keyboard Shortcuts

Press the question mark (?) key to open a window that shows the keyboard shortcuts that are applicable for that tool and for your status (Supervisor or Administrator).



---

**Tip** The keyboard shortcuts window does not open when you press the (?) key in a text field. Press the `esc` key to remove focus from the text field and then press the (?) key.

---

## System and Device Sync Alerts

Unified CCE Administration includes icons to notify users of any system alerts and device out-of-sync alert.

### System Alerts

In Unified CCE Administration, you can monitor the status of the systems. The Alerts icon on the page includes alert count.

To view the alert and validation rule of a machine, click the Alerts icon. The Inventory page opens where you can view more details on the errors. For more information on server status rules, see [Monitor Server Status Rules for Packaged CCE 2000 Agents Deployment, on page 19](#)

### Device Out of Sync Alerts

In Unified CCE Administration, the configured data is synchronized with respective devices deployed in the inventory. If configured data synchronization fails with any device, the device is marked as out-of-sync and the Out of Sync device alert icon appears at the top of the page.

You can click the icon to open the Inventory page, and view data synchronization status of Cisco Unified Customer Voice Portal (CVP), Cisco Finesse Primary, Cisco Unified Intelligence Center (CUIC) Publisher, Enterprise Email and Chat (ECE) Web Server, and Cisco Virtualized Voice Browser (VVB).

You can perform manual synchronization of data on each In Sync and Out of Sync device in the Inventory. See [Manual Synchronization of Configured Data, on page 160](#).

## Manual Synchronization of Configured Data

This procedure explains how to manually synchronize configured data. You can do a Full Sync (for CVP) or a Differential sync.

**Full Sync:** This option is enabled for all CVPs (Main site and remote site) . Full Synchronization reinitializes the device (CVP redeploy) and synchronizes all configuration data from the time when the initial configuration was done. Use this option after you reimaged or reinstall the CVP Server.

**Differential Sync:** This option synchronizes the configured data from the time the device was out of sync.

### Procedure

- 
- Step 1** Navigate to **Unified CCE Administration > Overview > Infrastructure Settings > Inventory**.
- Step 2** If the device Sync Status is **In Sync**, click the **Sync** icon and select **Full Sync**.
- Step 3** If the device Sync Status is **Out of Sync**, click the **Sync** icon and select one of the following options
- **Differential Sync**
  - **Full Sync**
- Step 4** Click the **Sync** button.

**Note** If the Full Sync operation is successful, you must restart the CVP device.

---

# Infrastructure Settings

## Smart Licensing

### Smart Licensing Overview

Cisco Smart Software Licensing is a flexible software licensing model that streamlines the way you activate and manage Cisco software licenses across your organization. Smart Licenses provide greater insight into software license ownership and consumption, so that you know what you own and how the licenses are being used. The solution allows you to easily track the status of your license and software usage trends. It pools the license entitlements in a single account and allows you to move licenses freely across virtual accounts. Smart Licensing is enabled across most of the Cisco products and managed by a direct cloud-based or mediated deployment model.

Smart Licensing registers the Product Instance, reports license usage, and obtains the necessary authorization from **Cisco Smart Software Manager (Cisco SSM)** or **Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem)**.

You can use Smart Licensing to:

- View license usage and count.
- View the status of each license type and the product instance.

- View the product licenses available on Cisco SSM or Cisco SSM On-Prem.
- Register or deregister the Product Instance, renew license authorization and license registration.
- Sign in additional agents to Unified CCX up to the maximum limit that is configured in your OVA.

## License Management

Smart Licensing can be managed by using Cisco SSM and License Management in Unified CCE Administration portal..

- **Cisco SSM**—Cisco SSM enables you to manage all your Cisco smart software licenses from a centralized website. With Cisco SSM, you organize and view your licenses in groups called virtual accounts (collections of licenses and product instances).

You can access Cisco SSM from <https://software.cisco.com>, by clicking the Smart Software Licensing link under the License menu.

- **License Management in Unified CCE Administration portal**—Using the License Management option in the Unified CCE Administration portal, you can register or deregister the product instance, select your License Type, set transport settings or view the licensing consumption summary.

## Prerequisites for Smart Licensing

The following are the prerequisites for configuring Smart Licensing:

- **Smart Licensing Enrollment**

Set up Smart and Virtual accounts. For more information, see <https://software.cisco.com/#module/SmartLicensing>.

- **Adoption of License Integration Strategy**

Decide how you want to connect your product instance to Smart Licensing servers:

- **On-Cloud:** Configure Packaged CCE to connect to Cisco SSM On-Prem Cisco SSM.
- **On-Premise:**
  1. Deploy the Cisco SSM On-Prem. For instructions on how to do this, see <https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html>.
  2. Configure Packaged CCE to connect to Cisco SSM On-Prem.

For more information, see [Smart License Deployments, on page 162](#).

- **Import the Rogger A certificate into the AW machines**

1. Export Logger/Rogger A certificate and save it by using the url `https:<Logger/Roggerhostname>:443`
2. Import the certificate in AW by using the following command:

```
• cd %CCE_JAVA_HOME%\bin
```

```
C:\Program Files (x86)\Java\jre1.8.0_221\bin>keytool.exe -keystore
Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"
-import -alias <alias name> -file <certicate with fully qualified path>
```

3. Enter the truststore password when prompted.

4. Enter 'Yes' when prompted to trust the certificate.
5. Restart the Tomcat service.

## Smart License Deployments

There are two software deployment options for Smart Licensing:

- Direct - Cisco Smart Software Manager (Cisco SSM)
- Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem)

### Direct - Cisco Smart Software Manager (Cisco SSM)

The Cisco SSM is a cloud-based service that handles your system licensing. The Product Instance can connect either directly to Cisco SSM or through a proxy server.

Cisco SSM allows you to:

- Create, manage, or view virtual accounts.
- Manage and track the licenses.
- Move licenses across the virtual accounts.
- Create and manage Product Instance Registration Tokens.

For more information about Cisco SSM, go to <https://software.cisco.com>.

### Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem)

Cisco SSM On-Prem is an on-premises component that can handle your licensing needs. When you choose this option, Packaged CCE registers and reports license consumption to the Cisco SSM On-Prem, which synchronizes its database regularly with Cisco SSM that is hosted on cisco.com.

You can use the Cisco SSM On-Prem in either Connected or Disconnected mode, depending on whether the Cisco SSM On-Prem can connect directly to cisco.com.

Configure Transport URL for Cisco SSM On-Prem with Smart Call-Home URL:  
<https://<OnpremCSSM>/Transportgateway/services/DeviceRequestHandler>




---

**Note** The <OnpremCSSM> value must match with the SSM Tomcat Certificate Common Name or Subject Alternative Name. In the above URL, replace <OnpremCSSM> with FQDN or IP, based on the SSM Tomcat Certificate.

---

- **Connected**—Use when there is connectivity to cisco.com directly from the Cisco SSM On-Prem. Smart account synchronization occurs automatically.
- **Disconnected**—Use when there is no connectivity to cisco.com from the Cisco SSM On-Prem. Cisco SSM On-Prem must synchronize with Cisco SSM manually to reflect the latest license entitlements.

For more information on Cisco SSM On-Prem, see <https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html>.

## Evaluation Mode

After installation, Packaged CCE runs under the 90-day evaluation period. At the end of the evaluation period, if the system is not registered with Cisco SSM, it will enter a state of Enforcement where system operations are restricted. For more information, see *Enforcement Rules*.

Customers must Register the system with Cisco SSM or Cisco SSM On-Prem within 90 days. If the system is not registered before the end of the evaluation period, it will be moved to the Enforcement state where certain system functions are restricted.

## Smart Licensing Task Flow

Complete these tasks to set up smart licensing for Packaged CCEUnified CVP.

| Steps  | Action                                           | Description                                                                                                                                                                                                                                                                                                                                             |
|--------|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Create your Smart Account                        | Use the Smart Account to organize licenses according to your needs. To create a Smart Account, go to <a href="http://software.cisco.com">http://software.cisco.com</a><br><br>After the Smart Account is created, Cisco SSM creates a default Virtual Account for this Smart Account. You can use the default account or create other Virtual Accounts. |
| Step 2 | Obtain the Product Instance Registration Token   | Generate a product instance registration token for your virtual account.<br><br>For more information, see <a href="#">Obtain the Product Instance Registration Token</a> .                                                                                                                                                                              |
| Step 3 | Configure Transport Settings for Smart Licensing | Configure the transport settings through which Packaged CCEUnified CVP connects to the Cisco SSM or Cisco SSM On-Prem.<br><br>For more information, see <a href="#">Configure Transport Settings for Smart Licensing</a> .                                                                                                                              |
| Step 4 | Select the License Type                          | Select the License Type before registering the product instance.<br><br>For more information, see <a href="#">Select License Type</a> .                                                                                                                                                                                                                 |
| Step 5 | Register with Cisco SSM                          | You can register Packaged CCEUnified CVP with Cisco SSM or Cisco SSM On-Prem.<br><br>For more information, see <a href="#">Register with Cisco Smart Software Manager</a> .                                                                                                                                                                             |



**Note** After performing the above steps, wait for 10-15 minutes for the correct status to get reflected in the UI. There is no need to restart the services.

## Obtain the Product Instance Registration Token

Obtain the product instance registration token from Cisco SSM or Cisco SSM On-Prem to register the product instance. Generate the registration token with or without enabling the Export-Controlled functionality.




---

**Note** The **Allow export-controlled functionality on the products that are registered with this token** check box does not appear for Smart Accounts that are not permitted to use the Export-Controlled functionality.

---

### Procedure

---

**Step 1** Log in to your smart account in either Cisco SSM or Cisco SSM On-Prem.

**Step 2** Navigate to the virtual account with which you want to associate the product instance.

**Step 3** Generate the Product Instance Registration Token.

**Note**

- Select the **Allow export-controlled functionality on the products registered with this token** check box to turn on the Export-Controlled functionality for a product instance you want in this smart account. When you select this check box and accept the terms, you enable higher levels of encryption for products that are registered with this registration token. By default, this check box is selected.

- Use this option only if you are compliant with the Export-Controlled functionality.

**Step 4** Copy the generated token. This token is required when registering Smart Licensing with Cisco SSM.

---

## Configure Transport Settings for Smart Licensing

Configure the connection mode between Packaged CCEUnified CVP and Cisco SSM.




---

**Note** Configure the transport setting individually for all CVP devices installed in the deployment.

---

### Procedure

---

**Step 1** From Unified CCE Administration, navigate to **Overview > Infrastructure Settings > License Management**.

**Step 2** The license information of the first CVP server in the **Device Name** drop-down list is displayed by default. From the **Device Name** drop-down list, select a CVP server.

**Note** The system displays the following error if the CVP server you selected is not reachable or is not compatible with your PCCE version.

The server is unreachable or is not on a version that supports this feature.

For details, see the *Contact Center Enterprise Solution Compatibility Matrix* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html>

- Step 3** Click **Transport Settings** to set the connection method.
- Step 4** Select the connection method to Cisco SSM:
- **Direct**—Packaged CCEUnified CVP connects directly to Cisco SSM on cisco.com. This is the default option.
  - **Transport Gateway**—Packaged CCEUnified CVP connects to Cisco SSM On-Prem for smart licensing. Enter the Cisco SSM On-Prem URL.
  - **HTTP/HTTPS Proxy**—Packaged CCEUnified CVP connects to a proxy server, which connects to Cisco SSM. Enter the Fully Qualified Domain Name (FQDN) of the proxy server along with the port.
- Step 5** Click **Save** to save the settings.

## Select License Type

Smart Licensing offers two types of license—Flex and Perpetual and it also provides two different usage mode—Production and Non-Production.

- **Flex**—Flex license is a recurring subscription of Standard and Premium license. These subscriptions are renewed periodically, for example 1, 3, or 5 years.
- **Perpetual**—Perpetual license is a permanent and one-time payment license that offers Premium license.
- **Production**—Production mode is when the licenses are used on live systems to handle actual production traffic. Yes
- **Non-Production**—Non-production mode is used for labs, testing and/or staging areas, and not for live systems handling actual end-consumer traffic.

Select the License Type and Usage Mode corresponding to what you have purchased before registering the product instance.



**Note** If you select incorrect License Type, the product instance is placed in the Out-of-Compliance state. If this issue is unresolved, the product instance is placed in the Enforcement state where the system operations are impacted.

## Procedure

- Step 1** From Unified CCE Administration, navigate to **Overview > Infrastructure Settings > License Management**.
- Step 2** Click **License Type**.  
The **Select License Type** page is displayed.
- Step 3** Select the License Type and the Usage Mode corresponding to what you have purchased before registering the product instance.
- Step 4** Select the License Type and the Usage Mode corresponding to what you have purchased before registering the product instance.

**Step 5** Click **Save**.

---

## Register with Cisco Smart Software Manager

The product instance has 90 days of evaluation period, within which, the registration must be completed. Else, the product instance gets into the enforcement state.

Register your product instance with Cisco SSM or Cisco SSM On-Prem to exit the Evaluation or Enforcement state.



**Note** After you register the product instance, you cannot change the license type. To change the license type, deregister the product instance.

---

### Procedure

---

**Step 1** In Unified CCE Administration, navigate to **Overview > Infrastructure Settings > License Management**.

**Step 2** The license information of the first CVP server in the **Device Name** drop-down list is displayed by default. From the **Device Name** drop-down list, select a CVP server.

**Note** The system displays the following error if the CVP server you selected is not reachable or is not compatible with your PCCE version.

The server is unreachable or is not on a version that supports this feature.

For details, see [Contact Center Enterprise Solution Compatibility Matrix](#).

**Step 3** Click **Register**.

**Note** • Before you register the product instance, ensure to select the **License Type** and the communication mechanism in **Transport Settings**.

**Step 4** In the **Smart Software Licensing Product Registration** dialog box, paste the product instance registration token that you generated from Cisco SSM or Cisco SSM On-Prem.

For information on generating the Registration Token, see the *Obtain the Product Instance Registration Token* section in [Cisco Unified Contact Center Express Features Guide](#).

**Step 5** Click **Register** to complete the registration process.

After registration, the **Smart Licensing Status** displays the following details.

**Table 10: Smart Licensing Status**

| Smart License Status                | Description  |
|-------------------------------------|--------------|
| <b>On Unsuccessful Registration</b> |              |
| Registration Status                 | Unregistered |
| License Authorization Status        | Evaluation   |



| Smart License Status              | Description                                 |
|-----------------------------------|---------------------------------------------|
| Export-Controlled Functionality   | Not Allowed                                 |
| <b>On Successful Registration</b> |                                             |
| Registration Status               | Registered (Date and time of registration)  |
| License Authorization Status      | Authorized (Date and time of authorization) |
| Export-Controlled Functionality   | Not Allowed                                 |
| Smart Account                     | The name of the smart account               |
| Virtual Account                   | The name of the virtual account             |
| Product Instance Name             | The name of the product instance            |
| Serial Number                     | The serial number of the product instance   |

Entitlements are a set of privileges customers and partners receive when purchasing a Cisco service agreement. Using Smart Licensing, you can view the License consumption summary for the entitlements of different license types. The License consumption summary displays the License Name, Usage Count, and Status against each entitlement name.

You can update or purchase entitlements on the Cisco Commerce website. For more information, see <https://apps.cisco.com/Commerce/>.

## Registration, Authorization, and Entitlement Status

### Registration Status

This table explains the various productUnified CVP registration status for Smart Licensing in the Unified CCE Administration portal:

**Table 11: Registration Status**

| Status               | Description                                                                                                             |
|----------------------|-------------------------------------------------------------------------------------------------------------------------|
| Unregistered         | Product is unregistered.                                                                                                |
| Registered           | Product is registered. Registration is automatically renewed every six months.                                          |
| Registration Expired | Product registration has expired because the ID Certificate issued by Cisco SSM is not renewed for more than 12 months. |

### Authorization Status

This table describes the possible productUnified CVP authorization status for Smart Licensing in the Unified CCE Administration portal:

Table 12: Authorization Status

| Status                | Description                                                                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Evaluation state      | Product is not registered with Cisco.                                                                                                                                                       |
| Evaluation Expired    | Product evaluation period has expired.                                                                                                                                                      |
| Authorized            | Product is in authorized or in compliance state. Authorization is renewed every 30 days.                                                                                                    |
| Authorization Expired | Product authorization has expired. This usually happens when the product has not communicated with Cisco for 90 days. It is in an overage period for 90 days before enforcing restrictions. |
| Out-of-Compliance     | Product is in out-of-compliance state because of insufficient licenses. It is in an overage period for 90 days before enforcing restrictions.                                               |
| Unauthorized          | Product is unauthorized.                                                                                                                                                                    |
| No License in Use     | No Licenses are in use.                                                                                                                                                                     |

### License Entitlement Status

This table describes the possible product Unified CVP instance license entitlement status for Smart Licensing in the Unified CCE Administration portal:

Table 13: License Entitlement Status

| Status                | Status Description                                                                                                                            |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Authorization Expired | Product authorization has expired, when the product has not communicated with Cisco for 90 days.                                              |
| Not Authorized        | Product instance is not authorized.                                                                                                           |
| Evaluation state      | Product is not registered with Cisco.                                                                                                         |
| Evaluation Expired    | Product evaluation period has expired.                                                                                                        |
| In Compliance         | Product is in authorized or in compliance state. Authorization is renewed every 30 days.                                                      |
| ReservedInCompliance  | Entitlement is in compliance with the installed reservation authorization code.                                                               |
| Out-of-Compliance     | Product is in out-of-compliance state because of insufficient licenses. It is in an overage period for 90 days before enforcing restrictions. |
| Not Applicable        | Entitlement is not applicable.                                                                                                                |
| Invalid               | Error condition state.                                                                                                                        |
| Invalid Tag           | Entitlement tag is invalid.                                                                                                                   |

| Status            | Status Description                                                                 |
|-------------------|------------------------------------------------------------------------------------|
| No License in Use | Entitlement is not in use.                                                         |
| Waiting           | Waiting for an entitlement request's response from Cisco SSM or Cisco SSM On-Prem. |
| Disabled          | Product instance is deactivated or disabled.                                       |

## Out-Of-Compliance and Enforcement Rules

### Out-of-Compliance

The Product Instance reports license usage to Cisco SSM every 15 minutes. If your license consumption is more than the entitlements for four consecutive reporting intervals, the Product Instance is pushed to the Out-of-Compliance state. The Out-of-Compliance period is for 90 days, within which you need to purchase the additional licenses. If you fail to take corrective action within the 90 days period, the Product Instance is pushed to the Enforcement state.

All CVPs in a virtual account share the licenses from a pool. If the license consumption exceeds than those available in the pool, all CVPs in the virtual account follow the Out-of-Compliance and Enforcement rules.

### Enforcement

The Product Instance is in the Enforcement state in the following scenarios:

- **Out-of-Compliance expiry:** When the Out-of-Compliance period of 90 days has expired.  
Purchase new licenses to exit the Enforcement state.
- **Authorization expiry:** When the Product Instance has not communicated with Cisco SSM or Cisco SSM On-Prem for 90 days and has not automatically renewed the entitlement authorizations.  
Renew the license authorizations to exit the authorization expiry state.
- **Evaluation expiry:** When the license evaluation period of 90 days has expired and the Product Instance is not registered with Cisco SSM.  
Register the Product Instance with Cisco SSM to exit the Evaluation expiry state.



**Note** In the Enforcement state, the following actions are blocked in CVP:

- Deploying application and updating application scripts in VXML server
- Deploying VXML applications REST call from the Unified CCE Administration interface

## Notifications and Alerts

The system maintains real-time status of license usage after Product Instances are registered and activated. Administrators are notified through alerts, event logs, and emails on the status of licenses in the Smart and Virtual Accounts. Pay attention to system alerts and banners to get regular information on compliance status and take necessary action.

Following are some of the notification methods:

- Banner Notifications
- System Alerts

### Banner Notifications

- The banner displays the aggregate license compliance status on the Unified CCE Administration portal. The banner is displayed only when any of the product instances in the deployment is in the Evaluation, Out-of-Compliance, or Enforcement state.

The **License Compliance report** displays the license status of product instances in the deployment. The reporting hierarchy is Enforcement, Out-of-Compliance, and Evaluation. This means that if any of the product instances in the deployment is in the Enforcement state, the banner displays Enforcement state as the overall status. Click the **Learn More** option to view the consolidated **License Compliance report**.

- When licenses are consumed in a Non-Production System, a banner message, "You are using a Non-Production System", is displayed.

### System Alerts

Smart Licensing related system alerts, which get auto-corrected, are displayed in Unified CCE Administration portal when:

- Smart License state is not initialized
- Smart Agent is not enabled
- Serial number is not generated

In the above conditions, a red system alert is displayed in the **Alerts** button on the Unified CCE Administration portal. The red circle against the name of the machine in the inventory indicates the identified issue and the immediate action needed. After the issue is resolved, a green circle against the name of the machine indicates the system is running fine, for example, when the Smart Agent is enabled or Smart License state is initialized.

## Smart Licensing Tasks

After you successfully register Smart Licensing, you can perform the following tasks as per the requirement:

- **Renew Authorization**—The license authorization is renewed automatically every 30 days. Use this option to manually renew the authorization.
- **Renew Registration**—The initial registration is valid for one year. Registration is automatically renewed every six months. Use this option to manually renew the registration.
- **Reregister**—Use this option to forcefully register the product instance again.
- **Deregister**—Use this option to release all the licenses from the current virtual account.

Renew Authorization and Renew Registration are automated tasks that take place at regular intervals. If there is a failure in the automated process, you can manually renew authorization and registration.

For more information, see *Smart License Management* section in [Cisco Unified Contact Center Express Admin and Operations Guide](#).



---

**Note** You have to Deregister and Reregister manually.

---

## Renew Authorization

The license authorization is renewed automatically every 30 days. The authorization status expires after 90 days if the product is not connected to Cisco SSM or Cisco SSM On-Prem.

Use this procedure to manually renew the License Authorization Status for all the licenses listed in the License Type.

### Procedure

---

**Step 1** In Unified CCE Administration, navigate to **Overview > Infrastructure Settings > License Management**.

**Step 2** The license information of the first CVP server in the **Device Name** drop-down list is displayed by default. From the **Device Name** drop-down list, select a CVP server.

**Note** The system displays the following error if the CVP server you selected is not reachable or is not compatible with your PCCE version.

The server is unreachable or is not on a version that supports this feature.

For details, see the *Contact Center Enterprise Solution Compatibility Matrix* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html>

**Step 3** Click **Action > Renew Authorization**.

This process takes a few seconds to renew the authorization and close the window.

---

## Renew Registration

Use this procedure to manually renew your certificates.

The initial registration is valid for one year. Renewal of registration is automatically done every six months, provided the product is connected to Cisco SSM or Cisco SSM On-Prem.

### Procedure

---

**Step 1** In Unified CCE Administration, navigate to **Overview > Infrastructure Settings > License Management**.

**Step 2** The license information of the first CVP server in the **Device Name** drop-down list is displayed by default. From the **Device Name** drop-down list, select a CVP server.

**Note** The system displays the following error if the CVP server you selected is not reachable or is not compatible with your PCCE version.

The server is unreachable or is not on a version that supports this feature.

For details, see the *Contact Center Enterprise Solution Compatibility Matrix* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html>

**Step 3** Click **Action** > **Renew Registration**.

This process takes a few seconds to renew the authorization and close the window.

## Reregister License

Use this procedure to reregister Packaged CCEUnified CVP with Cisco SSM or Cisco SSM On-Prem.



**Note** Product can migrate to a different virtual account when reregistering with the token from a new virtual account.

### Procedure

**Step 1** In Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings** > **License Management**.

**Step 2** The license information of the first CVP server in the **Device Name** drop-down list is displayed by default. From the **Device Name** drop-down list, select a CVP server.

**Note** The system displays the following error if the CVP server you selected is not reachable or is not compatible with your PCCE version.

The server is unreachable or is not on a version that supports this feature.

For details, see the *Contact Center Enterprise Solution Compatibility Matrix* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html>

**Step 3** Click **Action** > **Reregister**.

**Step 4** In the **Smart Software Licensing Product Registration** dialog box, paste the copied or saved Registration Token Key that you generated using the Cisco SSM or Cisco SSM On-Prem in the Product Instance Registration Token text box.

**Step 5** Click **Reregister** to complete the reregistration process.

**Step 6** Close the window.

## Deregister License

Use this procedure to deregister Packaged CCEUnified CVP from Cisco SSM or Cisco SSM On-Prem and release all the licenses from the current virtual account. All license entitlements that are used for the product are released to the virtual account and is available for other product instances to use.




---

**Note** If Packaged CCEUnified CVP is unable to connect to Cisco SSM or Cisco SSM On-Prem, and the product is deregistered, then a confirmation message notifies you to remove the product manually from Cisco SSM or Cisco SSM On-Prem to free up licenses.

---




---

**Note** After deregistering, the product reverts to the Evaluation state if the evaluation period is not expired. All the license entitlements that are used for the product are immediately released to the virtual account and are available for other product instances to use them.

---

### Procedure

- 
- Step 1** In Unified CCE Administration, navigate to **Overview > Infrastructure Settings > License Management**.
- Step 2** The license information of the first CVP server in the **Device Name** drop-down list is displayed by default. From the **Device Name** drop-down list, select a CVP server.
- Note** The system displays the following error if the CVP server you selected is not reachable or is not compatible with your PCCE version.
- The server is unreachable or is not on a version that supports this feature.
- For details, see the *Contact Center Enterprise Solution Compatibility Matrix* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html>
- Step 3** Click **Action > Deregister**.
- Step 4** On the **Confirm Deregistration** dialog box, click **Yes** to deregister.
- 

## Smart Licensing Configurations

Unified CVP Release 12.5 uses the following configuration files for Smart Licensing operations.

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




---

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

---

### Handling SocketTimeoutException:

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

1. In the OAMP server, navigate to the following location:  

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

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

## Manage Devices

You can configure any of the following components:

- CVP Server
- CVP Reporting Server
- VVB
- Finesse
- Single Sign-on Setup

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 CVP Server and a Reporting Server. In this case, each device is configured with the same IP address.

## CVP Server Services Setup

As part of Packaged CCE fresh install, the CVP Server is added with default configuration values. You can configure:

- ICM Service
- SIP Service
- IVR Service
- VXML Server
- Infrastructure




---

**Important** Except for the configurations that require a Call Server restart, configure all the other CVP Server configurations during off-peak hours (not during heavy call load).

---

For shutting down services of call server/reporting server, see [Graceful Shutdown of Call Server or Reporting Server](#), on page 616.



## 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. You install the ICM Service with the CVP Server.

You must configure the ICM Service if you add or edit a CVP Server and use any of these call flow models:

- Call Director
- VRU-Only
- Comprehensive

### Procedure

- Step 1** Navigate to **Unified CCE Administration > Overview > Infrastructure Settings > Device Configuration > CVP Server**.
- Step 2** Choose the site name for the ICM Service. By default, it is Main.
- Step 3** Complete the following fields:

*Table 14: ICM Service Configuration Settings*

| Field                                           | Required? | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>VRU Connection Port</b>                      | yes       | The port number on which the ICM Service 5000 listens for a TCP connection from the ICM PIM.<br><br>Default is 5000.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Maximum Length of DNIS</b>                   | yes       | The maximum length of an incoming Dialed Number Identification Service (DNIS). Range is 1 - 99999 characters.<br><br>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 must be 10.<br><br>The number of DNIS digits from the PSTN must be less than or equal to the maximum length of the DNIS field.<br><br><b>Note</b> If you use the Correlation ID method in your ICM script to transfer calls to Unified CVP, the maximum length of DNIS must be the length of the label that is returned from the ICM for the VRU leg of the call. When the ICM transfers the call, the Correlation ID is appended to the label. Unified CVP then separates the two, assuming that any digits greater than the maximum length of DNIS are the Correlation ID. The Correlation ID and the label are then passed to the ICM. |
| <b>Enable secure communication with VRU PIM</b> | -         | Enables secure communication between ICM and the Unified CVP Server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Field                                 | Required? | Description                                                                                                                                                                                                                |
|---------------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Trunk Utilization</b>              |           |                                                                                                                                                                                                                            |
| <b>Enable Gateway Trunk Reporting</b> | -         | Enables the gateway trunk reporting.                                                                                                                                                                                       |
| <b>Maximum Gateway Ports</b>          | no        | The value used for setting the maximum number of ports that a gateway supports in a CVP deployment. This is used to calculate the number of ports to report to the Unified ICM Server for each gateway.<br>Default is 700. |
| <b>Monitored Gateways</b>             | no        | The list of gateways available for trunk reporting.<br>Click + (Add) to add a new gateway.                                                                                                                                 |

**Step 4** Click **Save**.

## Set Up IVR Service

You must configure the IVR Service if you add a new Unified CVP Server or edit a Unified CVP Server in any of these call flow models:

- Call Director, using SIP protocol
- VRU-Only
- Comprehensive, using SIP protocol

The IVR Service creates VXML documents that implement the Micro-Applications based on Run Script instructions received by the ICM. The VXML pages are sent to the VXML Gateway to be run. The IVR Service can also generate external VXML through the Micro-Applications to engage the Unified CVP VXML Server to generate the VXML documents.

The IVR Service plays a significant role in implementing a failover mechanism: those capabilities that can be achieved without ASR/TTS Servers, and VXML Servers. Up to two of each such servers are supported, and the IVR Service orchestrates retries and failover between them.

### Before you begin

Configure the following servers before setting up the IVR Service:

- ICM Server
- Media Server
- ASR/TTS Server
- Unified CVP VXML Server
- Gateway

## Procedure

**Step 1** Navigate to **Unified CCE Administration > Overview > Infrastructure Settings > Device Configuration > CVP Server**.

**Step 2** Click the **IVR** tab. Complete the following fields:

**Table 15: IVR Service Configuration Settings**

| Field                                                | Required? | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Use Security for Media Fetches</b>                | -         | <p>If you select <b>No</b> (default), the HTTP URLs are generated to the Media Servers.</p> <p><b>Note</b> 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.</p> <p>Select <b>Yes</b> to generate the HTTPS URLs to the Media Servers.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Use Backup Media/VXML Servers</b>                 | -         | <p>If you select <b>Yes</b> (default) and a Media Server is unavailable, the gateway attempts to connect to the backup Media Server.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Use Host Names for Default Media/VXML Servers</b> | -         | <p>By default, the IP address is used for the VXML Server and the Media Server. If you enables this field, the hostnames are used rather than the IP addresses.</p> <p><b>Note</b> When you enable this field, enable the High Availability(HA) for Media Server in each CVP Server in the site after you save the configuration.</p> <p>To enable HA for Media Server, open the mediaServer.properties file in the C:\Cisco\CVP\conf folder and configure the following:</p> <ul style="list-style-type: none"> <li>• MediaServer.1.hostName = &lt;Media Server Host&gt;</li> <li>• MediaServer.1.ip = &lt;Media Server IP&gt;</li> </ul> <p>The IP and hostname must match the default media server IP and hostname in the Unified CCE Administration. Define the corresponding &lt;hostname&gt;-backup entry to backup Media Server IP in VXML Gateway and Virtualized Voice Browser(VVB). When the primary host name fails, the media files fetch request can be served from backup media server.</p> |

| Field                       | Required? | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Call Timeout</b>         | yes       | The number of seconds the IVR Service waits for a response from the SIP Service before timing out. This setting must be longer than the longest prompt, transfer, or digit collection at a Voice Browser. If the timeout is reached, the call is canceled but no other calls are affected. The only downside to making the number arbitrarily large is that if calls are being stranded, they are not removed from the IVR Service until this timeout is reached.<br><br>Minimum is 6 seconds. Default is 7200 seconds. |
| <b>Default Media Server</b> | no        | From the <b>Default Media Server</b> drop-down list, choose the default media server.                                                                                                                                                                                                                                                                                                                                                                                                                                   |

**Step 3** Click **Save**.

## Set Up SIP Service

You must set up the SIP Service if you add a new CVP Server in of these call flow models:

- 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

**Step 1** Navigate to **Unified CCE Administration > Overview > Infrastructure Settings > Device Configuration > CVP Server**.

**Step 2** Click the **SIP** tab. Complete the following fields:

*Table 16: SIP Service Settings*

| Field                        | Required? | Description                                                                                                                                  |
|------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable Outbound Proxy</b> | -         | Select <b>Yes</b> to use a Cisco Unified SIP proxy server.<br><br>Default is No.                                                             |
| <b>Outbound Proxy Host</b>   | no        | Select <b>Enable Outbound Proxy</b> to view the <b>Outbound Proxy Host</b> drop-down list. It displays a list of external SIP Server Groups. |
| <b>Outbound Proxy Port</b>   | no        | Default is 5060.                                                                                                                             |
| <b>DNS SRV</b>               |           |                                                                                                                                              |

| Field                                        | Required? | Description                                                                                                                                                                                                                                               |
|----------------------------------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable DNS SRV Type Query</b>             | -         | Select <b>Yes</b> to use DNS SRV for outbound proxy lookup.<br><b>Note</b> If you enable Resolve SRV records locally, you must select <b>Yes</b> to ensure the feature works properly.                                                                    |
| <b>Resolve DNS SRV Locally</b>               | -         | Select to resolve the SRV domain name with a local configuration file instead of a DNS Server.<br><b>Note</b> If you enable Resolve SRV records locally, you must select <b>Yes</b> to use the DNS SRV type query. Otherwise, this feature will not work. |
| <b>Outgoing Transport Type</b>               | no        | Specifies the outgoing transport. You can set it to TCP or UDP.<br>Default is TCP.                                                                                                                                                                        |
| <b>Port Number for Incoming SIP Requests</b> | yes       | Specifies the port to be used for incoming SIP requests.<br>Default is 5060.                                                                                                                                                                              |
| <b>Prepend Digits</b>                        | no        | Specifies the number of digits to be removed for SIP URI user number. Default is 0.                                                                                                                                                                       |
| <b>Use Error Refer</b>                       | no        | Flags for play error tone when a call fails to caller.<br>Default is False.                                                                                                                                                                               |
| <b>SIP Info Tone Duration</b>                | yes       | Specifies the wait time in milliseconds for the SIP info tone. It is an optional value for the list addition.<br>Default is 100.                                                                                                                          |
| <b>SIP Info Comma Duration</b>               | yes       | Specifies the wait time in milliseconds for the SIP info comma. It is an optional value for the list addition.<br>Default is 100.                                                                                                                         |
| <b>SIP Header Passing to ICM</b>             |           |                                                                                                                                                                                                                                                           |
| <b>Header Name</b>                           | no        | Specifies the SIP header name. Click + (Add) to add a new SIP header to be passed to ICM. It can support up to 255 characters.                                                                                                                            |
| <b>Parameter</b>                             | no        | This field is optional for list addition. It can support up to 255 characters.                                                                                                                                                                            |
| <b>Security Properties</b>                   |           |                                                                                                                                                                                                                                                           |
| <b>Incoming Secure Port</b>                  | no        | Specifies the port to be used.<br>Default is 5061.                                                                                                                                                                                                        |

| Field                        | Required? | Description                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Supported TLS Version</b> | yes       | <p>Allows you to select the TLS versions supported for securing the SIP signaling on the IVR leg. The TLS versions currently supported are TLSv1.0, TLSv1.1, and TLSv1.2. Default is TLSv1.2.</p> <p><b>Note</b> When you select a given TLS version, Unified CVP supports the SIP TLS requests for that version and the higher supported versions.</p>                      |
| <b>Supported Ciphers</b>     | no        | <p>This field defines the ciphers, which is supported by Unified CVP, with key size lesser than or equal to 2048 bits.</p> <p>The default cipher is TLS_RSA_WITH_AES_128_CBC_SHA, which is prepopulated and cannot be deleted as it is mandatory for TLSv1.2.</p> <p>Cipher configuration is available only if TLS is enabled.</p> <p>Click + (Add) to add a new cipher.</p> |

**Note** After you add the required ciphers restart the system for more information, refer to the topic *Generate CVP ECDSA Certificate with OpenSSL* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html>

**Note** The dialed number uses default values to play the ringtone and the error tone. These values cannot be edited.

**Step 3** Click **Save**.

## Set Up VXML Server

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 the call and the application session summary data. The call summary data includes call identifier, start and end timestamp of calls, ANI, and DNIS. The application session data includes application names, session ID, and session timestamps.

If you choose detailed reporting, the Unified CVP VXML Server application details are reported, including element access history, activities within the element, the element variables, and the 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 the data to be included and excluded from being reported.

### Procedure

**Step 1** Navigate to **Unified CCE Administration > Overview > Infrastructure Settings > Device Configuration > CVP Server**.

**Step 2** Click the **VXML Server** tab. Complete the following fields:

Table 17: VXML Server Configuration Properties

| Field                                                    | Required? | Description                                                                                                                                                                                                                                   |
|----------------------------------------------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable Reporting for this Unified CVP VXML Server</b> | -         | Indicates if 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.                                                      |
| <b>Enable Reporting for VXML Application Details</b>     | -         | Indicates whether VXML application details are reported.                                                                                                                                                                                      |
| <b>VXML Applications Details: Filters</b>                |           |                                                                                                                                                                                                                                               |
| <b>Inclusive Filters</b>                                 | no        | Lists applications, element types, element names, element fields, and ECC variables to include in the reporting data.<br><br>A semicolon-separated list of text strings. A wildcard character (*) is allowed within each element in the list. |
| <b>Exclusive Filters</b>                                 | no        | Lists applications, element types, element names, element fields, and ECC variables to exclude from the reporting data.                                                                                                                       |

**Step 3** Click **Save**.

## Set Up Infrastructure

The CVP Server provides SIP, IVR, and ICM call services. The CVP Reporting Server provides reporting services. Changes to the 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** Navigate to **Unified CCE Administration > Overview > Infrastructure Settings > Device Configuration > CVP Server**.

**Step 2** Click the **Infrastructure** tab. Complete the following fields:

Table 18: Infrastructure Service Configuration Settings

| Field                      | Required? | Description                                                                                                                      |
|----------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Log File Properties</b> |           |                                                                                                                                  |
| <b>Max Log File Size</b>   | yes       | The maximum size of a log file in megabytes before a new log file is created.<br><br>Range is 1 - 100MB.<br><br>Default is 10MB. |

| Field                                                  | Required? | Description                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Max Log Directory Size</b>                          | yes       | <p>The maximum size of a directory to allocate disk storage for log files.</p> <p>Range is 500 - 500000MB.</p> <p>Default is 20000MB.</p> <p><b>Note</b>      Modifying the value to a setting that is below the default value might cause logs to be quickly rolled over. Consequently, the log entries might be lost, which can affect troubleshooting.</p> <p>The log folder size divided by the log file size must be less than 5000.</p> |
| <b>Configuration: Primary Syslog Server Settings</b>   |           |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Primary Syslog Server</b>                           | no        | The hostname or the IP address of the primary syslog server to send the syslog events from a CVP application.                                                                                                                                                                                                                                                                                                                                 |
| <b>Primary Syslog Server Port Number</b>               | no        | The port number of the primary syslog server. It can be any available port number. Valid port numbers are integers between 1 and 65535.                                                                                                                                                                                                                                                                                                       |
| <b>Primary Backup Syslog Server</b>                    | no        | The hostname or the IP address of the primary backup syslog server to send the syslog events from a CVP application when the syslog server cannot be reached.                                                                                                                                                                                                                                                                                 |
| <b>Primary Backup Syslog Server Port Number</b>        | no        | The port number of the primary backup syslog server. It can be any available port number. Valid port numbers are integers between 1 and 65535.                                                                                                                                                                                                                                                                                                |
| <b>Configuration: Secondary Syslog Server Settings</b> |           |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Secondary Syslog Server</b>                         | no        | The hostname or the IP address of the secondary syslog server to send the syslog events from a CVP application.                                                                                                                                                                                                                                                                                                                               |
| <b>Secondary Syslog Server Port Number</b>             | no        | The port number of the secondary syslog server. It can be any available port number. Valid port numbers are integers between 1 and 65535.                                                                                                                                                                                                                                                                                                     |
| <b>Secondary Backup Syslog Server</b>                  | no        | The hostname or the IP address of the secondary backup syslog server to send the syslog events from a CVP application when the syslog server cannot be reached.                                                                                                                                                                                                                                                                               |
| <b>Secondary Backup Syslog Server Port Number</b>      | no        | The port number of the secondary backup syslog server. It can be any available port number. Valid port numbers are integers between 1 and 65535.                                                                                                                                                                                                                                                                                              |

**Step 3** Click **Save**.



## Unified CVP Security

### Secure GED 125 Communication between Call Server and ICM

You can secure GED 125 communication by:

- Exchanging the self-signed certificates between the components.
- Signing the certificates by a Certificate Authority.



**Note** By default, mutual authentication between ICM and Call Server is enabled. To disable mutual authentication, go to `%CVP_HOME%\conf\icm.properties` and set the **ICM.Security.UseClientAuth** property to *FALSE* and restart the Call Server.

#### Before you begin:

For generating ECDSA certificates in ICM, refer to the *How to enable ECDSA for Unified CCE core components* section in the *Security Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.6(1)* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html>.

### Self-Signed Certificates

#### Generate Certificate on CVP Call Server

##### Procedure

- 
- Step 1** <http://acrsrv-app-prd-01:8080/>Export the Call Server certificate by running `%CVP_HOME%\jre\bin\keytool.exe -export -v -keystore %CVP_HOME%\conf\security\keystore -storetype JCEKS -alias callserver_certificate -file %CVP_HOME%\conf\security\<callserver_certificate>`
- Step 2** Enter the keystore password when prompted.
- Step 3** Restart the Call Server service to load the new certificates.
- 

#### Import Certificate into ICM

##### Procedure

- 
- Step 1** Copy the self-signed CVP Call Server certificate downloaded from CVP to the ICM box (PG).
- Step 2** Open the command prompt and go to `c:\icm\bin`.
- Step 3** Type `CiscoCertUtil.exe /install <callserver_certificate>`.  
This imports the certificate to the Trusted Root Certification Authorities.

**Note** Repeat the procedure for multiple PIMs and for Side A and Side B.

---

## Generate Certificate on ICM Server

**Before you begin**

If there is an existing host.pem certificate in `c:\icm\ssl\certs`, then skip the following procedure and go to the Section, On Call Server.

**Procedure**


---

**Step 1** Log into the ICM (PG) box. Go to the command prompt and type **CiscoCertUtil.exe /generatecert**.

```
C:\icm\bin>ciscocertutil.exe /generatecert
SSL config path = C:\icm\ssl\cfg\openssl.cfg
SYSTEM command is C:\icm\ssl\bin\openssl.exe req -x509 -newkey rsa:2048 -days 7300 -nodes
-subj /CN=PG-SIDEA.pcce.com -out
C:\icm\ssl\certs\host.pem -keyout C:\icm\ssl\keys\host.key
Generating a 2048 bit RSA private key
.....
....
writing new private key to 'C:\icm\ssl\keys\host.key'
.....
Certificate path: C:\icm\ssl\certs\host.pem , Key path: C:\icm\ssl\keys\host.key
```

The client certificate and key are generated and stored as host.csr and host.key in `C:\icm\ssl\certs` folder.

**Step 2** Cycle VRU PG.

---

## Import ICM Certificate into CVP Call Server

**Procedure**


---

**Step 1** Log into the CVP Call Server box. Create a folder and copy host.pem to `c:\IcmCertificate`.

**Step 2** From the command prompt, run **%CVP\_HOME%\jre\bin\keytool.exe -import -v -alias icm\_certificate -storetype JCEKS -trustcacerts -keystore %CVP\_HOME%\conf\security\keystore -file c:\IcmCertificate\host.pem**.

**Step 3** Enter the keystore password when prompted. Click **Yes**.

**Step 4** Restart the Callserver service to load the new certificates.

**Note** Repeat the procedure if you have multiple Call Servers.

---

## CA Certificates

## Generate CA Certificate on CVP Call Server

Log in to the Call Server. Retrieve the keystore password from the `security.properties` file.



**Note** At the command prompt, enter **more %CVP\_HOME%\conf\security.properties**.  
 Security.keystorePW = <Returns the keystore password>  
 Enter the keystore password when prompted.

## Procedure

- Step 1** Remove the existing certificate by running the following command:
- ```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore
%CVP_HOME%\conf\security\keystore -delete -alias callserver_certificate
```
- Step 2** Enter the keystore password when prompted.
- Step 3** Generate a new key pair for the alias with the selected key size by running
- ```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore
%CVP_HOME%\conf\security\keystore -genkeypair -alias callserver_certificate -v -keysize 2048
-keyalg RSA.
```
- Enter keystore password: <enter the keystore password>  
 What is your first and last name?  
 [Unknown]: <Specify the FQDN of the CVP server. Example: cisco-cvp-211@example.com >  
 What is the name of your organizational unit?  
 [Unknown]: <specify OU> E.g. CCBU  
 What is the name of your organization?  
 [Unknown]: <specify the name of the org> E.g. CISCO  
 What is the name of your City or Locality?  
 [Unknown]: <specify the name of the city/locality> E.g. BLR  
 What is the name of your State or Province?  
 [Unknown]: <specify the name of the state/province> E.g. KAR  
 What is the two-letter country code for this unit?  
 [Unknown]: <specify two-letter Country code> E.g. IN
- Specify 'yes' for the inputs.
- Step 4** Generate the CSR certificate for the alias by running **%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\keystore -certreq -alias callserver\_certificate -file %CVP\_HOME%\conf\security\callserver.csr** and save it to a file (for example, callserver.csr).
- Step 5** Enter the keystore password when prompted.
- Step 6** Download the callserver.csr from %CVP\_HOME%\conf\security\ and sign it from CA.
- Step 7** Copy the root CA certificate and the CA-signed certificate to %CVP\_HOME%\conf\security\.
- Step 8** Install the root CA certificate by running **%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\keystore -import -v -trustcacerts -alias root -file %CVP\_HOME%\conf\security\.**
- Step 9** Enter the keystore password when prompted.
- Step 10** Install the signed certificate by running **%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\keystore -import -v -trustcacerts -alias callserver\_certificate -file %CVP\_HOME%\conf\security\.**

## Import Root CA Certificate into ICM

**Procedure**

- 
- Step 1** Copy the root CA certificate to the ICM (PG) box.
- Step 2** Open the command prompt and go to `c:\cisco\icm\bin`.
- Step 3** Type **CiscoCertUtil.exe /install rootCA.pem**.  
This imports the certificate to the Trusted Root Certification Authorities.
- 

## Generate CA Certificate on ICM

**Procedure**

- 
- Step 1** Navigate to `C:\icm\ssl\keys` and remove the old 'host.key'(if available).
- Step 2** Log into the ICM (PG) box. Go to the command prompt and type **CiscoCertUtil.exe /generateCSR**.

```
C:\icm\bin>CiscoCertUtil.exe /generateCSR
SSL config path = C:\icm\ssl\cfg\openssl.cfg
SYSTEM command is C:\icm\ssl\bin\openssl.exe req -new -key C:\icm\ssl\keys\host.key -out
C:\icm\ssl\certs\host.csr
```

```
Generating a 2048 bit RSA private key
```

```
.....
.....
```

```
writing new private key to 'C:\icm\ssl\keys\host.key'
```

```

```

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or a DN.
```

```
There are quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
```

```
If you enter '.', the field will be left blank.
```

```

```

```
Country Name (2 letter code) [AU]:IN
```

```
State or Province Name (full name) [Some-State]:KA
```

```
Locality Name (eg, city) []:BLR
```

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cisco
```

```
Organizational Unit Name (eg, section) []:ccbu
```

```
Common Name (e.g. server FQDN or YOUR name) []:abc.com
```

```
Email Address []:radmohan@cisco.com
```

```
Please enter the following 'extra' attributes
```

```
to be sent with your certificate request
```

```
A challenge password []:*****
```

```
An optional company name []:cisco
```

The client certificate and key are generated and stored as `host.csr` and `host.key` in `C:\icm\ssl\certs` and `C:\icm\ssl\keys` folders respectively.

- Step 3** Sign it from a CA. Follow the procedure [Import Root CA Certificate into ICM, on page 186](#).

- Note**
- Remove the existing `host.pem` (if any) from `C:\icm\ssl\certs`.
  - Save `host.cer` (CA-signed) as `host.pem` in `C:\icm\ssl\certs`.

- Step 4** From the command prompt, run `C:\icm\bin>CiscoCertUtil.exe /install c:\icm\ssl\certs\host.pem`.
- Step 5** Cycle VRU PG.

### Secure SIP Communication between Call Server and Cisco VVB

You can secure SIP communication by:

- Exchanging the self-signed certificates between the components.
- Signing the certificates by a Certificate Authority.

#### Self-Signed Certificates

##### On Call Server

Log in to the Call Server, retrieve the keystore password from the *security.properties* file.



**Note** At the command prompt, enter `more %CVP_HOME%\conf\security.properties`.

Security.keystorePW = <Returns the keystore password>

Enter the keystore password when prompted.

#### Procedure

- Step 1** Export the Call Server certificate by running `%CVP_HOME%\jre\bin\keytool.exe -export -v -keystore %CVP_HOME%\conf\security\keystore -storetype JCEKS -alias callserver_certificate -file %CVP_HOME%\conf\security\<callserver_certificate.cer>`.
- Step 2** Enter the keystore password when prompted.
- Step 3** Copy the VVB/VXML gateway self-signed certificate to `%CVP_HOME%\conf\security\` and import the certificate to the callserver keystore by running `%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP_HOME%\conf\security\keystore -storetype JCEKS -alias vb_cert -file %CVP_HOME%\conf\security\<vvb certificate>`.
- Note** See Step 5 of the *On Cisco VVB* section to download a VVB certificate.
- Step 4** Enter the keystore password when prompted.  
A message appears on the screen: Trust this certificate? [no]: Enter **yes**.
- Step 5** Use the list flag to check your keystore entries by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -list`.

##### On Cisco VVB

## Procedure

---

- Step 1** Copy the CVP CallServer self-signed certificate downloaded from CVP and upload it to VVB against tomcat-trust.
  - Step 2** Go to **OS Admin > Security > Certificate Management > Upload certificate/certificate chain**.
  - Step 3** In **Certificate Purpose**, select **tomcat-trust**.
  - Step 4** Select the self-signed certificate of the Call Server and click **Upload**.
  - Step 5** Download the self-signed certificate of the VVB.
  - Step 6** Go to **OS Admin > Security > Certificate Management**.
  - Step 7** In the **Certificate** column, find the certificate named **tomcat**.
  - Step 8** Select the self-signed tomcat certificate and click **Download**.
  - Step 9** After the new certificate is uploaded, restart the node(s) using the CLI command **utils system restart**.
  - Step 10** Go to **Cisco VVB Administration > System Parameters > TLS**.
  - Step 11** Check TLS as **Enable**.
  - Step 12** Select the supported TLS version and click **Update**.
  - Step 13** Restart Cisco VVB Engine from the **VVB Serviceability** page.
- 

## CA-Signed Certificate

### On Call Server

Log in to the Call Server. Retrieve the keystore password from the *security.properties* file.



- 
- Note** At the command prompt, enter **more %CVP\_HOME%\conf\security.properties**.
- Security.keystorePW = <Returns the keystore password>
- Enter the keystore password when prompted.
- 

### On Cisco VVB

## Procedure

---

- Step 1** To generate the CSR certificate on VVB, open the administration page. From the **Navigation** drop-down list, choose **Cisco Unified OS Administration** and click **Go**.
- Step 2** Go to **Security > Certificate Management > Generate CSR Generate Certificate signing Request**. Create the CSR against tomcat with the key-length as 2048.
- Step 3** To download the generated CSR, click **Download CSR**. After the **Generate Certificate signing Request** dialog opens, click **Download CSR**.
- Step 4** Open the certificate in Notepad, copy the contents and sign the certificate with CA.
- Step 5** Upload the root certificate generated from the CA into VVB against tomcat-trust:
  - a) Go to **Security > Certificate Management > Generate CSR > Upload certificate/certificate chain**.
  - b) Choose **tomcat-trust** from the drop-down list.

- c) Click **Browse** and select the certificate.
- d) Click **Upload** to upload the root certificate of the Certificate Authority.

- Step 6** Upload the signed certificate into VVB against tomcat.
- a) Go to **Security > Certificate Management > Upload certificate/certificate chain**.
  - b) Choose **tomcat** from the drop-down list.
  - c) Click **Browse** and select the certificate.
  - d) Click **Upload**.

After the certificate is uploaded successfully, VVB displays the certificate signed by <CA hostname>.

- Step 7** Restart the Tomcat service and the VVB engine.

---

For the configuration steps, see the *Manage System Parameters* section.

### Secure HTTP Communication between VXML Server and Cisco VVB

You can secure HTTP communication by:

- Exchanging the self-signed certificates between the VXML Server and VVB or VXML Gateway.
- Signing the certificates by a Certificate Authority.

#### Self-Signed Certificate

##### On VXML Server

Log in to the VXML Server. Retrieve the keystore password from the *security.properties* file.




---

**Note** At the command prompt, enter **more %CVP\_HOME%\conf\security.properties**.

Security.keystorePW = <Returns the keystore password>

Enter the keystore password wherever it prompts.

---

#### Procedure

- Step 1** Export the VXML SERVER certificate by running **%CVP\_HOME%\jre\bin\keytool.exe -export -v -keystore %CVP\_HOME%\conf\security\keystore -storetype JCEKS -alias vxml\_certificate -file %CVP\_HOME%\conf\security\<vxml\_certificate.cer>**.
- Step 2** Enter the keystore password when prompted.
- Step 3** Copy the VVB/VXML gateway self-signed certificate to %CVP\_HOME%\conf\security\ and import the certificate to the callserver keystore by running **keytool.%CVP\_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP\_HOME%\conf\security\keystore -storetype JCEKS -alias vb\_cert -file %CVP\_HOME%\conf\security\<vwb certificate>**.

**Note** See Step 5 of the following Section, *On Cisco VVB* to download a VVB certificate.

- Step 4** Enter the keystore password when prompted.  
A message appears on the screen: Trust this certificate? [no]: Enter **yes**.

- Step 5** Use the list flag to check your keystore entries by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -list`.
- 

On Cisco VVB

### Procedure

---

- Step 1** Copy the VXML Server self-signed certificate downloaded from CVP and upload it to VVB against tomcat-trust.
- Step 2** Go to **OS Admin > Security > Certificate Management > Upload certificate/certificate chain**.
- Step 3** In **Certificate Purpose**, select **tomcat-trust**.
- Step 4** Select the self-signed certificate of the VXML Server and click **Upload**.
- Step 5** Download the self-signed certificate of the VVB.
- Step 6** Go to **OS Admin > Security > Certificate Management**.
- Step 7** In the **Certificate** column, select the **tomcat** certificate.
- Step 8** Select the tomcat certificate and click **Download**.
- Step 9** After the new certificate uploads, restart the Cisco Tomcat service.
- Step 10** Go to **Cisco VVB Administration > System Parameters > TLS**.
- Step 11** Check the **TLS** check box as **Enable**.
- Step 12** Select the supported TLS version and click **Update**.
- Step 13** Restart the Cisco VVB Engine from the **VVB Serviceability** page.

**Note** To enable secured connection in Application Management from the Cisco VVB UI, see *Cisco Virtualized Voice Browser Administration and Configuration Guide* available at <https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/tsd-products-support-series-home.html>.

---

CA-Signed Certificate

On VXML Server

Log in to the VXML Server. Retrieve the keystore password from the *security.properties* file.



**Note** At the command prompt, enter **more %CVP\_HOME%\conf\security.properties**.  
 Security.keystorePW = <Returns the keystore password>  
 Enter the keystore password when prompted.

---

### Procedure

---

- Step 1** Remove the existing certificate by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -alias vxml_certificate`.



- Step 2** Generate a new key pair for the alias with selected key size by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypair -alias vxml_certificate -v -keysize 2048 -keyalg RSA`.
- ```

Enter keystore password: <enter the keystore password>
What is your first and last name?
  [Unknown]: <specify the CVP host name appended with "VXML_Server"> E.g
cisco-cvp-211_VXML_Server
What is the name of your organizational unit?
  [Unknown]: <specify OU> E.g. CCBU
What is the name of your organization?
  [Unknown]: <specify the name of the org> E.g. CISCO
What is the name of your City or Locality?
  [Unknown]: <specify the name of the city/locality> E.g. BLR
What is the name of your State or Province?
  [Unknown]: <specify the name of the state/province> E.g. KAR
What is the two-letter country code for this unit?
  [Unknown]: <specify two-letter Country code> E.g. IN
Specify 'yes' for the inputs.

```
- Step 3** Generate the CSR certificate for the alias by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -certreq -alias vxml_certificate -file %CVP_HOME%\conf\security\vxmlserver.csr` and save it to a file .
- Step 4** Enter the keystore password when prompted.
- Step 5** Download the vxmsvr.csr from CVP `%CVP_HOME%\conf\security\` and sign it from CA.
- Step 6** Copy the root CA certificate and the CA-signed certificate to `%CVP_HOME%\conf\security\`
- Step 7** Install the root CA certificate by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cert>`.
- Step 8** Enter the keystore password when prompted.
- Step 9** Install the signed certificate by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v -trustcacerts -alias vxml_certificate -file %CVP_HOME%\conf\security\<filename_of_CA_signed_cert>`.
- Step 10** Enter the keystore password when prompted.
- Step 11** Restart the VXML Server.

On Cisco VVB

Procedure

- Step 1** Upload the root certificate generated from the CA into VVB against tomcat-trust. Go to **OS Admin > Security > Certificate Management > Upload certificate/certificate chain**, select **tomcat-trust** and upload the root certificate of the Certificate Authority.
- Note** If you use the same root certificate that was used in the Call Server configuration as described in Section, Secure Communication between Call Server and Cisco VVB and the certificate is already imported, then you can skip this step.
- Step 2** Generate the CSR against tomcat with the key-length as 2048.
- Step 3** Open the certificate in Notepad. Copy the contents and sign the certificate with CA.

Step 4 Restart the Tomcat service and the VVB engine.

To enable secure communications on the VXML Server, see Unified CVP VXML Server Setup *Administration Guide for Cisco Unified Customer Voice Portal* available at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html>.

To enable secure communications on the VXML Server (standalone), see Unified CVP VXML Server (Standalone) Setup *Administration Guide for Cisco Unified Customer Voice Portal* available at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html>.

Secure HTTPS Communication between Media Server and Cisco VVB

This section describes how to import certificate from IIS MediaServer to Cisco VVB and how to import IIS CA-signed certificate.

Procedure

-
- Step 1** Enter `https://<mediaserver>:443/` in the address bar of the web browser.
- Step 2** In the **Security Alert** dialog box, click **View Certificate**.
- Step 3** Click the **Details** tab
- Step 4** Click **Copy to File**.
- Step 5** In the **Certificate Export Wizard** dialog box, click **Base-64 encoded X.509 (.CER)**, and then click **Next**.
- Step 6** In the **File to the Export** dialog box, specify a file name, and then click **Next**.
- Step 7** Click **Finish**.
A message indicates that the export was successful.
- Step 8** Click **OK** and close the **Security Alert** dialog box.
- Step 9** Copy the CVP MediaServer self-signed certificate downloaded from the CVP and upload into VVB against **tomcat-trust**.
- Step 10** Go to **OS Admin > Security > Certificate Management > Upload certificate/certificate chain > In Certificate Purpose*** select **tomcat-trust**, choose the self-signed certificate of the Call Server and press **Upload** button.
- Step 11** Restart Cisco VVB Engine.
-

Secure Communication on CUCM

You can secure communication on CUCM by:

- Exchanging the self-signed certificates.
- Signing the certificates by a Certificate Authority.

Self-Signed Certificate

Procedure

- Step 1** Log in to the CUCM OS Administration page.
- Step 2** Go to **Security > Certificate Management**.
- Step 3** Click **Generate Self-signed**.
- Step 4** On the pop-up window, click **Generate** button.
- Step 5** Restart Tomcat from CUCM CLI by running **utils service restart Cisco Tomcat**.

Note Tomcat will take a few minutes to stop and then start. If you access the CUCM UI during this time, you may receive a 404 error.

- Step 6** When the CUCM UI is available, open the CUCM OS Administration page.
 - Step 7** Go to **Security > Certificate Management**.
 - Step 8** Click **Find** and identify the Self-signed certificate generated by the system.
 - Step 9** Click the CallManager Certificate name.
 - Step 10** In the dialog box, click **Download**.
-

CA-Signed Certificate

To configure TLS and SRTP, see *Security Guide for Cisco Unified Communications Manager 11.6* available at <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>

Procedure

- Step 1** Enter the following command in the CLI to set the CUCM in the mixed mode, and to register the endpoints in the encrypted mode:

```
admin: utils ctl set-cluster mixed-mode
```

```
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n):y
```

```
Moving Cluster to Mixed Mode
```

```
Cluster set to Mixed Mode
```

```
You must reset all phones to ensure they received the updated CTL file.
```

```
You must restart Cisco CTIManager services on all the nodes in the cluster that have the service activated.
```

```
admin:
```

- Step 2** Choose **CUCM Admin Page > System > Enterprise Parameters**. Check if **Cluster Security Mode** is set to 1.

- Step 3** Set the minimum TLS version command from the CLI:

```
admin:set tls client min-version 1.2
```

```
**WARNING** If you are lowering the TLS version it can lead to security issues **WARNING**
```

```
Do you really want to continue (yes/no)?y
```

```
Run this command in the other nodes of the cluster.
```

Restart the system using the command 'utils system restart' for the changes to take effect

```
Command successful
admin:set tls ser
admin:set tls server mi
admin:set tls server min-version?
Syntax:
set tls server min-version
```

```
admin:set tls server min-version 1.2
```

****WARNING**** If you are lowering the TLS version it can lead to security issues ****WARNING****

Do you really want to continue (yes/no)?**y**
Run this command in the other nodes of the cluster.

Restart the system using the command 'utils system restart' for the changes to take effect

```
Command successful
admin:
```

- Step 4** Create an encrypted phone profile and the SIP trunk profile. Associate them with the phone and CUCM SIP trunk.
- Step 5** Go to **System > Security > SIP Trunk Security Profile** and create a new SIP trunk security profile.
- Step 6** On CUCM SIP Trunk, check the **SRTP Allowed** check box.
- Step 7** From **SIP Trunk Security Profile** drop-down list, choose **TLS Secure Profile**.
- Step 8** Restart the TFTP and Cisco CallManager services on all the nodes in the cluster that run these services.
- Step 9** Upload the root certificate generated from the CA to CUCM against CUCM-trust.
- Step 10** Generate the CSR against CallManager and select the key-length as 2048.
- Step 11** Sign the certificate on a CA <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/118731-configure-san-00.html>.
- Step 12** Click **Upload Certificate** on CUCM by selecting the certificate name as **CallManager**.
On successful completion, CUCM displays the description as *Certificate signed by <CA hostname>*.
- Step 13** Restart TFTP and Cisco CallManager services on all the nodes in the cluster that run these services.

Secure Communication between Ingress Gateway and Call Server

You can secure communication between the Ingress Gateway and the Call Server by:

- Exchanging the self-signed certificates.
- Signing the certificates by a Certificate Authority.

Self-Signed Certificate

To secure SIP connection between Cisco Ingress Gateway and Call Server, import the Call Server certificate on the IOS device during the device configuration.

Procedure

- Step 1** Open the certificate that was exported in [Step 1, on page 187](#).

- Step 2** Click **View Certificate**.
- Step 3** Click the **Details** tab.
- Step 4** Click **Copy to File**.
The **Certificate Export Wizard** window appears.
- Step 5** Click **Base-64 encoded X.509 (.CER)**, and then click **Next**.
- Step 6** Specify a file name in the **File to the Export** dialog box, and then click **Next**.
- Step 7** Click **Finish**. A message indicates that the export was successful.
- Step 8** Click **OK** and close the **Security Alert** dialog box.
- Step 9** Open the certificate in Notepad.
- Step 10** Access the IOS ingress GW in the privileged EXEC mode.
- Step 11** Access the global configuration mode by entering the configuration terminal.
- Step 12** Import the CVP CallServer Certificate to Cisco IOS Gateway by entering the following commands:
- ```
crypto pki trustpoint <Call Server trust point name>
enrollment terminal

exit
```
- Step 13** Open the exported Call Server certificate in Notepad and copy the certificate information that appears between the -BEGIN CERTIFICATE and END CERTIFICATE tags to the IOS device.
- Step 14** Enter the following command:
- ```
crypto pki auth <Call Server trust point name>
```
- Step 15** Paste the certificate from Notepad and end with a blank line or the word *quit* on a line by itself.
- Step 16** To generate the self-signed certificate of the Gateway, first generate 2048-bit RSA keys:
- ```
crypto key generatersageneral-keys Label <Your Ingress GW trustpointname> modulus 2048
```
- Step 17** Configure a trustpoint:
- ```
crypto pkitrustpoint<Your Ingress GW trustpointname>
enrollment selfsigned
fqdn none
subject-name CN=SIP-GW
rsaakeypair <Your Ingress GW trustpoint name>
```
- ```
Router(config)# crypto pki enroll<Your Ingress GW trustpointname>
% The fully-qualified domain name will not be included in the certificate
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes
Router Self Signed Certificate successfully created
```
- Step 18** View the certificate in PEM format, and copy the Self-signed CA certificate (output starting from “----BEGIN” to “CERTIFICATE----”) to a file named *ingress\_gw.pem*.
- ```
Router(config)# crypto pki export <Your Ingress GW trustpoint name> pem terminal
% Self-signed CA certificate:
----BEGIN CERTIFICATE-----
MIIB6zCCAUSgAwIBAgIBAjANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZTSVAt
R1cwHhcNMTCwOTI2MTQ1MTE2WhcNMjAwMTAxMDAwMDAwWjARMQ8wDQYDVQQDEwZT
SVAtR1cwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKdSDxIj8T6UaYxgujMk
9B2d5dq3Ni8s1e4yfsSB11bJ/AQk+aLDfE3/BeVkeXEjRCohhnZcEnMV4DdOPxj7
9MWzoJgxkMj7X3I6ijaL20112iQuBcjqYtAUP1xB3VTjqLMbxG30fb7xLCDTuo5
s07TLsElAbxrbrH62Za/C0e5AgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMBAF8wHwYD
```

```
VR0jBBGwFoAU+tJphvbvvc7yE6uqIh7VlgTrtPswHQYDVR0OBBYEFPrSaYb274HO
8hOrqiIe1zYE67T7MA0GCSqGSIs3DQEBBQUAA4GBADRAw930QErMEgRGWJJVLLbs
n8XnSbiw1k8KeY/AzgxBoBJtc0FKs4L0XUOE6eHUKCHoks1FDV211MM1zPe7MAC
vDd7EV/abx2UdFSL9jjm/YzIleVUj8b0T3qNSfOqDtV5CyCjPichNa2eCR1bTmGx
o3HqLeEl/+66L/174nlT
-----END CERTIFICATE-----
```

```
% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIB6zCCAUSgAwIBAgIBAjANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZTSVAt
R1cwHhcNMTcwOTI2MTQ1MTE2WhcNMjAwMTAxMDAwMDAwWjARMQ8wDQYDVQQDEwZT
SVAtR1cwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKdSDxIj8T6UaYxgujMk
9B2d5dq3Ni8s1e4yfsSB1lbJ/AQk+aLDfE3/BeVkeXEjRCohhnZcEnMV4DdOPxj7
9MWzoJgxmKj7X3I6ijaL20l12iQuBcjiqYtAUP1xB3VTjqLMbxG30fb7xLCDTuo5
s07TLsElAbxrbrH62Za/C0e5AgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMBAf8wHwYD
VR0jBBGwFoAU+tJphvbvvc7yE6uqIh7VlgTrtPswHQYDVR0OBBYEFPrSaYb274HO
8hOrqiIe1zYE67T7MA0GCSqGSIs3DQEBBQUAA4GBADRAw930QErMEgRGWJJVLLbs
n8XnSbiw1k8KeY/AzgxBoBJtc0FKs4L0XUOE6eHUKCHoks1FDV211MM1zPe7MAC
vDd7EV/abx2UdFSL9jjm/YzIleVUj8b0T3qNSfOqDtV5CyCjPichNa2eCR1bTmGx
o3HqLeEl/+66L/174nlT
-----END CERTIFICATE-----
```

Step 19 Test your certificate.

```
show crypto pkicertificates
```

Step 20 To configure TLS version on the Gateway:

```
router# configure terminal
router(config)# sip-ua
router(config-sip-ua)# transport tcp tls <version>
v1.0 Enable TLS Version 1.0
v1.1 Enable TLS Version 1.1
v1.2 Enable TLS Version 1.2
```

Note: SIP TLS version 1.2 is available in Cisco IOS Software Release 15.6(1)T and higher.

Step 21 To check if the TLS version is negotiated:

```
router# show sip-ua connections tcp tls detail
```

Step 22 To enable SRTP on the incoming/outgoing dial-peer, specify SRTP:

```
router# configure terminal
router(config)# dial-peer voice 100 voip
router(config-dial-peer)# srtp
```

Note: This command is supported in Cisco IOS Software Release 15.6(1)T and higher.

Step 23 Configure the SIP stack in Cisco IOS GW to use the self-signed certificate of the router to establish a SIP TLS connection from/to the CVP Call Server.

```
router# configure terminal
router(config)# sip-ua
router(config-sip-ua)# crypto signaling remote-addr <peer IP address> <peer subnet mask>
trustpoint <Your Ingress GW trustpoint name> strict-cipher
```

Example:

```
sip-ua
crypto signaling remote-addr 10.48.54.89 255.255.255.255 trustpoint VG-SIP-1 strict-cipher
```

Step 24 Configure an outbound VoIP dial-peer to route calls to the CVP Call Server.

```
session target ipv4:<Call Server IP address>:5061
session transport tcp tls
```

Example:

```
dial-peer voice 3 voip
destination-pattern 82...
session protocol sipv2
session target ipv4:10.48.54.89:5061
session transport tcp tls
dtmf-relay rtp-nte
codec g711ulaw
```

Step 25 To import GW or CUSP certificate into the CVP Call Server:

- a) Copy the Ingress GW/CUSP self-signed certificate to %CVP_HOME%\conf\security\ and import the certificate to the callserverkeystore. %CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP_HOME%\conf\security\keystore -storetype JCEKS -alias gw_cert -file %CVP_HOME%\conf\security\<ingress GW\CUSP certificate name>
- b) Enter the keystore password when prompted.
- c) A message appears on the screen: Trust this certificate? [no]: Enter yes.
- d) Use the list flag to check your keystore entries by running %CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -list

Step 26 To change the supported TLS version from Unified CCE Administration, see [CVP Server Services Setup, on page 174](#).

Step 27 Restart the Call Server.

CA-Signed Certificate

For the configuration steps, see the latest *Cisco Unified Border Element Configuration Guide* available at <https://www.cisco.com/c/en/us/support/unified-communications/unified-border-element/products-installation-and-configuration-guides-list.html>.

Before you begin

- To configure SIP TLS and SRTP on the gateway, apply a security-k9 license on the gateway.
- Time sync all the nodes (CVP, VVB, Gateway) with an NTP server.

Procedure

Step 1 Create a 2048-bit RSA key.

```
Router(config)# crypto key generate rsa general-keys Label <name of the key pair> modulus
2048
Generates 2048 bit RSA key pair.
```

Step 2 Create a trustpoint. A trustpoint represents a trusted CA.

Example:

```
Router(config)# crypto pki trustpoint ms-ca-name
Creates the trustpoint.
```


Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END CERTIFICATE-----
quit
% Router Certificate successfully imported
```

Step 7 Test your certificate.

```
show crypto pki certificates
```

Note

- To configure TLS version on the gateway:

```
router#
router# config terminal
router(config)# sip-ua
router(config-sip-ua)# transport tcp tls <version>
v1.0 Enable TLS Version 1.0
v1.1 Enable TLS Version 1.1
v1.2 Enable TLS Version 1.2
```

- To check if the TLS version is negotiated:

```
router# show sip-ua connections tcp tls detail
```

- To enable SRTP on the incoming/outgoing dial-peer, specify srtp:

```
router# configure terminal
router(config)# dial-peer voice 100 voip
router(config-dial-peer)# srtp
```

Step 8 Associate the created trustpoint in Step 2 with sip-ua.

```
router# configure terminal
router(config)# sip-ua
router(config-sip-ua)# crypto signaling remote-addr <peer IP address>
<peer subnet mask> trustpoint <trust point name created in step2>
```

Note Installing CVP Call/VXML Servers enables IIS (for media server functionality), which opens port 443 by default for TLS connections. This port allows TLSv1.0 and TLSv1.1 connections. To close these connections, change the **Enabled** value to 0 by selecting the **Decimal** option in the following registry keys:

- **TLSv1.0:** HKEY-LOCAL-MACHINE
 \SYSTEM\CurrentControlSet\Control\SecurityProviders\
 SCHANNEL\Protocols\TLS1.0\Server\Enabled
- **TLSv1.1:** HKEY-LOCAL-MACHINE\
 SYSTEM\CurrentControlSet\Control\SecurityProviders\
 SCHANNEL\Protocols\TLS1.1\Server\Enabled

This disables ports 443 and 3389 for TLSv1.0 and TLSv1.1 server-side connections. While Windows 8 and Windows Server 2012 remote desktop clients work by default, Windows 7 and Windows Server 2008 remote desktop clients cannot connect to these servers for the RDP port (3389). To re-enable this port, install the patch available at <https://support.microsoft.com/en-us/help/3080079/update-to-add-rds-support-for-tls-1-1-and-tls-1-2-in-windows-7-or-wind>.

Secure Communication on CUSP

You can secure communication on CUSP by:

- Exchanging the self-signed certificates between the components.
- Signing the certificates by a Certificate Authority.

Self-Signed Certificate

For the configuration steps, see the latest *CLI Configuration Guide for Cisco Unified SIP Proxy* https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cusp/rel9_0/cli_configuration/cusp_cli_config/configuration.html#72360.

CA-Signed Certificate

Procedure

Step 1 Create an RSA keypair in CUSP. From the CUSP foundation, enter the config mode and create the keypair:
democusp48(config)# crypto key generate rsa label <key-label> modulus 2048 default

Example

```
democusp48# conf terminal
democusp48(config)# crypto key generate rsa label cusp48-ca modulus 2048 default
Key generation in progress. Please wait...
The label name for the key is cusp48-ca
```

Step 2 Generate CSR signed by CA by running **democusp48(config)# crypto key certreq label <key-label> url ftp:**

An FTP or HTTP server is required to export the CSR. Make sure the label in the command matches the label used to create the rsa private key.

Example

```
democusp48(config)# crypto key certreq label cusp48-ca url ftp:
Address or name of remote host? 10.64.82.176
Username (ENTER if none)? test
Password (not shown)?
Destination path? /cusp48-ca.csr Uploading CSR file succeed
democusp48(config)#
```

- Step 3** Import the CA server root certificate into CUSP by running: **crypto key import trustcert label <rootCA-label> terminal.**

Example

```
democusp48(config)# crypto key import trustcert label rootCA terminal
Enter certificate...
End with a blank line or "quit" on a line by itself
-----BEGIN CERTIFICATE----- MIIEdTCCA12gAwIBAgIQaO1+pgDsy51NqtF3E
epB4TANBgkqhkiG9w0BAQUFADBC MRMwEQYKZCZImiZPyLQGBGRYDY29tMRcwFQYK
CZImiZPyLQGBGRYHQVJUR1NPTDES MBAGA1UEAxMjU01QUEhPTklyMB4XDTA3MDC
xMzExNTAyMVoXDTEyMDCxMzExNTgz MVowQjETMBEGCgMSJomT8ixkARKWA2NvbT
EXMBUGCgMSJomT8ixkARKWB0FSVEdT T0wxEjAQBGNVBAMTCVNUJUFBIT05JWDCCA
SIwDQYJKoZIhvcNAQEBBQADggEPADCC AQoCggEBAKbepxqDVZ5uWUVMWx8VaHVG
geg4CgDbzCz8Na0XqI/0aR91Imgx1Jnf ZD0nP1QvgUFSZ2m6Ee/pr2SkJ5kJSZo
zSmz2Ge4sKjZzbgQHmljWv1DswVDw0nyV F71ULTaNPsh81JVF5t2lqm75UnkW4x
P5qQn/rgfXv/Xse9964kiZhZYjtt2Ixt2V3imhh1i228YTihnTY5c3L0vD30v8dH
newsACKd/XU+czw8feWguXXCTovvXHIBFeHvLCk9FLDoV8n9FAIHWZRPnt+HQjsD
s+jaB3F9MPVYXYElpmWrpEPHUPNZG4LsFi 6tQtiRP2UANUKXZ9fvGZMXHCZOZJi
FUCaWEAAaOCAUWggFhMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA
1UdDgQWBRR39nck+fjRuAbWEof5na/+Sf58STCCAQ4GA1UdHwSQAQuWggEBMIH+o
IH7oIH4hoG4bGRhcDovLy9DTj1TSVBQSE90 SVgsQ049U01QUEhPTklyLULORE1B
LENOPUNEUCxDtj1QdWJsaW1MjBLZXXk1MjBT ZXJ2aWN1cyxDTj1TZXJ2aWN1cyx
DTj1Db25maWdlcmF0aW9uLERDPUFSVEdTT0ws REM9Y29tP2N1cnRpZmljYXRlUm
V2b2NhdG1vbXkxpc3Q/YmFzZT9vYmplY3RDbGFz czljUkxkaEaXN0cmliidXRpb25Qb
2ludIY7aHR0cDovL3NpcHBob25peC1pbmRpYS5h cnRnc29sLmNvbS9DZXJ0RW5y
b2xsL1NlUUFBIT05JWC5jcmwwEAYJKwYBAGCNxUB BAMCAQAwDQYJKoZIhvcNAQEB
FBQADggEBAHua4/pwvSZ48MnNZKdsW9hvuTV4jwTGErgc16bOR0Z1urRFIFr2NCP
yzZboTb+Z11kQFDMRPBoBwOvr7BciVyoTo7AKFheqYm9asXL18A6XpK/WqLj1CcX
rdzF8ot0o+dK05sd9ZG7hRckRhFPwwj5Z7z0Vsd/jc051Qjps4rzMZXXK2FnRvng
d5xmp4U+yJtPyr8g4DyAP2/UeSKe0SEYoTV5x5FpdyF4veZneB7+zffntWff4xwi
obf+UvW47W6pCj5nGLMBzOiaxeQ8pre+yjipL2ucWK4ynOfKzZ4X1kfkfITDSogQ
AlAS1quQVbKTKk+qLGD6M12P0LrcKQk=
-----END CERTIFICATE-----
Certificate info
*****
Owner: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
Issuer: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
Certificate fingerprint (MD5): 41:A2:31:9D:97:AF:A8:CA:60:FC:46:95:82:DE:78:03
Do you want to continue to import this certificate, additional validation will be perform?
[y/n]: y
democusp48(config)#
```

- Step 4** Import the signed certificate into CUSP by running **crypto key import cer label <key-label> url terminal.**

Example

```
democusp48(config)# crypto key import cer label cusp48-ca terminal
Enter certificate...
End with a blank line or "quit" on a line by itself
-----BEGIN CERTIFICATE----- MIIITCCBAmgAwIBAgIKGI1fqqAAAAAEDAN
BgkqhkiG9w0BAQUFADBCMRMwEQYK CZImiZPyLQGBGRYDY29tMRcwFQYKZCZImiZ
PyLQGBGRYHQVJUR1NPTDESMBAGA1UE AxMJU01QUEhPTklyMB4XDTA4MTIwOTA5M
```

```

DExOV0XDTA5MTIwOTA5MTExOVowYTEL MAkGA1UEBhMCJycxCzAJBgNVBAGTAicn
MQswCQYDVQHEwInJzELMAkGA1UEChMC JycxCzAJBgNVBAsTAicnMR4wHAYDVQQ
DExVTT0xURVNUQ0MuYXJ0Z3NvbC5jb20w gZ8wDQYJKoZIhvcNAQEBBQADgY0AMI
GJAoGBAOZz88nK51bJYjWgvuv4Wx1CGxTN YWgyNg+vDyQgKBXLL7b1CqBx1Yj14
eet04LiKkW/y4jSv3nCxCAdOrMvVF5lxFmY baMlR1R/qMCLzAMvmsWlH6VY4rcf
FGkjed3zCcI6BJ6fG9H9dt1J+47iM7SdZYz/ NrEqDnrpoHaUxdz1AgMBAAGjggJ
8MIICeDAdBgNVHQ4EFgQUYXLMfiZJP29UZ3w Mpj0e79sk4EwHwYDVROjBBgwFo
AUd/ZwpPhY0bgG1hKH+Z2v/kn+fEkwggEOBGNV HR8EggEFMIIBATCB/qCB+6CB+
IaBuGxkYXA6Ly8vQ049U01QUEhPTklYLENOPVNJ UFBIT05JWC1JTkRJSxDTj1D
RFAsQ049UHvibGljJTIwS2V5JTIwU2VydmljZXMs Q049U2VydmljZXMsQ049Q29
uZmlndXJhdGlvbixEQz1BU1RHU09MLERDPWNvbT9j ZXJ0aWZpY2F0ZVJldm9jYX
Rpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlz dHJpYnV0aW9uUG9pbnsGO
2h0dHA6Ly9zaXBwaG9uaXgtaw5kaWEuYXJ0Z3NvbC5j b20vQ2VydEVucm9sbC9T
SVBQSE9OSVguY3JSMIIBIqYIKwYBBQUHAQEgEgEUMIIB EDCBqAYIKwYBBQUHMAK
GgZtsZGFwOi8vL0NOPVNJUFBIT05JWCxDTj1BSUESQ049 UHVibGljJTIwS2V5JTI
IwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJh dGlvbixEQz1BU1RHU
09MLERDPWNvbT9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0 Q2xhc3M9Y2VydGlm
aWNhdGlvbklFldGhvcml0eTBjBgggrBgEFBQcwAoZXAHR0cDov L3NpcHBob25peC1
pbmRpYS5hcnRnc29sLmNvbS9DZXJ0RW5yb2xsL1NlJUFBIT05J WC1JTkRJSx5BU1
RHU09MLmNvbV9TSVBQSE9OSVguY3J0MA0GCSqGSIb3DQEBBQUA A4IBAQAxmOMPu
eXcMYxQhVlPR/Yaxw0n2epeNRwsPP31Pr9Ak3SYSzhoMRVadJ3z K2gt4qiVV8wL
tzTO2o70JXKx+0keZdOX/DQQndxBkiBKqdJ2Qvipv8Z8k3pza31N jANnYw6FL3/
Yvh+vWCLyGehfrUfKj/7H8GaXQVapj2mDs79/zgoSyIlo+STmWFwT GQy6iFO+pv
vMcyfjv2dsuwt1M10nli0LtkIKnRGLqnkA6sJo1P6kE+Wk7n3P2 yho/Lg98q
vWl+lFRC18DrkUhpNikXsP1ld9TcJGrdJP9zG7lI5Mf3Q/2NIAx2Jzd ZVAsXZMN
smOsOrgXzkcU/xU3BXkX -----END CERTIFICATE----- Import succeeded
democusp48 (config) #exit
democusp48#

```

Step 5 You can list the certificates by running **show crypto key all**.

Example

```

democusp48# sh crypto key all
Label name: rootca
Entry type: Trusted Certificate Entry
Creation date: Sat Jul 01 14:13:14 GMT+05:30 2017
Owner: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
Issuer: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
Valid from: Wed Mar 22 14:23:10 GMT+05:30 2017 until: Tue Mar 22 14:33:09 GMT+0
5:30 2022
Certificate fingerprint (MD5): 41:A2:31:9D:97:AF:A8:CA:60:FC:46:95:82:DE:78:03

Label name: cusp48-ca
Entry type: Key Entry
Creation date: Tue Jul 04 10:47:40 GMT+05:30 2017
Owner: CN=democusp48.cvpvb.cisco.com, OU='', O='', L='', ST='', C=''
Issuer: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
SubjectAltName: DNS:democusp48.cvpvb.cisco.com
Valid from: Tue Jul 04 10:41:56 GMT+05:30 2017 until: Thu Jul 04 10:41:56 GMT+0
5:30 2019
Certificate fingerprint (MD5): 91:ED:83:CA:3B:37:16:E8:AB:07:EA:85:04:1A:D1:05

```

Configure Media Server

The following instructions are applicable for the Media Server installed in CVP and also for the Media Server installed as a separate server.

Procedure

- Step 1** Goto **Start > Administrative Tools**.
 - Step 2** Choose **Sever Manager** and click **IIS**.
 - Step 3** Right-click on the server that you want to enable FTP server and choose **Internet Information Services (IIS) Manager** option from submenu.
 - Step 4** Goto **Connections** panel:
 - a) Expand CVP server that you want to add FTP site.
 - b) Right-click on **Site** and choose **Add FTP Site** option from submenu.
 - Step 5** Enter **FTP Site Name**.
 - Step 6** Browse **C:\Inetpub\wwwroot** in **Physical Path** field and click **Next**.
 - Step 7** Choose **IP Address** of CVP from the drop-down list.
 - Step 8** Enter **Port** number.
 - Step 9** Check **No SSL** check box and click **Next**.
 - Step 10** Check **Anonymus** and **Basic** check boxes in **Authentication** panel.
 - Step 11** Choose **All Users** from **Allow Access To** drop-down list.
 - Step 12** Check **Read** and **Write** check boxes and click **Finish**.
-

Configure Basic Settings for FTP Server

Procedure

- Step 1** Navigate to **FTP server** that you have created in **Connections** tab.
 - Step 2** Goto **Actions** tab and click **Basic Settings**.
 - Step 3** Click **Connect As**.
 - Step 4** Choose **Application User (pass-through authentication)** option and click **OK**.
 - Step 5** Click **OK** in **Edit Site** window.
-

Configure CVP Reporting Server

Reporting provides historical reporting to a distributed self-service deployment in a call center. The CVP Reporting Server receives the reporting data from one or more CVP Servers and CVP VXML Servers, and stores that data in an Informix database. The call data is stored in a relational database, on which you can write custom reports. The administrators can schedule data removal (delete) and database backups. Multiple CVP Call Servers can send data to a single CVP Reporting Server.

Reporting Server Users and Passwords

You can manage Reporting Server Users and Passwords using Windows Operating System Local User Management.



Note Please turn off all the Cisco services and IDs services on the CVP reporting server.

You can do this by using **Local Users and Groups** within the **Computer Management** console. To access this console, navigate to **Start > Administrative Tools > Computer Management**.

Changing Database User Passwords

You can change the password of Reporting Server database users. Navigate to **Computer Management > Local Users and Groups > Users**, choose **cvp_dbadmin (Database Administrator)** or **cvp_dbuser (Database User)**, then right click and select **Set Password**.

Associating Database User Passwords

You can associate the password of Reporting Server database users.

1. In the reporting server from the command prompt, navigate to the **C:\Cisco\CVP\bin** directory.
2. Run the command **report-init.bat -reporthashpwYourPassword** (same password that you set).
3. The **report-init.bat** command encrypts the **cvp_dbadmin** and **cvp_dbuser** passwords and stores them in the *reporting.properties* file that is located at the **C:\Cisco\CVP\conf** folder on the CVP Reporting server. The **RPT.DBPassword** and **RPT.DBAdminPassword** get updated in this process.



Note The password must meet all the reporting password requirements. You can ignore log4J errors which appear after executing this command.

4. Verify if the *reporting.properties* file is updated. The passwords for **cvp_dbadmin** and **cvp_dbuser** are encrypted.
5. Restart the CVP Reporting server and access the CVP Informix DB through **cvp_dbadmin** and **cvp_dbuser** accounts to verify the update.
6. Make a test call to verify if the data is getting populated.

Managing Reporting Server Users

You can add, modify, or delete the Reporting Server users. Navigate to **Computer Management > Local Users and Groups > Users**.

If you need database access, you can add your name to the **Informix-Admin** group.

Configure Reporting Properties

Procedure

- Step 1** Navigate to **Unified CCE Administration > Overview > Infrastructure Settings > Device Configuration > CVP Reporting Server**.
- Step 2** Click the **Properties** tab. Complete the following fields:

Table 19: Reporting Server Properties

Field	Required?	Description
Trunk Utilization		
Enable Reporting	-	Enables the Reporting Server to receive call data from the associated CVP Servers.
Maximum File Size	no	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. Default is 100MB. Range is 1 to 250.

Step 3 Click **Save**.

Configure Database

Procedure

Step 1 Navigate to **Unified CCE Administration > Overview > Infrastructure Settings > Device Configuration > CVP Reporting Server**.

Step 2 Click the **Database Configuration** tab. Complete the following fields:

Table 20: Database Configuration Properties

Field	Required?	Description
Schedule Daily Backups	-	Schedules backups of the Reporting database or runs backups on demand. When you enable backups, the files are saved to the Reporting Server's local file system. You are responsible for managing the backed-up files. The scheduled backups occur once each day. You can configure the time of day for the backups. A maximum of two backups and a minimum of one backup are available at any time on the local machine.
DB Admin Password	yes	The password for the Reporting Database administrator.
Data Retention		
Trunk Utilization Usage	yes	Retention days for the Gateway Trunk Utilization reporting data. Default is 15 days.
Call	yes	Detailed information about the calls received by Unified CVP. Default is 30 days.

Field	Required?	Description
Call Event	yes	Call state change event messages published by the Call Server and the CVP VXML Server. SIP and IVR Services publish call state change event messages when a SIP call changes its state. These states include call initiated, transferred, terminated, stopped, or error state. Default is 30 days.
Callback	yes	Retention days for the Courtesy Callback reporting data. Default is 15 days.
VoiceXML Session	yes	The VXML session data includes application names, session ID, and session variables. The session variables are global to the call session on the CVP VXML Server. Unlike element data, session data can be created and modified by all components (except the global error handler, hot events, and XML decisions). Default is 15 days.
VoiceXML Element	yes	A VXML element is a distinct component of a voice application call flow whose actions affect the caller experience. A VXML element contains the detailed script activity to the element level, such as Call Identifiers, activity timestamp, VXML script name, name and type of the VXML element, and event type. Default is 15 days.
VoiceXML ECC Variable	yes	Expanded Call Context (ECC) variables that are included in the VXML data. Unified CVP uses the ECC variables to exchange information with Unified ICME. Default is 15 days.
VoiceXML Voice Interact Detail	yes	The application detailed data at the script element level from the CVP VXML Server call services. This data includes input mode, utterance, interpretation, and confidence. Default is 15 days.
VoiceXML Session Variable	yes	The VXML session variables are global to the call session on the CVP VXML Server. Default is 15 days.
VoiceXML Element Detail	yes	The names and values of the element variables. Default is 15 days.
Set Time for Purging Data	no	The time set for purging data.

Step 3 Click **Save**.

Set Up Reporting Server Infrastructure

Procedure

- Step 1** Navigate to **Unified CCE Administration > Overview > Infrastructure Settings > Device Configuration > CVP Reporting Server**.
- Step 2** Click the **Infrastructure** tab. Complete the following fields:

Table 21: Infrastructure Properties

Field	Required?	Description
Configuration: Thread Management		
Maximum Threads	yes	The maximum thread pool size in the Reporting Server Java virtual machine. Default is 525. Range is 100 to 1000.
Advanced		
Statistics Aggregation Interval	yes	The interval at which the CVP Reporting Server publishes statistics. Default is 30 minutes. Range is 10 to 1440.
Log File Properties		
Maximum Log File Size	yes	The 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 5MB, CVP.2006-07-04.01.log is automatically created. Default is 10MB. Range is 1 to 100.
Maximum Log Directory Size	yes	The maximum size of the directory containing the CVP Reporting Server log files. Note Modifying the value to a setting that is below the default value might cause the logs to be quickly rolled over. Consequently, the log entries might be lost, which can affect troubleshooting. Default is 20000MB. Range is 500 to 500000.
Configuration: Primary Syslog Server Settings		

Field	Required?	Description
Primary Syslog Server	no	The hostname or the IP address of the primary syslog server to send the syslog events from a CVP application.
Primary Syslog Server Port Number	no	The port number of the primary syslog server. It can be any available port number. Valid port numbers are integers between 1 and 65535.
Primary Backup Syslog Server	no	The hostname or the IP address of the primary backup syslog server to send the syslog events from a CVP application when the syslog server cannot be reached.
Primary Backup Syslog Server Port Number	no	The port number of the primary backup syslog server. It can be any available port number. Valid port numbers are integers between 1 and 65535.
Configuration: Secondary Syslog Server Settings		
Secondary Syslog Server	no	The hostname or the IP address of the secondary syslog server to send the syslog events from a CVP application.
Secondary Syslog Server Port Number	no	The port number of the secondary syslog server. It can be any available port number. Valid port numbers are integers between 1 and 65535.
Secondary Backup Syslog Server	no	The hostname or the IP address of the secondary backup syslog server to send the syslog events from a CVP application when the syslog server cannot be reached.
Secondary Backup Syslog Server Port Number	no	The port number of the secondary backup syslog server. It can be any available port number. Valid port numbers are integers between 1 and 65535.

Step 3 Click **Save**.

Associate Unified CVP Call Servers with CVP Reporting Server

To store the call data that are handled by Call Servers in the Reporting Database, you must associate CVP Call Servers with CVP Reporting Server.



Note A Unified CVP Reporting Server can have one or more CVP Call Servers. However, a Unified CVP Call Server can only be associated with one CVP Reporting Server.

Procedure

Step 1 Navigate to **Unified CCE Administration > Overview > Infrastructure Settings > Device Configuration > CVP Reporting Server**.

- Step 2** Click the **Call Server Association** link.
The **Call Server Association** popup window opens.
- Step 3** Select a **Reporting Server** from the drop-down list. The list includes all the Reporting Servers available in the Packaged CCE inventory.
- Step 4** To associate CVP Call Servers with the selected CVP Reporting Server:
- Click the + icon to open the **Add CVP Call Server(s)** popup. The popup includes a list of CVP Call Servers that are available for reporting association.
 - Select one or more Call Servers from the list and close the popup.
The selected Call Servers appear in the **Configured Call Servers** table.
- Step 5** Click **Save**.
You can continue to associate other CVP Reporting Servers with available Call Servers.
- Step 6** Click **Cancel** to return to the **Device Configuration** page.
-

Cisco Virtualized Voice Browser (VVB) Setup

Cisco Virtualized Voice Browser (Cisco VVB) provides a platform for interpreting VXML documents. When an incoming call arrives at the contact center, Cisco VVB allocates a VXML port that represents the VoIP endpoint. Cisco VVB sends HTTP requests to the Unified CVP VXML server. The Unified CVP VXML server runs the request and sends back a dynamically generated VXML document.



Note After fresh install, add VVB to the System Inventory as an external device.

After Packaged CCE Fresh Install, you can configure the following Virtualized Voice Browser settings for the site:

- Configure Media Parameters
- Configure Security Parameters
- Configure Automatic Speech Recognition (ASR) and Text-to-Speech (TTS) servers.
- Configure the default applications types - Comprehensive, Ringtone, and Error, and add SIP triggers to invoke the application.

Configure Media and Security Parameters

To configure media and security parameters, add audio codec and MRCP version, and enable TLS and Secure Real-Time Transport Protocol (SRTP).

Procedure

- Step 1** Navigate to **Unified CCE Administration > Overview > Infrastructure Settings > Device Configuration > Virtualized Voice Browser**.
- Step 2** Select the site name from the list for which you want to set up the VVB media and security parameters. By default, it is 'Main'.

Step 3 Complete the following fields on the **General** tab:

Field	Required ?	Description
Media Parameters		
Note If you change a configuration, you must restart the VVB engine.		
Codec	Yes	G711 (U-law, A-law) and G729 Audio Codecs are supported. Default codec is G711U.
MRCP Version	Yes	Select the version of the MRCP protocol to communicate between Nuance (ASR/TTS) and Cisco VVB. Default is MRCPv2. Note ASR-TTS service is not supported using G729 codec; therefore, MRCP is not applicable for this codec.
User prompts override system prompts	-	By default, this feature is disabled. Click to allow the custom recorded prompts override the system default prompts. When enabled, the system plays the custom recorded prompt that is uploaded to the appropriate language directory.
Security Parameters		
Note If you change a configuration, you must restart the VVB engine.		
TLS(SIP)	Yes	TLS is disabled by default. Click to enable the secure SIP signalling on the IVR leg.
TLS (SIP) Version	Yes	Note Enable TLS(SIP) to use this security parameter. Choose the minimum TLS version of SIP to be supported from the drop-down list. Default value is TLSv1.2.
Cipher Configuration	Yes	Note Enable TLS(SIP) to use this security parameter. The default cipher <code>TLS_RSA_WITH_AES_128_CBC_SHA</code> is available in the Cipher Configuration list. The default cipher is mandatory for TLS version 1.2 and cannot be deleted. a. Click the + icon and enter the ciphers to be supported by Cisco VVB, with key size lesser than or equal to 1024 bits. Cipher support is as per Java Virtual Machine (JVM). b. Click Add

Field	Required ?	Description
SRTP	-	<p>Note Enable TLS(SIP) to use this security parameter.</p> <p>By default, SRTP is disabled.</p> <p>Enable SRTP to secure media on the IVR leg. When SRTP is enabled, the IVR media is encrypted. SRTP uses Crypto-Suite AES_CM_128_HMAC_SHA1_32 for encrypting the media stream.</p>
Allow RTP(Mixed Mode)	-	<p>Note Enable TLS(SIP) and SRTP to use this security parameter.</p> <p>Allow RTP (Mixed Mode) is available when you enable SRTP.</p> <p>Enable Allow RTP (Mixed Mode) if a nuance device is configured to work in the RTP mode. When enabled, VVB accepts both SRTP and RTP call flows.</p>

Step 4 Click **Save**.

Configure Speech Servers

Cisco VVB uses the Automatic Speech Recognition (ASR) and Text-To-Speech (TTS) speech servers. The ASR and TTS configurations involve specifying the hostname or IP address of the respective speech servers.

Before you begin

Order ASR and TTS speech servers from Cisco-supported vendors. To provision, install, and configure the ASR and TTS speech server software, consult the vendor's application requirement.



Note For more information about supported speech servers for Cisco VVB, see the Solutions Compatibility Matrix available at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html>

Procedure

- Step 1** Navigate to **Unified CCE Administration > Overview > Infrastructure Settings > Device Configuration > Virtualized Voice Browser**.
- Step 2** Select the site name from the list for which you want to set up the VVB media and security parameters. By default, it is 'Main'.
- Step 3** Click the **Speech Servers** tab.
- Step 4** Complete the following fields on the **Speech Servers** tab:

Fields	Required?	Description
ASR Servers		

Fields	Required?	Description
Configured ASR Servers	No	<p>a. Click the '+' icon and enter the hostname or IP address of ASR server.</p> <p>b. Click Add.</p>
TTS Servers		
Configured TTS Servers	No	<p>a. Click the '+' icon and enter the hostname or IP address of TTS server.</p> <p>b. Click Add.</p>

Configure Default Application Properties

Cisco VVB includes the call flow deployment models (applications) to support different business needs. Any VVB in PCCE deployment can be configured with the following three predefined applications:

- Comprehensive application
- Ringtone application
- Error application

Procedure

- Step 1** Navigate to **Unified CCE Administration > Overview > Infrastructure Settings > Device Configuration > Virtualized Voice Browser**.
- Step 2** Select the site name from the list for which you want to set up the VVB media and security parameters. By default, it is 'Main'.
- Step 3** Click the **Applications & Triggers** tab.
- Step 4** Complete the following on the **Applications & Triggers** tab:
- To configure **Comprehensive** application

Field	Required?	Description
Application	Yes	From the Application drop-down list, choose Comprel

Field	Required?	Description
Sigdigits	No	<p>Enter the number of digits that are used as the significant digits (SigDigit) prepended to the Dialed Number (DN). Range is 0 to 20.</p> <p>The call arrives at Unified CVP with the significant digits (SigDigit) prepended to the Dialed Number (DN). Unified CVP strips the digits and transfers the call to the Unified CVP. When ICM returns the label to Unified CVP to route the call to Cisco VVB, Unified CVP prepends the digits again. Cisco VVB uses the SigDigit configuration on the call. Comprehensive application to remove the prepended digits that when the IVR leg of the call is set up, the original digits are used on the incoming VoiceXML request.</p>
Maximum Sessions	Yes	<p>Enter the number of sessions you like to associate with the application. Range is 1 to 600.</p> <p>Note The number of sessions must be less than or equal to the license provided by Cisco VVB.</p>
Enable HTTPS	No	<p>By default, the Enable HTTPS option is disabled. Click to enable the option. When enabled, the communication between the Cisco VVB and VXML server is encrypted. If you have enabled secure communication, then you must:</p> <ul style="list-style-type: none"> • Upload the relevant certificate. To upload the certificate, see the Upload certificate or certificate trust store in <i>Cisco Unified Communications Operating System Administration Guide</i>. • Restart VVB services using the VVB Administration console (Unified Serviceability > Tools > Control Center > Network Services) or the system CLI command <code>service restart Cisco Tomcat</code>.

Field	Required?	Description
Configured Triggers	Yes	<p>The field contains default SIP trigger configured for the Comprehensive application. See Default SIP Triggers.</p> <p>To add a new trigger:</p> <ol style="list-style-type: none"> Click the '+' icon, and enter a new SIP trigger to be associated with the application. <p>Valid input characters are alphanumeric (0-9, x, X, T), and the special characters like period (.), exclamation (!), asterisk (*), and greater than (>). An error message appears for an invalid input.</p> <ol style="list-style-type: none"> Click Add. The trigger appears in the Configured Triggers list. <p>Note On adding a SIP trigger, push the trigger to VVB from the Device Configuration page for it to appear in the Configured Triggers list.</p> <p>To remove a trigger from the list, click the 'x' icon that is associated with the trigger in the list.</p>

- To configure **Ringtone** application

Field	Required?	Description
Application	Yes	From the Application drop-down list, choose Ringtone.
Maximum Sessions	Yes	<p>Enter the number of sessions you like to associate with the application. Range is 1 to 600.</p> <p>Note The number of sessions must be less or equal to the license provided by Cisco VVB.</p>
Configured Triggers	Yes	<p>The field contains default SIP trigger configured for the Ringtone application. See Default SIP Triggers.</p> <p>To add a new trigger:</p> <ol style="list-style-type: none"> Click the '+' icon, and enter a new SIP trigger to be associated with the application. <p>Valid input characters are alphanumeric (0-9, x, X, T), and the special characters like period (.), exclamation (!), asterisk (*), and greater than (>). An error message appears for an invalid input.</p> <ol style="list-style-type: none"> Click Add. The trigger appears in the Configured Triggers list. <p>Note On adding a SIP trigger, push the trigger to VVB from the Device Configuration page for it to appear in the Configured Triggers list.</p> <p>To remove a trigger from the list, click the 'x' icon that is associated with the trigger in the list.</p>

- To configure **Error** application

Field	Required?	Description
Application	Yes	From the Application drop-down list, choose Error.
Maximum Sessions	Yes	Enter the number of sessions you like to associate with the application. Range is 1 to 600. Note The number of sessions must be less or equal to the license provided by Cisco VVB.
Custom error prompt	No	Provide the custom error .wav file to play. Note The field is case-sensitive. The prompt file must be uploaded to Cisco VVB. If custom prompts are not uploaded or found, the default prompt is played.
Configured Triggers	Yes	The field contains default SIP trigger configured for the Error application. See Default SIP Triggers . To add a new trigger: a. Click the '+' icon, and enter a new SIP trigger to be associated with the application. Valid input characters are alphanumeric (0-9, x, X, T), period (.), exclamation (!), asterisk (*), and greater than (>). An error message appears for an invalid input. b. Click Add . The trigger appears in the Configured Triggers list. Note On adding a SIP trigger, push the trigger to VVB from the Device Configuration page for it to appear in the Configured Triggers list. To remove a trigger from the list, click the 'x' icon associated with the trigger in the list.

Step 5 Click **Save**.

Default SIP Triggers

The pre-defined applications have the default SIP triggers as shown in the table.

Table 22: Default SIP Triggers

Application	Description	Pre-configured SIP Trigger
Comprehensive	Used for comprehensive calls	777777777*
Ringtone	Used for playing ringtone and whisper	91919191*

Application	Description	Pre-configured SIP Trigger
Error	Used for playing error tone	92929292*

Finesse

Use this page to configure the following settings for Cisco Finesse administration:

- IP Phone Agent
- CTI Server
- Administration and Data Server
- Cluster Settings



Note The CTI Server, Administration and Data Server, and Cluster Settings are available only for Packaged CCE 4000 Agents deployment to 12000 Agents deployment.

IP Phone Agent Settings

You can set up the user credentials for an IP phone agent. Any changes that are made to these settings require a restart of Cisco Finesse Tomcat to take effect.

Procedure

- Step 1** In **Unified CCE Administration**, choose **Overview > Infrastructure Settings > Device Configuration > Finesse > IP Phone Agent Settings**.
- Step 2** Choose a site for the Finesse server. By default, it is Main for Packaged CCE 2000 Agents deployment.
- Step 3** From the **Peripheral Set** drop-down list, select a peripheral set that has the Cisco Finesse configured for the selected **Site**.

Note The **Peripheral Set** field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see [Add and Maintain Peripheral Set, on page 143](#).
- Step 4** Under **Phone URL Authentication Settings**, enter your **Username** and **Password**.
- Step 5** Click **Save** to save your settings.
- Step 6** Click **Revert** to retrieve the previously saved settings.

Related Topics

- [Contact Center Enterprise CTI Server Settings](#), on page 216
- [Contact Center Enterprise Administration and Data Server Settings](#), on page 219
- [Cluster Settings](#), on page 222

Contact Center Enterprise CTI Server Settings

Use the Contact Center Enterprise CTI Server Settings gadget to configure the A and B Side CTI servers.

All fields on this tab are populated with default system values or with values an administrator has previously entered. Change values to reflect your environment and preferences.

For configuring secure connection select the Enable SSL encryption check box.

Test the CTI connection for given configuration using the **Test Connection** button.



Note After you make any changes to the values on the Contact Center Enterprise CTI Server Settings gadget, you must restart all the nodes of Cisco Finesse Tomcat. To make changes to other settings (such as Contact Center Enterprise Administration & Data Server settings), you can make those changes and then restart Cisco Finesse Tomcat.

If you restart Cisco Finesse Tomcat, agents must sign out and sign in again. As a best practice, make changes to CTI server settings and restart the Cisco Finesse Tomcat Service during hours when agents are not signed in to the Finesse desktop.

The secure encryption and Test Connection functionality is supported only from Unified CCE 12.0.



Note Although the B Side Host/IP Address and B Side Port fields are not shown as required, A and B Side CTI servers are mandatory for a production deployment of Unified CCE and Cisco Finesse.

The following table describes the fields on the Contact Center Enterprise CTI Server Settings gadget:

Field	Explanation
A Side Host/IP Address	<p>The hostname or IP address of the A Side CTI server. This field is required.</p> <p>This value is typically the IP address of the Peripheral Gateway (PG). The CTI server runs on the PG.</p>
A Side Port	<p>The value of this field must match the port configured during the setup of the A Side CTI server.</p> <p>This field is required and accepts values between 1 and 65535.</p> <p>You can find this value using the Unified CCE Diagnostic Framework Portico tool on the PG box. For more information about Diagnostic Framework Portico, see the <i>Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise</i>.</p> <p>The default value is 42027.</p>

Field	Explanation
Peripheral ID	<p>The ID of the Agent PG Routing Client (PIM).</p> <p>The Agent PG Peripheral ID should be configured to the same value for the A and B Side CTI server.</p> <p>This field is required and accepts values between 1 and 32767.</p> <p>The default value is 5000.</p>
B Side Host/IP Address	The hostname or IP address of the B Side CTI server.
B Side Port	<p>The value of this field must match the port configured during the setup of the B Side CTI server.</p> <p>This field accepts values between 1 and 65535.</p>
Enable SSL encryption	Check this box to enable secure encryption.

Actions on the Contact Center Enterprise CTI Server Settings gadget:

- **Save:** Saves your configuration changes.
- **Revert:** Retrieves the most recently saved server settings.
- **Test Connection:** Tests the CTI connection.

CTI Test Connection

When you click **Test Connection**:

1. Input validation is done on the request attributes.
Host/IP Address must not be empty. Port and Peripheral IDs must be within the valid range.
2. Validation is done to check if the provided Host/IP is resolved by Finesse box.
3. Validation is done to check if AW Database is reachable and if a valid path ID is configured for the provided Peripheral ID.
4. Socket connection is established to the provided Host/IP and port. The connection might fail if there is no route to the provided IP. If SSL encryption box is checked, this step also checks for successful TLS handshake. For TLS handshake to be successful, mutual trust has to be established between Finesse and CTI server.

For information on how to establish trust between Finesse and CTI server, see *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html>
5. After successful socket connection, a CTI initialization request is sent to check if the provided host is a CTI host.

If the CTI response is a success for the CTI initialization request and peripheral provided is configured with Unified CCE, it is confirmed to be a CTI host.
6. CTI connection is closed by sending a CTI session close request.



Note If **Test Connection** is successful for Side A or B of the CTI cluster and the other side fails, it is a valid configuration as CTI server works in active-passive mode and connects to the active node. Inactive CTI node will refuse connection on the CTI port. However, Administrator has to ensure that the failed side also has a valid entry for CTI host and port field. System cannot verify this due to server restrictions.

If **Test Connection** is successful on Side A and B of the CTI cluster, then there is an error in the system configuration. Verify that the Side A and B of the CTI node have valid entries for port and host.

Test connection API success result does not guarantee peripheral to be online. It only validates if the peripheral provided is configured with Unified CCE.

Test connection API with insecure connection parameter will function as intended for earlier versions of Unified CCE deployments.

Configure Contact Center Enterprise CTI Server Settings

Procedure

Step 1 In the Contact Center Enterprise CTI Server Settings area, enter the CTI server settings as described in the following table. Refer to your configuration worksheet if necessary.

Field	Description
A Side Host/IP Address	Enter the hostname or IP address of the A Side CTI server. This value is typically the IP address of the Peripheral Gateway (PG). The CTI server runs on the PG.
A Side Port	Enter the port number of the A Side CTI server. The value of this field must match the port configured during the setup of the A Side CTI server.
Peripheral ID	Enter the ID of the Agent PG Routing Client (PIM). The Agent PG Peripheral ID should be configured to the same value for the A and B Side CTI servers.
B Side Host/IP Address	Enter the hostname or IP address of the B Side CTI server.
B Side Port	Enter the port of the B Side CTI server. The value of this field must match the port configured during the setup of the B Side CTI server.
Enable SSL encryption	Check this box to enable secure encryption.

Step 2 Click **Save**.

Contact Center Enterprise Administration and Data Server Settings

Use the Unified CCE Administration & Data Server Settings gadget to configure the database settings. These settings are required to enable authentication for Finesse agents and supervisors.



Note To connect to the AW Database (AWDB) in the Unified CCE Administration, Cisco Finesse supports both SQL and Windows authentication.

The Cisco Finesse Java Database Connectivity (JDBC) driver is configured to use NTLMv2. Therefore, Finesse can connect to the administration database even if the administration database is configured to use only NTLMv2.

Primary Administration & Data Server is configured on Side A and Secondary Administration & Data Server is configured on Side B. Make sure Cisco Finesse server on both sides connect to Primary Administration & Data Server on side A and fall back to Secondary Administration & Data Server on side B only when Primary Administration & Data Server goes down.

After you change and save any value on the Contact Center Enterprise Administration & Data Server Settings gadget, restart the Cisco Finesse Tomcat Service on the primary and secondary Finesse server. If you restart the Cisco Finesse Tomcat Service, agents must sign out and sign in again. To avoid this, you can make Contact Center Enterprise Administration & Data Server settings changes and restart the Cisco Finesse Tomcat service during hours when agents are not signed in to the Cisco Finesse desktop.

The following table describes the fields on the Unified CCE Administration & Data Server Settings gadget:

Table 23: Field Descriptions

Field	Description
Primary Host/IP Address	The hostname or IP address of the Unified CCE Administration & Data Server.
Backup Host/IP Address	(Optional) The hostname or IP address of the backup Unified CCE Administration & Data Server.
Database Port	The port of the Unified CCE Administration & Data Server. The default value is 1433. Note Cisco Finesse expects the primary and backup Administration & Data Server ports to be the same, hence the administration console exposes one port field. You must ensure that the port is the same for the primary and backup Administration & Data Servers.
AW Database Name	The name of the AW Database (AWDB). For example, <i>ucceinstance_awdb</i> .
Domain	(Optional) The domain name of the AWDB.

Field	Description
Username	<p>The username required to sign in to the AWDB.</p> <p>Note If you specify a domain, this user refers to the Administrator Domain user that the AWDB uses to synchronize with the logger. In which case, the AWDB server must use Windows authentication and the configured username must be a domain user.</p> <p>If you do not specify a domain, this user must be an SQL user.</p>
Password	The password required to sign in to the AWDB.

For more information about these settings, see the [Administration Guide for Cisco Unified Contact Center Enterprise](#) and the [Staging Guide for Cisco Unified ICM/Contact Center Enterprise](#).

Actions on the Unified CCE Administration & Data Server Settings gadget:

- **Save:** Saves your configuration changes
- **Revert:** Retrieves the most recently saved enterprise database settings

When you update any of the following fields and click Save, Cisco Finesse attempts to connect to the AWDB:

- Primary Host/IP Address
- Backup Host/IP Address
- Database Port
- AW Database Name

If Cisco Finesse cannot connect to the AWDB, an error message appears and you are asked if you still want to save. If you click **Yes**, the settings are saved. If you click **No**, the settings are not saved. You can change the settings and try again or click **Revert** to retrieve the previously saved settings.

When you update the Username or Password fields and click **Save**, Cisco Finesse attempts to authenticate against the AWDB. If authentication fails, an error message appears and you are asked if you still want to save. Click **Yes** to save the settings or click **No** to change the settings. Click **Revert** to retrieve the previously saved settings.



Note Finesse will not come into service in case of AWDB errors when connecting Cisco Finesse 11.5(1) and higher versions to Unified CCE 11.5(1) and higher versions.

Configure Contact Center Enterprise Administration and Data Server Settings

Configure the Unified CCE Administration & Data Server settings to enable authentication for Finesse agents and supervisors.

Procedure

- Step 1** In the Unified CCE Administration & Data Server Settings area, enter the Administration & Data Server settings as described in the preceding table. For more information, see [Table 23: Field Descriptions, on page 220](#). Refer to your configuration worksheet if necessary.
- Step 2** Click **Save**.
-

What to do next

The CTI test functionality documented in the *Configure Unified CCE CTI Server Settings* topic depends on AWDB connectivity to determine the CTI version. Or else, the test will not go through.

Cluster Settings

Use the Cluster Settings gadget to configure a secondary Finesse server. The purpose of a secondary Finesse server is to handle all agent requests if the primary server goes down.

You must complete this configuration *before* you install the secondary Finesse server. For more information about installing a secondary Finesse server, see the *Cisco Finesse Installation and Upgrade Guide*.

The following table describes the fields on the Cluster Settings gadget:

Field	Explanation
Hostname	The hostname of the secondary Finesse server.

Actions on the Cluster Settings gadget:

- **Save:** Saves your configuration changes
- **Revert:** Retrieves the most recently saved cluster settings

Configure Cluster Settings

Configure the cluster settings for the secondary Finesse node. The secondary Finesse node handles agent requests if the primary server goes down.

Procedure

- Step 1** Sign in to the administration console with the Application User credentials.
- Step 2** In the Cluster Settings area, in the Hostname field, enter the hostname of the secondary Finesse server.
- Step 3** Click **Save**.
-

Single Sign-On

Single sign-on (SSO) is an authentication and authorization process. (Authentication proves that you are the user you say that you are, and authorization verifies that you are allowed to do what you want to do.) SSO allows you to sign in to one application and then securely access other authorized applications without a

prompt to resupply user credentials. SSO permits Cisco supervisors or agents to sign on only once with a username and password. Supervisors and agents gain access to all of their Cisco browser-based applications and services within a single browser instance. By using SSO, Cisco administrators can manage all users from a common user directory and enforce password policies for all users consistently.

SSO is an optional feature. If you are using SSO, use the Single Sign-On tool to configure the Cisco Identity Service (IdS). You can then register and test components with the Cisco IdS, and set the SSO mode on components.

For complete instructions on setting up SSO in your deployment, see one of the following:

- *Cisco Unified Contact Center Enterprise Features Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html>
- *Cisco Packaged Contact Center Enterprise Features Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html>
- *Installing and Configuring Guide for Cisco HCS for CC* at <https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html>

Set Up the External HDS for Single Sign-On

If you have an external HDS in 2000 Agent deployments, manually associate it with a default Cisco IdS by performing the following instructions.

Procedure

- Step 1** In **Unified CCE Administration**, click **Infrastructure** > **Inventory** to open the **Inventory** page.
 - Step 2** Click the pencil icon for the External HDS to open the edit machine popup window.
 - Step 3** Click the Search icon next to **Default Identity Service**. The **Select Identity Service** popup window opens.
 - Step 4** Enter the machine name for the Cisco IdS in the **Search** field or choose the Cisco IdS from the list.
 - Step 5** Click **Save**.
-

Configure the Cisco Identity Service

The Cisco Identity Service (Cisco IdS) provides authorization between the Identity Provider (IdP) and applications.

When you configure the Cisco IdS, you set up a metadata exchange between the Cisco IdS and the IdP. This exchange establishes a trust relationship that then allows applications to use the Cisco IdS for single sign-on. You establish the trust relationship by downloading a metadata file from the Cisco IdS and uploading it to the IdP. You can then select settings that are related to security, identify clients of the Cisco IdS service, and set log levels. If desired, enable Syslog format.



Note In Packaged CCE 4000 or 12000 Agent deployments:

- Unified CCE AW, Unified Intelligence Center, Finesse, and external HDS gets automatically associated with a default Cisco Identity Service (Cisco IdS).
- Make sure that the Principal AW is configured, and is functional before using the Single Sign-On tool in the Unified CCE Administration. Also, add the SSO-capable machines to the Inventory.

In Packaged CCE 2000 Agent deployments, you must manually associate an external HDS with a default Cisco Identity Service (Cisco IdS). For more information, see [Set Up the External HDS for Single Sign-On, on page 223](#).

Procedure

Step 1 In the Unified CCE Administration, choose **Overview > Infrastructure Settings > Device Configuration > Single Sign-On Setup**.

Note Use a log in name in the format *username@FQDN* to log in to the Unified CCE Administration.

The **Identity Service Nodes**, **Identity Service Settings**, and **Identity Service Clients** tabs appear.

Step 2 Click **Identity Service Nodes**.

You can view the overall Node level and identify which nodes are in service. You can also view the **SAML Certificate Expiry** details for each node, indicating when the certificate is due to expire. The node **Status** options are **Not Configured**, **In Service**, **Partial Service**, and **Out of Service**. Click a status to see more information. The star to the right of one of the Node names identifies the node that is the primary publisher.

Step 3 Click **Identity Service Settings**.

Step 4 Click **Security**.

Step 5 Click **Tokens**.

Enter the duration for the following settings:

- **Refresh Token Expiry** -- Refresh token is used to get new Access tokens. This parameter specifies the duration after which the Refresh token expires. The default value is 10 hours. The minimum value is 2 hours. The maximum is 24 hours.
- **Authorization Code Expiry** -- Authorization code is used to get Access tokens from Cisco IdS. This parameter specifies the duration after which the Authorization code expires. The default value is 1 minute, which is also the minimum. The maximum is 10 minutes.
- **Access Token Expiry** -- Access token contains security credentials used to authorize clients for accessing resource server. This parameter specifies the duration after which the Access token expires. The default value is 60 minutes. The minimum value is 5 minutes. The maximum is 120 minutes.

Step 6 Set the **Encrypt Token** (optional); the default setting is **On**. Use this configuration to secure the tokens as Cisco IdS issues tokens in both plain text or encrypted formats.

Step 7 Click **Save**.

Step 8 Click **Keys and Certificates**.

The **Generate Keys and SAML Certificate** page opens and allows you to:

- Regenerate the **Encryption/Signature key** by clicking **Regenerate**. A message appears to say that the Token Registration is successful and advises you to restart the system to complete the configuration. An Administrator regenerates the Encryption/Signature key when it is exposed or compromised.
- Regenerate the **SAML Certificate** by clicking **Regenerate**. A message appears to say that the SAML certificate regeneration is successful. SAML certificate is regenerated when it expires or when IdS relying party trust configuration on IdP is deleted.

Note Establish the trust relationship again whenever the Encryption keys or SAML certificates are regenerated.

Step 9 Click **Save**.

Step 10 Click **Identity Service Clients**.

On the **Identity Service Clients** tab, you can view the existing Cisco IdS clients, with the client name, client ID, and a redirect URL. To search for a particular client, click the Search icon above the list of names and type the name of client.

Step 11 To add a client on the **Identity Service Clients** tab:

- a) Click **New**.
- b) Enter the name of client.
- c) Enter the Redirect URL. To add more than one URL, click the plus icon.
- d) Click **Add** (or click **Clear** and then click the X to close the page without adding the client).

Step 12 To edit or delete a client, highlight the client row and click the ellipses under **Actions**. Then:

- Click **Edit** to edit the client's name, ID, or redirect URL. On the **Edit Client** page, make changes and click **Save** (or click **Clear** and then click the X to close the page without saving edits).
- Click **Delete** to delete the client.

Step 13 Click **Identity Service Settings**.

Step 14 Click **Troubleshooting** to perform some optional troubleshooting.

Step 15 From the **Log Level** drop-down list, set the local log level by choosing **Error**, **Warning**, **Info** (the default), **Debug**, or **Trace**.

Step 16 To receive errors in Syslog format, enter the name of the Remote Syslog Server in the **Host** (Optional) field.

Step 17 Click **Save**.

You can now:

- Register components with the Cisco IdS.
- Enable (or disable) SSO for the entire deployment.

Application Gateway

Detailed information for Application Gateway is available in the *Cisco Packaged Contact Center Enterprise Features Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html>.

Peripheral Gateways

This display-only tool shows details about the peripheral gateways and peripherals in your deployment.

Click the **Site** tab to view the details of peripheral gateways and peripherals configured for that site.

Log Collection



Important Only set trace level to detailed and run log collection during off-peak hours. Do not run log collection during heavy call load.

Use the Log Collection tool to collect logs for these components:

- Unified CCE
- Unified Communications Manager
- Unified CVP
- Finesse
- Unified Intelligence Center

Unless limited by their role, administrators have full access to Log Collection. Supervisors have no access to this tool.

You can select individual or multiple components for log collection, and specify the start and end time for the logs. The maximum duration for log collection is eight hours. The logs for all selected components are consolidated into a single downloadable zip file. You can run one log collection at a time.

For most components, you can specify whether normal or detailed logs are collected using the **Trace Levels** option. Click **Trace Levels** to view the current trace level for each component and, if necessary, change it for future log collection.

The **Current Level** for each component can be Normal, Detailed, or Custom. Custom indicates that the level has been set outside of **Unified CCE Administration** and does not match the Normal or Detailed settings for that component.

System-wide trace levels are gathered periodically. If a trace level is changed outside of **Unified CCE Administration**, it may take several minutes before the new trace level appears in the **Log Collection** tool.

To use Log Collection to debug a problem:

1. In **Unified CCE Administration**, choose **Overview > Infrastructure Settings > Log Collection**.
2. To change trace level to detailed, click **Trace Levels**, and select **Detailed** from the drop-down menus for the relevant components. Click **Update Trace Levels** to apply the changes.
3. Recreate the problem in your deployment or wait until the problem occurs again.
4. Return to the Log Collection tool and collect logs for the appropriate date and time interval, during which detailed trace level was selected. For example, if you set the trace level to detailed on 01/27/2014 at 09:00, you can collect detailed logs for intervals after that date and time.
5. When you have finished debugging the problem, reset the trace level to **Normal**.

To collect log files:

1. In **Unified CCE Administration**, choose **Overview > Infrastructure Settings > Log Collection**.
2. Check each component for which you want to collect logs, or check **Select All**.
3. Click the **calendar** icon to select a **Start Time** and **End Time** for log collection. Select a date and time from the calendar, and then click anywhere outside the calendar to save your selection.
4. Click **Collect Logs**.

The new log collection appears in the list with an **in progress** icon in the Status column. When the log collection is complete, its **download** and **delete** icons are enabled automatically.



Note If errors are encountered during log collection, the **Status** column shows an **error** icon. Hover over the icon to view the tooltip which explains the error. If the Unified CCE Administration service restarts during log collection, a **cancelled** icon appears in the Status column. You can delete log collections that have errors or have been cancelled; you cannot download these collections.

5. Click the **download** icon to download the log zip file.

To delete a stored log collection, click the **delete** icon for that collection in the list.

Command Execution Pane

The Command Execution Pane provides a user interface in the Unified CCE Administration. This pane allows System Administrators to run REST API calls to Unified CVP, Unified CVP Reporting, and Virtualized Voice Browser.



Caution Use this pane to configure certain parameters in Unified CVP, Unified CVP Reporting, and Virtualized Voice Browser, for which no user interface is available in the Unified CCE Administration.

For example:

- To configure DNIS in CVP

For API details, see the *Unified CVP API Developer Guide* at <https://developer.cisco.com/site/customer-voice-portal/documents/rest-api/>.

- To configure Customer Virtual Assistant (CVA) feature in VVB 12.5(1), while keeping the Unified CCE Controller in ICM12.0(1)_ES 37 (or higher), in case of multi-stage upgrade.
-

Before you begin

If you do not have CA certificates, import self-signed certificates of CVP Call Server and Virtualized Voice Browser (VVB) into the AW machines. For more information, see and [Import VVB Self-Signed Certificate into AW Machines, on page 615](#).

Procedure

- Step 1** In Unified CCE Administration, choose **Overview > Infrastructure Settings > Command Execution Pane**.
- Step 2** Complete the following parameters.

Field	Description
Machine Type	Choose the machine type. Valid values are: <ul style="list-style-type: none"> • Unified CVP • Unified CVP Reporting • Virtualized Voice Browser
Site	Choose the site. You can run the REST API call on the Main site or the Remote site machines. Default is All Sites when a Machine Type is selected.
Host Name	Choose a Host Name or multiple Host Names. Host Names are displayed based on the selected Machine Type and Site.
Method	Choose the HTTP method. Valid values are: <ul style="list-style-type: none"> • GET • POST • PUT • DELETE Default is GET.
Path	Enter the relative URI of the API. Based on the Machine Type you select, most frequently used APIs are displayed as auto suggestions. For example, when the Machine Type is Unified CVP , the path displayed is <code>cvp-orm/rest/cvpconfig/properties</code> . For more information about APIs, refer to the respective CCE Component documentation.
Request Body	Enter the request data in JSON or XML format. Mandatory if the Method is POST or PUT.
Response Type	Choose the Response Type as JSON or XML. Default is JSON. Note Response Type is only applicable for Success result.

- Step 3** Click **Execute**.
The window displays the Success or Failure response.

Note The **RESET** button resets all the fields on the page to its default value.

User Setup

Manage Agents

Agents

Agents respond to contacts from customers. These contact requests are often phone calls, but can also be chat requests or emails.

You can configure the types of contacts that are routed to an agent. For example, if an agent is a member of a skill group that is set up for the Cisco_Voice routing domain only, that agent is a voice agent for that skill group. If an agent is a member of a skill group that is set up for a nonvoice routing domain, that agent is a multichannel agent for that skill group.

Agents can be located at a contact center site or designated as mobile agents who work elsewhere—perhaps from a home office. Setting up mobile agents is documented in the *Cisco Packaged Contact Center Enterprise Features Guide*, at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html>.

Agents can be assigned to skill groups and to one team. Teams are organizational units that reflect the reporting structure in a contact center. They can also be assigned attributes that indicate their proficiency—perhaps expertise in a certain language or technology.

Agents work from an agent desktop. Each agent is associated with one Desk Settings, either the current default desk settings or another desk settings. Desk settings are a set of permissions or characteristics that control the features agents can see and use while they are interacting with customers.

You can indicate that an agent is a supervisor. An agent with supervisor status can oversee multiple teams, can view reports that monitor activities of the agents on those teams, and can join and participate in agent/customer calls. Supervisors work from a supervisor desktop.

In **Unified CCE Administration**, choose **Users > Agents** to view the Agent list. the administrators can see and maintain all agents. Supervisors see a list of agents who are on teams they supervise.

Related Topics

[Add and Maintain Agents](#), on page 230

[Add an Agent by Copying an Existing Agent Record](#), on page 234

[Edit Description, Desk Settings, and Teams for Multiple Agents](#), on page 238

[Add Supervisor Status to an Agent](#), on page 241

[Attributes](#), on page 259

[Desk Settings](#), on page 322

[Roles](#), on page 241

[Skill Groups](#), on page 256

[Teams](#), on page 249

Add and Maintain Agents

This procedure explains how to add an agent. For information on maintaining agents, see [Update Objects, on page 154](#) and [Delete Objects, on page 157](#).

You can add agents one at a time from the **Agents** page, using this procedure. You can also do the following:

- Create a new agent by copying an existing agent record (see [Add an Agent by Copying an Existing Agent Record, on page 234](#)).
- Run bulk jobs to add or edit multiple agent records (see [Manage Bulk Jobs, on page 377](#)).
- Edit the skill group membership for multiple agents at once (see [Edit Skill Group Membership for Multiple Agents, on page 237](#)).
- Edit descriptions, desk settings, and teams for multiple agents at once (see [Edit Description, Desk Settings, and Teams for Multiple Agents, on page 238](#)).

Procedure

Step 1 In **Unified CCE Administration**, choose **Users > Agents**.

Step 2 Click **New** to open the **New Agent** page.

This page has **General**, **Description**, **Attributes**, **Skill Groups**, **Supervised Teams**, and **Email & Chat** tabs. You cannot save the agent until you have entered all the required fields on the **General** tab. You can complete other tabs as needed and in any order.

Step 3 Complete the fields on the **General** tab:

Field	Required?	Description
Enable SSO	no	Indicates whether the agent is set for single sign-on (SSO). When SSO is enabled, the agent uses Active Directory or other SSO credentials to sign into the agent desktop and other tools. You can check this check box to enable SSO for this agent if SSO is set globally to mixed mode. You cannot edit this setting if SSO is enabled or disabled globally. If SSO is enabled globally, saving the agent's new or updated record enables SSO for the agent.
Login Enabled	no	Checked by default. Uncheck the check box only if you do not want this agent to be able to sign in.

Field	Required?	Description
Is Supervisor	no	<p>Check to configure this agent as a Supervisor.</p> <p>Note</p> <ul style="list-style-type: none"> When you check this check box, a user account is created in Cisco Unified Intelligence Center with the supervisor's username and domain name. If the username and domain name exists in Unified Intelligence Center, the user account and supervisor's record is synchronized to have same username and domain name. For an existing supervisor's record, if you uncheck this check box, the corresponding user account is deleted from Unified Intelligence Center.
Support Email & Chat	no	This check box appears only when ECE is configured for a peripheral set or a data center. By default, it is not checked.
Username	yes	<p>Enter a unique username for the Agent.</p> <p>Enter up to 255 ASCII characters as the username for this agent. The login name supports the use of all characters from 33 to 126 in the ASCII character set, except for the following: double quotation mark ("), forward slash (/), backward slash (\), square brackets ([]), colon (:), semicolon (;), pipe (), equal to (=), comma (,), plus sign (+), asterisk (*), question mark (?), angle brackets (< >), hash (#), percent (%), and SPACE.</p> <p>For supervisors and for agents with single sign-on (SSO) enabled, the username is the user's Active Directory or SSO account username.</p> <p>For supervisors who are not enabled for single sign-on (SSO), the Active Directory username must be in the user@domain format.</p> <p>Remember An agent who is designated as a supervisor signs in to Unified CCE Administration with this username.</p> <p>Note Ensure that Agent ID (Peripheral number) and agent Login name is unique for each user.</p>
First Name	yes	See Character Sets, on page 601 .
Last Name	yes	See Character Sets, on page 601 .
Agent ID	-	<p>Enter a unique string of up to 11 digits.</p> <p>If you leave this field blank, Packaged CCE automatically generates a 7-digit agent ID, which you can later edit.</p> <p>The agent uses the Agent ID to sign in to Cisco Finesse.</p>
Description	no	<p>Enter a description of the agent.</p> <p>See Character Sets, on page 601.</p>

Field	Required?	Description
Desk Settings	-	The Desk Settings field defaults to show the current system-default. (See Main Site, on page 362 .) To change it, click the magnifying glass icon to display the Select Desk Settings list where you can select a different desk setting.
Department	yes (for departmental administrators)	<p>A departmental administrator must select one department from the pop-up list to associate with this agent. The list shows all administrator's departments.</p> <p>A global administrator can retain the default value for this field, which sets the agent as global (belonging to no departments), or can select a department for this agent.</p> <p>See Departments, on page 269 for more information about associating agents with departments.</p>
Site	-	<p>The Site field displays Main by default for Packaged CCE 2000 Agents deployment.</p> <p>For Packaged CCE 4000 Agents and 12000 Agents deployments, Site is a mandatory field and has no default value.</p> <p>To add a site:</p> <ol style="list-style-type: none"> a. Click the magnifying glass icon to display the list of sites. b. Select the required site.
Peripheral Set	yes	<p>This field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see Add and Maintain Peripheral Set, on page 143.</p> <p>To add a peripheral set:</p> <ol style="list-style-type: none"> a. Click the magnifying glass icon to display the list of peripheral sets configured for the selected Site. b. Select the required peripheral set.
Team	no	<p>The Team field defaults to <i>None</i>. To change the setting, click the magnifying glass icon to display the Select Team list and select a team. Only the teams associated to the selected site display.</p> <p>If the agent is associated with a department, you see global teams and teams that are associated with that department in the list. If the agent is a global agent, you see only global teams in the list.</p> <p>Note When you add a team to an agent, the same agent is added to the corresponding collection in Unified Intelligence Center.</p>
Set Password	no	<p>If single sign-on is not enabled, this setting is checked by default. Uncheck the check box if you do not want to create a password for this agent.</p> <p>If single sign-on is enabled, the password settings on the General tab are disabled.</p>

Field	Required?	Description
Enter Password	no	<p>Enter and reenter a maximum of 256 ASCII characters to establish and confirm a password for this agent. Password is case-sensitive.</p> <p>The default <i>Minimum Password Length</i> is set in system settings. (See Global, on page 360.)</p> <p>For a supervisor, the password must be the supervisor's Active Directory password.</p> <p>Tip An agent who is designated as a supervisor signs in to Unified CCE Administration with this password.</p>
Re-enter Password	no	—

Step 4 Complete the **Attributes** tab:

This tab shows the attributes associated with this agent and their current values.

Click the + icon to open a pop-up list of all attributes, showing the name and current default value for each.

- a) Click the attributes you want to add for this agent.
- b) From the **Value** drop-down list, choose the attribute value as appropriate for this agent.

Step 5 Complete the **Skill Groups** tab:

This tab shows the skill group membership for this agent.

- a) Click the + icon to open the **Add Skill Groups** pop-up. You can view only the skill groups associated to the selected site. Click the skill groups you want to add for this agent or supervisor.

Note You can view only the skill groups associated to the selected site in 2000 Agents deployment.

You can view only the skill groups associated to the selected site and peripheral set in 4000 Agents and 12000 Agents deployment.

- b) Select the default skill group for the agent from the **Default Skill Group** drop-down list.

Step 6 Complete the **Supervised Teams** tab, if **Is Supervisor** is checked.

To select a team, click the + icon to display the **Add Supervised Teams** list, and click the row to select a team.

- Note**
- You can view only the teams that are associated to the selected site in 2000 Agents deployment.
 - You can view only the teams that are associated to the selected site and peripheral set in 4000 Agents and 12000 Agents deployment.
 - If the supervisor is associated with a department, you see only teams associated with that department in the list. If the supervisor is a global supervisor, you see all global and departmental teams in the list.
 - When you associate teams for a supervisor, the same teams (collections in Unified Intelligence Center) are also associated to the corresponding user account (with Supervisor permission) in Unified Intelligence Center.

Step 7 Complete the following fields in the **Enable Email & Chat** tab if Cloud Connect is added and registered or ECE is configured.

Field	Required?	Description
Screen Name	yes	The screen name of the ECE-enabled agent. The screen name must be at least 1 character and no more than 30 characters. The following characters can be used in screen names: Uppercase and lowercase alpha numeric characters (A-Z, a-z, 0-9); at sign (@); space (); colon (:); period (.); underscore (_); hyphen (-); ampersand (&); and all the characters above ASCII codeset 128. This field is required if Support Email & Chat is checked.
Email Address	no	The email address of the ECE-enabled agent. Maximum length is 50 characters. Email address is mandatory when this checkbox is selected.

Step 8 Complete the **Email & Chat** tab. Enter the **Screen Name** and **Email Address**. Click **Save**.

Note The screen name of the ECE-enabled agent. Maximum length is 32 characters. Valid characters are period (.), underscore (_), and alphanumeric. The first character must be alphanumeric.

Note This tab is available only if ECE is configured for a peripheral set or a data center.

Step 9 Click **Save** to return to the List window, where a message confirms the successful creation of the agent.

Caution You cannot add a new agent in the following conditions:

- Out of Compliance expiry: The system is operating with an insufficient number of licenses and the system is in enforcement mode.
- Authorization expiry: The system has not communicated with **Cisco Smart Software Manager** or satellite for 90 days and the system has not automatically renewed the entitlement authorizations.
- Evaluation expiry: The license evaluation period has expired.

Add an Agent by Copying an Existing Agent Record

You can create a new agent by copying an existing agent record.

The following fields are copied to the new agent record:

- Department
- Description
- Desk settings
- Team
- Attributes
- Skill Groups
- Default Skill Group
- Site

All other fields are either cleared or set to the default value.

Procedure

- Step 1** In **Unified CCE Administration**, choose **Users > Agents**.
- Step 2** Click the agent you want to copy, and then click the **Copy** button in the **Edit Agent** page. The **New Agent** page opens.
- Step 3** Hover over the row for that agent, and click the **copy** icon that appears at the end of the row.
- Step 4** Review the fields on the **General**, **Attributes**, and **Skill Groups** tabs that were copied from the original agent record, and make any necessary changes. Enter information for the fields that were not copied.
- Step 5** If the new agent is a supervisor, complete the fields on the **Supervisor** tab.
- Step 6** Click **Save** to return to the List window, where a message confirms the successful creation of the agent.

Note If the new agent is a supervisor, a user account is created in Cisco Unified Intelligence Center with the supervisor's username and domain name.

Search for Agents

The Search field in the Agents tool offers an advanced and flexible search.

Click the + icon at the far right of the **Search** field to open a popup window, where you can:

- Select to search for agents only, supervisors only, or both.
- Select to search for all agents or only ECE enabled agents.
- Enter a username, agent ID, first or last name, or description to search for that string.
- Enter one or more site names separated by spaces. (Site is an OR search.)
- Enter one or more peripheral set names separated by spaces (Peripheral Set is an OR search). The search is case-insensitive and does not support partial matches.



Note Search by peripheral set is available only in Packaged CCE 4000 Agents and 12000 Agents deployments.

- Enter one or more team names separated by spaces. (Team is an OR search--the agent or supervisor must be a member of one of the teams.)
- Enter one or more attribute names separated by spaces. (Attributes is an AND search--the agent or supervisor must have all attributes.)
- Enter one or more skill group names separated by spaces. (Skill Groups is an AND search.)
- Select departments, with options for **Globals and Departments**, **Globals only**, or **Departments only**.
- Selecting **Globals and Departments** or **Departments only** enables an input field where you can enter a space-separated list of department names. (Departments is an OR search.)



Note Search by department is available only when departments are configured.
Search by site is available only when remote sites are configured.

Manage Agent Expertise

There are two ways that agents can be categorized such that calls are sent to them based on their experience and their expertise in handling specific types of customer concerns.

- You can add an agent to one or more skill groups. For example, agents who work on fulfilling orders might be added to a *Customer Service* or a *Tracking Orders* skill group.
- You can assign one or more attributes to an agent. For example, an agent who speaks fluent Spanish might be assigned an attribute of *Spanish*.

Agent Reskilling

Supervisors can reskill agents who are on teams that they supervise. This procedure explains how to reskill a single agent. For information on reskilling multiple agents at once, see [Edit Skill Group Membership for Multiple Agents, on page 237](#).



Note If you remove an agent from the agent's default skill group, the agent's default skill group is changed to the system defined default skill group.

Procedure

- Step 1** In **Unified CCE Administration Manage**, choose **Users > Agents** to view the Agents list.
- Step 2** Click the agent you want to reskill.

- Step 3** Click the **Skill Groups** tab.
- Step 4** To add a skill group, click the **magnifying glass** icon to open the pop-up list of skill groups. Work in the pop-up window to add skill groups to the agent.
- Step 5** To remove a skill group, click the skill group's **x** icon in the **List of Skill Groups** section of the **Skill Groups** tab.
- Step 6** Click **Save**.

Edit Skill Group Membership for Multiple Agents

Using the Agent tool, you can edit skill group membership for multiple agents at once.

In Packaged CCE deployments only, the agents must all belong to the same site and same department, or all be global agents. The **Edit** button disables if you select:

- Agents from multiple sites or multiple departments.
- A mix of global and departmental agents.
- A mix of agents on main site and remote site.

The agents must all belong to the same department or all be global agents. The **Edit** button is disabled if you select agents from multiple departments, or if you select a mix of global and departmental agents.

If you remove an agent from the agent's default skill group, the agent's default skill group is changed to the system defined default skill group.



Tip Use the **Search** field to find the agents whose skill group membership you want to edit. For example, you could find agents belonging to a particular department, team, or skill group, or with certain attributes. (See [Search for Agents, on page 235.](#))

Procedure

- Step 1** In **Unified CCE Administration**, choose **Users > Agents**.
- Step 2** Check the check box for each agent whose skill group membership you want to edit.
- To select all agents in a list, check the **select/deselect all** check box in the list header. (The check box is enabled for *select all* only when the number of agents in the list is less than or equal to 50.)
- The total number of selected agents appears above the agent list. To uncheck all agents, click the **select/deselect all** check box. (The check box is enabled for *deselect all* when you check one or more agents in the list, regardless of the number of agents in the list.)
- Step 3** Click **Edit > Skill Groups**.
- The **Edit Skill Groups** dialog opens with a list of skill groups.
- The **# of Selected Agents** column indicates how many of the selected agents currently belong to each skill group.

In Packaged CCE deployments only, if you select agents from a specific department and a site, global skill groups on that site, and skill groups for that department and site appear in the list. If you have selected global agents from a specific site, all global and departmental skill groups on that site appear in the list.

Step 4 In the **Action** column, click the + icon for each skill group to which you want to add the selected agents. Click the x icon for each skill group from which you want to remove the selected agents.

Note If all selected agents belong to a skill group, only the x icon appears for that skill group. If none of the selected agents belong to a skill group, only the + icon appears for that skill group.

The total number of skill groups that you are adding and removing appears at the bottom of the dialog.

Step 5 To undo a skill group membership change, click the **Undo Add** icon in the **Action** column for that skill group.

Step 6 Click **Save**, and then click **Yes** to confirm the changes.

Edit Description, Desk Settings, and Teams for Multiple Agents

Using the Agent tool, you can edit the description, desk settings assignment, and team membership for multiple agents at once.

The agents must all belong to the same site and same department, or all be global agents. The **Edit** button disables if you select:

- Agents from multiple sites or multiple departments.
- A mix of global and departmental agents.
- A mix of agents on main site and remote site.



Tip Use the **Search** field to find the agents whose settings you want to edit. For example, you could find agents belonging to a particular department, team, or skill group, or with certain attributes. (See [Search for Agents, on page 235.](#))

Procedure

Step 1 In **Unified CCE Administration**, choose **Users > Agents**.

Step 2 Check the check box for each agent whose description, desk settings, and team membership you want to edit.

To select all agents in a list, check the **select/deselect all** check box in the list header. (The check box is enabled for *select all* only when the number of agents in the list is less than or equal to 50.)

The total number of selected agents appears above the agent list. To clear all agents, check the **select/deselect all** check box. (The check box is enabled for *deselect all* when you check one or more agents in the list, regardless of the number of agents in the list.)

Step 3 Click **Edit > General**.

The **Edit General Details** pop-up windows opens.

- Step 4** To change the description for all selected agents, check the **Description** check box and enter the description in the text field.
- Step 5** To assign desk settings to all selected agents:
- Check the **Desk Settings** check box.
 - Click the **magnifying glass** icon to display the **Select Desk Settings** list, and then select the desk setting.
- Step 6** To assign all selected agents to a team:
- Check the **Team** check box.
 - Click the **magnifying glass** icon to display the **Select Teams** list, and then select the team.
- Step 7** Click **Save**, and then click **Yes** to confirm the changes.
-

Manage Supervisors

You can configure agents to have supervisor status.

Supervisors with Single Sign-on (SSO) enabled, use their SSO credentials to sign in to Unified CCE Administration.

Supervisors with Single Sign-on (SSO) disabled, use their Unified ICM credentials to sign in to Unified CCE Administration.

With Supervisor status, agents can perform the following tasks:

- Supervise multiple teams and can be both a supervisor and a member of a team.
- Generate reports and view data for the teams they supervise and the agents on those teams.
- Use a supervisor desktop to barge-in, intercept, silently monitor, and log out agents.
- Join an agent or customer call to assist on a consultative or emergency basis. The agent's ability to request supervisor assistance is a setting on the Desk Settings.
- Change the attributes, and skill groups of agents who are on teams they supervise. Supervisors can also change the passwords for agents who do not have single sign-on enabled.

To configure supervisors in **Unified CCE Administration**, choose **Users > Agents**. Click an agent and check the **Is Supervisor** check box on the **General** tab.

Supervisor Access and Permissions

Supervisors can access the following tools:

Tool	Permissions
Agents	<p>On the Agent List page, supervisors can see and edit settings for the agents that they supervise.</p> <ul style="list-style-type: none"> • General tab: Supervisors can edit the password for agents who do not have single sign-on enabled. Other fields are read-only. <p>After changing the agent's password,</p> <ul style="list-style-type: none"> • The agent can sign in to Cisco Finesse only after 30 minutes, or • Restart Unified Intelligence Center Reporting Service and then the agent can sign in to Cisco Finesse. <ul style="list-style-type: none"> • Attributes tab: Supervisors can add, modify, and remove attributes for agents on teams they supervise. • Skill Groups tab: Supervisors can add and remove the agent's membership in skill groups and can change the agent's default skill group. • Supervised Teams tab: Read-only for supervisors. <p>Supervisors can also change skill group or attribute assignments for up to 50 agents at once by selecting the agents on the Agent List page, and then clicking Edit > Skill Groups or Edit > Attributes.</p> <p>Note If a supervisor attempts to make numerous membership changes at once (in excess of 3500 in a single save), the system alerts the supervisor of attempting too many changes in a single operation.</p>
Attributes	<p>On the Attributes List window, supervisors can see and edit agent attribute assignments. Supervisors cannot add or delete attributes.</p> <ul style="list-style-type: none"> • General tab: Fields are read-only. • Agents tab: Supervisors can add and remove attribute assignments for agents that they supervise.
Precision Queues	Read-only.
Skill Groups	<p>On the Skill Group List page, supervisors can see and edit membership for skill groups. Supervisors cannot add or delete skill groups.</p> <ul style="list-style-type: none"> • General tab: Fields are read-only. • Members tab: Supervisors can add and remove skill groups for agents that they supervise.
Teams	Read-only.
Business Hours	On the Business Hours page, supervisors can see and edit all the fields for business hours. Supervisors cannot add or delete business hours.

Add Supervisor Status to an Agent

This procedure explains how to create a supervisor. For information on maintaining supervisors, see [Update Objects, on page 154](#) and [Delete Objects, on page 157](#).



Remember The agent to whom you are adding supervisor status must already exist in Active Directory.

In **Unified CCE Administration**, choose **Users > Agents**.

Procedure

Step 1 Create a new agent or edit an existing agent. See [Add and Maintain Agents, on page 230](#).

Step 2 Check **Is Supervisor** to configure this agent as a Supervisor.

- Note**
- When you check this check box, a user account is created in Cisco Unified Intelligence Center with the supervisor's username and domain name. If the username and domain name exists in Unified Intelligence Center, the user account and supervisor's record is synchronized to have same username and domain name.
 - For an existing supervisor's record in Packaged CCE, if you uncheck this check box, the corresponding user account is deleted from Unified Intelligence Center.

Step 3 Click the **Supervised Teams** tab.

Step 4 Select the teams for this supervisor:

- a) Click **Add** next to **List of Supervised Teams** to open **Add Supervised Teams**.
- b) Click the team name to add the team.

Note When you associate teams for a supervisor, the same teams (collections in Unified Intelligence Center) are also associated to the corresponding user account (with Supervisor permission) in Unified Intelligence Center.

Step 5 Click **Save** to create the supervisor.

Manage Roles

Roles

Roles specify which features and subfeatures an administrator can see and use. An administrator can be assigned to a built-in role or to a custom role. (An administrator who has no role cannot sign in.)

In **Unified CCE Administration**, choose **Users > Roles** to view the list of roles currently configured.

Features and subfeatures access for roles are defined by check boxes. You cannot alter the features and subfeatures access for built-in roles (all allowed features and subfeatures are checked). But, you can create custom roles to define customized sets of features and subfeatures access.



Note Role changes can take up to 30 minutes to take effect.

Built-In Roles

On the **Roles** page, click the built-in role to view the features and subfeatures associated with it.

Built-In Role Name	Associated Features and Subfeatures
AgentAdmin	<p>The administrators assigned with this role can access the following features and subfeatures.</p> <ul style="list-style-type: none"> • Agents: <ul style="list-style-type: none"> • Manage Agents • Manage Agent Attributes • Reskill Agents • Outbound Campaigns: <ul style="list-style-type: none"> • Campaign Status & Schedule • Campaign Contact • Desktop Settings: <ul style="list-style-type: none"> • Desktop Layout • Phonebook • Reason Codes • Workflow
ScriptAdmin	The administrators assigned with this role can access the Agent feature and Call Settings feature, and its subfeatures.
ConfigAdmin	The administrators assigned with this role can access all the features and subfeatures except for the Access feature and its subfeatures.
SystemAdmin	The administrators assigned with this role can access all the features and subfeatures.

Related Topics

[Add and Maintain Custom Roles](#), on page 242

Add and Maintain Custom Roles

To add, edit, or delete custom roles, an administrator must have the SystemAdmin role.

This procedure explains how to add a role. For information on maintaining roles, see [Update Objects](#), on page 154 and [Delete Objects](#), on page 157.

Procedure

- Step 1** In **Unified CCE Administration**, choose **Users > Roles**.
On the **Roles** page, you can view all the roles currently configured.
- Step 2** Click **New** to open the **New Role** page.
- Step 3** Complete the fields on the **General** tab:

Field	Required?	Description
Name	Yes	Enter a unique name for the role, using a maximum of 32 characters.
Description	No	Enter a maximum of 255 characters to describe the role. See Character Sets, on page 601 .
Features and Subfeatures Access fields	No	When you create a new (custom) role, check the check box corresponding to the features and subfeatures that you want administrators with this role to be able to see and use. Checking a check box corresponding to a feature checks all the subfeatures' check boxes in that feature. You can uncheck individual subfeatures within a feature. For example, you can check the Organization feature and then uncheck Precision Queues and Skill Groups subfeatures. Note You cannot add Access tools (Administrators, Departments, Roles) to a custom role.

- Step 4** Continue to the **Administrators** tab to add administrators to the role.
- Step 5** Click the + icon to open the **Add Administrators** pop-up window.
The row for each administrator has two columns: a column with Administrator's Username and a column with Administrator's Domain.
Clicking an administrator who already has a role removes that role and reassigns this role.
On the **Overview** page, the administrator can view only the cards and its access tools associated with the assigned role.
- Step 6** Click **Save** to return to the list of roles, where a message confirms the successful creation of the role.

Manage Administrators

The Packaged CCE deployment of Unified CCE Administration offers extensive flexibility in the configuration of administrator users and in ways to limit their system access.

Administrator access is controlled by the **Roles** tool available from the **User Settings** page and **Departments** tool available from the **Organization** menu. Only administrators with the SystemAdmin role can access these pages.



Note Administrator password and role changes can take up to 30 minutes to take effect.



Note If the system administrator is assigned to "None" (no role), then that administrator has access all the tools in the Configuration Manager.

Add and Maintain Administrators

This procedure explains how to add an administrator. For information on maintaining administrators, see [Update Objects, on page 154](#) and [Delete Objects, on page 157](#).

To add, edit, or delete administrators, an administrator must have the SystemAdmin role. Administrators cannot add, update, or delete themselves.

Before you begin

The administrators you create are added to the domain security group and CCE database based on their role, if `ADSecurityGroupUpdate` registry key is set to 1. If `ADSecurityGroupUpdate` registry key is set to 0 (default setting), the administrators are added only to the CCE database based on their role.

Procedure

Step 1 Navigate to **Unified CCE Administration > Users > Administrators**.

This displays a list of administrators who are currently configured.

Step 2 Click **New** to open the **New Administrator** window.

Step 3 Complete the following fields:

Field	Required?	Description
Domain	no	From the drop-down menu, select the domain for this administrator.
Username	yes	Enter a unique name for the administrator, using a maximum of 64 characters. The account must already exist in Active Directory under the selected domain.
Description	no	Enter a maximum of 255 characters to describe the role. See Character Sets, on page 601 for details on valid characters for this field.

Field	Required?	Description
Role	no	<p><i>ConfigAdmin</i> is the default role for a new administrator. Click the magnifying glass icon to open the List of Roles pop-up window. Select a role for this administrator.</p> <p>On the Overview page, the administrator can view only the cards and its access tools associated with the assigned role.</p> <p>For more information see the topic</p>
Access to All Departments	no	<p>This check box defaults to checked. You cannot uncheck it for the <i>SystemAdmin</i> role—SystemAdmins are always Global administrators.</p> <p>For all other roles, you can leave the check box checked to configure the new administrator as a Global administrator. Or you can uncheck the check box to configure the administrator as a Department Administrator and then:</p> <ul style="list-style-type: none"> • Click the + icon to open the Add Departments pop-up window. • Click one or more departments to select them; then close the popup window. The administrator is now a Department administrator who is associated with those departments. • Click the x icon to remove a department. <p>Note Department Administrator will have read-only access to non-departmental entities such as SIP Server Group, Media Routing Domain, Routing Pattern, and so on, even if the associated role grants full access.</p>

Step 4 Click **Save** to return to the list, where a message confirms the successful creation of the administrator.

Related Topics

[Changing Authorization Modes of Administrators](#) , on page 248

[Administrators and System Access](#), on page 245

[Departments](#), on page 269

[Roles](#), on page 241

Administrators and System Access

Administrators' access to the system can be restricted by their roles, the departments to which they are assigned, and whether they have full or read-only permission.

An administrator must have a role, which specifies which cards and access tools that an administrator sees on the **Overview** page.

Packaged CCE offers the option to create departments. A contact center for a university might have a department for each academic area, a department for admissions, a department for alumni, and so forth. An administrator

can be associated with one or more departments or can be a global administrator who is assigned to no departments and who therefore has access to all departments. Departmental administrators can add and edit objects only for the departments they administer.

An administrator's role and department associations are configured when the administrator is created. A SystemAdmin can change them.



Note If user's Use logon name (pre-Windows 2000) changes in Active Directory, you must update the same in Packaged CCE. Choose **Unified CCE Administration > Users > Administrators**. Select the user to open the details and click **Save**.

Related Topics

[Roles](#), on page 241

[Departments](#), on page 269

Limit Administrator Access

Limit Administrator Access by Departments

Packaged CCE allows you to create departments and to associate an object with one department. For example, a university might have department for Admissions, Billing, and each academic area.

The add/edit pages for those objects have a Department field. If you do not want an object to have a department association, you have two options:

- Do not create departments.
- Create departments, but select *Global* from the Department drop-down menu to give the object “global” status.

In the table below, Skill Group One is associated with the Admissions department. Skill Group Two is associated with the History department. Skill Group Three is global and belongs to no department.

Table 24: Object and Departments

Department	Object
Admissions	Skill Group One
History	Skill Group Two
Global	Skill Group Three

When you create or edit an administrator, you can either check **Access to All Departments**, which gives an administrator “global” access to all departments, or associate the administrator with one or more departments. To establish a department association for an administrator, click **Add New** next to the **List of Allowed Departments** and select one or multiple departments.



Note An administrator with the SystemAdmin role cannot be a departmental administrator.

In the following table, Administrator One can work with objects in the Admissions department. Administrator Two can work with objects in the History department. Administrator Three is a global administrator and can work with all objects in all departments.

Table 25: Administrators and Departments

Department	Administrator
Admissions	Administrator One
History	Administrator Two
Global	Administrator Three

Limit Administrator Access by Role and Permissions

An administrator must be assigned a role to be allowed to sign in to the Unified CCE Administration.

Permissions defined in the following table indicate which tools an administrator can view, add, edit, or delete, unless restricted by departmental association.

Table 26: Administrator Tools and Permissions

Administrator	Tool	Permissions
Administrator One	Agent Tools	<ul style="list-style-type: none"> • Full access to Agent Tools • View, add, edit, and delete Skill Group One • Add Admissions Department agents to Skill Group One • Add global agents to Skill Group One • View Skill Group Three
Administrator Two	Agent Tools	<ul style="list-style-type: none"> • Full access to Agent Tools • View, add, edit, and delete Skill Group Two • Add History Department agents to Skill Group Two • Add global agents to Skill Group Two • View Skill Group Three
Administrator Three	Script and Call Tools	<ul style="list-style-type: none"> • Full access to Script and Call Tools • Full access to agents and Skill Groups from all departments • Full access to global agents and Skill Groups

Changing Authorization Modes of Administrators

When you provide permissions to a user (account):

The registry settings in the local AW machine **HKEY_LOCAL_MACHINE > SOFTWARE > Cisco Systems Inc > ICM > <instance> > AW** with the key `ADSecurityGroupUpdate` decides whether a user will be added to the domain Config and Setup Security Groups.

Default Key Value

The default value of the `ADSecurityGroupUpdate` key is 0 which means that the AW is in local authorization mode. If the user is added using the Administrator Gadget or the API with **pre-defined** or **custom roles**, the user is not added to the corresponding domain security groups. The user is added to the database with the corresponding roles.

If you want to use the configuration manager tool, then you have to provide a user with the Config permissions, add the user to the `UcceConfig` local security group manually.

To provide a user the Setup permissions, add the user to the `UcceConfig` and local administrator security groups of the AW machine manually.

Key value Set to 1

If the value of the `ADSecurityGroupUpdate` key is set to 1, the AW machine is in the domain authorization mode. If the user is added using the Administrator Gadget or the API with **pre-defined** or , the user is added to the corresponding domain security group. The user is added to the database with the corresponding roles. There is no need to manually add the user to the local groups of the AW machine.

Move to Local Authorization Mode

To move to Local Authorization mode from domain authorization you have to change the registry `ADSecurityGroupUpdate` from 1 to 0.

All the existing users which are available in domain Config and Setup security groups under instance OU must be manually moved to `UcceConfig` local group of all AW machine except Admin Client machine. All the users in the domain setup security group has to be added to the local Administrators group of all AW machine except Admin Client machine.

Remove the users from domain Config and Setup security group under instance OU.

Move to Domain Authorization Mode

To move to domain authorization mode from local authorization mode you have to change the registry `ADSecurityGroupUpdate` from 0 to 1.

All the users in local `UcceConfig` group of all the AW except Admin Client has to be added manually to the domain Config security group.

Remove all users from local `UcceConfig` group.

Identify the system administrator role users from the Administrator Gadget and move those users from local Administrators group of all AW (except Admin Client) to the domain setup security group. Remove those users from local Administrators group.

Organization Setup

Manage Teams

Teams

You can create teams to associate a set of agents with supervisors. Supervisors can run reports on the team and receive Supervisor Assist requests from the team members.



Note Supervisor Assist must be indicated in the Desk Settings tool and must be supported by the agent desktop. Agent cannot be a member of more than one team.

After you create a team with agents and/or supervisors, you can assign resources such as custom desktop layout, phone books, reasons (not ready, sign out, and wrap-up), and workflow to the team.

The desktop layout, phone books, and workflow resources are preconfigured in **Desktop > Resources**. The reasons (not ready, sign out, and wrap-up) are preconfigured in **Desktop > Reason Labels**.

Administrators can see and maintain teams .

Supervisors have display-only access to the Teams tool.

To configure teams, navigate to **Unified CCE Administration > Overview > Organization Setup > Teams**, or choose **Organization > Teams** from the left navigation.

Related Topics

[Add and Maintain Teams](#) , on page 249

[Agents](#), on page 229

[Manage Supervisors](#), on page 239

[Add and Maintain Desk Settings](#), on page 322

Add and Maintain Teams

Procedure

- Step 1** In **Unified CCE Administration** , choose **Organization > Teams** from the left navigation.
- Step 2** Click **New** to open the **New Team** page.
- Step 3** Complete the following fields on the **Basic Details** tab:

Field	Required?	Description
Name	Yes	Enter up to 32 alphanumeric characters.
Description	No	Enter up to 255 characters to describe the team. See Character Sets , on page 601.

Field	Required?	Description
Site	-	<p>The Site field displays Main by default for Packaged CCE 2000 Agents deployment type.</p> <p>To add a different site:</p> <ol style="list-style-type: none"> Click the magnifying glass icon to display the list of sites with Agent PG configured. Select the required site.
Peripheral Set	Yes	<p>Note Before you add a Peripheral Set, you must select a Site.</p> <p>The Peripheral Set field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see Add and Maintain Peripheral Set, on page 143.</p> <p>To select a peripheral set:</p> <ol style="list-style-type: none"> Click the magnifying glass icon to display the list of peripheral sets that are configured for the selected Site. Select the applicable peripheral set.
Supervisor DN (Dialed Number)	No	<p>Click the magnifying glass icon to display the Select Supervisor Script Dialed Number list.</p> <p>The list includes all dialed numbers with a routing type of Internal Voice.</p> <p>Click a row to select a dialed number for the supervisor assistance and close the list.</p>

Step 4 Click the **Team Members** tab.

- Click the + icon to open the **Add Agents** popup window.
 The agents associated to the selected site (and Peripheral Set available for Packaged CCE 4000 Agents and 12000 Agents deployments) appear. If the team is associated with a department, you see only agents associated with that department in the list. If the team is a global team, you see both global and departmental agents in the list.

 The “i” icon indicates that the agent is a member of a team. Hover over the icon to see the name of that team. Clicking an agent who already has a team removes that agent from that team and reassigns the agent to this team.
- Click one or more rows to select agents. The agents are now in **List of Agents**.

Note When you add or remove agents to a team, the same information is updated in the corresponding collection in Unified Intelligence Center.

Step 5 Click the **Supervisors** tab.

- a) Click the + icon to add supervisors to the team. The supervisors associated to the selected site (and Peripheral Set available for Packaged CCE 4000 Agents and 12000 Agents deployments) appear in the **Add Supervisors** popup window. If the team is associated with a department, both global supervisors and supervisors associated with that department appear in the list. If the team is a global team, only global supervisors appear in the list.

- b) Click one or more rows to select the supervisors. The supervisors are now in **List of Supervisors**.

Note When you add Supervisors to a team, the same Supervisors (user accounts in Unified Intelligence Center) are added (with Supervisor permission) to the corresponding collection in Unified Intelligence Center.

Step 6 Click the **Team Resources** tab.

Note Before you configure **Team Resources**, add Agent(s) or Supervisor(s) to the team.

This tab includes the following subtabs to configure the team resources:

Subtab	Description
Desktop Layout	<p>To customize the site (and Peripheral Set available for Packaged CCE 4000 Agents and 12000 Agents deployments) specific desktop layout for the team:</p> <ol style="list-style-type: none"> a. Check the Customize check box. <p>You can now edit the Desktop Layout section. This section includes default desktop layout XML that is defined in Desktop > Resources > Desktop Layout.</p> b. Edit the XML. <p>To revert the changes, click Revert Changes.</p> <p>Note</p> <ul style="list-style-type: none"> • If you clear the Customize check box without saving the changes, the system reverts to the default desktop layout. • To add the Live Data report gadgets to the desktop layout, see Add Live Data Reports to Team Layout, on page 253.
Phone Books	<p>To assign phone books to the team:</p> <ol style="list-style-type: none"> a. Click the + icon. <p>The Add Phone Books pop-up window opens with a list of phone books that are configured for the site (and Peripheral Set available for Packaged CCE 4000 Agents and 12000 Agents deployments). The phone books are configured for Teams in Desktop > Resources.</p> b. Select one or more phone books from the list. Use the Sort a List and Search a List features to navigate the list. <p>The selected phone books are highlighted in the pop-up window, and appear in List of Phone Books. You can click the Name header to sort the phone books.</p> <p>To unassign a phone book from the team, click 'x' next to the phone book in List of Phone Books.</p>

Not Ready Reasons	<p>To assign not ready reasons to the team:</p> <ol style="list-style-type: none"> Click the + icon. <p>The Add Not Ready Reasons pop-up window opens with a list of not ready reasons. The reasons are configured as Team Specific in Desktop > Reason Labels > Phone Books.</p> <ol style="list-style-type: none"> Select one or more reasons from the list. Use the Sort a List and Search a List features to navigate the list. <p>Note The search field does not allow searching the list by code.</p> <p>The selected reasons are highlighted in the popup window, and appear in List of Not Ready Reasons. You can click the Label header to sort the reasons.</p> <p>To unassign a not ready reason from the team, click 'x' next to the reason in List of Not Ready Reasons.</p>
Sign Out Reasons	<p>To assign sign out reasons to the team:</p> <ol style="list-style-type: none"> Click the + icon. <p>The Add Sign Out Reasons popup window opens with a list of sign out reasons. The reasons are configured as Team Specific in Desktop > Reason Labels.</p> <ol style="list-style-type: none"> Select one or more reasons from the list. Use the Sort a List and Search a List features to navigate the list. <p>Note You cannot search the list by code in the pop-up window.</p> <p>The selected reasons are highlighted in the pop-up window, and appear in List of Sign Out Reasons. You can click the Label header to sort the reasons.</p> <p>To unassign a sign out reason from the team, click 'x' next to the reason in List of Sign Out Reasons.</p>
Wrap-Up Reasons	<p>To assign wrap-up reasons to the team:</p> <ol style="list-style-type: none"> Click the + icon. <p>The Add Wrap-Up Reasons pop-up window opens with a list of wrap-up reasons. The reasons are configured as Team Specific in Desktop > Reason Labels.</p> <ol style="list-style-type: none"> Select one or more reasons from the list. Use the Sort a List and Search a List features to navigate the list. <p>The selected reasons are highlighted in the popup window, and appear in List of Wrap-Up Reasons. You can click the Label header to sort the reasons.</p> <p>To unassign a wrap-up reason from the team, click 'x' next to the reason in List of Wrap-Up Reasons.</p>

Workflows	<p>To assign workflows to the team:</p> <ol style="list-style-type: none"> a. Click the + icon. <p>The Add Workflow pop-up window opens with a list of workflows that are configured for the site in Desktop > Resources > Workflows.</p> b. Select one or more workflows from the list. Use the Sort a List and Search a List features to navigate the list. <p>Note You cannot search the list by description in the pop-up window.</p> <p>The selected workflows are highlighted in the pop-up window, and also appear in List of Workflows.</p> c. Close the Add Workflow pop-up window. <p>The workflows are carried out in the order they appear in the List of Workflows. The Order column displays the order of the workflow. The newly added workflow appears at the end of the list.</p> d. To change the workflow order: <ol style="list-style-type: none"> 1. In the Order column, click the drop-down arrow that is associated with the workflow that you want to move. <p>The values in the drop-down are the number of workflows that are selected for the team. The number increments or decrements dynamically when you assign or unassign the workflow.</p> 2. Select a number from the drop-down list. <p>The workflow moves to the selected position in the List of Workflows table. The other workflows move a row up or down based on the new position of the workflow.</p> <p>To unassign a workflow from the team, click 'x' next to the workflow in List of Workflows.</p>
------------------	---

- Step 7** Click **Save** to return to the List window, where a message confirms the successful creation of the team. The team and the associated agents or supervisors appear in the List window. When you create a team in Packaged CCE, the same team record is also created as a collection in Cisco Unified Intelligence Center. The team resources that are assigned to the team appear in Cisco Finesse Admin.

Add Live Data Reports to Team Layout

The Finesse default layout XML contains commented XML code for the Live Data report gadgets available for the Finesse desktop. The gadgets are divided into two categories: HTTPS version of Live Data gadgets and HTTP version of Live Data gadgets.

This procedure explains how to add the Live Data report gadgets to the desktop layout of a specific team. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.

Procedure

Step 1 Copy the XML code for the report you want to add from the Finesse default layout XML.

Example:

To add the Agent Report for HTTPS, copy the following:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
  gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&
  filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
  filterId_2=agent.id=CL%20teamName
</gadget>
```

Step 2 Go to **Organization > Teams**, and open an existing team's record on the list window.

Step 3 Click the **Team Resources** tab.

Step 4 In the **Desktop Layout** tab, check the **Customize** check box.

Step 5 Paste the XML within the tab tags where you want it to appear.

Example:

To add the report to the home tab of the agent desktop:

```
<layout>
  <role>Agent</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
  </page>
  <tabs>
    <tab>
      <id>home</id>
      <label>finesse.container.tabs.agent.homeLabel</label>
      <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
        gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&
        filterId_1=agent.id=CL%20teamName&
        viewId_2=9AB7848B10000141000001C50A0006C4&
        filterId_2=agent.id=CL%20teamName
      </gadget>
    </tab>
    <tab>
      <id>manageCall</id>
      <label>finesse.container.tabs.agent.manageCallLabel</label>
    </tab>
  </tabs>
</layout>
```

Step 6 Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

Step 7 Optionally, change the gadget height.

Example:

The height specified in the Live Data gadget URLs is 310 pixels. If you want to change the height, change the gadgetHeight parameter in the URL to the desired value. For example, if you want the gadget height to be 400 pixels, change the code as follows:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
  gadgetHeight=400&viewId_1=99E6C8E210000141000000D80A0006C4&
  filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
  filterId_2=agent.id=CL%20teamName
</gadget>
```


To maintain the optimal display of the gadget with scroll bars, set the value for the gadget height to a minimum of 200 pixels. If the report does not require scroll bars, for example a one-row report, you can set a smaller gadget height (for example, 100 pixels). If you do not specify anything for the gadget height (if you remove the 310 from the URL), it defaults to 170 pixels.

Step 8 Click **Save**.

Note After you add a gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with a large number of rows, you may want to adjust the gadget height or the screen resolution on the computer used to access the desktop to make the report easier to read or make more rows appear on the screen without needing to scroll down.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.

Note You can also perform the above steps in Unified CCE Administration (<https://<Side A/B Unified CCE AW-HDS-DDS IP address>/cceedminnew>). In Unified CCE Administration, you can navigate to Desktop > Resources to copy the XML code from default layout, and then navigate to Organization > Teams to access the Team Resources paste the XML.

Search for Teams

The Search field in the Team tool offers an advanced and flexible search.

Click the + icon at the right of the Search field in the Team tool. In the popup window, you can:

- Search for a name or description.
- Enter one or more site names separated by spaces. (Site is an OR search.)
- Enter one or more peripheral set names separated by spaces (Peripheral Set is an OR search). The search is case-insensitive and does not support partial matches.



Note Search by peripheral set is available only in Packaged CCE 4000 Agents and 12000 Agents deployments.

- Select departments, with options for **Globals and Departments**, **Globals only**, or **Departments only**.

If you select **Globals and Departments** or **Departments only**, you can only enter a space-separated list of department names. (Department is an OR search.)



Note Search by department is available only when departments are configured.

Search by site is available only when remote sites are configured.

Manage Skills

Calls are queued to agents based on their membership in skill groups or their qualification in precision queues.

Administrators have access to all tools documented in this chapter .

Supervisors have limited access to Skill Groups and display-only access to Attributes and Precision Queues.

Skill Groups

A skill group is a collection of agents who share a common set of competencies that equip them to handle the same types of requests. Some examples of skill groups are a collection of agents who speak a specific language or who can assist callers with billing questions.

An agent can be a member of multiple skill groups. Each skill group is associated with a specific media routing domain (MRD) such as voice, chat, or email.

An agent's skill group membership can determine the types of contacts that are routed to that agent. For example, if an agent is a member of a skill group that is set up for the Cisco_Voice routing domain only, then that agent is a voice agent for that skill group. If an agent is a member of a skill group that is set up for a nonvoice routing domain, then that agent is a multichannel agent for that skill group.

Use Cisco Unified Intelligence Center reports to view agent activity in skill groups, to monitor call distribution among skill groups, or to see how one skill group is performing compared with others.

Navigate to **Unified CCE Administration > Organization > Skills > Skill Groups** to configure skill groups.

Administrators have full permission to configure skill groups. Supervisors have permission to add and remove their supervised agents on the Skill Groups Members tab.

Related Topics

- [Search for Skill Groups](#), on page 259
- [Add and Maintain Skill Groups](#), on page 256
- [Agents](#), on page 229
- [Skill Groups or Precision Queues?](#), on page 262
- [Manage Supervisors](#), on page 239

Add and Maintain Skill Groups

Procedure

- Step 1** Navigate to **Unified CCE Administration > Organization > Skills > Skill Groups**.
- Step 2** Click **New** to open the **New Skill Group** window.
- Step 3** Complete the fields on the **General** tab:

Field	Required	Description
Name	yes	Enter a name using up to 32 alphanumeric characters.
Description	no	Enter up to 255 characters to describe the skill group. See Character Sets , on page 601.

Field	Required	Description
Site	-	<p>The Site field displays Main by default for Packaged CCE 2000 Agents deployment type.</p> <p>To add a different site:</p> <ol style="list-style-type: none"> Click the magnifying glass icon to display the list of sites with Agent PG configured. Select the required site.
Peripheral Set	yes	<p>Note Before you add a Peripheral Set, you must select a Site.</p> <p>The Peripheral Set field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see Add and Maintain Peripheral Set, on page 143.</p> <p>To select a peripheral set:</p> <ol style="list-style-type: none"> Click the magnifying glass icon to display the list of peripheral sets configured for the selected Site. Select the applicable peripheral set.
Media Routing Domain	no	<p>MRDs organize how requests for media are routed. The system routes calls to skill groups or precision queues that are associated with a particular communication medium; for example, voice or email. This field defaults to <i>Cisco_Voice</i>.</p> <p>To select a different Media Routing Domain:</p> <ol style="list-style-type: none"> Click the magnifying glass icon to display Select Media Routing Domain . Click a row to make a selection and close the list.

Field	Required	Description
Bucket Interval	no	<p>Select the bucket interval whose bounds are to be used to measure the time slot in which calls are answered. The field defaults to the system default, see Global, on page 360.</p> <p>To select a different bucket interval:</p> <ol style="list-style-type: none"> Click the magnifying glass icon to display Select Bucket Intervals. Click a row to make a selection and close the list. <p>Click the x icon to clear the selection.</p>
Service Level Threshold	no	<p>Enter a value in seconds that you set as a goal for connecting a call with an agent.</p> <p>The field defaults to the threshold configured for this Media Routing Domain.</p> <p>Leave this field blank to use the service level threshold value for the Media Routing Domain.</p> <p>Enter a value of 0 seconds if you do not want a service level event to be set for the calls. These calls are not treated as service-level calls.</p>
Service Level Type	no	<p>Select a service level type.</p> <p>Service level type indicates how calls that are abandoned before the service level threshold affect the service level calculation.</p> <ul style="list-style-type: none"> • Use Media Routing Domain Value (the default): Select this option to use the value that is currently defined for the MRD. • Ignore Abandoned Calls: Select this option if you want abandoned calls to be excluded from the service level calculation. • Abandoned Calls have Negative Impact: Select this if you want only calls that are answered within the service level threshold time as to be counted as treated calls. The service level is negatively affected by calls that abandon within the service level time. • Abandoned Calls have Positive Impact: Select this if you consider a call abandoned within the service level threshold time as a treated call. With this configuration, abandoned calls have a positive impact on the service level.

Step 4 Complete the **Members** tab:

This tab shows the list of agents for this skill group.

- a) Click the + icon to open **Add Agents**. The agents associated to the selected site (and Peripheral Set available for Packaged CCE 4000 Agents and 12000 Agents deployments) display.
- b) Click the agents you want to add to this skill group.
- c) Close the window. The agents you chose appear on the **List of Agents**.
- d) Click **Save** on this tab to return to the List window, where a message confirms the successful creation of the skill group.

Search for Skill Groups

The Search field in the Skill Groups tool offers an advanced and flexible search.

Click the + icon in the Search field to open a popup window, where you can:

- Enter a name or description to search for that string.
- Enter one or more site names separated by spaces. (Site is an OR search.)
- Enter one or more peripheral set names separated by spaces (Peripheral Set is an OR search). The search is case-insensitive and does not support partial matches.



Note Search by peripheral set is available only in Packaged CCE 4000 Agents and 12000 Agents deployments.

- Select departments, with options for **Globals and Departments**, **Globals only**, or **Departments only**.

Selecting **Globals and Departments** or **Departments only** enables an input field where you can enter a space-separated list of department names. (Department is an OR search.)



Note Search by department is available only when departments are configured.
Search by site is available only when remote sites are configured.

Attributes

Attributes identify a call routing requirement, such as language, location, or agent expertise. You can create two types of attributes: Boolean or Proficiency.

- Use Boolean attributes to identify an agent attribute value as true or false. For example, you can create a Boston attribute that specifies that the agent assigned to this attribute must be located in Boston. An agent in Boston would have *Boston = True* as the term for that attribute.
- Use Proficiency attributes to establish a level of expertise in a range from 1 to 10, with 10 being the highest level of expertise. For a Spanish language attribute, for example, an original speaker would have the attribute *Proficiency = 10*.

When you create a precision queue, you identify which attributes are part of that queue and then implement the queue in a script. When you assign a new attribute to an agent and the attribute value matches the precision queue criteria, the agent is automatically associated with the precision queue.

An attribute can be associated with more than one precision queue, from multiple Media Routing Domains.

Navigate to **Unified CCE Administration > Organization > Skills** and click the **Attributes** tab to configure attributes.

Administrators can see and manage attributes. Supervisors can configure attributes for their supervised agents on the Attributes tab of the Agents tool.

Related Topics

[Add and Maintain Attributes](#), on page 260

[Precision Queues](#), on page 261

Add and Maintain Attributes

Procedure

-
- Step 1** Navigate to **Unified CCE Administration > Organization > Skills** and click the **Attributes** tab.
- Step 2** In the **List of Attributes** window, click **New**. The **New Attributes** window has two tabs: General and Member.
- Step 3** Complete the following fields on the **General** tab:

Field	Required?	Description
Name	yes	Type a unique attribute name. For example, to create an attribute for mortgage insurance, type <i>mortgage</i> .
Description	no	Enter a maximum of 255 characters to describe the attribute. See Character Sets , on page 601.
Type	no	Select the type: Boolean or Proficiency.
Default	no	Select the default (True or False for Boolean, or a number from 1 to 10 for Proficiency).

- Step 4** To associate one or more agents to this attribute, click on the **Agents** tab, and then click **New**.
- Step 5** Click **Add**.
- Step 6** In the **Add Agents** window, click on one or more of the agents listed to add them to the **List of Agents** window. Once you are finished, close the window.
- Step 7** Set the attribute value as appropriate for each agent using the **Attribute Value** drop-down menus.
- Step 8** Click **Save**.
-

Precision Queues

Precision routing offers a multidimensional alternative to skill group routing: using Unified CCE scripting, you can dynamically map the precision queues to direct a call to the agent who best matches the caller's precise needs. Precision queues are the key components of precision routing.

To configure Precision Routing, you must do the following:

1. Create attributes. Attributes are characteristics that can be assigned a True | False value or a Proficiency rating from 1 to 10.
2. Assign attributes to agents.
3. Create precision queues.
4. Create routing scripts.

There is no need to add an agent to a precision queue; agents become members of precision queues automatically based on their attributes. If a precision queue requires an agent who lives in Boston, who speaks fluent Spanish, and who is proficient in troubleshooting a specific piece of equipment, an agent with the attributes *Boston = True*, *Spanish = True*, and *Repair = 10* is automatically part of the precision queue. A Spanish caller in Boston who needs help with equipment is routed to that agent.

A precision queue includes:

- **Terms:** A term compares an attribute against a value. For example, you can create the following term: *Spanish == 10*. The term of the attribute is the highest proficiency in Spanish.

Each precision queue can have multiple attributes, and these attributes can be used in multiple terms. For example, to select an agent with a Spanish proficiency value between 5 and 10, you would create one term for *Spanish > 5* and another for *Spanish < 10*.

- **Expressions:** An expression is a collection of one or more terms. The terms in an expression must share the same operator—they must all be AND or must all be OR relationships.

- **Steps:** A precision queue step is a time-based routing point within the precision queue. A step is a collection of one or more expressions.

A step may also include wait time and a Consider If formula. Use wait time to assign a maximum amount of time to wait for an available agent. Use a Consider If formula to evaluate the step against predefined criteria, for example, another queue.

Steps

Name	Criteria
Step 1	[(Spanish == 10) and (Boston == true)] OR [(ServerXYZ >= 6) and (Spanish >= 6)]

302761

Navigate to **Unified CCE Administration > Organization > Skills > Precision Queues** to configure precision queues.

Navigate to **Unified CCE Administration > Organization > Skills > Precision Queues** to configure precision queues.

Administrators have full permission to configure precision queues. Supervisors have display-only access to the Precision Queues tool.

When you add or modify precision queues associated with a large number of agents, the system avoids potential overload conditions by updating the agent associations as system resources allow. Precision queue updates may be rejected if the system is too busy.

Skill Groups or Precision Queues?

Should you use skill groups or precision queues for the routing needs of your organization? This section distinguishes the two methods.

Use a Skill Group

A skill group represents a competency or responsibility. For example, it could be a predefined collection of traits, such as salespeople who are in charge of selling to England. The skill group could be called “English sales”. If you wanted to divide the agents in this group into two types of proficiencies (perhaps based on experience), you would need to set up two separate skill groups; for example, English Sales 1 and English Sales 2. You would then associate an agent with one of them, based on the agent's proficiency. Do this by accessing the skill group and locating the agent that you want to add to it (or add that skill group to the agent). To summarize, creating a skill group involves first building a concept of what combinations of traits you want for each agent, like English Sales 2.

Use a Precision Queue

In contrast to skill groups, a precision queue breaks down attribute definitions to form a collection of agents at an *attribute* level. The agents that match the attribute level of the precision queue become associated with that precision queue.

With precision queues, the preceding English sales example involves defining the attributes English and Sales, and associating agents that have those traits to them. The precision queue English Sales would dynamically map all those agents that had those traits to the precision queue. In addition, you can define more complex proficiency attributes to associate with those agents. This would allow you to build, in a single precision queue, multiple proficiency searches like English language proficiency 10 and sales proficiency 5.

To break down the precision queue example into skill groups, you would need to set up two separate skill groups: English language proficiency 10 and sales proficiency 5. With precision queues, you can refine agents by attributes. With skill groups, you define a skill group and then assign agents to it.

Decide on Skill Groups or a Precision Queue

Precision routing enhances and can replace traditional routing. Traditional routing looks at all of the skill groups to which an agent belongs and defines the hierarchy of skills to map business needs. However, traditional routing is restricted by its single-dimensional nature.

Precision routing provides multidimensional routing with simple configuration, scripting, and reporting. Agents are represented through multiple attributes with proficiencies so that the capabilities of each agent are accurately exposed, bringing more value to the business.

If your routing needs are not too complex, consider using one or two skill groups. However, if you want to conduct a search involving as many as ten different proficiency levels in one easily managed queue, use precision queues.

Add and Maintain Precision Queues

Before you begin

Before you can create precision queues, you must create attributes (see [Add and Maintain Attributes](#), on page 260).

Procedure

Step 1 Navigate to **Unified CCE Administration > Organization > Skills > Precision Queues**.

This opens a **List of Precision Queues** window showing all precision queues that are currently configured.

Step 2 Click **New** to open the **New Precision Queue** window. Complete the fields.

Name	Required?	Description
Name	yes	Enter up to 32 alphanumeric characters.
Description	no	Enter up to 255 characters to describe the precision queue. See Character Sets , on page 601.
Media Routing Domain	no	MRDs organize how requests for media are routed. The system routes calls to skill groups or precision queues that are associated with a particular communication medium; for example, voice or email. This field defaults to <i>Cisco_Voice</i> . To select a different Media Routing Domain: <ol style="list-style-type: none"> Click the magnifying glass icon to display Select Media Routing Domain. Click a row to make a selection and close the list.

Name	Required?	Description
Service Level Type	yes	<p>Select the service level type used for reporting on your service level agreement.</p> <p>Service level type indicates how calls that are abandoned before the service level threshold affect the service level calculation.</p> <ul style="list-style-type: none"> • Ignore Abandoned Calls (the default): Select this option if you want to exclude abandoned calls from the service level calculation. • Abandoned Calls have Negative Impact: Select this option if you want only those calls that are answered within the service level threshold time to be counted as treated calls. The service level is negatively affected by calls that abandon within the service level threshold time. • Abandoned Calls have Positive Impact: Select this option if you consider a call that is abandoned within the service level threshold time as a treated call. With this configuration, abandoned calls have a positive impact on the service level.
Service Level Threshold	yes	<p>Enter the time in seconds that calls are to be answered based on your service level agreement, from 0 to 2,147,483,647.</p> <p>The time that you enter in this field is used to report on service level agreements and does not affect how long a call remains in a precision queue. The length of time a call remains in a step is determined by the wait time for each individual step.</p>

Name	Required?	Description
Agent Order	yes	<p>Select an option to determine which agents receive calls from this queue.</p> <p>The ordering of agents does not dictate the agents who are selected into a Precision Queue step. Agents are included or excluded based on the conditions specified for the step.</p> <ul style="list-style-type: none"> • Longest Available Agent (the default): The default method of agent ordering for a precision queue. The call is delivered to the agent who has been in the available (or ready) state the longest. • Most Skilled Agent: The call is delivered to the agent who has the highest competency sum from all the attributes pertinent to the Precision Queue step. In an agent-rich environment, this can mean that more competent agents would be utilized more than less competent agents. • Least Skilled Agent: The call is delivered to the agent who has the lowest competency sum from all the attributes pertinent to the Precision Queue step.
Bucket Intervals	no	<p>Select the bucket interval whose bounds are to be used to measure the time slot in which calls are answered. The field defaults to the system default (see Global, on page 360).</p> <p>To select a different bucket interval:</p> <ol style="list-style-type: none"> a. Click the magnifying glass icon to display Select Bucket Intervals. b. Click a row to make a selection and close the list.

Step 3 Click the numbered Step Builder link (Step 1, Step 2, and so on) to build a precision queue step in the **Step Builder** popup window.

Step 4 When you have finished adding, click **Save**.

Build Precision Queue Steps

Every precision queue must have a step, and every step must have an Expression. An Expression is a collection of attribute terms.

Procedure

- Step 1** Click the numbered step link in the **Steps** panel (Step 1, Step 2, and so on).
The step number popup window opens.
- Step 2** Build the first step as follows.
- Click the **magnifying glass** icon to the right of the Select Attribute field in the Expression 1 panel.
 - Select an attribute from the list.
 - Use the two **Select** fields to establish the terms of the attribute. Click the first **Select** field to choose an operator.
 - For Boolean attributes, choices are the operators for Equal and Not Equal.
 - For Proficiency attributes, choices are the operators for True, False, Less Than, Less Than or Equal To, Greater Than, and Greater Than or Equal To.
 - Click the second **Select** field to choose a value.
 - For Boolean attributes, values are True and False.
 - For Proficiency attributes, values are numbers from 1 to 10.
- Your selection creates an attribute term for the Expression.
- Step 3** To add a second attribute to the first Expression, click **Add Attribute** in the **Expression 1** row.
- Select **AND** or **OR** to establish the relationship between the first and second attributes.
 - Repeat steps 2b, 2c, and 2d.
- Step 4** Continue to add attributes to Expression 1.
All attributes within an expression must be joined by the same logical operator. They must all be ANDs, or they must all be ORs.
- Step 5** To add a second Expression, click the **Add Attribute** drop-down in the **Expression 1** row and select **Add Expression**.
- Step 6** Select **AND** or **OR** to establish the relationship between the first and second Expressions.
- Step 7** Add attributes to Expression 2.
- Step 8** Continue to add Expressions as needed.

In this example, a Spanish caller located in the Boston area needs an onsite visit from a technician to repair his ServerXYZ. An ideal agent should be fluent in Spanish and have the highest proficiency in ServerXYZ. This can be seen in Expression 1. Expression 2 allows us to specify that the selected agent must also be from either Boston or the New England area.

Step 9 When you have completed the step, click **OK** to add it to the precision queue.

Step 10 To build the next step, click **Add Step**.

Each successive step is prepopulated with the Expressions and attributes of its predecessor. Decrease the attribute qualifications and competencies in successive steps to lower the bar such that the pool of acceptable agents increases.

Step 11 When you have created all steps, you can open any step *except the last* and enter values in the **Consider if** and **Wait for** fields.

- **Consider if** is a formula that evaluates a call within a step against additional criteria. (See [Consider If Formula for Precision Queue, on page 267](#) for more information about Consider If.)
- **Wait for** is a value in seconds to wait for an available agent. A call will queue at a particular step and wait for an available agent matching that step criteria until the number of seconds specified. A blank wait time indicates that the call will proceed immediately to the next step if no available agents match the step criteria. Wait time defaults to 0 and can take a value up to 2147483647.

Consider If Formula for Precision Queue

If you are not on the last step of the precision queue, then you can enter a *Consider If* formula for that step. A Consider If formula evaluates a call (within a step) against additional criteria. Each time a call reaches a step with a Consider If expression, the expression is evaluated. If the value for the expression returns as true, the call is considered for the step. If the value returns as false, the call moves to the next step. If no expression is provided for a step, the step is always considered for calls.

To add a Consider If formula, type the formula into the **Consider If** box. Alternatively, you can use the Script Editor to build the formula and then copy and paste it into the **Consider If** box. Objects used in Consider If formulas are case-sensitive. All Consider If formulas that you add to a precision queue must be valid. If you

add an invalid formula, you cannot save the precision queue. To ensure that the formula is valid, use Script Editor to build and validate the formula.

Only the following scripting objects are valid in a Consider If formula:

- Call
- PQ
- Skillgroup
- ECC
- PQ Step
- Call Type
- Custom Functions (You can create custom functions in Script Editor.)

It is possible that a valid Consider If formula can become invalid. For example, if you delete an object used in the formula after you create or update the precision queue, the formula is no longer valid.

Consider If Formula Examples

- **PQ.PQ1.LoggedOn > 1**--Evaluates whether there is more than one agent logged in to this queue.
- **CallType.CallType1.CallsRoutedToday > 100**--Evaluates whether more than 100 calls of this call type were routed today.
- **PQStep.PQ1.1.RouterAgentsLoggedIn > 1**--Evaluates whether there is more than one router agent logged in to this queue for Step 1.
- **CustomFunction(Call.PeripheralVariable1) > 10**--Evaluates whether this formula using a custom function returns a value greater than 10.

Precision Queue Call Flow Example

At a high level, consider a 5-step precision queue with a Consider If formula for *Caller is Premium Member* attached to the Step 1:

- Step 1 - Attribute: Skill > 8 - Consider If: Caller is Premium Member
- Step 2 - Attribute: Skill > 6
- Step 3 - Attribute: Skill > 4
- Step 4 - Attribute: Skill > 3
- Step 5 - Attribute: Skill >= 1

Caller John, who is not a premium customer, calls 1-800-repairs. John's call is routed to this precision queue.

- Since John is not a premium customer, John is immediately routed out of Step 1 (because of the Consider If on Step 1) and into Step 2 where John waits for the call to be answered.
- After the Step 2 wait time has expired, John's call moves to Step 3 to wait for an agent.
- After the Step 3 wait time has expired, John's call moves to Step 4 to wait for an agent.

- When it arrives at Step 5, John's call will wait indefinitely for an available agent. This step cannot be avoided by any call because there is no routing logic past this.

The overarching idea is that customer will use each successive step to expand the pool of available agents. Eventually, when you reach the "last" step (the step with the highest number), the call is waiting in a potentially very large pool of agents. With each extra step, the chances of the call being handled increase. This also puts the most valuable and skilled agents in the earlier precision queue steps. Calls come to them first before moving on the less appropriate agents in later steps.



Note When two or more agents have the same proficiency level for the attributes the PQ step leverages the Longest Available Agent (LLA).

Manage Departments

Departments

You have the option to create departments to facilitate contact center operation and maintenance. A contact center for a hospital might create departments for Surgery, Radiology, Obstetrics, and other operational units. A contact center for a university might create departments for Admissions, Alumni, and Registration. Departments are not required, and there are no built-in departments.

If you do not create departments, all administrators and objects are *global*, meaning that they are not associated with a department.

If you create departments, you have the option to associate a department with each administrator and object. These are called *departmental* administrators and objects. Your Packaged CCE configuration can include a mix of global and departmental administrators and objects.

You can create routing scripts for a department by referencing objects from that department in the scripts.

You can also create custom reporting collections in Cisco Unified Intelligence Center to report on departmental objects. See the *Cisco Unified Intelligence Center Report Customization Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-user-guide-list.html> for directions on customizing reports.

Departmental Objects

The following objects can be associated with a single department. If departments are configured, the List screens for these objects have a Department column. The New and Edit windows for these objects have a Department field.

- Agents
- Attributes
- Bucket intervals
- Call types
- Desk settings
- Dialed numbers

- Network VRU scripts
- Precision queues
- Skill groups
- Teams

Relationships Between Global and Departmental Objects

You can create relationships between objects in your configuration. For example, you can associate an agent with skill groups, a call type with a dialed number, and so on. An object's department assignment controls the relationships it can have to other objects.

The rules for creating relationships between objects are as follows:

- A **global** object can be associated with any global or departmental objects. For example, when you are assigning skill groups to a global agent, the skill group selection list includes global skill groups and skill groups in all departments to which you have access.
- A **departmental** object can be associated with global objects or with objects in the same department. For example, when you are assigning skill groups to an agent in Department A, the skill group selection list includes global skill groups and skill groups in Department A.

These rules are summarized in the following table.

Table 27: Rules for Relationships Between Global and Departmental Objects

Object Type	Can be associated with Global object?	Can be associated with Departmental object?
Global	yes	yes, with objects from any department
Departmental	yes	yes, with objects from same department only

The only exceptions to these rules are for the relationships between the following objects:

- **Teams and agent:** A global agent can belong only to a global team. A departmental agent can belong either to a global team or to a team that is associated with the same department.
- **Teams and supervisors:** Global supervisors can supervise both global and departmental teams. Departmental supervisors can supervise only teams that are associated with the same department.

These exceptions prevent departmental supervisors from modifying global agents, and are summarized in the following table.

Table 28: Rules for Relationships Between Teams and Agents and Teams and Supervisors

	Agent - Global	Agent - Departmental	Supervisor - Global	Supervisor - Departmental
Team - Global	yes	yes	yes	no
Team - Departmental	no	yes (same department only)	yes	yes (same department only)

Change Departments for an Object

When you change the department for an object, relationships with objects in the original department are cleared; relationships with global objects and objects in the new department remain intact. For example, if you change an agent from Department A to Department B, any skill groups in Department A that had been associated with the agent are cleared.

For some objects, such as call type, the Edit window does not show all related objects. If you try to change the department for those objects, you see an error indicating that you cannot change the department because a related object is in the original department. For example, you see this error if you try to change a call type from Department A to Department B and it is related to a dialed number in Department A. You must change the department of the dialed number before you can change the department of the call type.

System-wide Settings and Global Objects

Only global objects can be selected for system-wide settings in the **Call Settings > Labels**.

Global and Departmental Administrators

When you create administrators, you can configure them as global administrators or associate them with departments. See [Add and Maintain Administrators, on page 244](#).

Global administrators

Global administrators:

- Have read and write access to departmental objects and global objects on all tools and menus that are allowed for their role.
- Can use Script Editor or Internet Script Editor to modify routing scripts.

Departmental administrators

Departmental administrators:

- Can be associated with multiple departments. They have read and write access to global objects and objects in their departments on all tools and menus that are allowed for their role.
- A departmental administrator with the ConfigAdmin role has read-only access to the General tools on the System menu: Information, Settings, Deployment, and Agent Trace.
- Can use Internet Script Editor to modify scripts that reference objects associated with their departments. Departmental administrators cannot log into Script Editor.

Add and Maintain Departments

To add, edit, or delete departments, an administrator must have the SystemAdmin role.

This procedure explains how to add a department. For information on maintaining departments, see [Update Objects, on page 154](#) and [Delete Objects, on page 157](#).

Procedure

- Step 1** Navigate to **Unified CCE Administration > Organization > Departments**.
A **List of Departments** window opens.

- Step 2** Click **New** to open the **New Department** window.
- Step 3** Complete the fields on the **General** tab:
- Name** (Required) Enter a unique name for the department, using a maximum of 32 characters.
 - Description** (Optional) Enter a maximum of 255 characters to describe the department. See [Character Sets, on page 601](#) for details on valid characters for this field.
- Step 4** Click the **Administrators** tab.
- This tab shows the Username and Domain of the administrators who currently serve as department administrators and allows you to add or remove administrators.
- Click the + icon to open the **Add Administrators** popup window.
 - Click one or more rows to select administrators; then close the popup window. The administrators are now on the List of Administrators.
 - Click the x icon to remove an administrator from the list.
- Step 5** Click **Save** to return to the list window, where a message confirms the successful creation of the department.
-

Manage Campaigns

Add and Maintain Agent Based Campaigns

This procedure explains how to add an agent based campaign. For information on maintaining campaigns, see [Update Objects](#) and [Delete Objects](#).

Procedure

- Step 1** In **Unified CCE Administration**, choose **Organization > Campaigns**.
- Step 2** On the **Campaigns** page, click **New** and then choose **Agent Based**.
- Step 3** On the **New Agent Based Campaign**, complete the following information on the **General** tab.

Field	Required?	Description
Name	Yes	Enter a unique name for the campaign. Maximum length is 32 characters. Valid characters are alphanumeric, period (.), and underscore (_). The first character must be alphanumeric. Note You cannot use the system reserved terms such as dnc and none as a campaign name.
Status	-	The option to enable or disable the campaign. It is enabled by default.
Type	-	Displays Agent Based by default.

Field	Required?	Description
Dialing Mode	Yes	Select a dialing mode from the drop-down list. <ul style="list-style-type: none"> • Predictive: The Dialer component determines the number of customers to dial per agent, based on the abandoned rate. The agent must take the call if logged in to a campaign skill group. • Progressive: The administrator specifies a fixed number of lines to dial per agent instead of the Dialer component determining the number of lines. The agent must take the call if logged in to a campaign skill group. • Preview: The agent previews customer information on their desktop, and chooses to contact the customer, skip to another customer, or reject the call. • Preview Direct: This is similar to the Preview mode, except that the dialer automatically dials the call from the agent's phone after the agent accepts.
Description	No	Enter up to 255 characters to describe the campaign. See Character Sets , on page 601.
Schedule section		
Start Date	No	The date that the campaign starts.
End Date	No	The date that the campaign ends.
Start Time	Yes	The time the campaign starts dialing customer numbers.
End Time	Yes	The time the campaign stops dialing customer numbers.
Time Zone	Yes	The time zone where the campaign runs.
Dialing Option section		
Note	This section appears only after you select the Dialing Mode as Predictive or Progressive .	
Lines Per Agent	No	The number of lines dedicated to each agent in the campaign. Range is 1 – 100. Default is 1.5.
Maximum Lines Per Agent	No	This field appears only after you select the Dialing Mode as Predictive . The upper bound for the number of customers the dialer dials for a reserved agent when a campaign is running in predictive mode. Range is 1 – 100. Default is 2.

Field	Required?	Description
Call Abandon Limit	-	This field appears only after you select the Dialing Mode as Predictive . A call is considered abandoned if a person answers it and the contact center does not connect the call to an agent within two seconds of the person's completed greeting. The granularity is to one-tenth of a percent. Default is 3.
Limit	No	You can set the limit for abandon calls only after you enable the Call Abandon Limit option. You can set a limit (0.1-100) for the percentage of abandoned calls in a campaign. If the Call Abandon Limit option is disabled, the campaign dials without regard to the abandon limit.
Call Progress Analysis (CPA)	-	Enabled by default. Note If you keep it enabled, make sure you have configured and enabled Call Progress Analysis in the Voice Gateway.
Record CPA	-	If you enable this option, the gateway provides a media stream and the dialer records the .wav files.
Answering Machine Treatment	-	Enabled by default. This enables the dialer to detect an answering machine. From the drop-down list, choose one of the following actions that the dialer must perform when the dialer detects an answering machine: <ul style="list-style-type: none"> • Abandon Call: Drops the call, marks it as an answering machine, and schedules a retry. This option is selected by default. • Transfer to Agent: Transfers the call to an agent. • Transfer to IVR Route Point: Transfers the call to play a prerecorded message. The IVR route point is configured in the Skill Group selection dialog box on the Skill Groups tab.
Terminate Tone Detect	-	This field is activated only when the Answering Machine Treatment field enabled and you select the Transfer to IVR Route Point option from the drop-down list. You can enable this field to allow the dialer to transfer the call to IVR route point after detecting the answering machine beep.
Callback Settings section		
Personalized Callback	-	Enable this option allows an agent to schedule a callback to a customer for a specific date and time. A personal callback connects the same agent who initiated the callback to the customer.

Field	Required?	Description
Missed Callback	Yes (When Personalized Callback option is enabled.)	<p>Select an option from the drop-down list to handle the personal callback in case the agent is not available.</p> <ul style="list-style-type: none"> • Abandon: Abandon the personal callback. This option is selected by default. • Same time next business day: Reschedule the personal callback to the same time the next business day. • Use campaign dialed number: Use the alternate dialed number.

Step 4 On the **Skill Group** tab, click **Add** to open the **Add Skill Group** pop-up window.

Note You must add at least one Skill Group for a campaign.

Step 5 Complete the following information in the **Add Skill Group** pop-up window.

Field	Required?	Description
Site	Yes	Select a site from the drop-down list. Based on the site, you can select peripheral set, skill group and dialed number in the subsequent fields.
Peripheral Set	Yes	<p>This field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see Add and Maintain Peripheral Set, on page 143.</p> <p>Select a peripheral set from the drop-down list. The list contains the peripheral sets associated to the selected site.</p>
Skill Group	Yes	<p>Click the Search icon to open the Add a Skill Group pop-up.</p> <p>You can search and select the Skill Group based on the name and description.</p> <p>The search result does not display the Skill Groups that are already added to a Campaign.</p>
Dialed Number	Yes	<p>Click the Search icon to open the Add Dialed Number pop-up.</p> <p>By default, you can view all the dialed numbers for which the Routing Type is set as Outbound Voice.</p> <p>You can search and select the dialed number based on the string value and description.</p> <p>The search result does not display the dialed numbers that are already added to a Campaign.</p> <p>The selected number is dialed to reserve an agent in the configured skill group.</p>

Field	Required?	Description
Contact Records Cache Size	No	Enter the minimum number of dialing numbers that each dialer caches for each of the Outbound Option skill groups. Range is 1 – 400. Default is 1.
Reserve Additional Agents	No	This field is available only if the dialing mode is selected as Preview or Preview Direct on the General tab. Enter the number of agents reserved for the campaign. This ensures that there is always at least one extra agent reserved before the dialer begins dialing. Range is 0 – 100. Default is 0.
Dialed Numbers for Transferring to an IVR Section		
Answering machine to IVR	No	Click the Search icon to open the Add Dialed Number pop-up. By default, you can view all the dialed numbers for which the Routing Type is set as Outbound Voice . You can search and select the dialed number based on the string value and description. The selected number indicates the route point required to do the transfer to IVR routing script.
Agent not available for IVR	No	Click the Search icon to open the Add Dialed Number pop-up. By default, you can view all the dialed numbers for which the Routing Type is set as Outbound Voice . You can search and select the dialed number based on the string value and description. The selected number is dialed to play a message to the calls about to be disconnected due to lack of available agents.

Step 6 Click **Add**.

Note To delete the Skill Groups from the campaign, check the check box corresponding to Skill Groups on the **Skill Group** tab and click **Delete** and confirm your intention to delete.

Or

Hover the mouse pointer over the row for a Skill Group to see the **delete (x)** icon at the end of the row. Click the **x** icon and confirm your intention to delete.

Step 7 Click the **Advanced** tab and complete the following information:

Field	Required?	Description
Dialing Option section		
No answering ring limit	No	Enter the number of times the system allows a dialed phone number to ring. Range is 2 – 10. Default is 4.
Maximum attempts	No	Enter the maximum number of attempts, including callbacks and retries. Range is 1 – 100. Default is 3.

Field	Required?	Description
Abandoned call wait time	Yes	Enter the minimum duration (in seconds) of an outbound call. Range is 0 – 10. Default is 1. Note If the call duration is less than the specified value, the system considers the call to be customer abandoned and schedules the record for a retry. To disable this feature, set the parameter to 0.
Campaign prefix digits	No	Enter the digits to prefix to each customer number dialed from this campaign. Maximum length is 15 digits.
Retries section		
No answer delay	No	Enter the time (in minutes) the dialer waits before calling back a no-answer call. Range is 1 – 99999. Default is 60.
Busy signal delay	No	Enter the time (in minutes) the dialer waits before calling back a busy phone number. Range is 1 – 99999. Default is 60.
Customer abandoned delay	No	Enter the time (in minutes) the dialer waits before calling back, if a customer abandons a call. Range is 1 – 99999. Default is 30.
Dialer abandoned delay	No	Enter the time (in minutes) the dialer waits before calling back, if the dialer abandons a call. Range is 1 – 99999. Default is 60.
Answering machine delay	No	Enter the time (in minutes) the dialer waits before calling back, if an answering machine answers a call. Range is 1 – 99999. Default is 60.
Customer not home delay	No	Enter the time (in minutes) the dialer waits before calling back, if a customer is not home. Range is 1 – 99999. Default is 60.
Call Progress Analysis(CPA) Parameters section		
Minimum Silence Period(100-1000)	No	Minimum silence period required to classify a call as voice detected. If many answering machine calls are being passed through to agents as voice, then increasing this value accounts for longer pauses in answering machine greetings. Default is 608.
Analysis Period(1000-10000)	NO	Number of milliseconds spent analyzing this call. If there is a short agent greeting on an answering machine, then a longer value here categorizes that answering machine call as voice. If the call is to a business where the operator has a longer scripted greeting, a shorter value here categorizes the long, live greeting as answering machine. Default is 2500.
Minimum Valid Speech(50-500)	NO	Minimum number of milliseconds of voice required to qualify a call as voice detected. Default is 112.
Maximum Analysis Time(1000-10000)	NO	Maximum number of milliseconds allowed for analysis before identifying a problem analysis as dead air/low volume. Default is 3000.

Field	Required?	Description
Maximum termination tone analysis(1000-60000)	NO	Maximum milliseconds the dialer analyzes an answering machine voice message looking for a termination tone. If the message has an odd tone and the analysis does not recognize it, the call is not transferred or dropped until this timeout occurs. Default is 30000.

Step 8 Click **Save**.

Add and Maintain IVR Based Campaigns

This procedure explains how to add an IVR Based outbound campaign map the Skill Groups for the campaign. For more information about maintaining campaigns, see [Update Objects](#) and [Delete Objects](#).

Procedure

Step 1 In **Unified CCE Administration**, choose **Organization > Campaigns** to open the **Campaigns** page.

Step 2 Click **New** and choose **IVR Based** to open the **New IVR Based Campaign** page.

Step 3 Complete the following information on the **General** tab.

Field	Required?	Description
Name	Yes	Enter a unique name for the campaign. Maximum 32-character string, including alphanumeric characters, periods (.), and underscores (_). Alphabetic characters can be upper or lowercase. The name must begin with an alphanumeric character. Note You cannot use the system reserved terms such as dnc and none as a campaign name.
Status	-	The option to enable or disable the campaign. It is enabled by default.
Type	-	The default field value is set to IVR Based . You cannot edit this field.
Dialing Mode	Yes	From the drop-down list, choose the dialer type for the current IVR campaign. <ul style="list-style-type: none"> • Predictive: The dialer component determines the number of customers to dial per IVR port, based on the abandoned rate. • Progressive: The administrator specifies a fixed number of lines to dial per IVR port. Note An unattended campaign can use either the Progressive or Predictive mode. You can play a different prompt for a live customer or for an answering machine.
Description	No	Enter a description about the campaign using up to 255 characters. See Character Sets, on page 601 .

Field	Required?	Description
Schedule section		
Start Date	No	Select the date that the campaign starts.
End Date	No	Select the date that the campaign ends.
Start Time	Yes	Enter the time that the campaign starts dialing the customer numbers.
End Time	Yes	Enter the time that the campaign stops dialing the customer numbers.
Time Zone	Yes	Choose the time zone where the campaign runs.
Dialing Option section		
Lines Per Agent	No	The number of lines dedicated to each IVR port for the campaign. Range is 1 – 100. Default is 1.5.
Maximum Lines Per Agent	No	This field appears only after you select the Dialing Mode as Predictive . The upper bound for the number of customers the dialer dials for a reserved IVR port when a campaign is running in predictive mode. Range is 1 – 100. Default is 2.
Abandon Calls Limit	-	This field appears only after you select the Dialing Mode as Predictive . A call is considered abandoned if a person answers it and the contact center does not connect the call to IVR within two seconds of the person's completed greeting. The granularity is to one-tenth of a percent. Default is 3.
Limit	No	You can set the limit for abandon calls only after you enable the Call Abandon Limit option. You can set a limit (0.1-100) for the percentage of abandoned calls in a campaign. If the Call Abandon Limit option is disabled, the campaign dials without regard to the abandon limit.
Call Progress Analysis (CPA)	-	If you enable this option, the gateway provides a media stream and the dialer records the .wav files. Note If you keep it enabled, make sure you have configured and enabled Call Progress Analysis in the Voice Gateway.
Record CPA	-	If you enable this option, the gateway provides a media stream and the dialer records the .wav files.

Field	Required?	Description
Answering Machine Treatment	-	<p>This field is enabled by default to allow the dialer to detect an answering machine. From the drop-down list, choose one of the following actions that the dialer must perform when the dialer detects an answering machine:</p> <ul style="list-style-type: none"> • Abandon Call: Drops the call, marks it as an answering machine, and schedules a retry. This option is selected by default. • Transfer to IVR Route Point: Transfers the call to play a prerecorded message. The IVR route point is configured in the Skill Group selection dialog box on the Campaign Skill Groups tab. <p>Note After you configure a Transfer to IVR Route Point, you cannot set the AMD records as Retry. Use a customized query to identify such calls and create a new campaign.</p>
Terminate Tone Detect	-	<p>This field is activated only when the Answering Machine Treatment field enabled and you select the Transfer to IVR Route Point option from the drop-down list.</p> <p>You can enable this field to allow the dialer to transfer the call to IVR route point after detecting the answering machine beep.</p>
Callback Settings section		
Personalized Callback	-	Enable this option allows the IVR port to schedule a callback to a customer for a specific date and time.
Missed Callback	Yes (When Personalized Callback option is enabled.)	<p>Select an option from the drop-down list to handle the personal callback in case the agent is not available.</p> <ul style="list-style-type: none"> • Abandon: Abandon the callback. This option is selected by default. • Same time next business day: Reschedule the callback to the same time the next business day. • Use campaign dialed number: Use the alternate dialed number.

Step 4 Click the **Skill Group** tab and then click the **Add** button to add the skill groups for the current IVR campaign.

Note You must add at least one Skill Group for a campaign.

Step 5 Complete the following information in the **Add Skill Group** pop-up window.

Field	Required?	Description
Site	Yes	Select a site from the drop-down list. Based on the site, you can select peripheral set, skill group and dialed number in the subsequent fields.

Field	Required?	Description
Peripheral Set	Yes	<p>This field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see Add and Maintain Peripheral Set, on page 143.</p> <p>Select a peripheral set from the drop-down list. The list contains the peripheral sets associated to the selected site.</p>
Skill Group	Yes	<p>Click the Search icon to open the Add a Skill Group pop-up.</p> <p>You can search and select the Skill Group based on the name and description.</p> <p>The search result do not display the Skill Groups that are already added to a Campaign.</p>
Dialed Number	Yes	<p>Click the Search icon to open the Add Dialed Number pop-up.</p> <p>By default, you can view all the dialed numbers for which the Routing Type is set as Outbound Voice.</p> <p>You can search and select the dialed number based on the string value and description.</p> <p>The search result do not display the dialed numbers that are already added to a Campaign.</p> <p>The selected number is dialed to reserve an IVR port in the configured skill group.</p>
Contact Records cache Size	Yes	<p>Enter the minimum number of dialing numbers that each dialer caches for each of the Outbound Option skill groups. Range is 1 – 400. Default is 1.</p>
Number of IVR Ports	No	<p>Enter the total number of IVR ports allocated for the specified skill group.</p> <p>This value indicates how many ports are available for the dialer to transfer customer calls. The application uses one IVR to play different messages based on the route point where the contact is transferred. If there are multiple dialers associated with this skill group, each dialer dials a fraction of the total number of ports.</p>
Dialed Numbers for Transferring to an IVR Section		
Answering Machine to IVR	Yes	<p>Click the Search icon to open the Add Dialed Number pop-up.</p> <p>By default, you can view all the dialed numbers for which the Routing Type is set as Outbound Voice.</p> <p>You can search and select the dialed number based on the string value and description.</p> <p>When the dialer identifies the answering machine, the selected number is dialed to transfer the call to IVR routing script. The routing script transfers the call to an IVR.</p>

Step 6

Click **Add**.

The newly added Skill Group is displayed on the **Skill Group** tab for the current campaign.

Note To delete the Skill Groups from the campaign, check the check box corresponding to Skill Groups on the **Skill Group** tab and click **Delete**, and confirm your intention to delete.

Or

Hover the mouse pointer over the row for a Skill Group to see the **delete (x)** icon at the end of the row. Click the **x** icon and confirm your intention to delete.

Step 7

Click the **Advanced** tab and complete the following information.

Field	Required?	Description
Dialing Option section		
No answering ring limit	No	Enter the number of times the system allows a dialed phone number to ring. Range is 2 – 10. Default is 4.
Maximum attempts	No	Enter the maximum number of attempts, including callbacks and retries. Range is 1 – 100. Default is 3.
Abandoned call wait time	Yes	Enter the minimum duration (in seconds) of an outbound call. Range is 0 – 10. Default is 1. Note If the call duration is less than the specified value, the system considers the call to be customer abandoned and schedules the record for a retry. To disable this feature, set the parameter to 0.
Campaign prefix digits	No	Enter the digits to prefix to each customer number dialed from this campaign. Maximum length is 15 digits.
Retries section		
No answer delay	No	Enter the time (in minutes) the dialer waits before calling back a no-answer call. Range is 1 – 99999. Default is 60.
Busy signal delay	No	Enter the time (in minutes) the dialer waits before calling back a busy phone number. Range is 1 – 99999. Default is 60.
Customer abandoned delay	No	Enter the time (in minutes) the dialer waits before calling back, if a customer abandons a call. Range is 1 – 99999. Default is 30.
Dialer abandoned delay	No	Enter the time (in minutes) the dialer waits before calling back, if the dialer abandons a call. Range is 1 – 99999. Default is 60.
Call Progress Analysis(CPA) Parameters section		
Minimum Silence Period(100-1000)	No	Minimum silence period required to classify a call as voice detected. If many answering machine calls are being passed through to agents as voice, then increasing this value accounts for longer pauses in answering machine greetings. Default is 608.

Field	Required?	Description
Analysis Period(1000-10000)	NO	Number of milliseconds spent analyzing this call. If there is a short agent greeting on an answering machine, then a longer value here categorizes that answering machine call as voice. If the call is to a business where the operator has a longer scripted greeting, a shorter value here categorizes the long, live greeting as answering machine. Default is 2500.
Minimum Valid Speech(50-500)	NO	Minimum number of milliseconds of voice required to qualify a call as voice detected. Default is 112.
Maximum Analysis Time(1000-10000)	NO	Maximum number of milliseconds allowed for analysis before identifying a problem analysis as dead air/low volume. Default is 3000.
Maximum termination tone analysis(1000-60000)	NO	Maximum milliseconds the dialer analyzes an answering machine voice message looking for a termination tone. If the message has an odd tone and the analysis does not recognize it, the call is not transferred or dropped until this timeout occurs. Default is 30000.

Step 8 Click **Save**.

Edit Contacts

This procedure explains how to upload contacts to newly created campaigns. You can also use this procedure to edit the contacts of existing campaigns.

Procedure

- Step 1** On the **Campaigns** page, select one or more campaigns.
- Step 2** Choose **Edit > Contacts** to open the **Edit Campaign** page.
- Step 3** Click the download icon next to **Download Contacts Template (csv)** to download the contacts template. You can use this template to enter contacts and upload.
- Step 4** Click the download icon next to **Download All Contacts (csv)** to download all existing contacts in the campaign.
- Step 5** Click **Choose File** and upload the contacts file.
- Note** The file must be in CSV format with a file extension as .txt or .csv.
The file must contain at least one phone number without any special characters.
- Step 6** Check the **Delete Existing Contacts** check box to delete the existing contacts in the selected campaigns.
- Note** While uploading the contacts file, if you do not check the **Delete Existing Contacts** check box, the uploaded contacts are appended to the existing contacts.
- Step 7** Click **Save** and then click **Yes** to confirm the changes.

Edit Status and Schedule

This procedure explains how to edit the status and schedule of campaigns.

Procedure

- Step 1** On the **Campaigns** page, select one or more campaigns to edit.
- Step 2** Choose **Edit > Status and Schedule** to open the **Edit Campaign** page.
- If you have selected one campaign, edit the status and the schedule of the campaign.
 - If you have selected multiple campaigns,
 - a. Check the **Edit Status** check box and edit the status of the campaign.
 - b. Check the **Edit Schedule** check box to enable the fields under **Schedule** and select new values.
- Step 3** Click **Save** and then click **Yes** to confirm the changes.
-

Save File Path of Do Not Call List Import File

Many countries require phone solicitors to maintain do not call lists. A Do Not Call (DNC) list ensures that your contact center does not call those customers who request that you do not contact them.

The Do Not Call list is a list of phone numbers that are identified as off-limits for outbound calling. This list can include numbers from a national DNC list and numbers from customers who have directly requested that you not contact them. Outbound Campaigns do not dial entries in the Do Not Call list even if they are included in a contact list. The DNC list is shared across all campaigns and contains only phone numbers.

Before you begin:

1. Using a text editor, create a text file to contain the "Do Not Call" phone numbers.
2. For each "Do Not Call" entry, enter a phone number of up to 20 characters on a new line.

The following is an example of a Do Not Call list:

```
2225554444
```

```
2225556666
```

```
2225559999
```

3. Save the text file to the path that is accessible from the logger.

Procedure

- Step 1** In Unified CCE Administration, choose **Organization > Campaigns** to open the **Campaigns** page.
- Step 2** Click the **Do Not Call - Settings** link.
The **Do Not Call - Settings** pop-up window appears.
- Step 3** In the **File Path with Name** field, you must enter the DNC list import file path on the logger or the path accessible from the logger.

Step 4

Click **Save**.

The solution import the DNC phone numbers to Do_Not_Call table in BA database. The name of DNC list import file is renamed after the successful import.

Note On the **Campaigns** page, you can save only one DNC list import file path at a time.

The campaign validates that a number in the dialing list is not in the Do Not Call list before sending it to a dialer. The solution checks the list at the last minute before placing the call. You can update a Do Not Call list while a campaign is running.

To edit the DNC phone numbers import file path:

1. Click the **Do Not Call - Settings** link. The solution displays the existing file path of the DNC list import file in the **File Path with Name** field.
2. Enter the file path of the new or updated DNC list import file in the **File Path with Name** field.
3. (Optional) Check the **Delete existing "Do Not Call" Phone Numbers** check box to delete the existing phone numbers from the Do_Not_Call table.

If this check box is unchecked, the existing DNC phone numbers are appended to the new or updated DNC phone numbers in the Do_Not_Call table.

4. Click **Save**.

Business Hours

Business Hours

Business hours are the working hours during which you conduct business. You can create and modify business hours and set weekly and daily schedules for each business hour. You can create different business hour schedules for regular working days and holidays. You can also open or close the business hours if there is an emergency.

You can define the status reasons for business hours and assign codes for each status reason. Status reason is required when you force open or force close a business hour, and when you add special hours and holidays.

Search for Business Hours

The Search field on the Business Hours page offers an advanced and flexible search.

Click the + icon on the Search field to open a popup window, where you can:

- Enter a business hour name or description to search for that string.
- Select **Globals and Departments** or **Departments only** to enable an input field where you can enter a space-separated list of department names. (Departments is an OR search.)



Note Search by department is available only when departments are configured.

Add and Maintain Business Hours

Procedure

- Step 1** In **Unified CCE Administration**, choose **Organization > Business Hours**.
- Step 2** On the **Business Hours** page, click **New** to open the **New Business Hours** page.
- Step 3** Complete the following information on the **General** tab and click **Save**.

Field	Required?	Description
Status	-	Select one of the following statuses for the business hour: <ul style="list-style-type: none"> • Open/Closed as per Business Calendar • Force Open • Force Close
Status Reason	Yes, if the status is Force Open or Force Close.	This field is enabled only if the status is Force Open or Force Close. Search and select a status reason for the business hour.
Name	Yes	Enter a unique name for the business hour. Maximum length is 32 characters. Valid characters are alphanumeric, period (.), and underscore (_). The first character must be alphanumeric.
Description	No	Enter a description of the business hour.
Time Zone	Yes	Select a time zone of the business hour from the drop-down list.
Department	-	Search and select a department to associate with the business hour. Default is Global. <p>Note This is applicable for Packaged CCE deployment only.</p>

- Step 4** Click the **Regular Hours** tab and complete the following information:
- Select one of the following **Business Hour Type**:
 - **24x7**: Always open. You cannot customize the working hours.
 - **Custom**: You can customize the working hours.
 - If you select **Custom**, enable at least one business day and select the **Start Time** and **End Time**.

Step 5 Click the **Special Hours & Holiday** tab. You can either add or import special hours and holidays.

Step 6 Click **Add** to open the **Add Special Hours & Holiday** popup window. Complete the following information:

Field	Required?	Description
Date	Yes	Select a date from the calendar.

Field	Required?	Description
Description	No	Enter a description for the special hour.
Status	-	Select a status. If the status is Open , the Start Time and End Time fields are enabled.
Start Time	Yes, if status is Open.	Select a start time for the special hour.
End Time	Yes, if status is Open.	Select an end time for the special hour.
Duration	-	Displays the duration of the special hour.
Status Reason	Yes	Search and select a status reason.

Step 7 Click **Save** to add the special hours and holidays.

Step 8 To import special hours and holidays, follow these steps.

- Click **Import** to open the **Import Special Hours and Holidays** pop-up window.
- Click the download icon to download the Special Hours & Holidays template. Use this template to enter the special hours and holidays.
- Click **Choose File** and browse to the special hours and holidays file. Click **Import** to upload the file.

Note The file must contain at least one special hour and holiday.
The file must be in CSV format with a file extension as .txt or .csv.

Step 9 Click **Export** to download the special hours and holidays in .csv format.

Step 10 Click **Save**.

Note The imported business hours overwrites the existing ones.

Add Status Reasons

This procedure explains how to add and maintain status reasons for business hours.

Procedure

Step 1 In **Unified CCE Administration**, choose **Organization > Business Hours > Status Reasons**.

Step 2 Click **Add** to open the **Add Status Reason** popup window.

Step 3 Enter the Status Reason. Maximum length is 255 characters.

Step 4 Enter a unique Reason Code. Range is 1001 to 65535. Codes 1 to 1000 are reserved as system-defined reason codes.

- Step 5** Click **Save**.
To add more status reasons, repeat steps from 2 to 5.
- Step 6** Click **Done** to return to the List window.
-

Edit Status for Multiple Business Hours

Perform the following steps to edit the status of multiple business hours at once.

Procedure

- Step 1** On the **Business Hours** page, select two or more business hours to edit.
- Step 2** Choose **Edit > Status** to open the **Edit Business Hours** page.
- Step 3** Check the **Status** check box and select the required status.
- Step 4** If you select the status as **Force Open** or **Force Close**, search and select a **Status Reason**.
- Step 5** Click **Save**.
-

Edit Schedule for Multiple Business Hours

Perform the following steps to edit schedules of multiple business hours at once.

Procedure

- Step 1** On the **Business Hours** page, select two or more business hours to edit.
- Step 2** Choose **Edit > Schedule** to open the **Edit Business Hours** page.
- Step 3** Check the **Time Zone** check box and select the required time zone from the drop-down list.
- Step 4** Check the **Type** check box and select the required business hour type.
- Step 5** If you select **Custom**, enable at least one business day and select the **Start Time** and **End Time**.
- Step 6** Click **Save**.
-

Desktop Settings

Resources

Resources

The **Resources** page allows you to configure resources for the teams. In Unified CCE Administration, choose **Desktop > Resources** to open the **Resources** page. You can select a site from the **Site** drop-down list. By default **Main** is selected for Packaged CCE 2000 Agents deployment.

The Packaged CCE 4000 Agents or 12000 Agents deployment type provides an option to select a peripheral set that includes the Cisco Finesse component configured. For more information to add peripheral sets to a site, see [Add and Maintain Peripheral Set, on page 143](#).

After you select a site, select a peripheral set from the **Peripheral Set** drop-down list. The drop-down list includes the peripheral sets configured for the selected site.

This page contains the following tabs that you click to configure the respective resources:

- **Call Variables Layout:** Manage the call variables and (Extended Call Context ECC) variables that appear on the agent desktop call control gadget.
- **Desktop Layout:** Make changes to the default desktop layout for agents and supervisors.
- **Phone Books:** Add, edit, or delete phone books or phone book contacts.
- **Workflows:** Create and manage workflows and workflow actions.

The resources that you configure are case-sensitive. For example, you can create two workflows named WORKFLOW and workflow or two phone books named BOOK and book.

Manage Call Variables Layout

You can use the Call Variables Layouts gadget to define how call variables appear on the Finesse agent desktop. You can configure up to 200 unique Call Variables Layouts (one default layout and 199 custom layouts). As part of this functionality:

- Each layout has a name (required) and description (optional).
- After an upgrade from a release earlier than Cisco Finesse Release 11.0, Finesse migrates the previously configured default layout and assigns it the default name (Default Layout) and description (Layout used when no other layout matches the user layout Custom/ECC Variable).
- You can change the name and description of the default Call Variables Layout.
- You cannot delete the default Call Variables Layout.
- Finesse appends (*Default*) to the name of the default Call Variables Layout.
- To display a custom Call Variables Layout, in the Unified CCE routing script set the user.Layout ECC variable to the name of a configured Call Variables Layout. In this case, if no custom layouts match the user.Layout value (or no custom layouts are configured), the Finesse displays the default layout.
- Finesse retains the custom layout as specified by the user.Layout ECC variable on CTI server failover. During PG failover, Finesse changes the active call layout to the default layout while retaining the call variables and time indicators.

Call Variables

Each Call Variables Layout supports one variable in the header of the call control gadget and up to a total of 20 variables in two columns below the header (up to 10 in each column). You can use call variables, Extended Call Context (ECC) variables, or the following Outbound Option ECC variables:

- BACampaign
- BAAccountNumber
- BAResponse

- BAStatus
- BADialedListID
- BATimeZone
- BABuddyName

Columns can be empty.

The administrator can include the following additional fields in the Call Variables Layout. These variables appear as a drop-down list in the call variable gadget which the admin can assign to a layout.

- queueNumber
- queueName
- callKeyCallId
- callKeyPrefix
- callKeySequenceNum
- wrapUpReason



Note The callKeyPrefix indicates the day when the call was routed.

The callKeyCallId indicates the unique number for the call routed on that day.

To uniquely locate the call in Unified CCE database records, concatenate the two variables callKeyPrefix and callKeyCallId.

To enable Outbound Option data to appear in Cisco Finesse, the administrator must edit the Default Layout to include some or all Outbound Option variables.

Configure Call Variables Layouts

Procedure

- Step 1** From the Call Variables Layouts gadget:
- Click **New** to create a new Call Variables Layout.
 - Choose a layout from the list and click **Edit** to modify an existing Call Variables Layout (or click **Delete** to remove it).
- Step 2** Under **Create New Layout** (or under Edit <layout name> when editing an existing layout):
- Enter a name for the Call Variables Layout (maximum 40 characters).
 - Enter a description of the Call Variables Layout (maximum 128 characters).
- Step 3** Under Call Header Layout:

- Enter the display name that you want to appear in the header of the Call Control gadget on the desktop. For example, Customer Name (maximum 50 characters).
- From the drop-down list, choose the call variable or Outbound Option ECC variable that you want to appear in the header. For example, callVariable3 (maximum 32 characters).

Step 4 In the Call Body Left-Hand Layout and Call Body Right-Hand Layout areas:

- a) Click **Add Row** to add a new row (or click the “X” to delete a row).
- b) For each row:
 - Enter the display name that you want to appear on the desktop. For example, Customer Name (maximum 50 characters).
 - Enter the corresponding call variable or Outbound Option ECC variable from the drop-down list (maximum 32 characters).

Step 5 Select up to five call variables using the check box. The selected call variables are displayed in agent call popover and supervisor active call details.

Note If you do not select any call variables, the first two call variables from the Call Body Left-Hand layout area will be displayed in the agent call popover and supervisor active call details. If there are no call variables in the Left-hand layout area, then the call variables in the Right-Hand Layout will be selected.

Step 6 Click **Save** to save the changes, or **Cancel** to discard the changes.

Note When you modify the Call Variables Layout of the agent desktop, the changes you make take effect after three seconds. However, agents or supervisors who are signed in when the changes are made must sign out and sign back in to see those changes reflected on their desktops.

Step 7 To view the latest configured Call Variables Layout, click **Refresh** from the Call Variables Layouts gadget.

Add ECC Variables to Call Variables Layout

Procedure

Step 1 In the header or the row where you want the ECC variable to appear, from the Variable drop-down list, choose **Custom**.

Step 2 In the Custom/ECC Variable Name field, enter the name of the ECC variable you want to appear on the agent desktop.

Step 3 Click **Set**.

The ECC variable now appears in the Variable drop-down list for selection.

Assign Call Variables Layouts

Procedure

-
- Step 1** In CCE Configuration Manager, create an ECC variable called **user.Layout** in the Expanded Call Variable list.
- Note** If a user.layout and a user.Layout are specified, Finesse will prioritize user.layout over user.Layout. If the layout specified in the user.Layout or user.layout is not found, Finesse uses the Default layout.
- Step 2** Add **user.Layout** to the CCE routing script. Use a Set Variable node in an appropriate place in the script to set the value of user.Layout to the name of the call variables layout to display. The layout name should match the name of a call variables layout that was created on the Call Variables Layout tab.
-

Manipulate Call Variables Layouts with a Workflow

You can manipulate the call variables layout that an agent sees when a call is answered by using a workflow. To do so, configure an HTTP Request workflow action and set the value of the ECC variable user.Layout to the name of the custom layout to display.

Manage Desktop Layouts

You can define the layout of the Finesse desktop on the **Desktop Layouts** tab.



-
- Important** Requirements, such as processor speed and RAM, for clients accessing the Finesse desktop can vary. Desktops that receive events for more than one agent (such as agent and supervisor desktops running Live Data reports that contain information about other agents and skill groups) require more processing power than desktops that receive events for a single agent.
- Factors that determine how much power is required for the client include, but are not limited to, the following:
- Contact center traffic
 - Additional integrated gadgets in the desktop (such as Live Data reports or third-party gadgets)
 - Other applications that run on the client and share resources with the Finesse desktop
-

Gadgets and Components

Gadgets

Cisco Finesse is an OpenSocial gadget, which is an XML document that defines metadata for an OpenSocial Gadget container. The gadgets are applications that are placed within the Cisco Finesse desktop. This helps administrator to provide access to the contact center agents for all the applications that is required to service calls inside a single application.

Cisco Finesse comes with default gadgets such as, the team performance gadget, call control gadget, and call popover. JavaScript library is available for any customers with specific requirements that are not available out of the box.

Gadgets are listed in the desktop layout using the `<gadget>` tag.



Note Finesse Desktop is tested to perform well with an average of 20 gadgets per Desktop (across all tabs), over a sign in period of 8 minutes for 2000 users (agents and supervisors). When you increase the total number of gadgets that are configured on the Desktop, the CPU consumption marginally increases during users sign in. When all the configured gadgets are enabled for all the users, it impacts the Finesse server. Higher number of gadgets will also need more browser memory and network bandwidth.

If considerably larger number of gadgets are configured or if more users sign in (more than the tested number of users) in a short time frame, you must monitor the CPU consumption and network bandwidth during users sign in and ensure that the end-point devices have enough memory.

Failover uses optimization to sign in the users quickly and is not considered the same as a new browser sign in.

Third-party gadgets are hosted on the Cisco Finesse server using the `3rdpartygadget` web application or on an external web server. Gadgets can make REST requests to services hosted on external servers using the Cisco Finesse JavaScript Library API. To avoid browser cross-origin issues, REST requests are proxied through the backend Shindig web application. Third-party gadgets must implement their own authentication mechanisms for third-party REST services.

For more information about gadgets, see <https://developer.cisco.com/docs/finesse/>.

Components

Components are simple scripts that are loaded into the desktop directly at predefined positions as directed by the layout, without an enclosing frame and its document.

Components are introduced in the desktop to overcome a few rendering limitations and performance considerations inherent to gadgets.

The `<component>` tag lists the components in the desktop layout. Currently, the layout validations prevent creating custom components. Hence, default components are allowed in the desktop layouts. The default desktop functionalities are currently registered as components to provide flexibility and to reduce the load on the server.

Finesse Desktop Layout XML

The Finesse Layout XML defines the layout of the Finesse desktop, and the gadgets and components displayed on the desktop.

Use the Desktop Layout gadget to upload an XML layout file to define the layout of the Finesse desktop for agents and supervisors.

To configure Live Data, see [Configure Live Data Reports with Multiple Views, on page 295](#).

Actions on the **Desktop Layouts** gadget are as follows:

- **Finesse Default Layout XML** - Expands to show the layout XML for the default Finesse desktop.
- **Restore Default Layout** - Restores the Cisco Finesse desktop to the default layout.

- **Save** - Saves your configuration changes.
- **Revert** - Retrieves and applies the most recently saved desktop layout.

Modify Live Data Stock Reports for Finesse

This procedure describes how to modify the Live Data stock reports in Cisco Unified Intelligence Center and add the modified report to the Finesse desktop layout. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.



Note To make sure the modified gadget renders in the Finesse desktop, you must give the appropriate permission for that report in Cisco Unified Intelligence Center.

Procedure

Step 1 Copy the gadget URL for the report you want to modify from the Finesse default layout XML and paste it into a text editor.

Example:

If you want to modify the Agent Report for HTTPS, copy the following URL and paste it into a text editor:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
  gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&
  filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
  filterId_2=agent.id=CL%20teamName
</gadget>
```

Step 2 In Cisco Unified Intelligence Center, in Edit view of the report, select the view for which you want to create a gadget URL and then click **Links**.

The HTML Link field displays the permalink of the customized report.

Step 3 Copy the permalink of the customized report from the **HTML Link** field, and paste it in a text editor. Then copy the viewId value from this link into the desired view.

Example:

Copy the viewId, which is underlined in this example, from the permalink for the report.

```
https://<Server Name>:8444/cuic/permalink/PermalinkViewer.htmx?
viewId=5C90012F10000140000000830A4E5B33&linkType=htmlType&viewType=Grid
```

Step 4 Replace the desired viewId value in the gadget URL with the viewId value from the permalink of the customized report.

Step 5 Replace my-cuic-server with the FQDN of the Cisco Unified Intelligence Center Server.

Step 6 Add the customized gadget URL to the desktop layout XML in the Manage Desktop Layout gadget and click **Save**.

Note After you add the gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with a large number of rows, you may want to adjust the gadget height or the screen resolution on the computer used to access the desktop to make the report easier to read or make more rows appear on the screen without the need to scroll.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.

Configure Live Data Reports with Multiple Views

Cisco Unified Intelligence Center allows you to display multiple Live Data reports or views on a single gadget. Agents can select the desired view to display from a drop-down list on the gadget toolbar, which lists up to five report views in *Report Name - View Name* format.

This procedure describes how to add multiple Live Data views to the Finesse desktop layout using the `viewId_n` and `filterId_n` keys. You can specify up to five report views to appear in your gadget. The first view among the five is the default view. There is no defined order for how the remaining views are displayed.

Finesse still supports the display of a single gadget using a single `viewId`. However, if you specify the single `viewId` along with multiple `viewId_n` keys, the multiple views are used and the single `viewId` is ignored.



Note To make sure the modified gadget renders in the Finesse desktop, you must give the appropriate permission for that report in Unified Intelligence Center.

Procedure

Step 1 For each report or view that you want to include in the gadget, obtain the associated `viewId` from the permalink for the view:

- a) In Unified Intelligence Center, in Edit view of the report, select the desired view then click **Links**.
The HTML Link field displays the permalink of the customized report.
- b) Copy the permalink of the customized report from the **HTML Link** field, and paste it in a text editor, and then copy the `viewID` value from the permalink and save it.

Example:

Copy the `viewId`, which is underlined in this example, from the permalink for the report.

```
https://<Server Name>:8444/cuic/permalink/PermalinkViewer.htmx?  
viewId=5C90012F10000140000000830A4E5B33&linkType=htmlType&viewType=Grid
```

Step 2 From the Finesse default layout XML, copy the gadget URL for one of the Live Data reports and paste it into a text editor.

Example:

Copy the URL for the Agent Skill Group for HTTPS from the default layout XML and paste it into a text editor:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId_1=9AB7848B10000141000001C50A0006C4&filterId_1=agent.id=CL%20teamName</gadget>
```

Step 3 To update the URL to refer to a different report view, populate the viewId_1 value (after the equal sign) with the desired viewId obtained in step 1.

Example:

The following shows the URL updated with the example viewId copied from step 1.

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName</gadget>
```

Step 4 For each additional view you want to include:

a) At the end of the URL, copy and paste the viewId_1 and agentId_1 strings with a leading ampersand.

Example:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName&viewId_2=5C90012F10000140000000830A4E5B33&filterId_2=agent.id=CL%20teamName</gadget>
```

b) Update the copied viewId_1 and filterId_1 in the URL to the next available integer (in this example, viewId_2 and filterId_2).

Example:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName&viewId_2=5C90012F10000140000000830A4E5B33&filterId_2=agent.id=CL%20teamName</gadget>
```

c) Populate the copied viewId value (after the equal sign) with the value defined in the permalink for the desired report (in this example, 99E6C8E210000141000000D80A0006C4).

Example:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName&viewId_2=99E6C8E210000141000000D80A0006C4&filterId_2=agent.id=CL%20teamName</gadget>
```

d) Make sure that the filterId value matches the type required by the report type, as follows:

- Agent Reports: filterId_N=agent.id=CL%20teamName
- Agent Skill Group Reports: filterId_N=agent.id=CL%20teamName
- Skill Group Reports: filterId_N=skillGroup.id=CL%20teamName
- Precision Queue Reports: filterId_N=precisionQueue.id=CL%20teamName

Step 5 Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

Step 6 Add the customized gadget URL to the desktop layout XML in the Manage Desktop Layout gadget and click **Save**.

Note After you add the gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with a large number of rows, you may want to adjust the gadget height or the screen resolution on the computer used to access the desktop to make the report easier to read or make more rows appear on the screen without the need to scroll.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.

Default Layout XML

The Cisco Finesse default desktop layout XML for Unified CCE and Packaged CCE contains optional gadgets and notes. The notes describe how to modify the layout for your deployment type.

Optional Live Data gadgets in the layout XML are commented out. After you install and configure Live Data, remove the comment tags from the reports that you want to appear on the desktop.

Following are the updates available in the default layout XML for Cisco Finesse desktop:

- Horizontal Header is available in the layout configuration and the Header can be customized.
- Title and Logo of Cisco Finesse desktop can be customized.
- Desktop Chat, TeamMessage, Dialer, Agent Identity, and Non-Voice State Control are added as part of the header component.

For upgraded layouts, TeamMessage and Desktop Chat will not appear by default. The XML must be copied from the default layout and added to the respective custom layouts. See *Cisco Cisco Finesse Installation & Upgrade Guide*.

- Vertical tabs in Cisco Finesse desktop are moved to collapsible left navigation bar for which the icons can be customized.
- Support for inbuilt java script components has been added.
- The **ID** attribute (optional) is the ID of the HTML DOM element used to display the gadget or component. The ID should start with an alphabet and can contain alphanumeric characters along with hyphen(-) and underscore(_). It can be set through the Cisco Finesse Administrative portal and has to be unique across components and gadgets.
- The **managedBy** attribute (optional) for Live Data gadgets defines the gadgets which manage these Live Data gadgets. The value of **managedBy** attribute for Live Data gadgets is **team-performance**. This means that the rendering of the gadget is managed by the Team Performance gadget. These gadgets are not rendered by default, but will be rendered when the options Show State History and Show Call History are selected in the Team Performance gadget.

For upgraded layouts, the **managedBy** attribute will be introduced, and will have the value of the **ID** of the Team Performance gadget in the same tab. If there are multiple instances of Team Performance gadgets and Live Data gadget pairs, they will be associated in that order. If the **ID** of the Team Performance gadget is changed, the value of the **managedBy** attribute should also be updated to reflect the same **ID** for the Live Data gadgets. Otherwise, the Team Performance gadget instance will not show its respective Live Data gadgets.

- The **Hidden** attribute (optional) is used to support headless gadgets. When an attribute is set to `hidden="true"`, then the gadget is loaded by the container, but will not be displayed. The default value set for the attribute is "false".

- **maxRows** is changed from being a query parameter to an attribute.

Example of **maxRows** being a query parameter:

```
<gadget id="team-performance">/desktop/scripts/js/teamPerformance.js?maxRows=5</gadget>
```

Example of **maxRows** being an attribute:

```
<gadget id="team-performance" maxRows="5">/desktop/scripts/js/teamPerformance.js</gadget>
```

During an upgrade it will be removed from the URL of the team performance gadget and added as an attribute. The **maxRows** attribute (optional) is used to adjust the height of the Team Performance gadget. If there are multiple instances of the Team Performance gadget, each instance height can be set by using this attribute. During an upgrade the height of the team performance gadget will be retained. By default the **maxRows** attribute value is set to 10 rows.

If any changes are made to the component IDs or URLs in the default XML layout, the following features may not work as expected.

Note that the components can be rearranged in any order to show on the Cisco Finesse desktop.

Feature	Component ID	URL
Title and Logo	cd-logo	<url>/desktop/scripts/js/logo.js</url>
Voice State Control	agent-voice-state	<url>/desktop/scripts/js/agentvoicestate.component.js</url>
Non-voice state control	nonvoice-state-menu	<url>/desktop/scripts/js/nonvoice-state-menu.component.js</url>
TeamMessage	broadcastmessagepopover	<url>/desktop/scripts/js/teammessage.component.js</url>
Desktop Chat	chat	<url>/desktop/scripts/js/chat.component.js</url>
Dialer	make-new-call-component	<url>/desktop/scripts/js/makenewcall.component.js</url>
Agent identity	identity-component	<url>/desktop/scripts/js/identity-component.js</url>

Update Default Desktop Layout

When you modify the layout of the Finesse desktop, it can take up to 120 seconds to reflect the changes. However, agents who are signed in when the changes are made must sign out and sign in again to see those changes reflecting on the desktop.



Note The call control gadget is only supported at the page level. You must ensure that the call control gadget (<gadget>/desktop/scripts/js/callcontrol.js</gadget>) is placed within the <page></page> tag for it to work correctly. Don't place this gadget within a <tab></tab> tag.

The version tag of Desktop Layout XML can't be edited.

For the changes to take effect, refresh the page, or sign out and sign in again into Cisco Finesse.

To modify the Live Data gadget, see [Modify Live Data Stock Reports for Finesse, on page 294](#).

Procedure

Step 1 Click **Desktop Layout**.

Step 2 In the Finesse Layout XML area, make changes to the XML as required.

Example:

If you want to add a new tab called Reports, add the following XML within the tabs tags under the `<role>Agent</role>` tag:

```
<tab>
  <id>reports</id>
  <icon>Reports</icon>
  <label>Reports</label>
</tab>
```

If you want to add this tab to the supervisor desktop, add the XML within the tabs tags under the `<role>Supervisor</role>` tag.

To add a gadget to a tab, add the XML for the gadget within the gadgets tag for that tab.

```
<gadgets>
<gadget>http://<ipAddress>/gadgets/<gadgetname>.xml</gadget>
</gadgets>
```

Replace `<ipAddress>` with the IP address of the server where the gadget resides.

If you want to add multiple columns to a tab on the Finesse desktop, add the gadgets for each column within the columns tags for that tab. You can have up to four columns on a tab.

```
<tabs>
  <tab>
    <id>home</id>
    <icon>home</icon>
    <label>finesse.container.tabs.agent.homeLabel</label>
    <columns>
      <column>
        <gadgets>
          <gadget>/desktop/scripts/js/queueStatistics.js</gadget>
        </gadgets>
      </column>
    </columns>
  </tab>
  <tab>
    <id>myHistory</id>
    <icon>history</icon>
    <label>finesse.container.tabs.agent.myHistoryLabel</label>
    <columns>
      <column>
        <!-- The following gadgets are used for viewing the call history
and state history of an agent. -->
      </column>
    </columns>
  </tab>
  <tab>
    <id>manageCustomer</id>
    <icon>profile-settings</icon>
    <label>finesse.container.tabs.agent.manageCustomerLabel</label>
    <gadgets>
      <gadget>/3rdpartygadget/files/FinextGadget.xml</gadget>
```

```
</gadgets>
</tab>
```

Step 3 Click **Save**.

Note After you add a gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with many rows, you may want to adjust the gadget height, or the screen resolution on the computer used to access the desktop to make the report easier to read or make more rows appear on the screen without needing to scroll down.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.

Finesse validates the XML file to ensure that it's valid XML syntax and conforms to the Finesse schema.

Step 4 After you save your changes, if you want to revert to the last saved desktop layout, click **Revert**. If you want to revert to the default desktop layout, click **Restore Default Layout**.

Note During upgrade, any changes made to the Cisco Finesse Default Layout won't be updated. Click on **Restore Default Layout** to get the latest changes.

Horizontal Header

The Horizontal Header on the Finesse desktop has the following components from left to right. All these components can be removed and replaced with custom gadgets as required.

- **Logo:** Default is Cisco logo. Can be customized.
- **Product Name:** Default is Cisco Finesse. Can be customized.
- **Agent State for Voice:** Displays agent state for voice call.
- **Agent State for Digital Channels:** Displays agent state for digital channels.
- **Dialer Component:** Agent can make a new call.
- **Identity Component:** Displays agent name and signout functionality with reason codes.



Note The sum of widths set for all gadgets and components in the header (inside right aligned columns and left aligned columns) should not exceed the total header width. If it exceeds the header width, some of the gadgets/components will not be visible.

Customize Title and Logo in the Header

You can customize the title and logo displayed on the Finesse desktop:

Procedure**Step 1** Click **Desktop Layout**.**Step 2** Enter the product name in the config value tag with title key.

- Step 3** Upload the logo file just like any third-party gadget.
For more information, see section *Upload Third-Party Gadgets* in *Cisco Finesse Admin Guide*.
- Step 4** Enter the URL of the logo file in the config value tag with logo key.

Example:

```
<configs>
  <!-- The Title for the application which can be customised.-->
  <config value="product.full-name" Key="title"/>
  <!-- The logo file for the application-->
  <!--<config key="logo" value="/3rdpartygadgets/<some_sample_image>" /-->
</configs>
```

The customized logo and product name is displayed on the Finesse desktop.



Note The file size that can be uploaded for the logo must be kept within 40 pixels. The file types supported are .svg, .png, .gif, and .jpeg/jpg.

alternateHosts Configuration

The `<gadget>` element in the Finesse Layout XML provides an attribute to specify alternate hosts from which the gadget can be loaded. This allows the Cisco Finesse desktop to load the gadget using a different host if the primary server is unavailable.

The **alternateHosts** attribute contains a comma-separated list of FQDNs that will be used if the primary-host-FQDN is unavailable.

```
<gadget alternateHosts="host1,host2,host3,...">
  https://<primary-host-FQDN>/<gadget-URL>
</gadget>
```

The **alternateHosts** attribute is only applicable for gadgets with an absolute URL. That is URLs containing the FQDN of a host, an optional port, and the complete URL path to the gadget. For example: `<gadget alternateHosts="host1,host2">https://primary host/relative_path</gadget>`

If loading the gadget from the primary-host fails, the Cisco Finesse container attempts to load the gadget from the alternate hosts in the order specified in the **alternateHosts** attribute.

The Cisco Finesse desktop may fail to load the gadget even if some of the hosts are reachable. In such cases, refresh the Cisco Finesse desktop.

When the gadget is specified with a relative URL, for example: `<gadget >/3rdpartygadgets/relative_path</gadget>`, the **alternateHosts** attribute does not apply and is ignored by the Cisco Finesse desktop.



Note If the host serving the gadget fails after the Cisco Finesse desktop was successfully loaded, the desktop must be refreshed in order to load the gadget from an alternate host. The gadget does not implement its own failover mechanism.

Headless Gadget Configuration

Headless gadgets are gadgets which do not need a display space, but can be loaded and run like a background task in the browser. The **Hidden** attribute (optional) is used to support headless gadgets in the layout XML. When an attribute is set to "hidden=true", then the gadget is loaded by the container, but will not be displayed. The default value set for the attribute is "false".

Customize Icons in Left Navigation Bar

You can add icons (both custom and inbuilt) to the collapsible left navigation bar of the Finesse desktop:

Procedure

- Step 1** Click **Desktop Layout**.
- Step 2** Enter name of the gadget or component in the id tag.
- Step 3** Enter the value of the icon in the icon tag.
- Step 4** Upload the icon file just like any third-party gadget.

For more information, see section *Upload Third-Party Gadgets* in *Cisco Finesse Admin Guide*.

Note When adding a custom icon, provide the path in the icon tag and if you are adding an inbuilt icon, provide the icon value in the icon tag

Example:

Note The file size that can be uploaded in the left navigation bar as custom icons is 25 pixels by 25 pixels. The maximum width of the tab title in the left navigation bar must be 80 pixels or less. The file types supported are .svg, .png, .gif, and .jpeg/jpg.

XML Schema Definition

You must ensure that the XML uploaded conforms to the XML schema definition for Finesse. The XML schema definition for Finesse is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://www.cisco.com/vtg/finesse" targetNamespace="http://www.cisco.com/vtg/finesse"
elementFormDefault="qualified">
  <!-- definition of version element -->
  <xs:element name="version">
    <xs:simpleType>
      <xs:restriction base="xs:double">
        <xs:pattern value="[0-9\.]+" />
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
  <!-- The below elements are for common desktop header and configs -->
  <!-- Copied from:
https://github5.cisco.com/cbu-shared/common-desktop/blob/master/java/layout-manager/src/main/resources/layoutSchema.xsd
-->
  <!-- If the common-desktop XSD changes, this too needs to be updated -->
  <!-- Only difference is that, column has been renamed to headercolumn, since column is
already there in finesse desktop layout -->
  <xs:complexType name="configs">
    <xs:sequence>
```



```

        <xs:element name="config" type="config" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
</xs:complexType>
<xs:complexType name="config">
    <xs:attribute name="key">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="[a-zA-Z]*" />
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>
    <xs:attribute name="value" type="xs:string" />
</xs:complexType>
<xs:complexType name="header">
    <xs:choice>
        <xs:sequence>
            <xs:element name="leftAlignedColumns" type="listOfColumns" minOccurs="1"
maxOccurs="1" />
            <xs:element name="rightAlignedColumns" type="listOfColumns" minOccurs="0"
maxOccurs="1" />
        </xs:sequence>
        <xs:sequence>
            <xs:element name="rightAlignedColumns" type="listOfColumns" minOccurs="1"
maxOccurs="1" />
        </xs:sequence>
    </xs:choice>
</xs:complexType>
<xs:complexType name="component">
    <xs:sequence>
        <xs:element name="url" type="xs:string" minOccurs="1" maxOccurs="1" />
        <xs:element name="stylesheet" type="xs:string" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
    <xs:attribute name="id" use="required">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="."+ />
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>
    <xs:attribute name="order">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="[0-9]{0,10}" />
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>
</xs:complexType>
<xs:complexType name="listOfColumns">
    <xs:sequence>
        <xs:element name="headercolumn" type="headercolumn" minOccurs="1"
maxOccurs="unbounded" />
    </xs:sequence>
</xs:complexType>
<xs:complexType name="headercolumn">
    <xs:choice minOccurs="0" maxOccurs="1">
        <xs:element ref="gadget" />
        <xs:element name="component" type="component" />
    </xs:choice>
    <xs:attribute name="width">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="[0-9]+(px|%)" />
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>

```

```

    </xs:attribute>
</xs:complexType>
<!-- The above elements are for common desktop header and configs -->
<!-- definition of role type -->
<xs:simpleType name="role">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Agent" />
    <xs:enumeration value="Supervisor" />
    <xs:enumeration value="Admin" />
  </xs:restriction>
</xs:simpleType>
<!-- definition of simple elements -->
<xs:element name="id">
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:pattern value="[a-zA-Z]([-_:\.a-zA-Z0-9])*" />
    </xs:restriction>
  </xs:simpleType>
</xs:element>
<xs:element name="label">
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:minLength value="1" />
      <xs:pattern value="^[^\r\n]+" />
      <!-- This regex restricts the label string from carriage returns or newline
characters -->
    </xs:restriction>
  </xs:simpleType>
</xs:element>
<xs:element name="icon" type="xs:anyURI" />
<xs:element name="gadget">
  <xs:complexType>
    <xs:simpleContent>
      <xs:extension base="restrictWhiteSpaces">
        <!-- <xs:attribute name="staticMessage" type="xs:string"/> -->
        <xs:attribute name="id">
          <xs:simpleType>
            <xs:restriction base="xs:string">
              <xs:pattern value="[a-zA-Z]([-_a-zA-Z0-9])*" />
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
        <xs:attribute name="alternateHosts" type="xs:string" />
        <xs:attribute name="managedBy" type="xs:string" />
        <xs:attribute name="hidden" type="xs:boolean" />
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
</xs:element>
<xs:element name="role" type="role" />
<xs:element name="gadgets">
  <!-- Grouping of a set of gadgets -->
  <xs:complexType>
    <xs:sequence minOccurs="0" maxOccurs="unbounded">
      <!-- No limit to number of gadget URIs for now -->
      <xs:element ref="gadget" />
      <!-- URI of the gadget xml -->
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:simpleType name="restrictWhiteSpaces">
  <xs:restriction base="xs:anyURI">
    <xs:minLength value="1" />
    <xs:pattern value="\S+" />
  </xs:restriction>
</xs:simpleType>

```

```

        <!-- This regex restricts anyURI from containing whitespace within -->
    </xs:restriction>
</xs:simpleType>
<xs:element name="column">
    <!-- Grouping of a set of gadgets within a column -->
    <xs:complexType>
        <xs:sequence minOccurs="0" maxOccurs="unbounded">
            <!-- No limit to number of gadget URIs for now -->
            <xs:element ref="gadgets" />
            <!-- URI of the gadget xml -->
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="columns">
    <!-- Grouping of a set of columns -->
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="column" minOccurs="0" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="page">
    <!-- Grouping of a set of persistent gadgets -->
    <xs:complexType>
        <xs:sequence minOccurs="0" maxOccurs="unbounded">
            <!-- No limit to number of gadget URIs for now -->
            <xs:element ref="gadget" />
            <!-- URI of the gadget xml -->
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="tab">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="id" />
            <!-- Id of the tab selector in the desktop -->
            <xs:element ref="icon" minOccurs="0" maxOccurs="1" />
            <xs:element ref="label" />
            <!-- Label of the tab selector -->
            <xs:choice>
                <xs:element ref="gadgets" minOccurs="0" maxOccurs="1" />
                <xs:element ref="columns" minOccurs="0" maxOccurs="1" />
            </xs:choice>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="tabs">
    <!-- Grouping of tabs -->
    <xs:complexType>
        <xs:sequence maxOccurs="unbounded">
            <!-- No limit to number of tabs for now -->
            <xs:element ref="tab" />
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="layout">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="role" />
            <!-- Type of the role -->
            <xs:element ref="page" />
            <!-- List of page gadgets -->
            <xs:element ref="tabs" />
            <!-- Grouping of tabs for this particular role -->
        </xs:sequence>
    </xs:complexType>
</xs:element>

```

```

        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="finesseLayout">
    <!-- Layout of the desktop -->
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="version" />
            <xs:element name="configs" type="configs" minOccurs="0" maxOccurs="1" />
            <xs:element name="header" type="header" minOccurs="1" maxOccurs="1" />
            <xs:sequence maxOccurs="3">
                <!-- only support 3 roles for now -->
                <xs:element ref="layout" />
            </xs:sequence>
        </xs:sequence>
    </xs:complexType>
</xs:element>
</xs:schema>

```

Manage Phone Books

On the **Phone Books** section, you can create and manage global and team phonebooks and phonebook contacts. Global phonebooks are available to all agents; team phonebooks are available to agents in that specific team.

The system supports the following number of phone books:

- 10 global phone books
- 300 team phone books

The system supports a total of 50,000 contacts. The total number of contacts per agent across all phone books is limited to 1500.

Use the **Phone Books** gadget to view, add, edit, or delete phone books and phone book contacts. Click the Name or Assign To headers to sort the phone books in ascending or descending order. Click the Last Name, First Name, Number, or Note headers to sort the contacts in ascending or descending order.

The following table describes the fields on the **Phone Books** gadget.

Field	Explanation
Name	The name of the phone book. The name must be unique, and can be a maximum length of 64 alphanumeric characters.
Assign To	Indicates if the phone book is global (All Users) or team (Teams).
Last Name	The last name of a contact. The last name can be a maximum length of 128 characters. This field is optional.
First Name	The first name of a contact. The first name can be a maximum length of 128 characters. This field is optional.
Number	The phone number for the contact. The phone number can be 1-32 characters long and cannot be blank.
Note	Optional text that describes the contact. The note can be a maximum length of 128 characters.

Actions on the Phone Books gadget:

- **New:** Add a new phone book or contact
- **Edit:** Edit an existing phone book or contact
- **Delete:** Delete a phone book or contact
- **Refresh:** Reload the list of phone books or contacts from the server
- **Import:** Import a list of contacts to the phone book
- **Export:** Export a list of contacts from the phone book

Add Phone Book

Procedure

- Step 1** In the **Phone Books** gadget, click **New**.
The New Phone Book area appears.
- Step 2** In the **Name** field, enter a name for the phone book.
Note Phone book names can be a maximum of 64 characters.
- Step 3** From the **Assign To** drop-down, select **All Users** if the phone book is global or **Teams** if the phone book is available to specified teams.
- Step 4** Click **Save**.
-

Edit Phone Book

Procedure

- Step 1** In the **Phone Books** gadget, select the phone book you want to edit.
- Step 2** Click **Edit**.
- Step 3** In the **Name** field, enter the new name for the phone book. If you want to change who can access the phone book, in the **Assign To** drop-down, choose **All Users** or **Teams**.
- Step 4** Click **Save**.
If you change the Assign To field from Teams to All Users, click **Yes** to confirm the change.
-

Delete Phone Book

Procedure

- Step 1** In the **Phone Books** gadget, select the phone book that you want to delete.
- Step 2** Click **Delete**.

- Step 3** Click **Yes** to confirm the deletion of the selected phone book.
-

Add Contact

Procedure

- Step 1** In the **Phone Books** gadget, select the phone book to which you want to add a contact.
The List of Contacts for <phone book name> area appears.
- Step 2** Click **New**.
- Step 3** Complete the fields. The First Name, Last Name, and Note fields are optional and have a maximum length of 128 characters. The Number field is required and has a maximum length of 32 characters.
- Step 4** Click **Save**.
-

Edit Contact

Procedure

- Step 1** In the **Phone Books** gadget, select the phone book that contains the contact you want to edit.
The List of Contacts for <phone book name> area appears.
- Step 2** Select the contact you want to edit.
- Step 3** Click **Edit**.
- Step 4** Edit the fields that you want to change. The First Name, Last Name, and Note fields are optional and have a maximum of 128 characters. The Number field is required and has a maximum of 32 characters.
- Step 5** Click **Save**.
-

Delete Contact

Procedure

- Step 1** In the **Phone Books** gadget, select the phone book that contains the contact you want to delete.
The List of Contacts for <phone book name> area appears.
- Step 2** Select the contact that you want to delete.
- Step 3** Click **Delete**.
- Step 4** Click **Yes** to confirm the deletion of the selected contact.
-

Import Contacts

The Import function allows you to replace all the contacts in a phone book with a new list of contacts, or to populate a new phone book with contacts.

The import list must be in the specified comma separated values (CSV) format, and can contain a maximum of 1500 contacts. Import lists that contain more than 1500 contacts are rejected with an error message.

The CSV file contains the fields described in the following table:

Field	Max Length	Can Be Blank?	Permitted Characters
First Name	128	Yes	Note The CSV file that contains the contacts to import must use Latin encoding.
Last Name	128	Yes	
Phone Number	32	No	
Notes	128	Yes	

The following is an example of a phone book CSV file:

```
"First Name", "Last Name", "Phone Number", "Notes"
"Amanda", "Cohen", "6511234", ""
"Nicholas", "Knight", "612-555-1228", "Sales"
"Natalie", "Lambert", "952-555-9876", "Benefits"
"Joseph", "Stonetree", "651-555-7612", "Manager"
```

A phone book CSV file must conform to this format and include the headers in the first line. During import, the file is scanned for illegal characters. If any are found, they are replaced with question marks.



Note Exported CSV files always show each field enclosed in double quotes to ensure that any commas or double quotes that are part of the actual filed data are not mistaken for field delimiters. If your data does not include these characters, you can omit the double quotes in files you prepare for importing.

Procedure

-
- Step 1** In the **Phone Books** gadget, select the phone book into which you want to import a list of contacts.
- Step 2** Click **Import**.
- Step 3** Click **Browse** and navigate to the location of the CSV file containing the contacts you want to import.
- Note** The CSV file must use Latin encoding.
- Step 4** Click **OK**.
-

Export Contacts

The Export function allows you to extract a list of contacts from an existing phone book. The exported list is saved in CSV format.

Procedure

- Step 1** In the **Phone Books** gadget, select the phone book that contains the contacts you want to export.
- Step 2** Click **Export**.
- Step 3** Click **Open** to open the CSV file in Excel, or click the **Save** drop-down list and choose **Save**, **Save as**, or **Save and open**.
- Step 4** A message appears that gives you the option to view the downloaded file, open the folder into which the download was saved, view the Internet Explorer View Downloads window, or dismiss the message without viewing the file.
- Step 5** A message appears that gives you the option to view the downloaded file, open the folder into which the download was saved, view the Internet Explorer View Downloads window, or dismiss the message without viewing the file.
-

Manage Workflows

On the **Workflows** tab, you can create and manage workflows and workflow actions.

Workflows and Workflow Actions

You can use workflows to automate common repetitive agent tasks. A workflow has a unique name and a helpful description. Use the Manage Workflows and Manage Workflow Actions gadgets to view, add, edit, or delete workflows and workflow actions.

All workflows are team-level workflows. You cannot create a global workflow. If you need a global workflow, create a team workflow and assign it to all teams.

Cisco Finesse supports the following number of workflows and workflow actions:

- 100 workflows per Cisco Finesse system
- 100 actions per Cisco Finesse system
- 20 workflows per team
- Five conditions per workflow
- Five actions per workflow
- Five variables per action

The following fields can be used to configure workflows:

- queueNumber
- queueName
- callKeyCallId
- callKeyPrefix
- callKeySequenceNum
- wrapUpReason

- For Voice - Call variables, Outbound Option variables, queue details, wrap-up reasons, agent details, or team details.
- For Email - Queue name and email attributes like From, To, Cc, Bcc, or Subject.
- For Chat - Queue name, chat type, or system defined customer details as available from the web chat form.

Click the column headers to sort workflows and workflow actions in ascending or descending order.

The following table describes the fields on the Manage Workflows gadget:

Field	Explanation
Name	The name of the workflow must be unique and can have a maximum length of 40 characters.
Description	The description of the workflow can have a maximum length of 128 characters.
Media	The media of the workflow. You can configure the media to Voice and any preferred Digital Channel.

The following table describes the fields on the Manage Workflow Actions gadget:

Field	Explanation
Name	The name of the workflow action must be unique and can have a maximum length of 64 characters.
Type	The type of workflow. Possible values are Browser Pop and HTTP Request.

Actions on the Manage Workflows and Manage Workflow Actions gadgets:

- **New:** Add a new workflow or workflow action
- **Edit:** Edit a workflow or workflow action
- **Delete:** Delete a workflow or workflow action
- **Refresh:** Reload the list of workflows or workflow actions from the server.

You can configure workflow actions to be handled by the Cisco Finesse desktop or in a third-party gadget. A third-party gadget can be designed to handle the action differently than Cisco Finesse does.

Each workflow must contain only one trigger. Triggers are based on Cisco Finesse dialog events.



Note You can configure the trigger only after you select the media.

- Voice dialog events include the following:
 - When a Call arrives
 - When a Call is answered
 - When a Call ends

- When making a Call
- While previewing an Outbound Option call.
- Digital Channels dialog events include the following:
 - When a task is offered
 - When a task is accepted



Note Some solutions such as ECE don't provide a separate accept task functionality. Therefore, the tasks that are offered are auto accepted, which simultaneously generate the **task is accepted** event along with the **task is offered** event. In such scenarios, use only one event (**task is accepted** or **task is offered**) for configuring workflows because there is no difference between these two events.

- When a task is active
- When a task is paused
- When a task is interrupted
- When a task is closed

The workflow engine uses the following simple logic to determine whether to run a workflow:



Note The workflow logic and examples are similar for all media.

- Its trigger set and conditions are evaluated against each dialog event received.
- The workflow engine processes workflow events for the first call that matches any configured workflow's trigger set and conditions. No other workflows run until this call has ended. If the agent accepts a second call while still on the first call, workflows do not run on the second call even after the first call has ended.
- After a workflow for a particular trigger type (for example, Call Arrives) runs, it never triggers again for the same dialog ID.

The workflow engine caches workflows for an agent when the agent signs in. Workflows do not change for the agent until the agent signs out and signs in again or refreshes the browser.



Note Whenever the browser is refreshed, the workflows that trigger the following events run:

- when a call arrives
- when a call is answered
- when making a call

When an agent refreshes the browser, the workflow engine considers the call as newly arrived or newly made. If an HTTP request action is part of the workflow, the HTTP request is sent when the agent refreshes the browser. Applications that receive the HTTP requests must account for this scenario.

An example of a workflow is a Call Arrival event that triggers an action that collects information from the dialog event (for example, the ANI or customer information) and displays a web page containing customer information.

You can filter trigger events by the value of the data that comes in the event. You can configure a workflow to run if any of the conditions are met or if all the conditions are met.

Individual conditions comprise of the following:

- A piece of event data to be examined. For example, **DNIS** or call variables.
- A comparison between the event data and the values entered (for example **contains**, **is equal to**, **is not equal to**, **begins with**, **ends with**, **is empty**, **is not empty**, and **is in list**).

When the trigger and its conditions are satisfied, a list of actions assigned to the workflow are run. The actions are run in the listed order.

Workflows run only for agents and supervisors who are Cisco Finesse users. The Workflow Engine is a JavaScript library that runs client-side on a per-user basis within the Cisco Finesse desktop application. The desktop retrieves the workflows that are to be run for a user from the server when the user signs in or when the browser is refreshed.



Note Changes made to a workflow or its actions while a user is signed in are not automatically pushed to that user.

It is possible to set workflows, conditions, and actions that are contradictory so that a workflow or action cannot function. Workflows are not validated.

If multiple workflows are configured for a team, the Workflow Engine evaluates them in the configured order. The Workflow Engine ignores workflows with no actions. When the Workflow Engine finds a workflow with a matching trigger for an event and the workflow conditions evaluate to true, that workflow is used, and the subsequent workflows in the list are not evaluated. Workflows with no conditions evaluate to true if the event matches the workflow trigger. All workflows are enabled by default. Only one workflow for a specific user can run at a time.

The Workflow Engine retrieves dialog-based variables that are used in workflow conditions from the dialog that triggered the workflow. If a variable is not found in the dialog, its value is considered to be empty.

The Workflow Engine runs the actions that are associated with the matched workflow in the order in which they are listed. The Workflow Engine runs actions in a workflow even if the previously run action fails. Failed actions are logged.

The Cisco Finesse server controls the calls that are displayed to the Cisco Finesse user. If the user has multiple calls, the workflow applies only to the first call that matches a trigger. If the first call displayed does not match any triggers but the second call does match a trigger, the Workflow Engine evaluates and processes the triggers for the second call.

A call is considered to be the first displayed call if it is the only call on the Cisco Finesse desktop when it appears. If two calls on a phone are merged (as they are in a conference call), then the first displayed call flag value of the surviving call is used.

If a user has a call and the user refreshes the browser, the Workflow Engine evaluates the call as it is. If the dialog data (call variable values) change, the data may not match the trigger and conditions of the original workflow. The data may match a different workflow or no workflows at all.

If a user has multiple calls and the user refreshes the browser, the Workflow Engine treats the first dialog received from the Cisco Finesse server as the first displayed call. This call may not be the same call that was first displayed before the refreshing the browser. Dialogs received for any other call are ignored because they are not considered as first displayed calls. After refreshing the browser, if dialogs for more than one call are received before the Workflow Engine is loaded, none of the dialogs are evaluated because they are not considered as first displayed calls.

Workflows that are run for both Cisco Finesse agents and supervisors. The team to which the supervisor belongs (as distinguished from the team that the supervisor manages) determines which workflows run for the supervisor. Put the supervisors in their own team to keep agent workflows from being run for them.

Workflow Triggers and Outbound Calls



Note When you create a workflow specifically for Outbound Option calls, add a condition of BAStatus is not empty (except for the Workflow Trigger 'When a call arrives' as BAStatus will be empty at that point of time). This condition ensures that the workflow can distinguish Outbound Option calls from agent-initiated outbound calls.

The following table illustrates when workflows trigger in outbound call scenarios:

Workflow Trigger	Direct Preview Outbound Call	Preview Outbound Call	Progressive/Predictive Outbound Call
While previewing a call	When the agent previews the call (before accepting or rejecting it)	When the agent previews the call (before accepting or rejecting it)	Does not trigger
When a call arrives	Does not trigger	When the agent accepts the call	When the call arrives on the agent desktop
When a call is answered	When the customer answers the call and during failover	When the customer answers the call and during failover	When the customer answers the call
When a call is made	When the customer call is initiated	When the customer call is initiated	When the customer call is initiated, and during failover
When a call ends	When the customer call ends	When the customer call ends	When the customer call ends

Add Browser Pop Workflow Action

The Browser Pop workflow action opens a browser window or tab on the user's desktop when workflow conditions are met.



Note Whether the action opens a new window or tab on the desktop depends on the target user's browser settings.

Procedure

Step 1 In the Workflow Actions gadget, click **New**.

Step 2 In the Name box, enter a name for the action.

Note Workflow action names are limited to 64 characters.

Step 3 From the Type drop-down list, choose **Browser Pop**.


Step 4 From the Handled By drop-down list, choose what will run the action, either the Finesse Desktop or Other (a third-party gadget).

Step 5 In the Window Name box, enter the ID name of the window that is opened. Any action that uses this window name reuses that specific window.

Note Window names are limited to 40 characters, and can be blank. If you leave the window name blank, a new window opens every time the action runs.

Step 6 Enter the URL of the browser window and click the tag icon at the right of the box and select one or more variables from the drop-down list to add tags.

Example:

`http://www.google.com/search?q=` 

For every variable you select, you can enter test data in the Sample Data box. A sample URL is automatically built in the Browser URL box below the Sample Data area. To test the URL, click Open to open the URL in your browser.

Note The system does not validate the URL you enter.

Step 7 Click **Save**.

Add HTTP Request Workflow Action

The HTTP Request workflow action makes an HTTP request to an API on behalf of the desktop user.

Procedure

Step 1 In the Workflow Actions area, click **New**.

Step 2 In the Name box, enter a name for the action.

A workflow action name can contain a maximum of 64 characters.

Step 3 From the Type drop-down list, select **HTTP Request**.

Step 4 From the Handled By drop-down list, select what will run the action, the Finesse desktop or Other (a third-party gadget).

Step 5 From the Method drop-down list, select the method to use.

You can select either PUT or POST.

Step 6 From the Location drop-down list, select the location.

If you are making the HTTP request to a Finesse API, select **Finesse**. If you are making a request to any other API, select **Other**.

Step 7 In the Content Type box, enter the content type.

The default content type is application/xml, which is the content type for Finesse APIs. If you are using a different API, enter the content types for that API (for example, application/JSON).

Step 8 In the URL box, enter the URL to which to make the request. To add variables to the URL, click the tag icon at the right of the box and select one or more variables from the drop-down list.

Example:

The following is the URL example for a Finesse API:

/finesse/api/User/  3700993

Note If you want to make a request to another API, you must enter the entire URL (for example, http://googleapis.com).

You can click the tag icon at the right of the box and select one or more variables from the drop-down list to add tags to the URL. In the preceding example, to add the dialogId, click the tag icon and select dialogId from the list.

Step 9 In the Body box, enter the text for the request. The body must match the content type (for example, if the content types is application/xml, the body must contain XML). To add variables to the body, click the tag icon at the right of the box and select one or more variables from the drop-down list.

Example:

To make an HTTP request to the Dialog - Start a recording API, enter the following into the Body box:

```
<Dialog>
<requestedAction>START_RECORDING</requestedAction>
<targetMediaAddress>  </targetMediaAddress>
</Dialog>
```

390214

To add the extension, click the tag icon and select extension.

For every variable you add, you can enter test data in the Sample Data box.

Step 10 Click **Save**.

Edit Workflow Action

Procedure

- Step 1** In the Workflow Actions gadget, select the action that you want to edit.
 - Step 2** Click **Edit**.
 - Step 3** Edit the fields that you want to change.
 - Step 4** Click **Save**.
-

Delete Workflow Action

Procedure

- Step 1** In the Workflow Actions gadget, select the action that you want to delete.
 - Step 2** Click **Delete**.
 - Step 3** Click **Yes** to confirm the deletion of the selected action.
-

Add Workflow

Procedure

- Step 1** In the Workflows gadget, click **New**.
- Step 2** From the **Choose Media** drop-down, select the media.
 - Note** In case of a voice only configuration, the **Choose Media** drop-down will display only Voice.
- Step 3** In the **Name** box, enter the name of the workflow.
 - Note** The name is limited to 40 characters.
- Step 4** In the **Description** box, enter a description of the workflow.
 - Note** The description is limited to 128 characters.
- Step 5** In the **When to perform Actions** drop-down list, select the event that triggers the workflow.
 - Note** The drop-down actions change depending on the selected media.
- Step 6** In the **How to apply Conditions** box, select if all conditions are met, or if any conditions are met, and then click **Add Condition** to add up to five conditions.
 - Note** Variables in the drop-down for conditions are grouped depending on the selected media.

Example:

For example, you can specify that the action is taken when CallVariable 1 equals 123 and CallVariable 2 begins with 2.

- Step 7** In the Ordered List of Actions area, click **Add** to open the Add Actions area. Click an action in this area to add it to the Ordered List of Actions.
- Step 8** Use the up and down arrows next to the Ordered List of Actions to move actions into the performance order.
- Step 9** Click **Save**.
- Step 10** Assign the workflow to one or more teams.

Note A workflow does not run until it is assigned to a team.

Edit Workflow

Procedure

- Step 1** In the Workflows gadget, select the workflow you want to edit.
- Step 2** Click **Edit**.
- Note** The media for an existing workflow can be changed by editing the workflow.
- Step 3** Edit the fields that you want to change.
- Step 4** Click **Save**.
-

Delete Workflow

Procedure

- Step 1** In the Workflows gadget, select the workflow that you want to delete.
- Step 2** Click **Delete**.
- Step 3** Click **Yes** to confirm the deletion of the selected workflow.
-

Reason Labels

Reason Labels

The Reason Labels feature in Packaged CCE is used to configure the Not Ready, Sign Out, and Wrap-Up reason labels. Agents select the reason on their agent desktops (Cisco Finesse) to provide the work status. Reason label appears in the Unified Intelligence Center reports, and helps to identify the agents' work behavior, for example, if the agent is spending long time in meetings or taking an inappropriate number of breaks, and so on.

The Reason Labels configured in Packaged CCE webadmin appear in the Finesse desktop of all sites in a global deployment.

Supervisors cannot access this Reason Labels feature.

To configure the reason labels, navigate to **Unified CCE Administration > Overview > Desktop Settings > Reason Labels**, or choose **Desktop > Reason Labels** from the left navigation.



Note To view the maximum limit for Not Ready reason codes, Sign Out reason codes, and Wrap-up reason labels for the Global and Team Specific reasons, click **Capacity** on the left navigation. For more information, see [Capacity Info, on page 392](#).

The Reason Labels list window has some predefined system reason labels for Not Ready and Sign Out reasons. You cannot delete these system reason labels, however you can modify the label and description. To view the list of system reason codes, see [Predefined System Reason Codes, on page 320](#).



Note After upgrade, the system defined reason labels pre-populate in the Reason Labels List window. However, you must reconfigure all the custom defined reason labels. See [Add and Maintain Reason Labels, on page 319](#)

Add and Maintain Reason Labels

This procedure explains how to add a reason label. For information on maintaining reason labels, see [Update Objects, on page 154](#) and [Delete Objects, on page 157](#).

Procedure

- Step 1** In **Unified CCE Administration**, choose **Desktop > Reason Labels** from the left navigation.
- Step 2** Click **New**.
- Step 3** Complete the following fields:

Fields	Required?	Description
Type	-	Select a reason type from the drop-down list - Not Ready, Sign Out, Wrap-Up .
Label	Yes	Enter a label for the selected reason type. The field allows maximum of 40 characters. Both alphanumeric and special characters are supported. Note Enter unique labels for the Wrap-Up reasons.
Code	Yes	Enter a unique code for the selected reason type. The valid range is from 1 to 65535. Note The Code field is not available for the Wrap-Up reasons.

Fields	Required?	Description
Description	No	Enter a maximum of 255 characters to describe the reason label. See Character Sets, on page 601 .

Step 4 To assign the reason label to one or more teams, select the **Team Specific** option.

Note By default, the **Global** option is selected to make the reason label generic or visible to all teams.

Step 5 Click **Save** to return to the List screen, where a message confirms the successful creation. You can perform the [Sort a List](#), [Search a List](#), and [Delete Objects](#) tasks on the List screen.

What to do next

To assign the configured team specific reason labels to one or more teams, navigate to **Organization > Teams (Team Resources tab)** from the left navigation. For more information, see [Add and Maintain Teams, on page 249](#).

Predefined System Reason Codes

For Not Ready system reason codes and Sign Out system reason codes, only the reason code label can be edited and saved. The Global attribute and system code cannot be modified. In case the system reason code label is modified and you wish to revert to the default label, refer to the following list of predefined system reason codes:

System Reason Code	Reason Label	Reason Label Description
32767	Not Ready - Call Not Answered	Agent state changed because the agent did not answer the call.
32762	Ready - Offhook Not Ready - Offhook	The system issues this reason code in the following scenarios: <ul style="list-style-type: none"> When the agent goes off the hook to place a call. If the agent remembers to do this task the corresponding agent-triggered reason code is displayed. If the agent does not remember to do this task, the system issues this reason code. When the agent is in Ready state and a call is placed from the ACD (Automatic Call Distribution) line, the system issues this reason code.
50001	Logged Out - System Disconnect	The CTI OS client disconnected, logging the agent out.
50002	Logged Out - System Failure	A CTI OS component disconnected, causing the agent to be logged out or set to the Not Ready state. This could be due to closing the agent desktop application, heart beat time out, or a CTI OS Server failure.

50002	Not Ready - Connection Failure	The system issues this reason code when the agent is forcibly logged out in certain cases.
50003	Logged Out - Device Error	Agent was logged out because the Unified CM reported the device out of service.
50004	Logged Out - Inactivity Timeout	Agent was logged out due to agent inactivity as configured in agent desk settings.
50005	Not Ready - Non ACD Busy	For a Unified CCE agent deployment, where the Agent Phone Line Control is enabled in the peripheral and the Non ACD Line Impact is configured to impact agent state, the agent is set to Not Ready while talking on a call on the Non ACD line with this reason code.
50010	Not Ready - Call Overlap	Agent was set to Not Ready state because the agent was routed two consecutive calls that did not arrive.
50020	Logged Out - Queue Change	Agent was logged out when the agent's skill group dynamically changed on the Administration & Data Server.
50030	Logged Out - Device Conflict	If an agent is logged in to a dynamic device target that is using the same dialed number (DN) as the PG static device target, the agent is logged out.
50040	Logged Out - Mobile Agent Call Fail	Mobile agent was logged out because the call failed.
50041	Not Ready - Mobile Call Not Answered	Mobile agent state changed to Not Ready because the call fails when the mobile agent's phone line rings busy.
50042	Logged Out - Mobile Agent Disconnect	Mobile agent was logged out because the phone line disconnected while using nailed connection mode.
65535	Not Ready - System Reinitialized	Agent reinitialized (used if peripheral restarts).
65534	Not Ready - System Reset	PG reset the agent, normally due to a PG failure.
65533	Not Ready - Extension Modified	An administrator modified the agent's extension while the agent was logged in.
20001	Not Ready - Starting Force Logout	Places the agent in the Not Ready state first before forcefully logging them off.
20002	Logged Out - Force Logout	Forces the logout request; for example, when Agent A attempts to log in to Cisco Agent Desktop and Agent B is already logged in under that agent ID, Agent A is asked whether or not to force the login. If Agent A answers yes, Agent B is logged out and Agent A is logged in. Reports then show that Agent B logged out at a certain time with a reason code of 20002 (Agent B was forcibly logged out).

20003	Not Ready - Agent Logout Request	If not already in the Logout state, request is made to place agent in the Not Ready state. Then logout request is made to log agent out.
999	Not Ready - Supervisor Initiated	The system issues this reason code when the agent's state is forcibly changed to Not Ready by the Supervisor.
999	Logged Out - Supervisor Initiated	The system issues this reason code when the agent's state is forcibly changed to Logout by the Supervisor.
255	Logged Out - Connection Failure	The system issues this reason code when the agent is forcibly logged out when there is a connection failure between the Cisco Finesse Desktop and the Cisco Finesse Server.

Desk Settings

Desk Settings

Desk settings are a collection of permissions or characteristics for the agent, such as how and when calls to the agent are redirected, how and when the agent enters various work states, and how requests to the supervisor are handled.

To configure desk settings, go to **Unified CCE Administration > Desktop > Desk Settings**.

Administrators have unlimited access to Desk Settings configuration. Supervisors cannot access Desk Settings.



Note For any change, you perform in the **Agent Desk Settings** to take effect, log out and then log in to the Finesse Agent Desktop.

Add and Maintain Desk Settings

Procedure

- Step 1** Navigate to **Unified CCE Administration > Desktop > Desk Settings**.
- Step 2** Click **New** to open the **New Desk Settings** window.
- Step 3** Complete the following fields:

Field	Required?	Description
Name	yes	Enter a unique name that will identify the desk settings, using a maximum of 32 alphanumeric characters.
Description	no	Enter a description for the desk settings.

Logout Inactivity Time	no	<p>Enter the number of seconds an agent can be inactive while in the Not Ready state before the system logs the agent out. This number can be from 10 seconds to 7200 seconds (2 hours). Leave this field blank to disable the timer.</p> <p>For agents who handle both voice and nonvoice tasks in the Cisco Finesse agent desktop, leave this field blank.</p>
Wrapup on Incoming	yes	<p>From the drop-down menu, select Optional (the default), Required, Not Allowed, or Required with wrap-up data to indicate whether the agent is allowed or required to enter wrap-up data after an incoming call. A selection of Optional means the agent can choose to enter wrap-up data or to answer another call.</p>
Wrapup on Outgoing	yes	<p>From the drop-down menu, select Optional (the default), Required, or Not Allowed to indicate whether the agent is allowed or required to enter wrap-up data after an outgoing call. A selection of Optional means the agent can choose to enter wrap-up data or to answer another call.</p>
Wrapup Timer	no	<p>Enter a value in seconds between 1 and 7200 to specify the time within which the agent can enter wrap-up data before being timed out. The default is 7200 seconds.</p>
Supervisor Assist Call Method	no	<p>From the drop-down menu, select either:</p> <ul style="list-style-type: none"> • Consultative Call (default): The caller is aware when the supervisor joins the call. This option is supported in CTI OS and Finesse agent desktops. • Blind Conference: The caller is not aware when the supervisor joins the call. This option is supported only in CTI OS agent desktops.
Emergency Call Method	no	<p>From the drop-down menu, select either:</p> <ul style="list-style-type: none"> • Consultative Call (default): The caller is aware when the supervisor joins the call. This option is supported in CTI OS and Finesse agent desktops. • Blind Conference: The caller is not aware when the supervisor joins the call. This option is supported only in CTI OS agent desktops.
Agent State after RONA	no	<p>From the drop-down menu select either:</p> <ul style="list-style-type: none"> • Not Ready (default): The agent is set as not ready after RONA. • Ready: The agent is set as ready after RONA.

Mobile Agent	no	From the drop-down menu select one of the following: <ul style="list-style-type: none"> • Not Allowed: In this mode, Mobile Agent is not allowed. • Call by Call: In this mode, the Mobile Agent's phone is dialed for each incoming call. When the call ends, the Mobile Agent's phone is disconnected before being made ready for the next call. • Nailed Up: In this mode, the agent is called at login time and the line stays connected through multiple customer calls. • Agent Chooses: In this mode, an agent can select a call delivery mode at login.
Enable mobile agent	no	Unchecked by default. When checked, indicates that the agent is a Mobile Agent who can sign in remotely and take calls from any phone. With this selected, the agent can also sign in as a usual agent.
Require Idle Reason	no	Unchecked by default. When checked, indicates that the agent must enter a reason before entering the Idle state.
Require Logout Reason	no	Unchecked by default. When checked, indicates that the agent must enter a reason before logging out.
Play zip tone	no	Unchecked by default. Checked, will play a zip tone to the agent when call is auto-answered. Note Only if the administrator enables the Auto answer option, Play ziptone can be enabled.

Note There is no RONA timer field on the Desk Settings tool. The Requery on No Answer (RONA) timer on the Unified Cisco Unified Voice Portal (CVP) controls the agent desk settings for Packaged CCE.

Step 4 Save the desk settings to return to the List window, where a message confirms the successful creation.

Agent Trace

Agent Trace

Enabling agent trace allows you to track and report on every state an agent passes through. You might enable agent trace if you have concerns about the productivity or performance of one or more agents.



Important Enabling trace can affect system performance, as it requires additional network bandwidth and database space. Typically, you use this feature for short-term tracking of specific agents. The system imposes a configuration limit on the number of agents for whom you can enable trace.

Use this tool to view, add, and remove agents for whom agent trace is enabled.

Add and Maintain Agent Trace

Procedure

- Step 1** In **Unified CCE Administration**, navigate to **Desktop > Agent Trace**.
 - Step 2** Click the + icon to open the **Add Agents with Trace Enabled** popup window. Use the sort and search features to navigate the list.
 - Step 3** Click one or more agent usernames to give them the trace-enabled status.
 - Step 4** Close **Add Agents with Trace Enabled** to return to the list.
 - Step 5** Click **Save** on the List window to confirm the trace status for the agents you added. Click **Revert** before you save to remove an agent from the Trace Enabled list.
-

Remove Agent Trace

Procedure

- Step 1** In **Unified CCE Administration**, navigate to **Desktop > Agent Trace**.
 - Step 2** On the **List of Agents with Trace Enabled** list, locate the agent whose trace status you want to remove.
 - Step 3** Click the x icon to clear trace status for that agent.
 - Step 4** Click **Save** on the List window to confirm the removal. To cancel, click **Revert**.
-

Call Settings

Route Settings

The **Route Settings** page allows you to configure the initial settings for the call flow.

Media Routing Domains

Media Routing Domains (MRDs) organize how requests for each communication medium, such as voice and email, are routed to agents.

An agent can handle requests from multiple MRDs. For example, an agent can belong to a skill group in an MRD for email and to a skill group in an MRD for voice calls.

Configure at least one MRD for each communication medium your system supports. You do not need to configure an MRD for voice; the Cisco_Voice MRD is built in.

You can add and update only Cisco_Task MRDs using the Unified CCE Administration Media Routing Domain tool.



Note To add or update Multichannel MRDs for Enterprise Chat and Email, use the Configuration Manager Media Routing Domain List tool.

Add and Maintain Media Routing Domains

This procedure explains how to add a Multichannel Media Routing Domain (MRD). For information on maintaining MRDs, see [Update Objects](#) and [Delete Objects](#).

Procedure

- Step 1** In **Unified CCE Administration**, navigate to **Overview > Call Settings > Route Settings**. The **Route Settings** window opens that shows the list of configured Media Routing Domains.
- Step 2** Click **New**.
- Step 3** Complete the following fields:

Field	Description
Type	The read-only type of the Media Routing Domain.
Name	Enter a unique name for the Media Routing Domain.
Description	Enter a description for the Media Routing Domain. See Character Sets, on page 601 .
Service Level Threshold	Enter the maximum time, in seconds, that a customer should wait before being connected with an agent.
Interruptible	Select whether tasks assigned from another MRD can interrupt an agent. Note If you change the MRD from interruptible to non-interruptible or vice versa, the change takes effect once the agent logs out and then logs back in on that MRD.
Life	Enter the amount of time, in seconds, that the system waits before ending all tasks if the connection goes down.
Start Timeout	Enter the amount of time, in seconds, that the system waits for an agent to accept a task. When this time is reached, the system makes the agent Not Routable and re-queues the task.
Max Duration	Enter the maximum duration for a task, in seconds.
Max in Queue	Enter the maximum number of tasks allowed to be queued at one time.
Max Time in Queue	Enter the maximum amount of time, in seconds, a task can be queued.

- Step 4** Click **Save**.

Dialed Number

Dialed numbers are string values used to select the appropriate routing script so that a voice call or a nonvoice task (such as an email or a request for a web chat) can be delivered to an agent. Each dialed number string is configured with a routing type and a Media Routing Domain and can be mapped to a call type. For incoming calls, you can configure post call survey and add the customized ringtone media file.

A typical call center requires multiple dialed number strings. In addition to creating dialed number strings for each telephone number that customers can use to reach you, you must set up dialed number strings for the following reasons:

- So that an agent can transfer to, or conference in, another agent
- For requery on no answer (RONA)
- For supervisor/emergency assist calls

Related Topics

[Add and Maintain Dialed Numbers](#)

[Call Type](#), on page 342

Search for Dialed Numbers

The Search field in the Dialed Numbers tool offers an advanced and flexible search.

Click the + icon at the far right of the Search field to open a popup window, where you can:

- Enter a name or description to search for that string.
- Enter one or more site names separated by spaces. (Site is an OR search.)
- Enter one or more peripheral set names separated by spaces. (Peripheral Set is an OR search.)



Note Search by peripheral set is available only in Packaged CCE 4000 Agents and 12000 Agents deployments.

- Select departments, with options for **Globals and Departments**, **Globals only**, or **Departments only**.

Selecting **Globals and Departments** or **Departments only** enables an input field where you can enter a space-separated list of department names. (Department is an OR search.)



Note Search by department is available only when departments are configured.
Search by site is available only when remote sites are configured.

Add and Maintain Dialed Numbers

This procedure explains how to add a dialed number. For information on maintaining dialed numbers, see [Update Objects](#) and [Delete Objects](#). After you have created Dialed Numbers, you can also add, or edit ringtone media files for multiple Dialed Numbers at once (see [Add and Update Ringtone Media File for Multiple Dialed Numbers](#), on page 333).

Procedure

- Step 1** In **Unified CCE Administration**, navigate to **Overview > Call Settings > Route Settings**.
- Step 2** Click the **Dialed Number** tab.
- Step 3** Click **New** to open the **New Dialed Number** window.
- Step 4** Complete the following fields:

Field	Required?	Description
Dialed Number String	yes	<p>The value used to route the call or direct the nonvoice task.</p> <p>Enter a string value that is unique for the routing type, maximum of 25 characters.</p> <p>Note The External Voice and PCS routing types must not have the same dialed number strings.</p>
Description	no	Enter a maximum of 255 characters to describe the dialed number string.
Department	- (yes for departmental administrators)	<p>A departmental administrator must select one department from the popup list to associate with this dialed number. The list shows all this administrator's departments.</p> <p>When a departmental administrator selects a department for the dialed number, the popup list for call type includes global call types and call types in the same department as the dialed number.</p> <p>A global administrator can leave this field as Global (the default), which sets the dialed number as global (belonging to no departments). A global administrator can also select a department for this Dialed Number.</p> <p>When an administrator changes the department, selections for call type are cleared if the selections don't belong to the new department or the global department.</p>
Site	-	<p>The Site field displays Main by default for Packaged CCE 2000 Agents deployment.</p> <p>For Packaged CCE 4000 Agents and 12000 Agents deployments, Site is a mandatory field and has no default value.</p> <p>To add a site:</p> <ol style="list-style-type: none"> a. Click the magnifying glass icon to display the list of sites. b. Select the required site.

Field	Required?	Description
Peripheral Set	Yes	<p>This field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see Add and Maintain Peripheral Set, on page 143.</p> <p>To add a peripheral set:</p> <ol style="list-style-type: none"><li data-bbox="885 443 1498 506">a. Click the magnifying glass icon to display the list of peripheral sets configured for the selected Site.<li data-bbox="885 527 1284 558">b. Select the required peripheral set.

Field	Required?	Description
Routing Type	-	

Field	Required?	Description
		<p>From the drop-down menu, select one of the following options: (For remote sites, options may vary depending on the PG types configured on the selected remote site.)</p> <ul style="list-style-type: none"> <p>• External Voice: Select this option for dialed number strings that apply to voice calls coming from Cisco Unified Customer Voice Portal (CVP). These calls are referred to as external because they typically come from outside of the enterprise through a gateway. External Voice is the selection for calls that come in from customers and must be answered by agents or sent to the VRU.</p> <p>If you select External Voice, the Ringtone Media File field appears to enter the ringtone filename for the user-defined Dialed Numbers.</p> <p>For remote sites, the External Voice option is available if the site is configured to VRU PG.</p> <p>• Internal Voice: Select this option for dialed number strings that can be called from a Cisco Unified Communications Manager phone. These calls must have a route point on Unified Communications Manager that corresponds to the internally dialed number. They are referred to as internal because they can be accessed only by Unified Communications Manager.</p> <p>Internal Voice is used for dialed numbers that agents use to transfer calls to other agents, to enable the system to redirect calls internally when the agent doesn't answer, and to direct a call from an agent to a supervisor for assistance.</p> <p>Dialed numbers with the routing type Internal Voice appear on the Supervisor Script Dialed Number list when you create or edit a team.</p> <p>For remote sites, the Internal Voice option is available if the site is configured to Agent PG.</p> <p>• Outbound Voice: Select this option for dialed number strings that are used by the Cisco Outbound Option Dialer. These dialed number strings are referenced and used to route calls to agents or to VRU scripts in the Campaign Skill Group Selection.</p> <p>For remote sites, the Outbound Voice option is available if the site is configured to Multichannel PG.</p> <p>• Post Call Survey: Select this option for Post Call Survey dialed number strings that apply to voice calls coming from Cisco Unified Customer Voice Portal (CVP). This option is similar to External Voice where</p>

Field	Required?	Description
		<p>the calls come from outside of the enterprise through a gateway. However, Unified CVP directs the calls internally to Post Call Survey after agent ends the call. This option allows you to enter the Post Call Survey Dialed Number and associate the Dialed Number Patterns to the Post Call Survey Dialed Number.</p> <p>For remote sites, the Post Call Survey option is available if the site is configured to VRU PG.</p> <p>The following multichannel routing types are available if you have configured the peripherals for the multichannel machines using Peripheral Gateway Setup tool, and added external multichannel machines to the System Inventory:</p> <ul style="list-style-type: none"> • SocialMiner: Select this option for dialed number strings that originate from SocialMiner and are routed to an agent who interacts with a customer by Agent Request. • Enterprise Chat and Email: Select this option for dialed number strings that originate from Enterprise Chat and Email and are routed to an agent who interacts with a customer by email or by web chat. • 3rd Party Multichannel: Select this option for dialed number strings that originate from a third-party application and are routed to an agent who interacts with a customer by email or by web chat. <p>See the <i>Cisco Packaged Contact Center Enterprise Features Guide</i> at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html for information about configuring the peripherals using Peripheral Gateway Setup.</p>
Media Routing Domain	no	<p>The Media Routing Domain associated with the dialed number. Media Routing Domains (MRDs) organize how requests for media are routed. The system routes calls to agents who are associated with a particular communication medium; for example, voice or email. The selection of Routing Type determines what appears in this field.</p> <ul style="list-style-type: none"> • If the Routing Type is External Voice, Internal Voice, or Outbound Voice, the Media Routing Domain is Cisco_Voice and you can't change it. • If the Routing Type is Multichannel, click the magnifying glass icon to display the Select Media Routing Domain popup window.

Field	Required?	Description
Call Type	no	Use the drop-down menu to select a valid call type to map to this dialed number strings. Associating a dialed number with a call type ensures appropriate routing and affects reporting. The default is the system default set in Overview > Call Settings > Miscellaneous . To select a different call type: <ul style="list-style-type: none"> • Click the magnifying glass icon to display the Select Call Type popup window. • Click a row to make a selection and close the list.
PCS Enabled Dialed Number Patterns	no	Note The PCS Enabled Dialed Number Patterns field appears if the Routing Type is Post Call Survey . Enter one or more dialed number patterns of type External Voice to transfer calls to the Post Call Survey dialed number entered in the Dialed Number String field. The field allows maximum of 512 characters that can have the comma-separated list without any spaces. Both alphanumeric and special characters are supported.
Ringtone Media File	no	Note The Ringtone Media File field appears if the Routing Type is External Voice . Enter filename of the custom ringtone for the user-defined Dialed Numbers - maximum of 256 characters without any spaces.

Step 5 Click **Save** to return to the List screen, where a message confirms the successful creation.

The configured Dialed Number is synchronized to Unified CVP machine deployed in Inventory. If the Sync fails, the Device Sync Alert icon appears on the status bar at the top-right of the List screen. Click the icon to perform the manual synchronization. See [Device Out of Sync Alerts, on page 159](#)

Add and Update Ringtone Media File for Multiple Dialed Numbers

You can add or edit a ringtone media file for multiple Dialed Numbers at once. The Dialed Numbers must be of the type **External Voice** to add or update the ringtone media filename.

Procedure

Step 1 In **Unified CCE Administration**, choose **Overview > Call Settings > Route Settings**.

Step 2 Click the **Dialed Number** tab.

The List window appears with the configured dialed numbers.

- Step 3** To add or update the ringtone media filename for multiple Dialed Numbers, check the check box that is associated with Dialed Numbers of the type **External Voice**.
- Step 4** Click **Edit > Ringtone Media File**.
The **Edit Details of Dialed Number Strings** popup window appears.
- Step 5** In **Ringtone Media File**, enter filename of the custom ringtone.
- Step 6** Click **Save**, and then click **Yes** to confirm the changes.

Routing Pattern

A routing pattern comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a destination which can be a device or a group of devices. Routing patterns provide flexibility in network design.

Search for Routing Patterns

The Search field on the Routing Pattern page offers an advanced and flexible search.

Click the + icon on the Search field to open a popup window, where you can:

- Enter a routing pattern, description, or destination to search for that string.
- Select a pattern type.
- Enter one or more site names separated by spaces. (Site is an OR search.)
- Select if Send to Originator is enabled.
- Select if RNA Timeout is configured.



Note Search by site is available only when remote sites are configured.

Add and Maintain Routing Pattern

This procedure explains how to add a routing pattern. For information on maintaining routing patterns, see [Update Objects](#) and [Delete Objects](#).

Procedure

- Step 1** In **Unified CCE Administration**, choose **Overview > Call Settings > Route Settings**.
- Step 2** Click the **Routing Pattern** tab.
- Step 3** Click **New** to open the **New Routing Pattern** page.
- Step 4** Complete the following fields:

Field	Required?	Description
Routing Pattern	yes	Enter a name for the routing pattern. Maximum length is 24 characters. Valid characters are alphanumeric, wildcard characters such as letter X, period (.), exclamation(!), greater than (>), and asterisk (*).

Field	Required?	Description
Description	no	Enter a description for the routing pattern. See Character Sets , on page 601.
Site	-	Displays Main by default. Search and select the routing pattern site.
Pattern Type	yes	Select the type of pattern from the drop-down list.
Destination	yes	To select the SIP Server Group or FQDN: <ul style="list-style-type: none"> a. Click the field to open the Add SIP Server Group popup window. Based on the selected Site and Pattern Type, the popup window lists the SIP Server Groups. The SIP Server Groups are configured in Call Settings > Route Settings > SIP Server Group. b. Search and select a SIP Server Group from the list.
RNA Timeout	no	Enter the number of seconds that the destination should ring before the call is taken away. Range is 5 to 60 seconds.
Send to originator	no	Check the check box to configure calls to be sent to the originator. Note Send to originator is not applicable when you select the VRU pattern type for Cisco Virtualized Voice Browser (VVB).

Step 5 Click **Save**.

Location Configuration

The Location feature is used to route calls to the agent or IVR available in the local branch office instead of routing calls to the central or main office.

Locations are used to implement call admission control in a centralized call-processing system. In a centralized call-processing system, a single Cisco Unified Communications Manager cluster provides call processing for all locations on the IP telephony network. Call admission control enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between the locations.

If the required locations are configured in Cisco Unified Communications Manager (CUCM), Packaged CCE enable you to fetch the locations from CUCM through the Synchronization (Sync) option. This option allows you to select a Unified Communications Manager server and extract the location routing code. You can then assign the Ingress router to identify the call origin and subsequent routing.

Packaged CCE also allows you to create a new location and add location information.

Search for Locations

The Search field on the Location page offers an advanced and flexible search.

Click the + icon on the Search field to open a popup window, where you can:

- Enter name or description of a location to search for that string.
- Enter the hostname or IP address of the gateway. The search is case-insensitive and does not support partial matches.
- Enter a site. The search is case-insensitive and does not support partial matches.

Add and Maintain Location Configurations

Procedure

Step 1 In **Unified CCE Administration**, choose **Overview > Call Settings > Route Settings**.

Step 2 Click the **Location** tab.

Step 3 Click **New**.

Step 4 Complete the following fields:

Fields	Required?	Description
Location Name	Yes	Enter a name for the location.
Description	No	Enter a description of the location. See Character Sets , on page 601.
Location Routing Code	Yes	A unique location code that is appended to the ICM label for routing the calls to the destination devices. See Location Properties , on page 337.
Sites	No Required if you add Gateways to the location.	Site of the location. The configured sites are listed in the Sites field. To add sites, select the applicable check boxes in the Sites field.
Gateways	No Required if you select Site(s) for the location.	Gateways that are associated with the location. To associate a gateway to the location: a. Click the + icon. The Add Gateways popup window opens with a list of gateways. b. Select a gateway from the list. Use the Search a List feature to navigate the list.

Step 5 Click **Save**.

Synchronize the Location Information

Location synchronization is a user-initiated task. A single synchronization operation runs in the background when initiated. When initiated, the system synchronizes and merges the locations from the Unified CM server selected during the configuration.

To complete a synchronizing operation:

- The system retrieves the location data from the Unified CM database.
- The system merges the retrieved data with any existing location data.

Procedure

- Step 1** In **Unified CCE Administration**, choose **Overview > Call Settings > Route Settings**.
- Step 2** Click the **Location** tab.
- Step 3** Click the **Sync** button.
The **Synchronize Location** popup window opens.
- Step 4** Select a Unified CM server from the **Select CUCM Publisher** drop-down list.
- Step 5** Click **Sync**.
The synchronized locations appear on the List window.
-

What to do next

You can add **Location Routing Code** and associate applicable **Sites** and **Gateways** to the required Locations.

Location Properties

The Location Properties feature provides options for the placement of the location routing code. The Location Properties setting applies to all the configured locations.

You can place the routing code at the beginning of the Network VRU label, in the middle of the Network VRU label and the correlation ID, or can choose not to insert the routing code.

Procedure

- Step 1** In **Unified CCE Administration**, choose **Overview > Call Settings > Route Settings**.
- Step 2** Click the **Location** tab.
- Step 3** Click the **Properties** link.
The **Properties** popup window opens.
- Step 4** Select an option to insert the location routing code.
The options are:
- Insert routing code between Network VRU label and the correlation ID.
 - Insert routing code at the beginning of the Network VRU label.
 - Do not insert routing code.

The **Insert routing code between Network VRU label and the correlation ID** option is the default selection.

Step 5 Click **Save** to return to the List window.

What to do next

After you change the routing code insertion setting, you must recreate Routing Patterns and VVB Triggers associated to locations.

SIP Server Group

You can add the SIP Server groups to perform SIP dynamic routing by Cisco Unified Customer Voice Portal (CVP).

A SIP Server Group consists of one or more destination addresses (elements), and is identified by a Server Group domain name. This domain name is also known as the Fully Qualified Domain Name (FQDN).



Note The site specific SIP Server Groups' configuration is updated to all the Unified CVP of the corresponding site present in the Inventory (see [System Inventory for Packaged CCE 2000 Agents Deployment, on page 9](#)).

Related Topics

- [Search for SIP Server Groups](#), on page 338
- [Add and Maintain SIP Server Group](#), on page 338
- [SIP Server Group Properties](#), on page 340

Search for SIP Server Groups

The Search field in the SIP Server Group tool offers an advanced and flexible search.

Click the + icon at the right of the Search field in the SIP Server Group tool. In the popup window, you can:

- Search for a name or description.
- Enter one or more site names separated by spaces (Site is an OR search).
- Select SIP Server type.
- Enter hostname/IP address of the element. The search is case-sensitive and does not support partial matches.



Note Search by site is available only when you configure remote sites.

Add and Maintain SIP Server Group

This procedure explains how to add a SIP Server Group. For information about maintaining SIP Server Groups, see [Update Objects](#) and [Delete Objects](#).

Procedure

- Step 1** In **Unified CCE Administration**, choose **Overview > Call Settings > Route Settings**.
- Step 2** Click the **SIP Server Group** tab.
- Step 3** Click **New** to open the **New SIP Server Group** page.
- Step 4** Complete the following fields on the **General** tab:

Field	Required?	Description
Domain Name FQDN	yes	Enter the SIP Server Group Fully Qualified Domain Name (FQDN). Must be a valid FQDN limited to 128 characters. Can contain a combination of uppercase and lowercase alphanumeric characters, underscore [_], and period [.].
Description	no	Enter a maximum of 255 characters to describe the SIP Server Group. See Character Sets, on page 601 .
Site	-	To select the site of the group. Displays Main by default. To select a remote site: <ol style="list-style-type: none"> Click the magnifying glass icon to display the list of configured sites. Select the required site.
Type	yes	To select the type of group. From the drop-down list, choose one of the following options: <ul style="list-style-type: none"> VRU - For Cisco Virtualized Voice Browser (VVB), Cisco Unified SIP Proxy (CUSP), and VXML Gateway devices. Agent - For Cisco Unified Communications Manager (CUCM) and CUSP devices. External - For Ingress Gateway and CUSP devices.

- Step 5** Click **Members** tab.
- Click the + icon.
The **Add Group Members** popup window appears with the hostname or IP address of the configured devices based on the **Site** and **Type** selected in the **General** tab.

Note To search a device configured in a different site, choose a site from the **Site** drop-down list.
 - Choose one or more devices from the **Add Group Members** popup window.
The selected devices appear in the **List of Group Members** table.
 - Enter appropriate values in the following fields:

Field	Required?	Description
Priority	yes	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. Range is 1 to 2147483647
Weight	yes	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. Range is 10 to 2147483647.
Port	yes	Port number of the element in the server group. The default value is 5060. Range is 1 to 65535
Secure Port	no	The listening port for secure connection. Range is 1 to 65535

Step 6 Click **Save** to return to the List screen, where a message confirms the successful creation.

SIP Server Group Properties

The SIP Server Group properties configure the heartbeat parameters to exchange the heartbeat message between SIP Server Group elements and SIP Server Group.



Note The configuration of SIP Server Group properties forms the global setting for all SIP Server Groups across all sites.



Note 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 a specific interval and sends 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).

Update SIP Server Group Properties

Procedure

- Step 1** In **Unified CCE Administration**, choose **Overview > Call Settings > Route Settings**.
- Step 2** Click the **SIP Server Group** tab.
- Step 3** Click the **Properties** link.

The **SIP Server Properties** window opens to configure SIP Server Group properties.

Step 4 Update any of the following fields values:

Fields	Description	Default
Use Heartbeats to Endpoints	Check the check box 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.	Enabled (Checked)
Number of Failed Heartbeats for Unreachable Status	The number of failed heartbeats before marking the destination as unreachable.	3
Heartbeat Timeout	The amount of time, in milliseconds, before timing out the heartbeat.	800 milliseconds
Up Endpoint Heartbeat Interval	The ping interval for heart beating an endpoint (status) that is up.	5000 milliseconds
Down Endpoint Heartbeat Interval	The ping interval for heart beating an endpoint (status) that is down.	5000 milliseconds
Heartbeat Local Listen Port	The heartbeat local socket listen port. Responses to heartbeats are sent to this port on CVP by endpoints.	5067
Heartbeat SIP Method	The heartbeat SIP method. Note PING is an alternate method; however, some SIP endpoints do not recognize PING and will not respond at all.	OPTIONS
Heartbeat Transport Type	During transportation, Server Group heartbeats are performed with a UDP or TCP socket connection. If CVP Server encounters unreachable or overloaded callbacks invoked in the Server Group, that element is marked as being down for both UDP and TCP transports. When the element is up again, it is routable for both UDP and TCP. Note TLS transport is not supported.	UDP
Overloaded Response Codes	The response codes are used to mark an element as overloaded when received. If more than one code is present, it is presented as a comma delimited list. An OPTIONS message is sent to an element and if it receives any of those response codes, then this element is marked as overloaded.	503,480,600
Options Override Host	The contact header hostname to be used for a heartbeat request (SIP OPTIONS). The given value is added to the name of the contact header of a heartbeat message. Thus, a response to a heartbeat would contain gateway trunk utilization information.	cvp.cisco.com

Step 5 Click **Save**.

Call Type

Call types categorize calls. Based on call type, the system maps a dialed number to a routing script that ultimately sends the call to the appropriate destination. Consider the call types you need to create to meet your reporting needs, and configure a separate call type for each type of call treatment that you want to offer.

For example, you might create call types for the following:

- Calls answered by agents
- Calls abandoned at the VRU
- Calls that reroute when the agent does not answer
- Calls that are transferred and conferenced
- Outbound Option calls
- Calls that require supervisor assistance

Related Topics

[Add and Maintain Call Types](#), on page 342

[Dialed Number](#), on page 327

Add and Maintain Call Types

This procedure explains how to add a call type. For information on maintaining call types, see [Update Objects](#) and [Delete Objects](#).

Procedure

Step 1 In **Unified CCE Administration**, navigate to **Overview > Call Settings > Route Settings**.

Step 2 Click the **Call Type** tab.

Step 3 Click **New** to open the **New Call Type** window.

Step 4 Complete the following fields :

Field	Required?	Description
Name	yes	Enter a name for the call type using a maximum of 32 characters. This name must be unique among call types in the system.
Description	no	Enter a maximum of 255 characters to describe the call type. See Character Sets , on page 601.

Field	Required?	Description
Service Level Threshold	no	<p>This value is used in reports to identify the percentage of calls that are answered within that time threshold, enabling you to see whether agents are meeting the target goal. The field defaults to the System Default set in Call Settings > Miscellaneous > Global (see Global, on page 360).</p> <p>To select a different service level threshold, enter a value in seconds, from 0 to 2,147,483,647.</p>
Service Level Type	no	<p>Indicates how the system software calculates the service level. The field defaults to the System Default set in Call Settings > Miscellaneous > Global (see Global, on page 360). To override the system default for this call type, select one of these other options from the drop-down menu:</p> <ul style="list-style-type: none"> • Ignore Abandoned Calls: Select this option to exclude abandoned calls from the service level calculation. • Abandoned Calls have Negative Impact: Select this option if you want only calls that are answered within the service level threshold time to be counted as treated calls. The service level is negatively affected by calls that abandon within the service level time. • Abandoned Calls have Positive Impact: Select this option if you consider a call abandoned within the service level threshold time as a treated call. Abandoned calls have a positive impact on the service level.
Bucket Interval	-	<p>Bucket intervals appear in call type reports and display the number of calls answered and abandoned for different time intervals.</p> <p>Configure the bucket interval associated with this call type.</p> <p>The field defaults to the System Default set in Call Settings > Miscellaneous > Global (see Global, on page 360).</p> <p>To select a different bucket interval:</p> <ul style="list-style-type: none"> • Click the magnifying glass icon to display Select Bucket Interval. • Click the row to select a bucket interval and close the List.

Step 5 Click **Save** to return to the List window, where a message confirms the successful creation.

Expanded Call Variables

Calls can carry data with them as they move through the system. This data, called expanded call variable data, is embedded within the call and is visible to the agent on the agent desktop. ECC variables are passed back and forth in ECC payloads. Expanded call variable data can assist the agent in working with the caller.

The expanded call variable can be set or updated by Cisco Unified Customer Voice Portal (CVP), by Unified CCE scripting, or by an agent who is transferring the call.

- If the call is at Unified CVP for VRU treatment, the call context is exchanged between Unified CVP and Unified CCE.
- If the call is at an agent, the call context is exchanged between the desktop and Unified CCE.

Note that this is a two-way exchange: in some cases the expanded call variable data is sent to Unified CCE from Unified CVP or the agent desktop, and in some cases the data is sent by Unified CCE based on script configuration to Unified CVP or the agent desktop.

Built-in expanded call variables are identified by the **BuiltIn** check box on the Edit Expanded Call Variable window. You cannot delete these expanded call variables. You can create new expanded call variables subject to certain sizing constraints.

For Packaged CCE 4000 and 12000 Agents deployment, see *Configuration Guide for Cisco Unified Customer Voice Portal* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html> for the list of ECC Variables.

Related Topics

[Add and Maintain Expanded Call Variables](#), on page 346

[Sizing Expanded Call Variables](#), on page 349

ECC Payloads

You can define as many ECC variables as necessary. But, you can only pass 2000 bytes of ECC variables on a specific interface at any one time. To aid you in organizing ECC variables for specific purposes, the solution has *ECC payloads*.

An ECC payload is a defined set of ECC variables with a maximum size of 2000 bytes. You can create ECC payloads to suit the necessary information for a given operation. You can include a specific ECC variable in multiple ECC payloads. The particular ECC variables in a given ECC payload are called its *members*.



Note For ECC payloads to a CTI client, the size limit is 2000 bytes plus an extra 500 bytes for the ECC variable names. Unlike other interfaces, the CTI message includes ECC variable names.

In certain cases, mainly when using APIs, you might create an ECC payload that exceeds the CTI Server message size limit. If you use such an ECC payload in a client request, the CTI Server rejects the request. For an OPC message with such an ECC payload, the CTI Server sends the message without the ECC data. In this case, the following event is logged, “CTI Server was unable to forward ECC variables due to an overflow condition.”

You can use several ECC payloads in the same call flow, but only one ECC payload has scope at a given moment. TCDs and RCDs record the ID of the ECC payload that had scope during that leg of the call. The *Call.ECCPayloadID* variable contains the ID of the ECC payload which currently has scope.

In solutions that only use the default ECC payload, the system does not create an ECC variable that exceeds the 2000-byte limit for an ECC payload or the 2500-byte CTI Message Size limit.



Note Packaged CCE 2000 Agent deployment allows you to use only the default ECC payload for the Network VRU.

If you create another ECC payload, the system no longer checks the 2000-byte limit when creating ECC variables. The system creates the ECC variables without assigning them to an ECC payload. Assign the new ECC variable to an appropriate ECC payload yourself through the ECC Payload Tool.

You can create and modify ECC payloads in the **Configuration Manager > List Tools > Expanded Call Variable Payload List** tool. In Packaged CCE 4000 Agent and 12000 Agent deployments, you can assign an ECC payload to Network VRU using the Network VRU Explorer tool in Configuration Manager.

Default ECC Payload

The solution includes an ECC payload named "Default" for backward compatibility. If your solution does not require more ECC variable space, you only need the Default payload. The solution uses the Default payload unless you override it.

If your solution only has the Default payload, the solution automatically adds any new ECC variables to the Default payload until it reaches the 2000-byte limit.



Note You cannot delete the Default payload. But, you can change its members.



Important During upgrades, when the system first migrates your existing ECC variables to the Default payload, it does not check the CTI message size limit. The member names might exceed the extra 500 bytes that is allocated for ECC payloads to a CTI client. Manually check the **CTI Message Size** counter in the **Expanded Call Variable Payload List** tool to ensure that the Default payload does not exceed the limit. If the Default payload exceeds the limit, modify it to meet the limit.

In a fresh install, the Default payload includes the predefined system ECC variables. In an upgrade, the Default payload's contents depend on whether the starting release supports ECC payloads:

- **ECC payloads not supported**—During the upgrade, a script adds your existing ECC variables to the Default payload.
- **ECC payloads are supported**—The upgrade brings forward the existing definition of your Default payload.



Note If your solution includes PGs from a previous release that does not support ECC payloads, the Router always sends the Default payload to those PGs. Those PGs can properly handle the Default payload.

ECC Payload Node

The **ECC Payload** node is available from the **General** tab on the **Object Palette**:

Figure 2: Payload icon



Use this node to change the ECC payload that has scope for the following part of your script. Once you select an ECC payload, it has scope for all non-VRU operations until changed. You can select the ECC payload either statically or dynamically by the payload's EnterpriseName or ID.

Add and Maintain Expanded Call Variables

Procedure

Step 1 In **Unified CCE Administration**, navigate to **Overview > Call Settings > Route Settings > Expanded Call Variables** to open the **List of Expanded Call Variables**.

The window tracks the number of bytes used by the expanded call variables, measured against the system total and the CTI Server total.

Step 2 Click **New** to open the **New Expanded Call Variable** page.

Step 3 Complete the following fields:

Field	Required?	Description
Name	yes	The name of the expanded call variable, prepended by user. This field allows a maximum of 32 characters. (This maximum includes the four characters in user.)
Description	no	Enter up to 255 characters to describe the expanded call variable. There is no restriction of characters. See Character Sets, on page 601 .
Max Length	yes	Specifies the maximum number of characters allowed in the value that will be stored in the expanded call variable value. The range is from 1 to 210 characters.
Array	no	This check box is unchecked by default to indicate that the expanded call variable is scalar. Check the check box to configure the expanded call variable as an array, not a scalar.
Maximum Array Size	no	This field appears when Array is checked. Use it to indicate the maximum number of elements (1-255) in the array.

Field	Required?	Description
Enabled	no	Checking this check box indicates that the expanded call variable is currently enabled—it can be used in scripts and appears on the agent desktop.
Persistent	no	Checking this check box indicates that data for this expanded call variable will be written to the historical database; specifically to the Termination Call Detail (TCD) and Route Call Detail (RCD) tables. Note that storing excessive call variable data can degrade historical database performance. Only persistent call variables are written to the historical database. Nonpersistent variables can be used in routing scripts, but are not written to the database.
Cisco Provided	—	This check box is display-only, and appears when editing existing built-in or custom expanded call variables. The New Expanded Call Variable window does not include this check box.
Bytes Required (if enabled)	—	This display-only field indicates the number of bytes required to store the expanded call variable in the system.
Bytes Required in CTI Server (if enabled)	—	This display-only field is similar to Bytes Required, above, but applies to the CTI Server. In CTI Server, the number of bytes required includes the length of the expanded call variable name.
Total Bytes Required for Enabled Variables: # of maximum 2000 bytes (# bytes remaining)	—	This display-only field keeps a running total of the number of bytes used by all expanded call variables. The maximum limit allowed is 2000 bytes per ECC payload.
Total Bytes Required for Enabled Variables in CTI Server: # of maximum 2500 bytes (# bytes remaining)	—	This display-only field keeps a running total of the number of bytes used by all expanded call variables in CTI Server. The maximum limit allowed is 2000 bytes per ECC payload with an extra 500 bytes to add the names of the ECC variables in that payload.

Step 4 Save the expanded call variable and return to the List window, where a message confirms the successful creation.

What to do next

If you change the configuration of any ECC variable, restart the Unified CVP Call Server or VRU PIM to force a renegotiation of the ECC variables.

Before you can use the new ECC variable, you must add it to an ECC payload.



Note If your solution only has a Default payload, the solution automatically adds any new ECC variables to the Default payload until it reaches the 2000-byte limit.

Define ECC Payloads

You can create and modify ECC payloads in the **Expanded Call Variable Payload List** tool.



Note The tool checks that the ECC payload does not exceed the 2000-byte limit only when you save your changes. The counters on the **Members** tab only show what the current size is with all the selected members. They are only informational and do not enforce the limit. The limit is enforced when you attempt to save the changes.

To define an ECC payload, you create the ECC payload and then add its members.

Procedure

-
- Step 1** In the Configuration Manager, open **Tools > List Tools > Expanded Call Variable Payload List**.
The **ECC Payload List** window appears.
 - Step 2** Click **Retrieve** to enable adding ECC payloads.
 - Step 3** Click **Add**.
The **Attributes** property tab appears.
 - Step 4** Complete the **Attributes** property tab. See the *List Tools Online Help* for details on the **Attributes** property tab.
 - Step 5** On the **Members** tab, click **Add**.
A dialog box listing all the existing ECC variables appears.
 - Step 6** Select the members for your ECC payload and click **OK**.
Watch that the **ECC Variable Size** counter does not exceed 2000 bytes. For ECC payloads that go to CTI clients, watch that the **CTI Message Size** counter does not exceed 2500 bytes.
 - Step 7** Click **Save** to apply your changes.
-

Sizing Expanded Call Variables

Expanded call variable usage impacts PG, Router, and Logger bandwidth. The Expanded Call Variables List, Add, and Edit windows track the space that your expanded call variables are consuming, as compared with the system maximums.

The maximum amount of space that all the ECC variables in each ECC payload can take up in Unified Contact Center cannot exceed 2000 bytes.

Each expanded call variable in Unified CCE is calculated using the following formula:

- For scalar: $5 + \text{Maximum_Length}$
- For array: $5 + (1 + \text{Maximum_Length}) * (\text{Maximum_Array_Size})$

The maximum amount of space that all the ECC variables in each ECC payload can take up in CTI Server cannot exceed 2500 bytes. The allowed limit is 2000 bytes per ECC payload with an extra 500 bytes to add the names of the ECC variables in that payload. Each expanded call variable in CTI Server is calculated using the following formula:

- For a scalar variable, the size is $\text{length of Name} + \text{Maximum Length} + 4$.
- For an array variable, the size is $(\text{length of Name} + \text{Maximum Length} + 5) * \text{Maximum Array Size}$.

IVR Settings

The IVR Settings page allows you to configure the Network VRU Scripts and File Transfers.

Network VRU Scripts

Not all calls are delivered directly to agents. Some are sent to a Voice Response Unit (VRU) instead of, or before, they are sent to an agent. In the Packaged CCE deployment, the VRU is Cisco Unified Customer Voice Portal (Unified CVP). You must configure network VRU scripts to direct Unified CVP on how to handle the treatment of individual calls, using Unified CVP microapplication functions.

There are six Unified CVP microapplication types:

- **Play Media (PM):** Retrieves and plays a media file such as a welcome.wav or an agent greeting.
- **Play Data (PD):** Retrieves and plays data of various types, such as numbers, characters, time of day, or currency.
- **Get Digits (GD):** Plays a media file and retrieves digits from the caller.
- **Menu (M):** Plays media menu file and retrieves a single telephone keypad entry from the caller.
- **Get Speech (GS):** A "GS,Server,V" script is provided with Packaged CCE and appears in the List of Network VRU Scripts.
- **Capture:** Allows you to trigger the storage of current call data at various points.

Related Topics

[Access to VRU Scripts in Packaged CCE Routing Scripts](#), on page 455

Add and Maintain Network VRU Scripts

Procedure

Step 1 In **Unified CCE Administration**, choose **Overview > Call Settings > IVR Settings > Network VRU Scripts** to open the **List of Network VRU Scripts**.

Step 2 Click **New** to open the **New Network VRU Script** window. Complete the following fields:

Field	Required?	Description
Name	yes	Enter a unique name to identify the script, using a maximum of 32 alphanumeric characters.
Description	no	Enter additional information about the script. See Character Sets, on page 601 .
Routing Type	yes	Retain the default (Voice) or select Multichannel from the drop-down menu. Voice routes the script to Unified CVP. Multichannel routes the script to Enterprise Chat and Email (ECE).
VRU Script Name	yes	Enter the name of the script as it is known on the Unified CVP. See VRU Script Name Parameters, on page 351 .
Configuration Param	no	A string used by Unified CVP to pass additional parameters to the IVR Service. The content of the string depends on the microapplication to be accessed.
RNA Timeout	yes	Enter a number to indicate the number of seconds for the system to wait for a response from the routing client after directing it to run the script. The default value is 180 seconds. Valid values are 1 to 2147483647. The destination phone rings until it exceeds the ring-no-answer (RNA) timeout setting.
Interruptible	no	Checked by default, this check box indicates whether or not the script can be interrupted; for example, when an agent becomes available to handle the call.

Step 3 Click **Save** to return to the List window, where a message confirms the successful creation.

After you add a network VRU script, it is visible in the Script Editor Run External Script node. Processing this script node sends the network VRU script parameters to Unified CVP. After the system establishes that

the call has been successfully delivered, the Run VRU Script node executes, instructing Unified CVP to run the network VRU script and apply the call treatment.

Related Topics

- [VRU Script Name Parameters](#), on page 351
- [Sample VRU Script Names](#), on page 352
- [Configuration Parameters](#), on page 353
- [Sample Configuration Values](#), on page 356

VRU Script Name Parameters

VRU Script Name parameters have a “positional” sequence format-- the format is Micro_app acronym,parameter,parameter.

- The microapplication acronym is case-insensitive (enter PM or pm).
- Use double commas (,,) to skip a parameter; Unified CVP will supply the default.

The Play Media position sequence is PM,media file name,media library type,Uniqueness value.

The Play Data position sequence is PD,Data Playback Type,Uniqueness value.

The Get Digits position sequence is GD,media file name,media library type,Uniqueness value.

The Menu position sequence is M,media file name, media library type,Uniqueness value.

Parameter Name	Used For	Notes
<p>Media File Name options are as follows:</p> <ul style="list-style-type: none"> • A filename--(for instance, a .wav file) • (number 1-10)--Unified CVP plays the file in the corresponding Call.PeripheralVariable file. <p>For example, a value of 2 instructs Unified CVP to look at Call.PeripheralVariable2.</p> <p>If you use the (number 1-10) option and set the Media Library Type to "V," Unified CVP plays the external VoiceXML file specified in the corresponding Call.PeripheralVariable.</p> <p>If you set the value to (no value) and set the Media Library Type to “A” or “S”, the IVR Service creates VoiceXML without a media prompt.</p> <ul style="list-style-type: none"> • a--Unified CVP automatically generates the media file name for agent greeting when this option is specified. The filename is based on GED-125 parameters received from Unified ICM. This option is only valid if the Media Library Type is not set to V. 	Play Media Get Digits Menu	a is used for PlayMedia only

Parameter Name	Used For	Notes
<p>Data Playback Type options are as follows:</p> <ul style="list-style-type: none"> • Number • Char (Character) • Date • Etime (Elapsed time) • TOD (Time of Day) • 24TOD (24-hour Time of Day) • DOW (Day of Week) • Currency (USD only) 	Play Data	
<p>Media Library Type Flag indicates the location of the media files to be played. Options are as follows:</p> <ul style="list-style-type: none"> • A--(Default) Application • S--System • V--External VoiceXML 	Play Media Get Digits Menu	V is an option for PlayMedia only.
<p>Uniqueness value (optional) A string identifying a VRU Script Name as unique.</p>	Play Media Play Data Get Digits Menu	

Sample VRU Script Names

This VRU Script Name	Instructs Unified CVP
PM,July,S	To use the Play Media (PM) microapplication to play the "July.wav" Media file, using the System (S) Media library.
PM,WebSite,,1	To use the Play Media (PM) microapplication to play the "Website.wav" media file, using the default Media Type (Application library), and setting 1 as the Uniqueness value.
GD>Password,A,O	To use the Get Digits microapplication to play the media file named password.wav, using the Application (A) media library and setting 0 as the Uniqueness value.
M,Main_Menu	To use the Menu microapplication to play the media file named Main_Menu.wav.

Configuration Parameters

Configuration parameters have a “positional” sequence format-- the format parameter,parameter,parameter.

Use double commas (,,) to skip a parameter; Unified CVP supplies the default.

The Play Media position sequence is *Barge-in allowed,RTSP Timeout,Type-ahead Buffer Flush*.

The Play Data position sequence is *Location of files to be played,Barge-in allowed,Time Format,Type-ahead Buffer Flush*.

The Get Digits position sequence is *Minimum Field Length,Minimum Field Length,Barge-in allowed,Inter-digit Timeout,No Entry Timeout,Number of Invalid Tries,Timeout Message Override,Invalid Entry Message Override,Dtmf Termination Key,IncompleteTimeout*.

The Menu position sequence is *List of Menu Choices,Barge-in allowed,No Entry Timeout,Number of No Entry Tries,Number of Invalid Tries,Timeout Message Override,Invalid Entry Message Override*.

Parameter Name	Used For	Notes
<p>Barge-in Allowed Valid options are as follows:</p> <ul style="list-style-type: none"> • Y--Barge-in is allowed. <p>Note that DTMF barge-in is supported. Voice barge-in is not.</p> <ul style="list-style-type: none"> • N --(Default) Barge-in is not allowed 	Play Media Play Data Get Digits Menu	Unified CVP handles barge-in as follows: <ul style="list-style-type: none"> • If barge-in is not allowed, the SIP/H.323 Service/Gateway continues prompt play when a caller starts entering digits, and the entered digits are discarded. • If barge-in is allowed, the H.323Service/Gateway discontinues prompt play when the caller starts entering digits.
<p>DTMF Termination Key A single character that, when entered by the caller, indicates digit entry is complete. Valid options are as follows:</p> <ul style="list-style-type: none"> • 0 to 9 • * (asterisk) • # (pound sign, the default) • N (no termination key) 	Get Digits	
<p>Incomplete Timeout The amount of time after a caller stops speaking to generate an invalid entry error because the caller input does not match the defined grammar. The valid options are 0 to 99. The default is 3.</p>	Get Digits	V is an option for Play Media only.

Parameter Name	Used For	Notes
<p>Inter-digit Timeout The number of seconds the caller is allowed between entering digits. If exceeded, the system times out.</p> <p>The valid options are 1 to 99. The default is 3.</p>	Get Digits	
<p>Invalid Entry Message Override The valid options are:</p> <ul style="list-style-type: none"> • Y--Override the system default with a pre-recorded Application Media Library file • N-- (Default) Do not override the system default 	Get Digits Menu	
<p>List of Menu Choices Valid options are as follows:</p> <ul style="list-style-type: none"> • 0 to 9 • * (asterisk) • # (pound sign) 	Menu	<p>Formats allowed are:</p> <ul style="list-style-type: none"> • Individual options delimited by a / (forward slash) • Ranges delimited by a - (hyphen) with no space
<p>Location of the data to be played Valid options are as follows:</p> <ul style="list-style-type: none"> • Null--(Default) If you leave this option empty, the system uses the expanded call variable named user.microapp.play_data. • A number representing a Call Peripheral Variable number (for example, a 1 to represent Call.PeripheralVariable1). 	Play Data	
<p>Maximum Field Length Maximum number of digits entered by the caller. The valid options are 1 to 32. The default is 1.</p>	Get Digits	
<p>Minimum Field Length Minimum number of digits entered by the caller. The valid options are 1 to 32. The default is 1.</p>	Get Digits	
<p>No Entry Timeout The number of seconds a caller is allowed to begin entering digits. If exceeded, the system times out. The valid options are 0 to 99. The default is 5.</p>	Get Digits Menu	
<p>Number of Invalid Tries Unified CVP repeats the "Get digits" cycle when the caller enters invalid data. (Total includes the first cycle.) The valid options are 1 to 9. The default is 3.</p>	Get Digits Menu	

Parameter Name	Used For	Notes
Number of No Entry Tries Unified CVP repeats the "Get Digits" cycle when the caller does not enter any data after the prompt has been played. (Total includes the first cycle.) The valid options are 1 to 9. (The default is 3.)	Get Digits Menu	
RTSP Timeout Specifies the Real-time Streaming Protocol (RTSP) timeout—in seconds—when RTSP is used. The valid range is 0 to 43200 seconds. The default is 10 seconds. If the value is set to 0 or a timeout value is not provided, the stream will not end.	Play Media	
Time format Valid only for the time Data Playback types Etime, TOD, and 24TOD. The available formats are as follows: <ul style="list-style-type: none"> • Null--Leave this option empty for non-time formats • HHMM--Default for time formats • HHMMSS • HHMMAP--Includes a.m. or p.m.; valid only for TOD 	Play Data	
Timeout Message Override. The valid options are as follows: <ul style="list-style-type: none"> • Y--Override the system default with a pre-recorded Application Media Library file • N--(Default) Do not override the system default 	Get Digits Menu	

Parameter Name	Used For	Notes
<p>Type-ahead buffer flush The Cisco VoiceXML implementation includes a type-ahead buffer that holds DTMF digits collected from the caller. When the VoiceXML form-interpretation algorithm collects user DTMF input, it uses the digits from this buffer before waiting for further input. This parameter controls whether the type-ahead buffer is flushed after the prompt plays out. A False value (default) means that the type-ahead buffer is not flushed after the prompt plays out. If the prompt allows barge-in, the digit that barges in is not flushed. Valid options are as follows:</p> <ul style="list-style-type: none"> • Y—Flush the type-ahead buffer • N—(Default) Do not flush the type-ahead buffer 	Play Media Play Data	

Sample Configuration Values

This Configuration sequence	Instructs Unified CVP
(for a Menu microapplication) 0-2/9,,4,2,2	To accept numbers 0, 1, 2, and 9. , (Skipped parameter) To accept the default barge-insetting (Y). To set the no entry timeout value to 4 seconds. To allow 2 no entry tries. To allow 2 invalid tries. To accept all other defaults.
(for a Get Digits microapplication) GD,Password,A,O	To use the Get Digits micro-application to play the media file named password.wav, using the Application (A) media library and setting 0 as the Uniqueness value.
(for a Menu microapplication) M,Main_Menu	To use the Menu micro-application to play the media file named Main-Menu.wav.

File Transfers

Use the **File Transfers** page to transfer the VXML application files to VXML Servers. Upload the application files to the Administration and Data Server (AW) and deploy the application files on the VXML Server.

Click the file transfer record to view the details for that file transfer. On the details page, you can also download the job details file and the log file for a file transfer job.

Add Files to Server

This procedure explains how to upload files to the AW.

Procedure

- Step 1** In **Unified CCE Administration**, choose **Overview > Call Settings > IVR Settings > File Transfers**.
- Step 2** Click **New** to open the **New File Transfer** page.
- Step 3** Click **Add to Server** to open the **Upload File** pop-up.

Note You can upload one file at a time.

- Step 4** Click **Click to select** and select a zip file to upload.
- Step 5** Click **Upload**.

The file is uploaded to AW and listed under **Available Files in the Server**.

Note You can hover over a row and click the **x** icon to delete a file from the server.

Add and Maintain File Transfers

This procedure explains how to create a new file transfer job. For information on deleting file transfers, see [Delete Objects, on page 157](#).

Procedure

- Step 1** In **Unified CCE Administration**, choose **Overview > Call Settings > IVR Settings > File Transfers**.
- Step 2** Click **New** to open the **New File Transfer** page.
- Step 3** Select one or more sites for the file transfer.
- Step 4** Enter a description for the file transfer.
- Step 5** On the **Available Files in the Server** list, select the files that you want to transfer and click **Save**. This initiates the transfer of the selected files to VXML Server of the selected sites.
-

View Details for a File Transfer

On the **IVR Settings** page > **File Transfers** tab, click the file transfer record to view the details for that file transfer.

For details page fields' description, refer the following table:

Field	Description
State	Shows one of the following status options for the file transfer: <ul style="list-style-type: none"> • Queued: Indicates that the file transfer job has been queued and is processed after any file transfer jobs submitted ahead of it are completed. When multiple file transfer jobs are submitted, they are run in the order they are created. • Processing: Indicates that the file transfer is being processed. • Succeeded: Indicates that all operations in the file transfer were successful. • Partially Succeeded: Indicates that some operations were successful, and some were unsuccessful. • Failed: Indicates that all operations were unsuccessful. • Cancelled: Indicates that the file transfer job is cancelled when the preceding job is terminated due to unrecoverable error while this job was in the queued state.
Description	Displays the description of the file transfer.
Host	Displays hostname of the Administration and Data server where the file transfer was initiated and is stored.
Creation Time	Displays the date and time the file transfer was submitted.
Start Time	Displays the date and time the file transfer entered the processing state.
Total Time	Displays the total time taken for processing the file transfer to reach the current state.
Job Details	Click the download icon to open or download the file transfer job details file in .csv format.
Log File	Click the download icon to open or download the log file (in .txt format) for this file transfer job. If the job is in processing state, click the download icon to view the job progress. A log file is generated for each file transfer job. The log file contains detail of each operation that was run, and a summary indicating if the file transfer is completed successfully or had failures.

Bucket Intervals

Configure bucket intervals to report on how many calls are handled or abandoned during specific, incremental time slots. Each bucket interval has a maximum of nine configurable time slots, called *Upper Bounds*. Upper Bounds are ranges measured in seconds to segment and capture call-handling activity. You can run reports that show calls answered and calls abandoned for these intervals.

For example, if your goal is to have calls handled within 1 minute, you might set up Upper Bounds for intervals that show how many calls are handled in less than or more than 1 minute. Intervals might be for 30 seconds, 60 seconds, 80 seconds, 120 seconds, 150 seconds, 180 seconds, and 240 seconds. Using these intervals, you can see if calls are being answered within 1 minute or if callers are waiting longer. The intervals also give you insight into how long callers are willing to wait before abandoning a call. Perhaps many callers do not abandon a call until they have waited for two minutes. This might indicate that you can modify your goal.

You can associate bucket intervals with call types, skill groups, and precision queues.

The system automatically creates a built-in bucket interval, which you cannot edit or delete.

Add and Maintain Bucket Intervals

Procedure

Step 1 In **Unified CCE Administration**, navigate to **Overview > Call Settings > Bucket Intervals**.

Step 2 Click **New** to open the **New Bucket Interval** window.

Step 3 Complete the following fields:

Field	Required?	Description
Name	yes	Enter a name for the call type using a maximum of 32 characters.
Upper Bound 1	yes	Enter a value in the Upper Bound 1 field, using a number greater than 0 and less than 2147483647. This value is interpreted as seconds. For example, your entry of 10 in this field creates an Upper Bound 1 interval with a time slot of 0 to 10 seconds.
Upper Bound 2 - 9	no	<p>The value for each Upper Bound must be higher than the value of the previous Upper Bound. If you leave an Upper Bound field blank, all remaining fields must be blank.</p> <p>For example: To configure three intervals that span 10 seconds each and then have all other calls grouped into an interval that extends beyond your third defined interval, enter the following values:</p> <ul style="list-style-type: none"> • Upper Bound 1 interval: 10 This time slot is 0 to 10 seconds. Reports will show the total number of calls answered and calls abandoned from 0 to 10 seconds. • Upper Bound 2 interval: 20 This time slot is any time greater than 10 seconds and less than 20 seconds. Reports will show the total number of calls answered and calls abandoned between 10 and 20 seconds. • Upper Bound 3 interval: 30 This time slot is any time greater than 20 seconds and less than 30 seconds. Reports will show the total number of calls answered and calls abandoned between 20 and 30 seconds. • All other Upper Bound fields blank. Reports will show the total number of calls answered and calls abandoned after 30 seconds.

Step 4 Click **Save** to return to the List screen, where a message confirms the successful creation of the bucket interval.

Miscellaneous

Use this page to configure miscellaneous call settings. The **Unified CCE Administration > Call Settings > Miscellaneous** page has various tabs such as Global, Main Site, and the configured remote sites. Navigate to the required tab to configure the settings.



Note Packaged CCE 4000 Agents and 12000 Agents deployment contains the Global tab only.

Global

This tab contains the following sections:

- Congestion Control
- Agent
- Call Reporting
- Script

Congestion Control

You can review congestion control fields in this section. This section contains the following fields:

Field	Description
Congestion Control fields	<ul style="list-style-type: none"> • Treatment Mode This display-only field shows Treat call with DN default label. • System Default Label This display-only field is blank for Packaged CCE and Packaged CCE Lab Mode deployments. If your system was changed from another deployment type, this field retains the system default label for that deployment. • Maximum Calls Per Second This display-only field displays the current value for maximum calls per second for the deployment.

Agent

Enter values in this section to define system-level values for agents. This section contains the following fields:

Field	Required?	Description
Minimum Password Length	yes	Enter a value between 0 and 32 to set the minimum required length for passwords. Changing this value affects new passwords only and does not apply to existing ones.
Username Case Sensitivity	no	Check this check box to indicate that all usernames are case-sensitive. Leave it unchecked to indicate that case does not matter.

Call Reporting

Enter values in this section to define system-level values for calls. This section contains the following fields:

Field	Required?	Description
Bucket Interval	yes	<p>Click the magnifying glass icon to display the popup list of configured bucket intervals.</p> <p>Select a bucket interval to use as the system default. You can change the bucket interval for individual call types, skill groups, and precision queues. (See Call Type, on page 342, Skill Groups, on page 256, and Precision Queues, on page 261.)</p>
Call Type	yes	<p>Click the magnifying glass icon to display the popup list of configured call types.</p> <p>Select a call type to use as the system default. You can change the call type for individual Dialed Number, on page 327.</p>
Service Level Type	yes	<p>From the drop-down menu, select an option to configure the default method by which the system software calculates the service level type. You can change the service level type for individual call types and precision queues. You have the following service level options:</p> <ul style="list-style-type: none"> • Ignore Abandoned Calls: This selection excludes abandoned calls from the service level calculation. • Abandoned Calls have Negative Impact: Select this if you want only calls that are answered within the service level threshold time to be counted as treated calls. The service level is negatively affected by calls that abandon within the service level time. • Abandoned Calls have Positive Impact: Select this if you consider a call abandoned within the service level threshold time as a treated call. Abandoned calls have a positive impact on the service level.
Service Level Threshold	yes	<p>Enter a value in seconds, from 0 to 2,147,483,647, for the maximum time that a caller spends in a queue before being connected to an agent. This value is used in reports to identify the percentage of calls that are answered within that time threshold, enabling you to see whether agents are meeting the target goal. Set the value to 0 seconds if you do not want a service level threshold to be set for calls. The value here sets the system default for service level threshold. You can change the value for individual call types and precision queues. (See Call Type, on page 342 and Precision Queues, on page 261.)</p>
Abandon Call Wait Time	yes	<p>Enter a value in seconds (between 1 and 14400) to configure the minimum time an incoming call must be queued before the call is considered abandoned if the caller disconnects the call.</p>
Answered Short Call Threshold	no	<p>Enter a value in seconds (between 0 and 14400) to configure the maximum duration for a short call. Calls with a duration below that value are considered short. Set the threshold to factor out short calls from handle times.</p>

Field	Required?	Description
Reporting Interval	yes	From the drop-down menu, select 15 Minutes or 30 Minutes to configure the system to store historical information in 15-minute or half-hour summaries. The Unified CCE PG sends these records to the Logger, which in turn writes them to the Central Database. Note that the 15-minute interval requires a larger amount of database space than the 30-minute interval.

Script

Use this section to set the number of retained script versions.

Field	Description
Script Versions to Retain	Enter a value from 1 to 100 to define the maximum number of versions of each routing script you want to maintain in the database. When you select a number, the system automatically deletes the oldest version when the limit is exceeded.

Login Session

Main Site

This tab contains the following sections:

- Agent
- Labels

Agent

Enter values in this section to define system-level values for agents. This section contains the following fields:

Field	Required?	Description
Desk Settings	yes	Click the magnifying glass icon to display the popup list of configured desk settings. This list shows only global desk settings. The desk settings you select will be the system default for all agents. You can change the desk settings for individual agents. (See Add and Maintain Agents, on page 230.)
Agent Phone Line Control	yes	Select Single Line or All Lines to indicate whether all agents supported on the agent peripheral can have one or more than one line configured. Important <ul style="list-style-type: none"> • If you select All Lines, you must access Cisco Unified Communications Manager to set Busy Trigger to 1 and Max Number of Calls to 2 for each phone. Use the Unified Communications Manager Bulk Administration tool to change these settings for all agent devices. • If you change the Agent Phone Line Control setting, you must restart the peripheral gateways for the change to take effect. To restart the PGs, access the Unified CCE PG on Side A and Side B. Open Service Control and restart all PG services on Side A and Side B.

Labels

Use this section to view and edit labels for Unified CM, Outbound, and Unified CVP. This section contains the following fields:

Field	Description
Unified CM Label	This field contains a 10 digit string that matches the Unified CM route pattern.
Outbound Label	This field contains a 10 digit string that matches the IOS Voice Gateway dial-peer.
Unified CVP Label	<p>This field contains a 10 digit string that matches the CVP dialed number pattern.</p> <p>When this label is used for all Unified CVP routing clients, the Same Label for All Unified CVPs check box is checked.</p> <p>To use a different label for each Unified CVP routing client, uncheck the Same Label for All Unified CVPs check box, and enter a 10 digit string in each routing client field.</p>

Remote Sites

The miscellaneous settings vary based on the type of peripheral gateways configured for a particular remote site.

PGs Configured	Settings
Agent	Agents, Unified CM Label
VRU	Unified CVP Label
Multichannel	Outbound Label

If a remote site has all the PGs configured, the settings options are same as that of Main Site. If it has a combination of two PGs configured, the respective combination of settings appears.

Feature Setup

Manage Features

Packaged CCE webadmin provides the following optional features that you can configure anytime after your Packaged CCE system is installed, configured, and operational:

Courtesy Callback

To improve caller and workforce experience, Packaged CCE enables you to configure Courtesy Callback feature. The Courtesy Callback feature is available in Unified CVP.

With Courtesy Callback, the caller can choose to receive a callback from the contact center, rather than having to wait for an extended time on hold. Callers do not lose their place in the queue. The feature allows the system to offer callers who meet certain criteria, for example, callers with the possibility of being in the queue for more than X minutes, the option to be called back by the system when the wait time would be considerably shorter.

The system collects callback information from the caller, monitors the agent availability, and calls the customer when the agent is close to available. For example, 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.

To set up Courtesy Callback, you must configure Ingress Gateway, VXML Gateway, Call Studio, and CCE Scripts. For more information on the Courtesy Callback feature, see *Cisco Packaged Contact Center Enterprise Features Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html>.

Configure Courtesy Callback

Before you begin

A CVP Reporting Server is required for the Courtesy Callback feature. The Reporting Server must be installed before completing the following task. Download the self-signed certificate for CVP Reporting Server from the browser, and import the certificate to the AW machine. For instructions to install the CVP Reporting server and import the self-signed certificate to AW machine, see the *Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-installation-guides-list.html>.

Procedure

-
- Step 1** In **Unified CCE Administration**, choose **Overview > Features > Courtesy Callback**.
- Step 2** From the **Site** drop-down list, choose a site for which you want to configure the Courtesy Callback feature. By default, it is 'Main'.
- Step 3** From the **CVP Reporting Server** drop-down list, choose a Reporting Server to use for storing Courtesy Callback data.
- Note** The list includes all the Reporting Servers configured for the site.
- If you leave the selection blank by selecting '-', no Reporting Server is associated with the Courtesy Callback deployment.
- Step 4** In the **Dialed Number Configuration** section, complete the following:

Fields	Required?	Description
Maximum Callbacks per Dialed Number	Yes	<p>By default, the Unlimited option is selected, which is equivalent to an unlimited number of callbacks offered per calling number. The maximum value is 1000.</p> <p>To limit the number of calls, from the same calling number that are eligible to receive a callback:</p> <ol style="list-style-type: none"> Select the Limited option. Enter a positive number in the text field to allow Courtesy Callback to validate and allow the specified number of callbacks per calling number.
Allow unmatched Dialed Numbers	No	<p>Check the Allow unmatched Dialed Numbers check box to allow callbacks to the dialed numbers that are not available in the Allowed Dialed Number Patterns list.</p> <p>Note If no dialed numbers are present in the Allowed Dialed Number Patterns list, then Courtesy Callback does not allow any callbacks.</p>
Allowed Dialed Number Patterns	No	<p>The list of allowed dialed numbers to which callbacks can be sent. By default, the list includes preconfigured allowed dialed number patterns.</p> <p>To add a dialed number pattern:</p> <ol style="list-style-type: none"> Click the '+' icon and enter a dialed number pattern. <ul style="list-style-type: none"> Valid characters are alphanumeric, period (.), Exclamation (!), asterisk(*), greater than(>), and backslash (\). The field does not allow you to enter any invalid characters. Click Add. <p>To remove a dialed number pattern, click the 'x' icon associated with the number in the list.</p>

Fields	Required?	Description
Denied Dialed Number Patterns	No	<p>The list of denied dialed numbers to which callbacks are never sent.</p> <p>By default, the list includes preconfigured denied dialed number patterns.</p> <p>To add a dialed number pattern:</p> <ol style="list-style-type: none"> a. Click the '+' icon and enter a dialed number pattern. <ul style="list-style-type: none"> Valid characters are alphanumeric, period (.), Exclamation (!), asterisk(*), greater than(>), and backslash (\). The field does not allow you to enter any invalid characters. b. Click Add. <p>To remove a dialed number pattern, click the 'x' icon associated with the number in the list.</p> <p>Denied numbers take precedence over allowed numbers.</p> <ul style="list-style-type: none"> • Wildcarded DN patterns can contain "." and "X" in any position to match a single wildcard character. • Any of the wildcard characters in the set ">*" matches multiple characters but can only be used trailing values because they always match all remaining characters in the string. • The highest precedence of pattern matching is an exact match, followed by the most specific wildcard match. • When the number of characters match equally by wildcarded patterns in both the Allowed Dialed Numbers and Denied Dialed Numbers lists, precedence is given to the one in the Denied Dialed Numbers list.

Step 5 Click **Save**.

Context Service

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

Various components in the CCE Solution provide out of the box integration with Context Service. Context Service also provides an API for integration with your own applications or third-party applications to capture end-to-end customer-interaction data.

For more information about Context Service, see *Cisco Packaged Contact Center Enterprise Features Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html>

Register Cisco Customer Voice Portal (CVP), Cisco Finesse, SocialMiner and Enterprise Chat and Email with Context Service

From the Unified CCE Administration Context Service tool, you can register CVP, Finesse, SocialMiner and Enterprise Chat and Email with Context Service in order to store data about tasks from these applications. For SocialMiner, Context Service can store data about tasks from the Task Routing APIs.



Note If you are in a non-Packaged CCE deployment, or Packaged CCE 4000 Agents and 12000 Agents deployments, use the System Inventory to set the Principal AW to manage credentials for Context Service before registering.

When registering with Context Service:

- For Packaged CCE deployments, the Unified CCE AW must be able to reach Context Service.
- For non-Packaged CCE deployments, or Packaged CCE 4000 Agents and 12000 Agents deployments, the Principal AW that manages Context Service credentials must be able to reach Context Service.
- You are asked to provide administrator credentials for your organization.

In addition to registering:

- Add SocialMiner to the System Inventory in order to connect with Context Service.
- Enable the built-in POD.ID expanded call variable to send task context data through the system.

For Packaged CCE, use the Expanded Call Variable tool in Unified CCE Administration. For other deployments, use the Expanded Call Variable List tool in Configuration Manager.

Deregister CVP, Finesse, SocialMiner from Context Service

If you no longer want to use Context Service with CVP, Finesse, SocialMiner and Enterprise Chat and Email, you can deregister. You are asked to provide the administrator credentials that you used to register to Context Service.

Configure Context Service Settings

Use the Context Service tool in Unified CCE Administration to register Unified CVP, Finesse, SocialMiner and Enterprise Chat and Email to the Context Service.

For more information about Context Service registration, see <https://cisco.com/go/contextservice>.

Procedure

Step 1 In Unified CCE Administration, choose **Overview > Features > Context Service**.

Step 2 Complete the following parameters and click **Save**.

Field	Description
Proxy Server URL	Optional. If you are using a proxy server to connect to Context Service, enter the URL of the proxy server.

Field	Description
Timeout	The amount of time, in milliseconds, that the system waits for a response from Context Service before abandoning the attempt to perform the operation. Valid values are 200 to 15000 ms. Default is 1200 ms.
Lab Mode	Whether Context Service is in lab mode. Default is false (unchecked).

Step 3 To register with Context Service, click **Register**.

Step 4 After a successful registration, you can deregister from the Context Service by clicking **De-Register**.

What to do next

If you configured a proxy server for Context Service, configure the browser proxy with the proxy server URL you specified. Refer to your browser's documentation for information about configuring proxy settings.

Related Topics

[System Inventory for Packaged CCE Deployments](#)

Set up Single Sign-On

Before you begin

- Disable pop-up blockers. This is necessary to see all test results correctly.
- If you are using Internet Explorer, verify that it is not in Compatibility Mode and that you are using the AW's fully qualified domain name to access CCE Administration (for example, <https://fully-qualified-name.com/cceadmin>).

Procedure

Step 1 In **Unified CCE Administration**, choose **Features > Single Sign-On**.

Step 2 On the **Single Sign-On (SSO)** page, click the **Register** button to register all SSO-compatible components with the Cisco IdS.

The component status table displays the registration status of each component.

If a component fails to register, correct the error, and then click **Retry**.

Step 3 When registration has completed successfully, click the **Test** button. When the new browser tab opens, you may be prompted to accept a certificate. In order for the page to load, accept any certificates. Then, when prompted, log in as a user that has SSO credentials.

The test process verifies that each component has been configured correctly to reach the Identity Provider, and that the Cisco IdS successfully generates access tokens. Each component that you are setting up for SSO is tested.

The component status table displays the status of testing each component.

If a test is unsuccessful, correct the error, and then click Test again.

Test results are not saved. If you refresh the page, run the test again before enabling SSO.

Step 4 Select the SSO mode for the system from the **Set Mode** drop-down list:

- Non-SSO: This mode disables SSO for all agents and supervisors. They use existing Active Directory-based and local authentication.
- Hybrid: This mode allows you to enable agents and supervisors selectively for SSO.
- SSO: This mode enables SSO for all agents and supervisors.

The component status table displays the status of setting the SSO mode on each component.

If the SSO mode fails to be set on a component, correct the error, and then select the mode again.

If you add any SSO-compatible machines to the System Inventory after you register components with the Cisco IdS, those machines are registered automatically. If you have already set the SSO mode for the system, the SSO mode is set on those machines automatically.

Third-party Integration



Note To enable this feature in Packaged CCE 12.0(1), install the ICM12.0(1)_ES patch. For more information, see *Release Notes for Packaged Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html>.



Note Third-party gadgets can be added or modified only from a principal AW machine.

Third-party integration enables you to add user interfaces of third-party components your Contact Center employs in to Unified CCE Administration. You can add custom gadgets such as an agent reskilling gadget or third-party pages such as a browser-based CRM tool. Integrate the user-interfaces and administer multiple third-party components from Unified CCE Administration.

This feature also allows you to personalize the layout of Unified CCE Administration.

The system-defined cards in the layout have been placed in the order in which an administrator would typically use them. Menus with common or similar functionalities are grouped in a single card or menu. (For example, the User Setup card contains menus that allow you to manage agents, administrators, and assign permissions to user roles.)

You can add the third-party user interface to system-defined menu or card with a common or similar functionality. If the functionality does not match, add the third-party user interface to a user-defined menu or card. For more information on how to customize the layout, see [Customize the Unified CCE Administration Layout, on page 374](#).

Role-Based Access

Only system administrators can add, edit, or delete a third-party user interface and customize the Unified CCE Administration layout.

System administrators can assign access to a third-party user interface to custom roles. For information on how to assign access, see [Assign Access to Administrators, on page 372](#)

Manage Third-party Integration

Complete the following procedures to add, edit, search, and delete the third-party user interfaces.

Add Third-party User Interface

While adding a third-party user interface, you can define data that the third-party user interface can use while its rendered. Define the data as custom key-value pairs or choose from an array of system-defined data.

For example, define a custom key-value pair called "license-key" with a fixed value, which a third-party page can use to call an API from its own server. Select system-defined data such as "Current User" so that the user interface can call UnifiedConfig API.



Note You can access a UnifiedConfig API from the third-party user interface only if the role you are assigned with has the required permissions. For more information on Packaged CCE APIs and how to use them, see the *Cisco Packaged Contact Center Enterprise Developer Reference Guide*.

Complete the following procedure to add a third-party user interface to Unified CCE Administration.

Procedure




- Step 1** In Unified CCE Administration, choose **Overview > Features > Third-party Integration**.
- Step 2** On the **Manage Third-party Integration** tab, click **New**.
- Step 3** In the **General Tab** complete the following.

Field	Description
General Tab	
Integrate as Gadget	Select this check box if you are adding a custom gadget. Leave the check box unselected, if you are adding a third-party page.
URL	Enter the secure URL of the third-party user interface.
Name	Enter a unique name for the third-party user interface, using a maximum of 15 characters. There is no restriction on the special characters. Note Once the third-party user interface is added, you cannot change the name.
Description	Optional. Enter up to 255 characters to describe the third-party user interface. There is no restriction on the special characters.

Field	Description
System Defined Data	<p>Optional. Define data that the third-party user interface can use while its rendered. Click + and select from the following list.</p> <ul style="list-style-type: none"> • Deployment Type: The current deployment type. • Current User: The credentials of the logged on user. • Current Role: The role of the logged on user. • API-based URL: The base URL on to which the APIs are loaded. • Locale: The current locale setting.
User Defined Data	<p>Optional. Define custom key-value pairs you need to render the third-party user interface. To add a key-value pair:</p> <ol style="list-style-type: none"> a. Click +. b. Enter the name and value in the respective fields. <ul style="list-style-type: none"> Note The Value field is optional. You can only enter up to 1024 characters in the Value field. c. Optional. Hide the value you enter by selecting the Mask check box. d. Click ✓ to add. e. To add another parameter, click + again.


Step 4 To set the placement of the third-party user interface in the Unified CCE Administration layout, click the **Placement** tab.

To add to a new menu in a new card:

- a) Scroll using the < and > icons and select the **Add New Card** card.
- b) Click  to choose a color and icon for the card.
- c) Click  next to **Add Title** to enter the card title.
- d) Click **Save**. The new card is displayed in the list of cards.
- e) In the new card, click  to enter the menu name. Click ✓ to save.

Note You can only add up to eight cards.

To add to a new menu in a system-defined card:

- a) Scroll using the < and > icons to select a system-defined card.
- b) Click  to enter the menu name. Click ✓ to save.

Note You can only add up to seven menus in each card and in each menu up to five tabs.

To add to a system-defined menu in a system-defined card:

- a) Select the menu by clicking on it. The selected menu is highlighted in a red box.

Note You can only add up to seven menus in each card and in each menu up to five tabs.

Step 5 Click **Save**.

What to do next

[Assign Access to Administrators, on page 372](#)

Assign Access to Administrators

System administrators can assign access to the third-party user interface to custom roles. Complete the following procedure to assign access.

Procedure

Step 1 Go to **User Setup > Roles**.

Step 2 Select the custom role.

Step 3 Under **Third-party Integration**, select the check box that is named after the third-party user interface (for example, if the name of the third-party user interface is "CRM", **CCE Administration** creates a checkbox named "CRM") and click **Save**.

Access to the third-party user interface is assigned to the custom role.

Edit Third-party User Interface

Complete the following procedure to edit a third-party user interface.

Procedure

Step 1 In Unified CCE Administration, choose **Overview > Features > Third-party Integration**.

Step 2 From the list of pages, click the row of the page or gadget you want to edit.




Step 3 Edit the following fields.

Field	Description
General Tab	
Integrate as Gadget	Select this check box if you are adding a custom gadget. Leave the check box unselected, if you are adding a third-party page.
URL	Enter the secure URL of the third-party user interface.
Name	This field is not editable.
Description	Optional. Enter up to 255 characters to describe the third-party user interface. There is no restriction on the special characters.

Field	Description
System Defined Data	<p>Optional. Define data that the third-party user interface can use while its rendered. Click + and select from the following list.</p> <ul style="list-style-type: none"> • Deployment Type: The current deployment type. • Current User: The credentials of the logged on user. • Current Role: The role of the logged on user. • API-based URL: The base URL on to which the APIs are loaded. • Locale: The current locale setting. <p>For more information, see the <i>Cisco Packaged Contact Center Enterprise Developer Reference Guide</i></p>
User Defined Data	<p>Optional. Define custom key-value pairs you need to render the third-party user interface. To add a key-value pair:</p> <ol style="list-style-type: none"> a. Click +. b. Enter the name and value in the respective fields. <ul style="list-style-type: none"> Note The Value field is optional. You can only enter up to 1024 characters in the Value field. c. Optional. Hide the value you enter by selecting the Mask check box. d. Click ✓ to add. e. To add another parameter, click + again.


Step 4 To change the placement of the third-party user interface in the Unified CCE Administration layout, click the **Placement** tab.

To add to a new menu in a new card:

- a) Scroll using the < and > icons and select the **Add New Card** card.
- b) Click  to choose a color and icon for the card.
- c) Click  next to **Add Title** to enter the card title.
- d) Click **Save**. The new card is displayed in the list of cards.
- e) In the new card, click  to enter the menu name. Click ✓ to save.

Note You can only add up to eight cards.

To add to a new menu in a system-defined card:

- a) Scroll using the < and > icons to select a system-defined card.
- b) Click  to enter the menu name. Click ✓ to save.

Note You can only add up to seven menus in each card and in each menu up to five tabs.

To add to a system-defined menu in a system-defined card:

- a) Select the menu by clicking on it. The selected menu is highlighted in a red box.

Note You can only add up to seven menus in each card and in each menu up to five tabs.

Step 5 Click **Save**.

Sort and Search Third-party User Interface

Complete the following procedure to sort the list of third-party user interfaces and to search for specific user-interfaces.

Procedure

- Step 1** In **Unified CCE Administration**, choose **Overview > Features > Third-party Integration**.
- Step 2** On the **Manage Third-party Integration** tab, the **Name** and **Description** columns has an arrow icon in the column header. Click the arrow to sort in the ascending or descending order.
- Step 3** To search for a user-interface, enter the name or description of the page in the text box in the far left corner. As you type, user-interfaces that match your search term appear.
-

Delete Third-party User Interface

Complete the following procedure to delete a third-party user interface.

Procedure

- Step 1** In Unified CCE Administration, choose **Overview > Features > Third-party Integration > Manage Third-party Integration**.
- Step 2** Hover the mouse pointer over the row of that third-party user interface to see the **x** icon at the end of the row. Click the **x** icon and confirm your intention to delete. The third-party user interface is deleted from Packaged CCE.
-

Customize the Unified CCE Administration Layout

In Unified CCE Administration, choose **Overview > Features > Third-party Integration > Manage Layout**.

From the Manage Layout page you can:

- Add a third-party user interface to the menu you select or create.



Note The third-party user interface is always added as a new tab in the menu.

- Add up to eight new cards, and in each card up to seven menus, and in each menu up to five tabs. You can add up to 100 third-party user interfaces to Unified CCE Administration.



Note You cannot add a third-party user interface to the following menus: Inventory, Deployment Settings, and Device Configuration menus in the Infrastructure Settings card, Third-party Integration menu in the Features card, Email and Chat menu in the Email and Chat card, Resources menu in the Desktop Settings card.

- While creating a card, enter a title and choose the color and icon from a pre-defined list. For details, see [Manage User-Defined Cards](#) , on page 375
- Add, rename, and delete menus in system-defined cards. For details, see [Manage System-Defined Cards](#) , on page 376



Note Color, name, and title of system-defined cards are not customizable.

- Drag and drop the user-defined cards in the order in which you want them to appear in the Unified CCE Administration layout.

Manage User-Defined Cards

Complete the following procedure to add new cards and menus.



Procedure

Step 1 In Unified CCE Administration, choose **Overview > Features > Third-party Integration**. The **Manage Layout** page displays all the cards.

Step 2 To add a new card:





- Click the **Add New Card** card.

Note The **Add New Card** card is disabled after you have added eight cards.

- Click  to choose a color and icon for the card.
- Click  next to **Add Title** to enter the card title.
- Click **Save**.

The new card is displayed on the **Manage Layout** page.

Step 3 To edit a card, click on any of the following icons at the bottom right corner of the card.

- Click  to change the icon, color, or title of the card.
- Click  to add or edit a menu. To delete a menu, click .
- Click  to delete the card.

Note You cannot delete a card or menu if it contains a third-party user interface.



Note Your changes take effect on the **Overview** page after you log into **Unified CCE Administration** again.

Manage System-Defined Cards




You can add menus to system-defined cards. You can also rename or delete user-defined menus.

Procedure

Step 1 In Unified CCE Administration, choose **Overview > Features > Third-party Integration**. The **Manage Layout** page displays all the cards.



Step 2 To add a menu to the card:

Note You cannot add more than seven menus to a card.

- a) Click  at the bottom right corner of the card.
- b) In the **Manage Menus** page, click  next to **Add Menu**.
- c) In the text box that appears, enter the menu name.
- d) Click  to save the menu. Or click **x** to cancel.
- e) Click **Done**.

Step 3 To rename or delete a menu:

Note Only user-defined menus can be renamed or deleted.

- a) Click  to rename the menu or click  to delete.
 - b) Click **Done**.
-



Note Your changes take effect in the **Overview** page when you log into **Unified CCE Administration** again.

Email and Chat

Email and Chat

Enterprise Chat and Email (ECE) is an optional feature that provides email and chat functionality to the contact center. To configure ECE from Unified CCE Administration, you need to add ECE Web Server into the **Inventory** page as an external machine. For more information, see [Add External Machines, on page 127](#).

In **Unified CCE Administration**, choose **Overview > Email and Chat** to configure the email and chat functionality.

Configuration Tasks[Configure Email and Chat, on page 132](#)

Bulk Imports

Manage Bulk Jobs

Bulk jobs are a fast and efficient way to enter data at initial setup and to incorporate large-scale changes, such as changing agent skill groups between shifts and incorporating a new contact center with multiple new agents.

Changes to an individual record are made directly to that record, using the appropriate tool (Agent, Dialed Number, and so on).

Although bulk job content files create records explicitly, they also implicitly create related records, as follows:

- An agent bulk job content file contains cells for agent team, skill groups, and attributes. Entering content in those cells creates those objects if they do not exist.
- A dialed number bulk job content file contains cells for call type. Entering content in those cells creates those objects if they do not exist.



Important Run bulk jobs:

- Only during off-peak hours. Do not run bulk jobs during heavy call load.
- Only when the Sync Status is **In Sync** for all the devices.

Supervisors have no access to the Bulk Jobs tool.

Download Bulk Job Content File Template

Bulk jobs apply changes entered in content file templates. Content file templates are in .csv format.

The content file is syntactically validated before the bulk job is created. Database-related errors and conflicts are reported during execution of the job.



Note If you are using the Packaged CCE Lab deployment, you can download the Inventory content file. Use this file to enable the System Inventory and certain features, by providing machine information and credentials.

Procedure

-
- Step 1** Navigate to **Unified CCE Administration > Overview > Bulk Import** to open the **List of Bulk Jobs** page.
- Step 2** Click **Templates**.

The **Download Templates** popup window opens.

- Step 3** Click the **Download** icon for the template you want to use.
- Step 4** Click **OK** to close the **Download Templates** popup window.
- Step 5** Open the template in Microsoft Excel.
- Step 6** Populate the file.
- Step 7** Save the populated file locally.

Related Topics

[Inventory Content File](#) , on page 121

Content File Rules



Note The rules in this section do not apply to the SSO Migration content file.

For more information about using the SSO Migration content file, see the *Cisco Packaged Contact Center Enterprise Features Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html>.

Content File Create Operations

The content file spreadsheets follow these CREATE rules:

- All columns in the spreadsheet must be present, but the cells for optional fields can be left blank.
- Rows in the file are processed sequentially. It is possible for a content file to fail at any point (at any row), in which case objects up to but not including that row are added or updated.
If a row fails, all additions or updates before that row succeed, but all subsequent create and update operations fail.
- **Agent:** Creating an agent with the following cells populated implicitly creates the objects if they do not exist: agent team, skill group, attributes, supervisor team, and department.
- **Dialed number:** Creating a dialed number with the call type and department populated implicitly creates those objects, if they do not already exist.

Content File Update Operations

The Content file spreadsheets follow these UPDATE rules:

- Enter a value in a field to change the existing value.
- Leave a field blank to keep the existing value.
- Enter ~ in a field to clear the value in the existing value.

Bulk Agent Content File

The content file for the agent bulk job contains the fields detailed in the table below.



Note Ensure that the number of agent records do not exceed 1000.

Field	Required?	Description
operation	yes	Enter one of the following (case-insensitive): <ul style="list-style-type: none"> • CREATE • UPDATE
agentID	no	Enter a unique string of up to 11 digits. AgentID is automatically generated if you leave the field blank. In an UPDATE operation: <ul style="list-style-type: none"> • You cannot change agentID • If you leave the field blank, the userName must reference an existing agent
userName	yes	Enter up to 255 ASCII characters. The login name supports the use of all characters from 33 to 126 in the ASCII character set, except for the following: double quotation mark ("), forward slash (/), backward slash (\), square brackets ([]), colon (:), semicolon (;), pipe (), equal to (=), comma (,), plus sign (+), asterisk (*), question mark (?), angle brackets (< >), hash (#), percent (%), and SPACE. For supervisors and for agents with single sign-on (SSO) enabled, the username is the user's Active Directory or SSO account username. For supervisors who are not enabled for single sign-on (SSO), the Active Directory username must be in the user@domain format.
firstName	yes	Enter a maximum of 32 characters.
lastName	yes	Enter a maximum of 32 characters.
password	no	Enter a maximum of 256 ASCII characters. Password is case-sensitive. If SSO is enabled, the password is not saved. The default <i>Minimum Password Length</i> has been set in Call Settings > Miscellaneous (see Global, on page 360).
loginEnabled	no	Indicates whether the agent is able to log in to the agent desktop. If not specified, defaults to True.
ssoEnabled	no	Indicates whether single-sign on is supported at the agent level. This field takes effect only when the global level of SSO is mixed.
description	no	Enter up to 255 characters to describe the agent. If description is left blank during a CREATE operation, it is set to the ID of the bulk job performing the CREATE operation.

Field	Required?	Description
agentStateTrace	no	Indicates whether agent state trace is enabled for this agent. Defaults to False.
agentDeskSettingsName	no	Enter the desk settings associated with this agent. In a CREATE operation, your entry of agentDeskSettingsName generates an error when there is no desk settings with that name. Leaving this blank applies the System Default Desk Settings.
agentTeamName	no	Enter the team in which this agent is a member. In a CREATE operation, your entry of agentTeamName creates that team if it does not already exist. It appears in the List of Teams with the description BulkJob ID #####, where ##### is the number of the bulk job.
skillgroup(s)	no	Enter the skill groups with which this agent is associated, delimited by the ";" character. For example: sales;billing;support. In a CREATE operation, your entry of skillgroup creates that skill group if it does not already exist. It appears in the List of Skill Groups with the description BulkJob ID #####, where ##### is the number of the bulk job.
defaultSkillGroup	no	Enter the default skill group associated with this agent. If the field is specified, it must reference a skill group defined for the agent. In an UPDATE operation, an error is generated if the value is no longer one of the agent's skill groups.

Field	Required?	Description
attributes	no	<p>These fields are name = value pairs delimited by the ";" character, where = value is optional for existing attributes. For example, english=true;sales=7.</p> <p>Adding an attribute with a data type (Boolean or Proficiency) and a value (true or 9), either directly in the Attributes tool or with a bulk job, defines and protects the data type and establishes that value as the default.</p> <p>If an attribute does not yet exist in the Attributes tool, entering an attribute name without a value generates an error. For example if english is not yet an attribute, then english returns an error.</p> <p>You cannot change the data type, but you can change the value. If english was created as True, entering english retains the True value in a bulk update. You can also enter english=false, which sets the agent attribute value to False, leaving the attribute default value at True. You cannot enter english=10.</p> <p>To clear an agent's attribute value and reestablish the attribute default on a bulk update, just specify the attribute name, for example, english.</p> <p>In a CREATE operation, your entry of attribute creates that attribute if it does not already exist. It appears in the List of Attributes with the description BulkJob ID #####, where ##### is the number of the bulk job.</p>
supervisor	no	Indicates whether the agent is a supervisor. Defaults to False.
supervisorTeams	no	<p>Enter names of teams that will be supervised by this supervisor, delimited by the ";" character. For example: team1;team2;team3. Populating this field but leaving supervisorUserName blank generates an error.</p> <p>In a CREATE operation, your entry of supervisorTeams creates that team if it does not already exist. It appears in the List of Teams with the description Bulk Job ID: #####, showing the number of the bulk job.</p>
siteName	no	<p>The site name for this dialed number.</p> <p>If specified, the value must match an existing site name.</p> <p>If not specified, this field is set to default Main site.</p>
ecePerson	no	Indicates whether the agent is a ECE enabled. Defaults to False.
screenName	yes, if ecePerson is entered	
emailAddress	no	The email address of the ECE-enabled agent. Maximum length is 50 characters.

Field	Required?	Description
peripheralSetName	yes	<p>Note This field is available only for Packaged CCE 4000 agent and 12000 agent deployments.</p> <p>The peripheral set name for this agent.</p> <p>The value must match an existing peripheral set name configured for the site specified in the siteName column.</p> <p>In an UPDATE operation, you cannot change peripheralSetName.</p> <p>In a DELETE operation, you cannot delete peripheralSetName.</p>

Related Topics

[Content File Rules](#), on page 378

Bulk Dialed Number Content File for 2000 Agent Deployments

The content file for the dialed number bulk job contains these fields:

Field	Required?	Description
operation	yes	<p>Enter one of the following (case-insensitive):</p> <ul style="list-style-type: none"> • CREATE • UPDATE • DELETE
dialedNumberString	yes	<p>The dialedNumberString for this dialed number.</p> <p>Enter a string value that is unique for the routing type, maximum of 25 characters.</p> <p>Valid values are alphanumeric, +, and @.</p> <p>Note You cannot update dialedNumberString.</p>

Field	Required?	Description
routingType	yes	<p>The routing type for this dialed number. Values are 1 to 7.</p> <ul style="list-style-type: none"> • 1 (External Voice): Dialed number strings that apply to voice calls coming from Cisco Unified Customer Voice Portal (CVP). • 2 (Internal Voice): Dialed number strings that can be called from a Cisco Unified Communications Manager phone. • 3 (Outbound Voice): Dialed number strings that are used by the Cisco Outbound Option Dialer. • 4 (Multichannel 1). Requests that come from Enterprise Chat and Email, SocialMiner, or third party. • 5 (Multichannel 2). Requests that come from Enterprise Chat and Email, SocialMiner, or third party. • 6 (Multichannel 3). Requests that come from Enterprise Chat and Email, SocialMiner, or third party. • 7 (Post Call Survey). Post Call Survey dialed number strings that apply to voice calls coming from Cisco Unified Customer Voice Portal (CVP). <p>Multichannel routing types are available only if you have configured the peripherals for Enterprise Chat and Email, SocialMiner, and/or Third Party Multichannel using Peripheral Gateway Setup tool, and added external multichannel machines to the System Inventory.</p> <p>The order in which peripherals for these machines appear on the Peripheral Gateways tab (Overview > Infrastructure Settings > Peripheral Gateways), determines the routingType number (4, 5, or 6) for the machine. For example, if SocialMiner peripheral appears first on the tab, it is routingType 4.</p> <p>See the <i>Cisco Packaged Contact Center Enterprise Features Guide</i> at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html for information about configuring the peripherals using Peripheral Gateway Setup.</p>
description	no	<p>The description for this dialedNumberString. Enter a maximum of 255 characters. If the description field is left blank in a CREATE operation, it is set to the ID of the bulk job performing the CREATE operation.</p>

Field	Required?	Description
callTypeName	no	<p>Enter a name for the call type using a maximum of 32 characters. Valid characters are period(.), underscore (_), and alphanumeric. The first character must be alphanumeric.</p> <p>In a CREATE operation, your entry of callTypeName creates that call type if it does not already exist. It appears in the List of Call Types with the description BulkJob ID ####, where #### is the number of the bulk job.</p>
mediaRoutingDomainName	yes, for routingType 4, 5, and 6	<p>Optional for routingTypes 1, 2, and 3. If supplied, must be Cisco_Voice.</p> <p>Required for routingTypes 4, 5, and 6. The value must be Cisco_Voice or match an existing Media Routing Domain name.</p>
departmentName	no	<p>The department for this dialed number.</p> <p>A global administrator's entry of department creates that department if it does not already exist. It appears in the List of Departments with the description BulkJob ID ####, where #### is the number of the bulk job.</p> <p>If the department already exists, then that department can be entered by a global administrator or by an administrator who administers that department.</p>
siteName	no	<p>The site name for this dialed number.</p> <p>If specified, the value must match an existing site name.</p> <p>If not specified, this field is set to default Main site.</p>
ringtoneMediaFileName	no	<p>Note Use this field when the routing type is External Voice.</p> <p>Enter the custom ringtone filename. Enter a maximum of 255 characters without any spaces.</p>
pcsEnabledDialedNumberPatterns	no	<p>Note Use this field when the routing type is Post Call Survey.</p> <p>Enter Post Call Survey dialed number in the dialedNumberString field.</p> <p>Enter one or more dialed number patterns of routing type External Voice. Enter maximum of 512 characters. You can have a space-separated list of dialed numbers.</p>

Related Topics

[Content File Rules](#), on page 378

[System Inventory for Packaged CCE 2000 Agents Deployment](#), on page 9

Bulk Dialed Number Content File for 4000 and 12000 Agent Deployments

The content file for the dialed number bulk job contains these fields:

Field	Required?	Description
operation	yes	Enter one of the following (case-insensitive): <ul style="list-style-type: none">• CREATE• UPDATE• DELETE
dialedNumberString	yes	The dialedNumberString for this dialed number. Enter a string value that is unique for the routing type, maximum of 25 characters. Valid values are alphanumeric, +, and @. Note You cannot update dialedNumberString.

Field	Required?	Description
routingType	yes	<p>The routing type for this dialed number. Values are 1 to 7.</p> <ul style="list-style-type: none"> • 1 (External Voice): Dialed number strings that apply to voice calls coming from Cisco Unified Customer Voice Portal (CVP). • 2 (Internal Voice): Dialed number strings that can be called from a Cisco Unified Communications Manager phone. • 3 (Outbound Voice): Dialed number strings that are used by the Cisco Outbound Option Dialer. • 4 (Multichannel 1). Requests that come from Enterprise Chat and Email, SocialMiner, or third party. • 5 (Multichannel 2). Requests that come from Enterprise Chat and Email, SocialMiner, or third party. • 6 (Multichannel 3). Requests that come from Enterprise Chat and Email, SocialMiner, or third party. • 7 (Post Call Survey). Post Call Survey dialed number strings that apply to voice calls coming from Cisco Unified Customer Voice Portal (CVP). <p>Multichannel routing types are available only if you have configured the peripherals for Enterprise Chat and Email, SocialMiner, and/or Third Party Multichannel using Peripheral Gateway Setup tool, and added external multichannel machines to the System Inventory.</p> <p>To determine the routingType number (4, 5, or 6) for each peripheral, see the chapter <i>Routing Type API</i> in the <i>Cisco Packaged Contact Center Enterprise Developer Reference</i> at https://d1nmyq4gcgsfi5.cloudfront.net/site/packaged-contact-center/documentation/.</p> <p>See the <i>Cisco Packaged Contact Center Enterprise Features Guide</i> at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html for information about configuring the peripherals using Peripheral Gateway Setup.</p>
description	no	<p>The description for this dialedNumberString. Enter a maximum of 255 characters. If the description field is left blank in a CREATE operation, it is set to the ID of the bulk job performing the CREATE operation.</p>

Field	Required?	Description
callTypeName	no	<p>Enter a name for the call type using a maximum of 32 characters. Valid characters are period(.), underscore (_), and alphanumeric. The first character must be alphanumeric.</p> <p>In a CREATE operation, your entry of callTypeName creates that call type if it does not already exist. It appears in the List of Call Types with the description BulkJob ID #####, where ##### is the number of the bulk job.</p>
mediaRoutingDomainName	yes, for routingType 4, 5, and 6	<p>Optional for routingTypes 1, 2, and 3. If supplied, must be Cisco_Voice.</p> <p>Required for routingTypes 4, 5, and 6. The value must be Cisco_Voice or match an existing Media Routing Domain name.</p>
departmentName	no	<p>The department for this dialed number.</p> <p>A global administrator's entry of department creates that department if it does not already exist. It appears in the List of Departments with the description BulkJob ID #####, where ##### is the number of the bulk job.</p> <p>If the department already exists, then that department can be entered by a global administrator or by an administrator who administers that department.</p>
siteName	no	<p>The site name for this dialed number.</p> <p>If specified, the value must match an existing site name.</p> <p>If not specified, this field is set to default Main site.</p>
ringtoneMediaFileName	no	<p>Note Use this field when the routing type is External Voice.</p> <p>Enter the custom ringtone filename. Enter a maximum of 255 characters without any spaces.</p>
pcsEnabledDialedNumberPatterns	no	<p>Note Use this field when the routing type is Post Call Survey.</p> <p>Enter Post Call Survey dialed number in the dialedNumberString field.</p> <p>Enter one or more dialed number patterns of routing type External Voice. Enter maximum of 512 characters. You can have a space-separated list of dialed numbers.</p>

Field	Required?	Description
peripheralSetName	yes	<p>The peripheral set name for this dialed number.</p> <p>The value must match an existing peripheral set name configured for the site specified in the siteName column.</p> <p>In an UPDATE operation, you cannot change peripheralSetName.</p> <p>In a DELETE operation, you cannot delete peripheralSetName.</p>

Bulk Call Type Content File

The content file for the call type bulk job contains these fields:

Field	Required?	Description
operation	yes	<p>Enter one of the following (case-insensitive):</p> <ul style="list-style-type: none"> • CREATE • UPDATE • DELETE
name	yes	<p>Enter a name for the call type using a maximum of 32 characters. Valid characters are period(.), underscore (_), and alphanumeric. The first character must be alphanumeric.</p>
description	no	<p>The description for this call type. Enter a maximum of 255 characters. There is no restriction on characters. If the description field is left blank in a CREATE operation, it is set to the ID of the bulk job performing the CREATE operation.</p>
serviceLevelThreshold	no	<p>Maximum time in seconds that a caller should wait before being connected with an agent.</p> <p>Enter a value in seconds, using positive 32-bit integers only.</p>
serviceLevelType	no	<p>Indicates how the system calculates the service level:</p> <ul style="list-style-type: none"> • 1 = Ignore Abandoned Calls • 2 = Abandoned Calls have Negative Impact • 3= Abandoned Calls have Positive Impact <p>If not specified, this field is set to the system default.</p>
bucketIntervalName	no	<p>Identifier of the bucket interval, used for reporting.</p> <p>If specified, the value must match an existing bucket interval.</p> <p>If not specified, this field is set to the system default.</p>

Field	Required?	Description
departmentName	no	<p>The department for this call type.</p> <p>A global administrator's entry of department creates that department if it does not already exist. It appears in the List of Departments with the description BulkJob ID #####, where ##### is the number of the bulk job.</p> <p>If the department already exists, then that department can be entered by a global administrator or by an administrator who administers that department.</p>

Related Topics

[Content File Rules](#), on page 378

Bulk Skill Group Content File

The content file for the skill group bulk job contains these fields:

Field	Required?	Description
operation	yes	<p>Enter one of the following (case-insensitive):</p> <ul style="list-style-type: none"> • CREATE • UPDATE • DELETE
name	yes	<p>Enter a name for the skill group using a maximum of 32 characters. Valid characters are period(.), underscore (_), and alphanumeric. The first character must be alphanumeric.</p>
description	no	<p>The description for this skill group. Enter a maximum of 255 characters. There is no restriction on characters. If the description field is left blank in a CREATE operation, it is set to the ID of the bulk job performing the CREATE operation.</p>
serviceLevelThreshold	no	<p>Maximum time in seconds that a caller should wait before being connected with an agent.</p> <p>Enter a value in seconds, using positive 32-bit integers only.</p>
serviceLevelType	no	<p>Indicates how the system calculates the service level:</p> <ul style="list-style-type: none"> • 1 = Ignore Abandoned Calls • 2 = Abandoned Calls have Negative Impact • 3= Abandoned Calls have Positive Impact <p>If not specified, this field is set to the system default.</p>

Field	Required?	Description
bucketIntervalName	no	Identifier of the bucket interval, used for reporting. If specified, the value must match an existing bucket interval. If not specified, this field is set to the system default.
mediaRoutingDomainName	no	Enter a name for the Media Routing Domain using a maximum of 32 characters. Valid characters are period(.), underscore (_), and alphanumeric. The first character must be alphanumeric. If specified, the value must match an existing Media Routing Domain name. If not specified, this field is set to Cisco_Voice. You cannot change the mediaRoutingDomainName in an UPDATE operation. You must either leave this field blank or enter the existing mediaRoutingDomainName value.
departmentName	no	The department for this skill group. A global administrator's entry of department creates that department if it does not already exist. It appears in the List of Departments with the description BulkJob ID ####, where #### is the number of the bulk job. If the department already exists, then that department can be entered by a global administrator or by an administrator who administers that department.
siteName	no	The site name for this dialed number. If specified, the value must match an existing site name. If not specified, this field is set to default Main site.
peripheralSetName	yes	Note This field is available only for Packaged CCE 4000 agent and 12000 agent deployments. The peripheral set name for this skill group. The value must match an existing peripheral set name configured for the site specified in the siteName column. In an UPDATE operation, you cannot change peripheralSetName. In a DELETE operation, you cannot delete peripheralSetName.

Related Topics

[Content File Rules](#), on page 378

Add and Maintain Bulk Jobs

Procedure

-
- Step 1** Navigate to the **Unified CCE Administration > Overview > Bulk Import** to maintain (Add, Review, and Delete) bulk jobs.
- Step 2** Click **New** to open the **New Bulk Job** window.
- Step 3** In the optional **Description** fields, enter up to 255 characters to describe the bulk job. See [Character Sets, on page 601](#).
- Step 4** In the required **Content File** field, browse to the content file you have completed for this bulk job. The content file is validated before the bulk job is created.
- Step 5** Click **Save**.
-

Review Bulk Job Details

To review the details for a bulk job, click the bulk job row on the **List of Bulk Jobs** page. Fields on the page are display-only.

Field	Description
ID, Description, and Type	Show the ID, description entered and type of bulk job selected when the bulk job was created.
State	Shows one of: <ul style="list-style-type: none"> • Queued: The bulk job has been queued and will process when any jobs submitted ahead of it have completed. When multiple bulk jobs are submitted, they are run in the order they are created. • Processing: The bulk job is being processed. To view the progress, click Log File Download to monitor the log file. • Succeeded: All operations in the bulk job were successful. • Partially Succeeded: Some operations were successful, and some were unsuccessful. • Failed: All operations were unsuccessful. • Cancelled: A bulk job is canceled when the preceding bulk job is terminated due to unrecoverable error while this job was in the queued state.

Field	Description
Host	The hostname of the AW server where the bulk job was initiated and will be stored. When deleted, bulk job content files and log files will be deleted from this host.
Created	The time the bulk job was submitted.
Started	The time the bulk job entered the processing state.
Finished	The time the bulk job completed or failed (left the processing state).
Total Time	The time the bulk job spent in the processing state. This is calculated as Finished - Started.
Content File	Click Download to open the Content .csv file that was submitted for this bulk job. You must authenticate to open or save this file. If your deployment includes two AW hosts, this button is disabled if the bulk job was created using Unified Web Administration on a host that is different from the host on which the job is being viewed.
Log File	<p>Click Download to open the log file for this bulk job. If the job is still processing, click Download again to the review updates the job progresses. You must authenticate to open or save this file. If your deployment includes two AW server hosts, this button is disabled if the bulk job was created using Unified CCE Administration on a host that is different from the host on which the job is being viewed.</p> <p>A log file is generated for each bulk job. The log file is retained until the bulk job is deleted and contains detail of each operation that was run, as well as a summary indicating if the bulk job completed successfully or had failures.</p>

Capacity

Capacity Info

In **Unified CCE Administration**, click **Capacity** in the left navigation menu to see a table that provides following system capacity information:

Column	Description
Status	The status column shows where your system stands with respect to the capacity limit. The status icons are: <ul style="list-style-type: none">• Green for 0-75% of capacity.• Yellow for 76-95%.• Orange for 96-99%.• Red for when you are at 100%.
Number of Configured	Shows the name of the object.
At Most	Shows the maximum capacity of each configurable object that is allowed.
Actual	Shows the number of objects currently configured on your system.
% Used	Shows the percentage of the maximum capacity represented by your configuration.



PART I

Using Configuration Manager

- [Configuration Manager, on page 397](#)



CHAPTER 4

Configuration Manager

You perform most Packaged CCE configuration with the Unified CCE Administration gadgets. Limited configuration is performed in the legacy Configuration Manager toolset. This section describes the tools in Configuration Manager and explains how and why to access them for Packaged CCE.

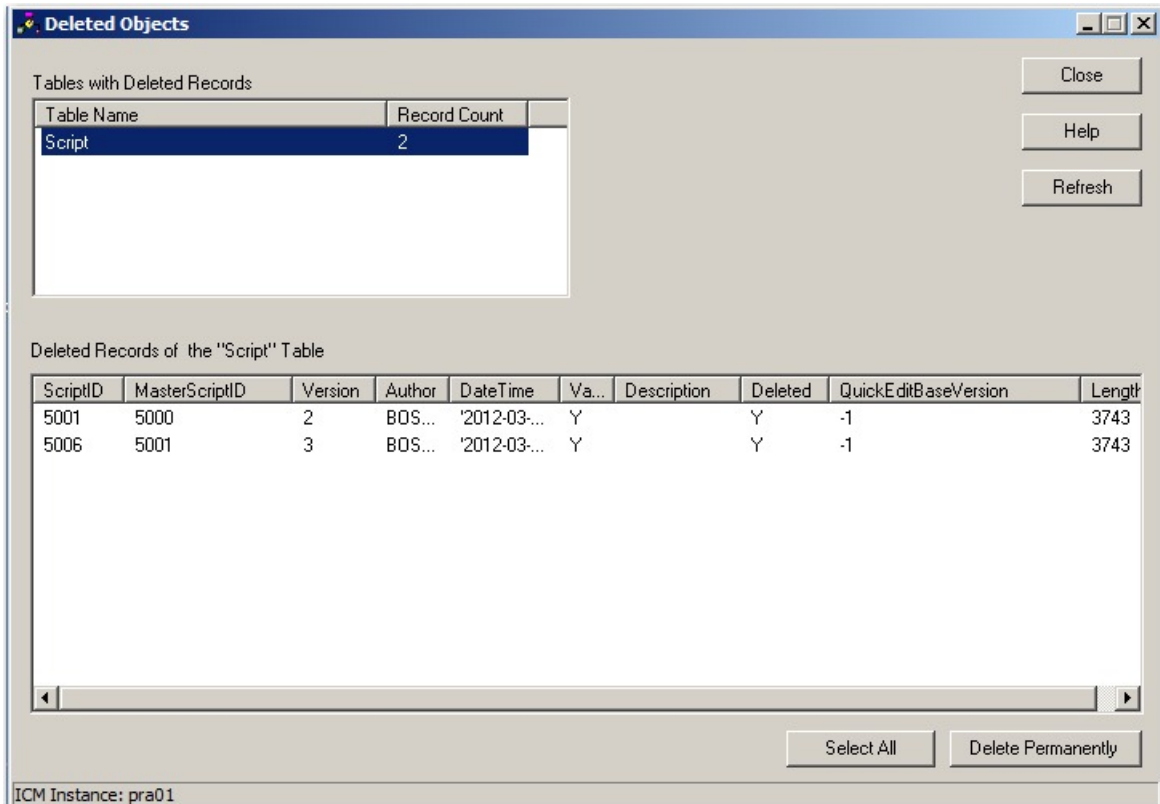
- [Permanent Deletion, on page 397](#)
- [Packaged CCE 4000 and 12000 Agent Supported Tools, on page 398](#)
- [Packaged CCE 2000 Supported Tools, on page 402](#)

Permanent Deletion

Some objects are “marked for deletion” only in Unified CCE Administration. They remain in the system for reporting and record-keeping purposes. Follow this procedure to delete them permanently:

Procedure

- Step 1** Open Configuration Manager.
 - Step 2** Select **Tools > Miscellaneous Tools > Deleted Objects**.
 - Step 3** Click the table name for the object you want to delete. This action opens a panel showing all records for that table that have been marked for deletion.
 - Step 4** Select one, several, or all records.
 - Step 5** Click **Delete Permanently**.
-

Example


The screenshot shows a window titled "Deleted Objects" with the following content:

Tables with Deleted Records

Table Name	Record Count
Script	2

Deleted Records of the "Script" Table

ScriptID	MasterScriptID	Version	Author	DateTime	Va...	Description	Deleted	QuickEditBaseVersion	Length
5001	5000	2	BOS...	'2012-03-...	Y		Y	-1	3743
5006	5001	3	BOS...	'2012-03-...	Y		Y	-1	3743

ICM Instance: pra01

Packaged CCE 4000 and 12000 Agent Supported Tools

You can perform some of the configurations for Packaged CCE 4000 and 12000 Agent deployments using the Configuration Manager tool. For information on how to use the tools, see the online help provided in each tool.



Note Only Packaged CCE configuration users who have been added to the `UcceConfig` group in all the local distributors can access the Configuration Manager. For details on how to add users to a local security group, see [Add Users to Local Security Group, on page 146](#)

Following is the list of tools that are supported in the Configuration Manager.



Note To enable the following configuration tools, navigate to **Unified CCE Administration > User setup > Roles** page and then select the required permissions.

Tools	List
Explorer Tools	<ul style="list-style-type: none"> • Agent Explorer • Announcement Explorer • Database Lookup Explorer • ICM Instance Explorer • Network VRU Explorer • Network Trunk Group Explorer • NIC Explorer • PG Explorer • Region Explorer • Service Explorer • Skill Group Explorer • Translation Route Explorer
List Tools	<ul style="list-style-type: none"> • Agent Desk Settings List • Agent Targeting Rule • Application Gateway List • Agent Instance List • Application Path List • Dialed Number/Script Selector List • Enterprise Service List • Enterprise Skill Group List • Expanded Call Variable Payload List • Label List • Media Class List • Media Routing Domain List • Person List • User Variable List

Tools	List
Bulk Tools	Bulk Insert Tools <ul style="list-style-type: none"> • Agent Bulk Insert • Dialed Number Bulk Insert • Label Bulk Insert • Network Trunk Group Bulk Insert • Peripheral Bulk Insert • Person Bulk Insert • Route Bulk Insert • Trunk Bulk Insert • Trunk Group Bulk Insert • Service Bulk Insert • Skill Group Bulk Insert Bulk Edit Tools <ul style="list-style-type: none"> • Agent Bulk Edit • Dialed Number Bulk Edit • Label Bulk Edit • Network Trunk Group Bulk Edit • Peripheral Bulk Edit • Person Bulk Edit • Route Bulk Edit • Trunk Bulk Edit • Trunk Group Bulk Edit • Service Bulk Edit • Skill Group Bulk Edit

Reenable Association for Existing Custom Roles

If you are upgrading to PCCE 12.0(1) ES26 , you must reenable the association for the existing custom roles post upgrade. This table explains how to reenable the association in each tool.

Table 29: Reenable Association for Existing Custom Roles

Configuration Manager Tool	To reenable the association
Agent Explorer	<ol style="list-style-type: none"> 1. Go to Unified CCE Administration > User Setup > Roles > Agent. 2. Unselect the Manage Agent checkbox and then click Save. 3. Select the Manage Agent checkbox and then click Save.
Person List	<ol style="list-style-type: none"> 1. Go to Unified CCE Administration > User Setup > Roles > Agent. 2. Unselect the Manage Agent Attributes checkbox and then click Save. 3. Select the Manage Agent Attributes checkbox and then click Save.
Dialed Number/Script Selector List	<ol style="list-style-type: none"> 1. Go to Unified CCE Administration > User Setup > Roles > Call Settings. 2. Unselect the Dialed Number checkbox and then click Save. 3. Select the Dialed Number checkbox and then click Save.
Skill Group Explorer	<ol style="list-style-type: none"> 1. Go to Unified CCE Administration > User Setup > Roles > Organization. 2. Unselect the Skill Groups checkbox and then click Save. 3. Select the Skill Groups checkbox and then click Save.
Application Gateway List	<ol style="list-style-type: none"> 1. Go to Unified CCE Administration > User Setup > Roles > Infrastructure. 2. Unselect the Application Gateway checkbox and then click Save. 3. Select the Application Gateway checkbox and then click Save.

Configuration Manager Tool	To reenable the association
Expanded Call Variables Payload List	<ol style="list-style-type: none"> 1. Go to Unified CCE Administration > User Setup > Roles > Call Settings. 2. Unselect the Expanded Call Variables checkbox and then click Save. 3. Select the Expanded Call Variables checkbox and then click Save.
Agent Desk Settings Tool	<ol style="list-style-type: none"> 1. Go to Unified CCE Administration > User Setup > Roles > Desktop Settings. 2. Unselect the Desk Settings checkbox and then click Save. 3. Select the Desk Settings checkbox and then click Save.
Bulk Configuration Tools	<ol style="list-style-type: none"> 1. Go to Unified CCE Administration > User Setup > Roles. 2. Unselect the Bulk Import checkbox and then click Save. 3. Select the Bulk Import checkbox and then click Save.

For information on restrictions that apply to Configuration Manager tools while configuring Avaya or ICM-to-ICM Gateway, see the *Cisco Packaged Contact Center Enterprise Features Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html>.

Related Topics

[Avaya Configurations](#), on page 145

[ICM-to-ICM Gateway Configurations](#), on page 148

Packaged CCE 2000 Supported Tools

You can perform some of the configurations for Packaged CCE 2000 Agents deployment using the Configuration Manager tool.

Following is the list of tools that are supported in the Configuration Manager.

Tools	List
Explorer Tools	<ul style="list-style-type: none"> • Region Explorer

Tools	List
List Tools	<ul style="list-style-type: none"> • Agent Targeting Rule • Applications Instance List • Application Path List • Media Class List • Media Routing Domain List • User Variable List
Miscellaneous Tools	<ul style="list-style-type: none"> • Deleted Objects • Region Editor
Outbound Option	<ul style="list-style-type: none"> • Campaign • Dialer • Import Rule • Query Rule • System Option

For more information on the tools, see the *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html>.



PART II

Routing and Scripting

- [Script Editor and Internet Script Editor, on page 407](#)
- [Common Tasks, on page 411](#)
- [Call Types, Contact Data, and Scripting, on page 421](#)
- [Contact Categorization, on page 425](#)
- [Routing Target Selection, on page 441](#)
- [Network VRUs, on page 455](#)
- [Multichannel Routing, on page 469](#)
- [Use of Formulas, on page 487](#)
- [Scripting Specifics in a Packaged CCE Environment, on page 505](#)
- [Utility Nodes, on page 511](#)
- [Unified CVP Scripting, on page 515](#)
- [Outbound Option Scripting, on page 575](#)



CHAPTER 5

Script Editor and Internet Script Editor

- [Script Editor and Internet Script Editor](#), on page 407
- [Administrator Privileges in Internet Script Editor](#), on page 407
- [Install Internet Script Editor](#), on page 408
- [Start Internet Script Editor](#), on page 408
- [Upgrade Internet Script Editor](#), on page 409

Script Editor and Internet Script Editor

In a Packaged CCE deployment, two tools are available for creating routing and administration scripts—Script Editor and Internet Script Editor. You can use either or both of these two tools. They provide the same functionality, and that functionality is documented in this section. This table lists some considerations:

Script Editor	Internet Script Editor
Is automatically deployed as part of the Unified CCE AW-HDS or AW-HDS-DDS installation.	Must be enabled during the installation of the Unified CCE AW-HDS or AW-HDS-DDS Server by selecting it in Web Setup, then downloaded and installed.
Requires a full Administration and Data server. You must run it from the Unified CCE AW-HDS or AW-HDS-DDS Server, based on your deployment.	Can be run on a local machine.
Can be used by global administrators.	Can be used by global administrators and departmental administrators.
Imposes no scripting access restrictions for global administrators.	Imposes scripting access restrictions for departmental administrators.

Administrator Privileges in Internet Script Editor

In a Packaged CCE deployment, global administrators and departmental administrators have different access permissions in Internet Script Editor.

Global administrators have access as follows:

- Full access to scripts and can reference all global and all departments objects when they create scripts.

- Full access to dynamic scripting nodes.

Departmental administrators have access as follows:

- Full access to scripts that reference global objects and objects in their departments.
- Read-only access to scripts that reference Dynamic Scripting Nodes such as formulas.
- No access to scripts that reference objects that are associated with departments they do not administer.

Install Internet Script Editor

You cannot install Internet Script Editor directly on a VM.

For Packaged CCE, this means that you cannot install Internet Script Editor on the Unified CCE AW-HDS-DDS or on an external HDS.

Procedure

- Step 1** Point your browser to `server-name/install/iscripteditor.htm`, where *server-name* is the name of the computer on which you installed the distributor with the Internet Script Editor client package.
- Step 2** Click **Download Internet Script Editor**.
- Note** You can also open the `iscripteditor.exe` file directly from the web page.
- Step 3** Navigate to the directory where you want to save `iscripteditor.exe`.
- Step 4** Click **Save** to begin the download.
- Step 5** After the download is complete, close the browser.
- Step 6** On your desktop, navigate to `iscripteditor.exe` and run the file.
- Step 7** When the InstallShield Wizard for Internet Script Editor starts, click **Next** to continue.
- Step 8** Select the default Destination Folder by clicking **Next**; or click **Browse** to navigate to the desired Destination Folder, and then click **Next**.
- Step 9** After the InstallShield Wizard indicates that the installation is complete, click **Finish**.
-

A shortcut for Internet Script Editor (IScriptEditor) appears on the desktop, and in the Start menu in the `Programs/Cisco Systems Inc.` program group.

Start Internet Script Editor

Procedure

- Step 1** Double-click the desktop shortcut for Internet Script Editor (IScriptEditor).
- Step 2** Click **Connection**.

- Step 3** Enter the correct **Address**, **Port**, and **ICM Instance** information.
 - Step 4** Click **OK**.
 - Step 5** Enter your **User Name** and **Password**. Be sure to use a Security Account Manager (SAM) username, as the name must not exceed 20 characters in length.
 - Step 6** Enter the **Domain** of Unified ICM system.
 - Step 7** Click **OK**.
 - Step 8** Upgrade Internet Script Editor as necessary.
-

Upgrade Internet Script Editor

After you start Internet Script Editor, if there is a newer version, you receive a message informing you that you can upgrade Internet Script Editor.



Note Some upgrades are optional; these upgrades typically contain GUI enhancements. Other upgrades, typically involving protocol or database changes, are mandatory. You cannot use Internet Script Editor until you accept mandatory upgrades.

Procedure

- Step 1** Accept a software upgrade.
A web page opens from which you can download the new Internet Script Editor.
 - Step 2** Click **Download Internet Script Editor**.
 - Note** You cannot use Internet Script Editor during the upgrade.
You can also open the `iscripteditor.exe` file directly from the web page.
 - Step 3** Navigate to the directory where you want to save `iscripteditor.exe`.
 - Step 4** Click **Save** to begin the download.
 - Step 5** After the download is complete, close the browser.
 - Step 6** On your desktop, navigate to `iscripteditor.exe` and run the file.
 - Step 7** When the InstallShield Wizard for Internet Script Editor starts, click **Next** to continue.
 - Step 8** Select the default Destination Folder by clicking **Next**; or click **Browse** to navigate to the desired Destination Folder, and then click **Next**.
 - Step 9** After the InstallShield Wizard indicates that the installation is complete, click **Finish**.
-



CHAPTER 6

Common Tasks

- [Common Tasks](#), on page 411
- [The Palette](#), on page 412
- [General Tab](#), on page 412
- [Routing Tab](#), on page 412
- [Targets Tab](#), on page 412
- [Queue Tab](#), on page 413
- [Create Routing Script](#), on page 413
- [Add Comments to a Node](#), on page 414
- [Specify a Connection Label Location for a Node](#), on page 414
- [Validate Scripts](#), on page 415
- [Open Script Explorer](#), on page 415
- [Schedule Routing Script](#), on page 416
- [Viewing Modes](#), on page 418
- [Making Packaged CCE Work with Unified CVP](#), on page 418

Common Tasks

This section contains information about common tasks you perform in Script Editor. This section does not contain information about every possible task you can perform. For more information on Script Editor, see the Script Editor online help.



Note If you are a department administrator for Packaged CCE deployments (Packaged CCE: CCE-PAC-M1 and Packaged CCE: CCE-PAC-M1 Lab Only), then you will not have access to the Script Editor. Instead, you have to use the Internet Script Editor client, unless restricted by the feature control of the client or by your role.

The Palette

Figure 3: Palette Icon



You can display the Palette by clicking the **Palette** icon in the Main toolbar or by selecting **Palette** from the **View** menu. The Palette contains the icons that represent the nodes used in scripts.

Related Topics

[General Tab](#), on page 412

[Routing Tab](#), on page 412

[Targets Tab](#), on page 412

[Queue Tab](#), on page 413

General Tab

The General tab contains icons for the following scripting activities:

Related Topics

[Comment Node](#), on page 511

[Categorization by Time and Date](#), on page 430

[Nodes Used to Stop Script Processing](#), on page 450

[Categorize by External Applications](#), on page 437

[Line Connector Node](#), on page 512

[Formula Usage](#), on page 487

[Start Node](#), on page 511

Routing Tab

The Routing tab contains icons for the following scripting activities:

Related Topics

[Categorization and Call Type](#), on page 425

[Media Routing Domains](#), on page 471

Targets Tab

The Targets tab contains icons for the following scripting activities:

Related Topics

[Agent Routing Nodes](#), on page 441

[Transfer Calls from Agents to Agents](#), on page 441

[Nodes Used to Stop Script Processing](#), on page 450

Queue Tab

The Queue tab contains icons for the following scripting activities:

Related Topics

[Remove Call from a Queue](#), on page 466

[Place a Call in Queue](#)

[Adjust Priority of a Call in a Queue](#), on page 465

[Queue to Agent Node](#), on page 474

[Run External Scripts](#), on page 456

[Send Call to a VRU with Send to VRU Node](#), on page 455

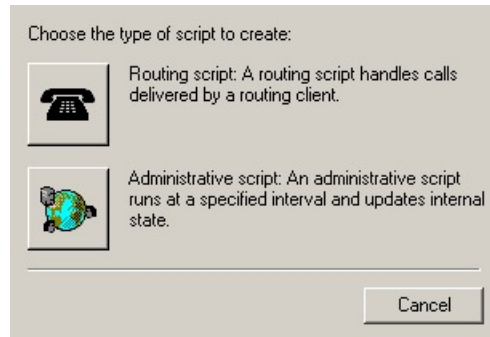
[Temporarily Halt Script Execution](#), on page 467

Create Routing Script

Procedure

Step 1 In Script Editor, choose **File > New** or click **New**. You are prompted to select a Routing Script or an Administrative Script:

Figure 4: New Dialog Box



Step 2 Click the following icon.

Figure 5: Routing Script



The new script opens in the Edit window, with a Start node. (See [Start Node](#), on page 511.)

Step 3 Build the script.

Step 4 To save the script, choose **File > Save** or click **Save**. You are prompted for a script name.

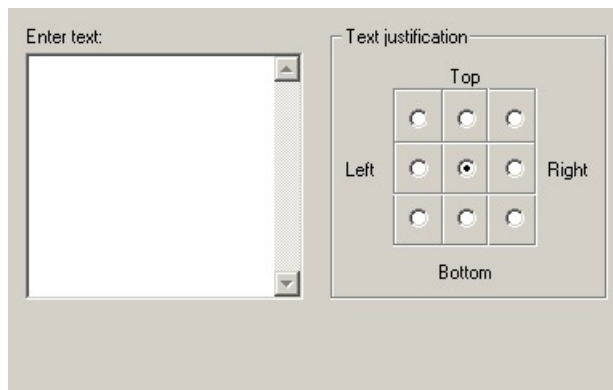
Add Comments to a Node

Figure 6: Comment icon



Most nodes have a Comment tab :

Figure 7: Comment Tab



Procedure

-
- Step 1** To add a comment, type in the **Enter text** field.
- Step 2** To select the location where you want your comment to appear in the node, select a radio button in the **Text justification** area.
-

Specify a Connection Label Location for a Node

Most nodes have a **Connection Labels** tab.

Procedure

-
- Step 1** When viewing a script in monitor mode, you can specify the location of connection labels by moving the slider in the Label position area to one of the following locations:
- Origin**, displays the connection label close to the node you are editing.
 - Destination**, displays the connection label close to the targeted node.
 - Center**, displays the connection label between the nodes.

Step 2 You can remove the connection label by clearing the **Display monitor labels** check box.

Validate Scripts

Procedure

Step 1 To validate a single script, with the script open in the active window, choose **Script > Validate** or click the **Validate** Icon on the toolbar.




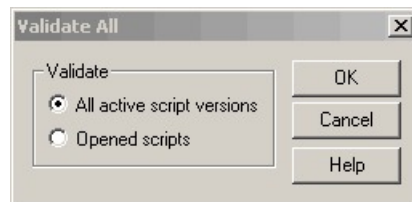
Step 2 To validate multiple scripts, choose **Script > Validate All**  or on the toolbar, click the **Validate All** Icon. You are prompted to choose between validating active versions of all scripts or all the opened scripts.

Figure 8: Validate All Query Dialog




Step 3 Make the appropriate selection and click **OK**.

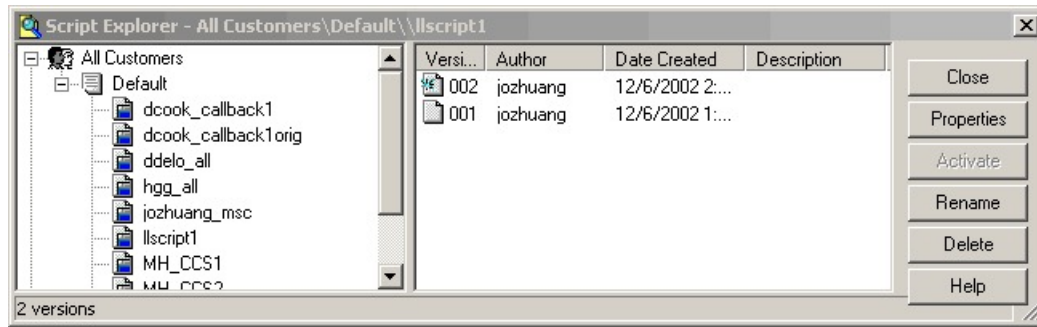
- If a script is valid, a dialog box opens stating that script is valid.
- If the script is not valid, the Validate Script dialog box opens with a list of the errors and warnings. When you select an error, the node where the error occurs is highlighted in the Edit window.

Open Script Explorer

Procedure

In Script Editor, choose **File > Script Explorer** or on the toolbar, click the **Explorer** Icon. 

The Script Explorer dialog box opens, listing scripts by customer and business entity:



You can then set the active version of the script, view its properties, rename it, or delete it. For more information, see the *Script Editor Online Help*.

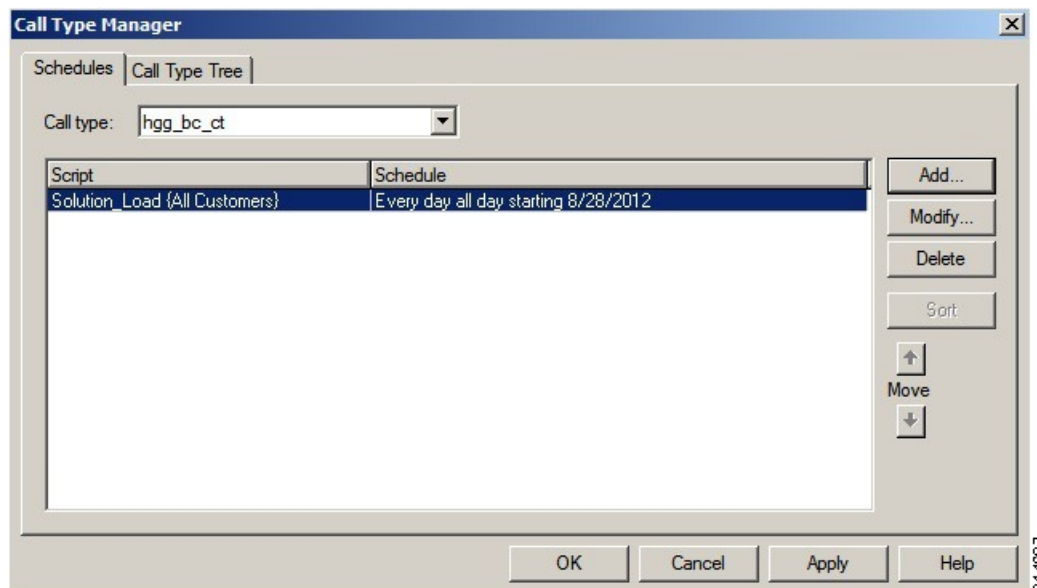
Schedule Routing Script

You schedule a script by associating it with a call type as follows:

Procedure

Step 1 Choose **Script > Call Type Manager**. The Call Type Manager dialog box opens.

Figure 9: Call Type Manager Dialog Box—Schedules Tab

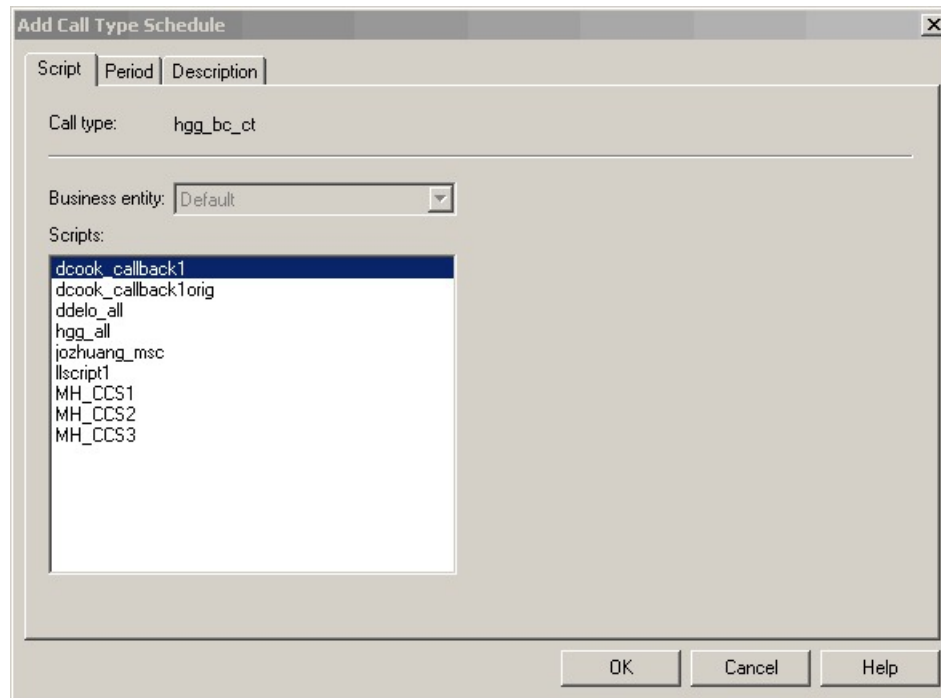


Step 2 Select the call type to associate with the script.

Step 3 Click **Add**. The Add Call Type Schedule dialog box opens.

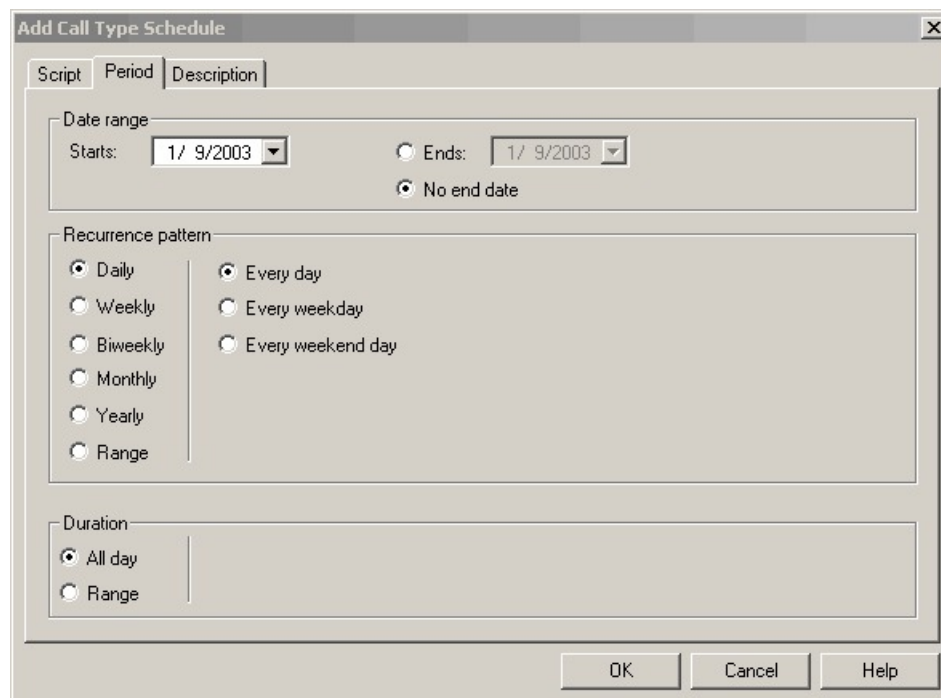
Step 4 In the Script tab, select the script to schedule:

Figure 10: Add Call Type Dialog Box - Script Tab



Step 5 In the **Period** tab, choose the information to define the period for which the schedule will be effective.

Figure 11: Add Call Type Schedule Dialog Box - Period Tab



Step 6 Optionally, in the **Description** tab, enter a description of the schedule.

Step 7 Click **OK** in the Add Call Type Schedule dialog box.

Step 8 Click **OK** in the Call Type Manager dialog box.

Note The schedule is not saved until you click **OK** in the Call Type Manager dialog box.

Viewing Modes

You can view a script in four different modes:

- **Browse** - Allows you to view the script.
- **Edit** - Allows you to edit the script.
- **Monitor** - Allows you to monitor the script
- **Quick Edit** - Allows you to make certain modifications to a script, with the following guidelines:
 - In Quick Edit mode, you cannot add or delete a node.
 - In Quick Edit mode, you can adjust most of the properties of the script nodes you select in the Node Control table of your assigned feature control set. However, in Quick Edit mode you cannot edit any properties of the selected nodes that change the structure of a script or that reset previous reporting data.
- As a Quick Edit Only User:
 - You can only edit scripts through Quick Edit mode.
 - You cannot create or delete a script.
 - You can access the Properties of any script node in any mode by either right-clicking the node and selecting Properties, or by double-clicking the node.
 - You cannot edit the Call Type Manager dialog box (Script > Call Type Manager).
 - You cannot edit the Administrative Manager dialog box (Script > Administrative Manager).
 - You cannot edit the Custom Functions dialog box (Script > Custom Functions).
 - You can choose the viewing mode from the Scripting toolbar, or from the Script menu.

Making Packaged CCE Work with Unified CVP

The following sections describe the differences between Packaged Contact Center Enterprise (Packaged CCE) and Unified Customer Voice Portal (Unified CVP) scripting and show how they work together in common tasks.

Difference Between Unified CCE and Unified CVP Scripting

Packaged CCE scripting offers call control such as how a call should be treated based on time of day, call type, and so on. It also handles queuing for an agent based on skill group or service. It determines when to

send the call to Unified CVP (for example, to play prompts, collect call entered digits, and get or put information in a database), or for queuing the call while waiting for an agent.

Unified CVP scripting offers IVR interaction, like playing a prompt based on an audio file or text-to-speech or collecting caller-entered digits via touch tone or speech. It also offers advanced features such as accessing an external database or web service for information used in creating a dynamic caller interaction experience. Examples include accessing current balance or storing collected customer information in a database.

Packaged CCE scripting is used for routing the call; but when the call needs to go to the Unified CVP, a self-service component is enlisted with Unified CVP scripts that have been created in Call Studio. For example, if a customer calls a credit card company and gets a voice recorded message, the Packaged CCE component makes the decision which script to run, whether the interaction is treated as a sales call or a service call and then selects which VRU (voice response unit) scripts get run. The call is then sent to a VRU, which connects the call to the Unified CVP "self-service engine". It accomplishes these tasks without the customer talking to an agent, such as getting the account balance with touch tone activation or speech. Once the information is collected control is then returned to the Packaged CCE script. The Packaged CCE script queues the customer for an agent, and connects the customer to an agent.

How Packaged CCE and Unified CVP Work Together

To summarize, Packaged CCE and Unified CVP work together to perform such tasks as:

- Playing media, such as a recording stating office hours, to a caller.
- Playing streaming audio, such as a radio broadcast, to a caller.
- Retrieving caller-entered data, DTMF, or speech.
- Playing back different types of data, such as an account number or balance, to a caller.
- Moving calls to other destinations. For example, forwarding calls to an agent.

Packaged CCE uses Unified CVP messaging technology to direct Unified CVP and to receive the responses from Unified CVP.

For more information about Packaged CCE working with Unified CVP, proceed to [Before You Begin, on page 515](#).



CHAPTER 7

Call Types, Contact Data, and Scripting

- [Call Types, on page 421](#)
- [Default Call Types, on page 421](#)
- [Relation Between Call Types and Scripts, on page 421](#)
- [Call Type Qualifiers, on page 422](#)
- [Association of Contacts with Call Types, on page 422](#)
- [Determination of Call Type for Voice Contact, on page 422](#)
- [Determination of Call Type for ECE Web Request, on page 423](#)
- [Determination of Call Type for a Task Routing Task, on page 423](#)

Call Types

When writing scripts to route contacts, you must understand call types and contact data.

A call type is the first-level category of a contact and is determined by data associated with the contact. You associate a script with a call type. When a contact of a certain call type is received, the associated script runs on that contact.

You create call types through the Call Type tool in Unified CCE Administration. See the section on call types for more information.

Default Call Types

A default call type is the call type used when a contact does not map to a defined call type.

You specify the system default call type in the Settings tool of Unified CCE Administration. For more information, see the section on system settings for call reporting.

Relation Between Call Types and Scripts

Scripts are scheduled by **call type**. In other words, when the system receives a request to route a contact, it determines the call type of that contact, then runs the associated script.

Call types provide the first level of **categorization of contacts**, enabling you to write scripts to route contacts differently depending on their call type. While other types of categorization take place within a script, call

types enable you to provide contacts with different treatment by running different scripts to begin with. Call types enable categorization before a script begins to run.

Call Type Qualifiers

The following data determine the call type. This data is referred to as the call type qualifier.

The call type qualifiers described in this section apply to contacts from all media. The terminology used is applicable to voice contacts; where the terminology differs for other media, the differences are explained in this section.



Note You can also use the call type qualifiers for categorization within a script.

Dialed Number (DN)

A Dialed number (DN) is a string that represents the telephone number dialed by the caller, preceded by the name of the routing client and a period. For example, "ucm.18005551212" might be a dialed number.

Typically, a dialed number is associated with one or more call types.

Association of Contacts with Call Types

Following is the general process of how the system attempts to associate a contact with a call type:

1. If the dialed number of the contact maps to a defined call type, the system uses that call type.
2. If no call type matches the contact, the system uses the default call type.
3. If no default call type is defined, the system returns an error to the routing client.

Determination of Call Type for Voice Contact

The following example demonstrates how the system determines the call type for a voice contact and runs the appropriate script:

1. When configuring Packaged CCE, you create a call type called "MASSACHUSETTS_SALES". This call type is defined as:
 - Having a dialed number of "ucm.8005551234".
2. You create a script called "MASSACHUSETTS_SALES_SCRIPT," which finds the longest available agent in the "NORTHEAST_SALES" skill group.
3. You schedule the script to run for the "MASSACHUSETTS_SALES" call type.
4. Packaged CCE determines that the call type is "MASSACHUSETTS_SALES" and runs the "MASSACHUSETTS_SALES_SCRIPT" script.

5. Packaged CCE assigns the task to a particular agent.

Determination of Call Type for ECE Web Request

The following basic example demonstrates how the system determines the call type for a Enterprise Chat and Email chat web request:

1. When configuring the Packaged CCE, you create a call type called "SSC_CT". This call type is defined as having a Script Selector (Dialed Number) of "SSC_DN".
2. When configuring ECE, set the value of the Script Selector for Media Routing Domain to "SSC_DN".
3. You create a script called "SSC_SCRIPT," which finds the longest available agent in the "COLLABORATION_SALES" skill group.
4. You schedule the script to run for the "SSC_CT" call type.
5. An e-mail is sent or a web user requests a chat session.
6. A route request is sent to Packaged CCE.
7. Packaged CCE determines that the Call Type is "SSC_CT" and runs the "SSC_SCRIPT" script.
8. Packaged CCE instructs ECE to assign the task to a particular agent.

Determination of Call Type for a Task Routing Task

This example is for a multichannel task from a third-party multichannel application that uses the Task Routing APIs. It demonstrates how the system determines the call type for the task and runs the appropriate script. In this example, the task is a chat task.

1. When configuring CCE, you create a multichannel MRD called "Chat_Task_MRD". You create a call type called "Chat". You create a dialed number/script selector "Chat_DN", and associate it with "Chat_Task_MRD" and the "Chat" call type.
2. You create a SocialMiner Chat application from which a user can request to chat with an agent. You set the value of the script selector in the chat form to the "Chat_DN" dialed number.
3. You create a script called "Universal_Queue_script" that finds the longest available agent in the "Sales" skill group in the "Chat" MRD.
4. You schedule the script to run for the "Chat" call type.
5. A user requests a chat session from the SocialMiner Chat application, using the SocialMiner Task API.
6. SocialMiner submits the task request to CCE, including the dialed number/script selector.
7. CCE uses the script selector to determine the call type, and runs the "Universal_Queue_script".
8. CCE assigns the task to an agent who is logged into the "Sales" skill group in the "Chat" MRD.



CHAPTER 8

Contact Categorization

- [Contact Categorization, on page 425](#)
- [Categorization and Call Type, on page 425](#)
- [Categorization by Call Type Qualifiers, on page 428](#)
- [Categorization by Time and Date, on page 430](#)
- [Categorization by Branching, on page 433](#)
- [Categorize by External Applications, on page 437](#)

Contact Categorization

When you create a routing script, you typically use the nodes available in Script Editor to define how the script is to categorize contacts. By categorizing contacts, a script can provide unique solution for different customer needs.

Categorization and Call Type

Categorization is the process of classifying a contact based on certain data associated with the contact. Through categorization, a script can determine the best way to process a contact.

When you create a routing script, you typically use the nodes available in Script Editor to define how the script is to categorize contacts. By categorizing contacts, a script can provide unique solutions for different customer's needs.

Categorization Through Scheduling Scripts by Call Type

Call types provide the first level of categorization for routing scripts. You schedule scripts by call type; therefore, the call type of a contact determines which script is run, enabling you to create different scripts for different types of contacts.

Change Call Type to Static

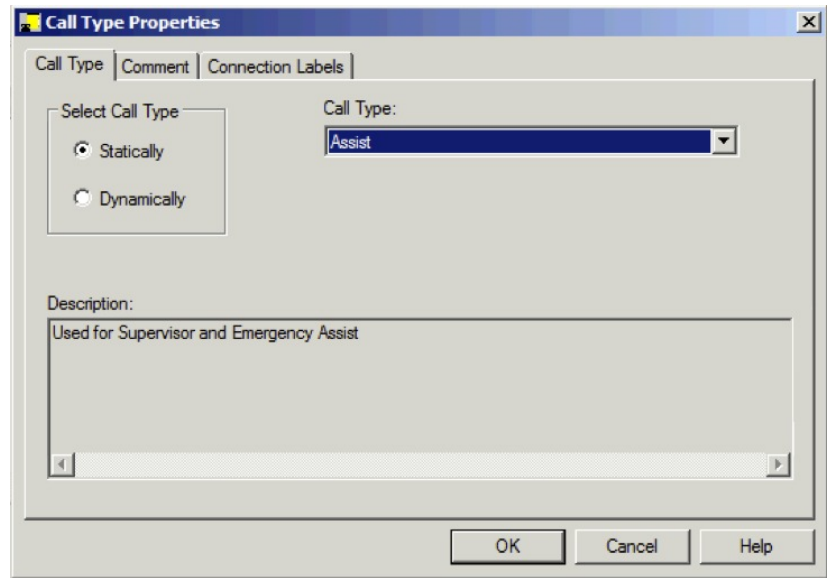
You can change the call type of a contact to static by using the Call Type node in a script. The Call Type node is in the Routing tab of the Palette.

Figure 12: The Call Type Icon



The following figure is the Call Type Properties dialog box of the Static Call Type node:

Figure 13: Call Type Properties Dialog Box - Static Call Type



To define a static call type node, complete the following steps.

Procedure

-
- Step 1** In the Call Type tab, click the **Statically** radio button.
- Step 2** From the Call Type list, click the call type to assign to the contact.
-

What to do next



-
- Warning** The Call Type node changes the call type and continues running the current script. The Requalify Call node stops running the current script and runs a new script associated with that call type.
-

Change Call Type to Dynamic

You can change the call type of a contact to dynamic by using the Call Type node in a script. The Call Type is on the Routing tab of the Palette.

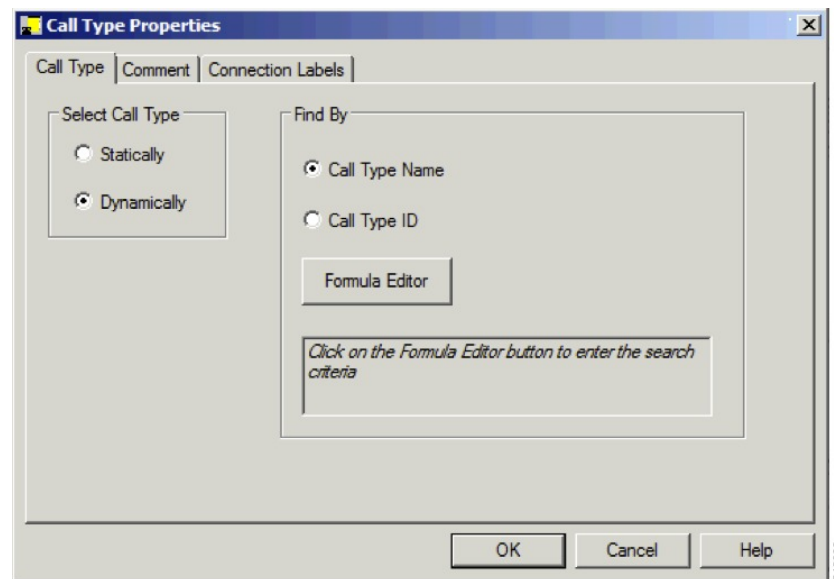
Figure 14: Call Type Icon



Note The dynamic call type option is enabled only for System Administrators. For other users, this option is disabled.

The following figure is the Call Type Properties dialog box of a dynamic call type node:

Figure 15: Call Type Properties Dialog Box - Dynamic Call Type



To define a dynamic call type node, complete the following steps.

Procedure

-
- Step 1** On the call type tab, select the **Dynamically** radio button.
 - Step 2** To dynamically change the call type of a contact by call type name, In the Find By section, select the **Call Type Name** radio button.
 - Step 3** To dynamically change the call type of a contact by call type ID, In the Find By section, select the **Call Type ID** radio button.
 - Step 4** To determine which call type name or ID to use to change the call type of a contact, click the Formula Editor button to create a formula.
-

Change Call Type and Run a New Script

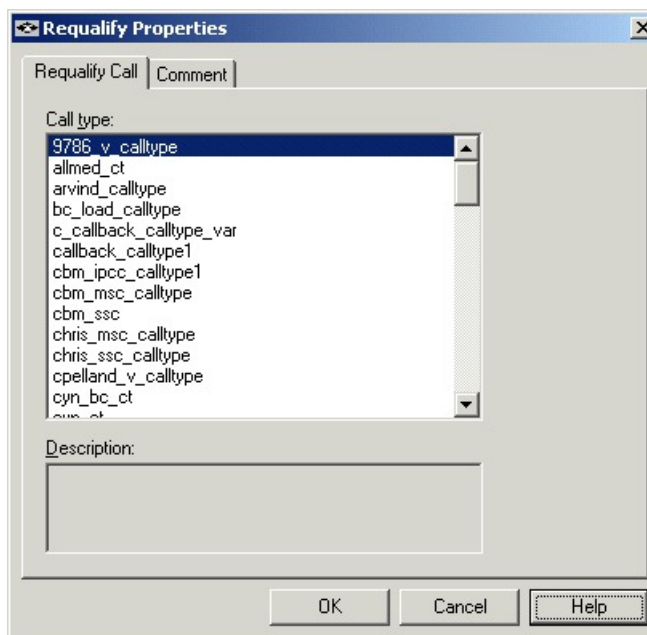
You can change the call type of a contact from within a script and run a new script associated with the call type by using the Requalify Call node (in the Routing tab of the Palette).

Figure 16: The Requalify Call Icon



Following is the Requalify Properties dialog box of the Requalify Call node:

Figure 17: The Requalify Properties - Requalify Call Tab



Define Requalify node properties as follows:

Procedure

-
- Step 1** In the Requalify Call Tab, select the Call type to assign to the contact.
- Step 2** Optionally, add comments.
-

What to do next



Warning The Call Type node changes the call type and continues running the current script. The Requalify Call node stops running the current script and runs a new script associated with that call type.

Categorization by Call Type Qualifiers

A contact's call type is determined by the dialed number qualifier.

When the system determines a contact's call type based on these qualifiers, it runs the associated script.

However, after the script is run, you can further categorize the contact based on the values of the call type qualifiers.

Categorize Contact by Dialed Number

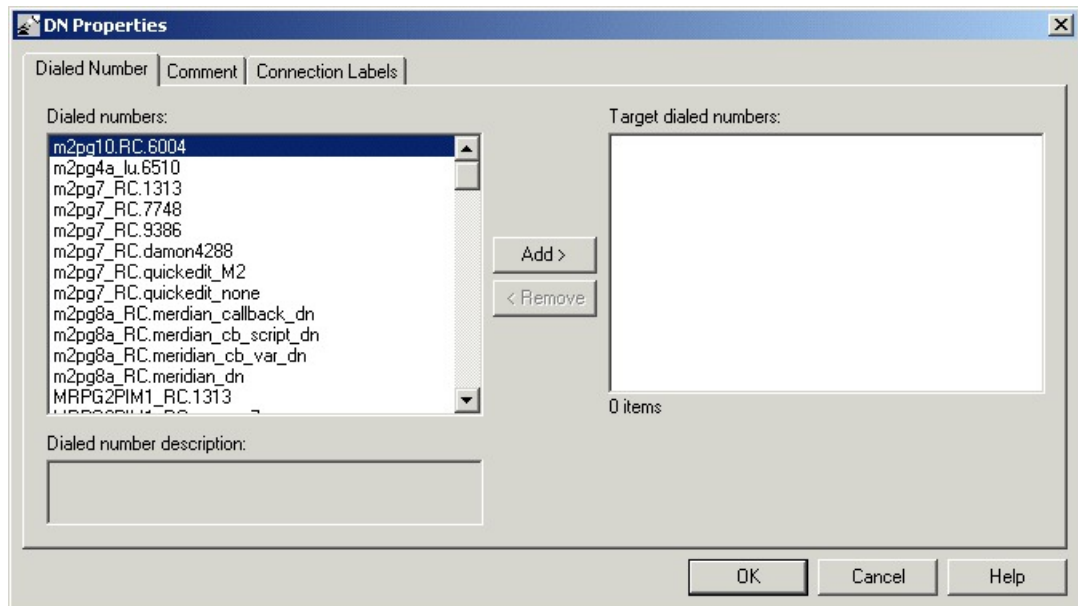
You can categorize a contact based on its dialed number by using the Dialed Number (DN) node (in the Routing tab of the Palette).

Figure 18: The Dialed Number Icon



Following is the DN Properties dialog box of the Dialed Number node:

Figure 19: DN Properties - Dialed numbers Tab



You can define the Dialed Number node properties as follows:

Procedure

-
- Step 1** Select one or more dialed numbers or Script Selectors from the Dialed numbers list and click **Add>** to move them to the Target dialed numbers list. If the current contact matches one of the selections in the Target dialed numbers list, processing continues on the node's success branch; otherwise, processing continues on the failure branch.
- Step 2** Optionally, add comments and connection labels.
-

Categorization by Time and Date

You schedule a script by associating it with a call type. When a contact of a certain call type is received, the associated script runs for that contact.

However, after the script is run, you can further categorize the contact based on the time and day of week. This categorization refines the schedule.



Note The time and day of the week are determined by the settings on the CallServer virtual machine.

For example, a call type named "CHAT_CT" may be defined to include all chat web requests. A script named "CHAT_SCRIPT" runs every time a contact with the call type "CHAT_CT" is received. Typically, this script instructs Enterprise Chat and Email to assign the request to the longest available agent in the "Chat" skill group. However, the contact center is staffed differently over the weekend and the supervisor wants to report to improved weekend activity. Therefore, for chat web requests received on Saturday or Sunday, the script branches differently and instructs Enterprise Chat and Email to assign the request to the longest available agent in the "WKEND_SUPPORT" skill group.

As another example, for a contact center where no phone support is available during night hours or weekends, you may choose to design a script that routes a phone call to an announcement instead to an agent, during the off hours.

Categorize Contact by Date and Time

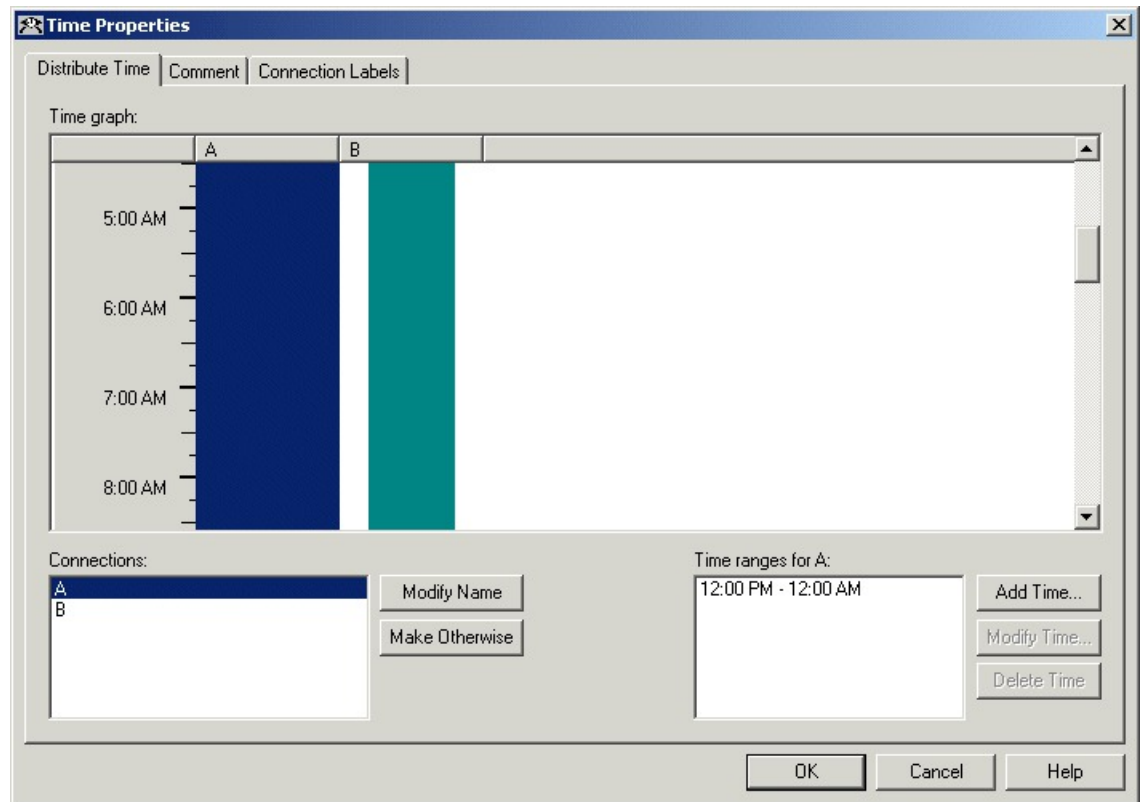
You use the Time node (in the General tab of the Palette) to choose from among several paths within the script based on the current time at Packaged CCE Central Controller. Following is the Time Properties dialog box of the Time node.

Figure 20: Time Icon



Following is the Properties dialog box of the Time node:

Figure 21: Time Properties

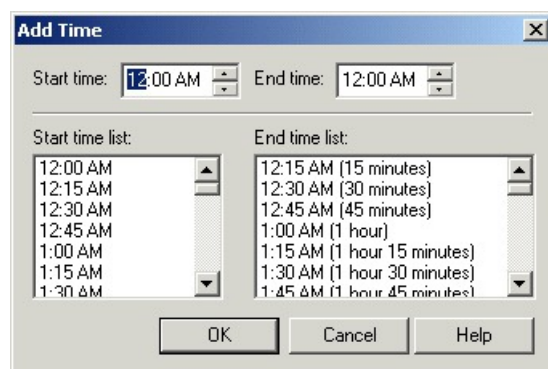


You must insert targets and connections from the Time node before you can define the node's properties. Then define Time node properties as follows:

Procedure

- Step 1** For each branch listed in the Connections list, define a Time Range. You can define multiple time ranges for a single branch. Click **Add Time** to add a new time range to the branch, or select a time range listed and click **Modify Time** to modify it. A dialog box opens in which you can define the time range (the Add Time dialog box is shown below; the Modify Time dialog box looks and functions similarly):

Figure 22: Add Time Dialog



- Step 2** To delete a time associated with the branch, select the time and click **Delete Time**.
- Step 3** You can define a branch as Otherwise by selecting the branch and clicking **Make Otherwise**. Execution follows this branch if none of the specified time ranges apply. You can specify only one Otherwise branch for the node. If you do not want to define the branch as **Otherwise**, select the branch and click **Delete Otherwise**.
- Step 4** Optionally, add comments and connection labels.

What to do next



Note If you delete a connection, the time-range information you specified in the Properties dialog box is also deleted.

Categorize Contact by the Day of Week

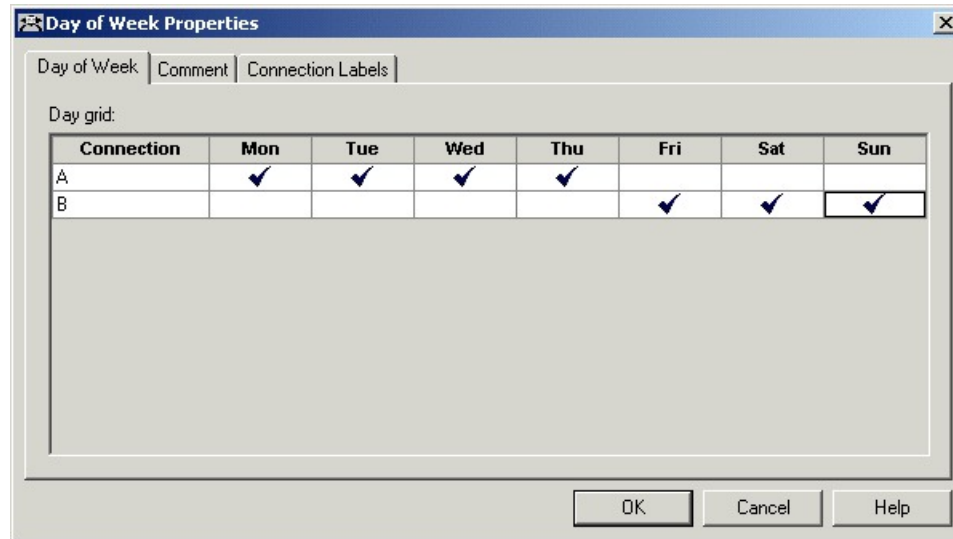
You use the Day of Week node (in the General tab of the Palette) to transfer control to one of several branches depending on the current day of week (Sunday, Monday, etc.).

Figure 23: Day of Week Icon



Following is the Properties dialog box of the Day of Week node:

Figure 24: Day of Week Properties



You can define multiple output connections from the Day of Week node and associate each with one or more days of the week.

You must insert targets and connections from the Day of Week node before you can define the node's properties.

Define Day of Week node properties as follows:

Procedure

-
- Step 1** For each branch listed in the Connection list, check the days of the week in which processing should continue on that branch. To check the day for that connection, left-click in a spot in the grid corresponding to that connection and day. A check mark appears in the grid. You can associate each day of week with one connection. However, you can associate each connection with one or more days of the week.
- Step 2** Optionally, add comments and connection labels.
-

Categorization by Branching

Within a script, you can create multiple branches to direct script processing based on certain conditions. Branching allows you to use a single script that processes contacts differently, depending on data associated with the contact, or on conditions at the contact center.

Run a Different Script

You use the **Go To Script** node (in the General tab of the Palette) to direct contact processing to another script without changing the call type. When Packaged CCE encounters a Go To Script node, it stops running the current script and starts the script indicated in the node.

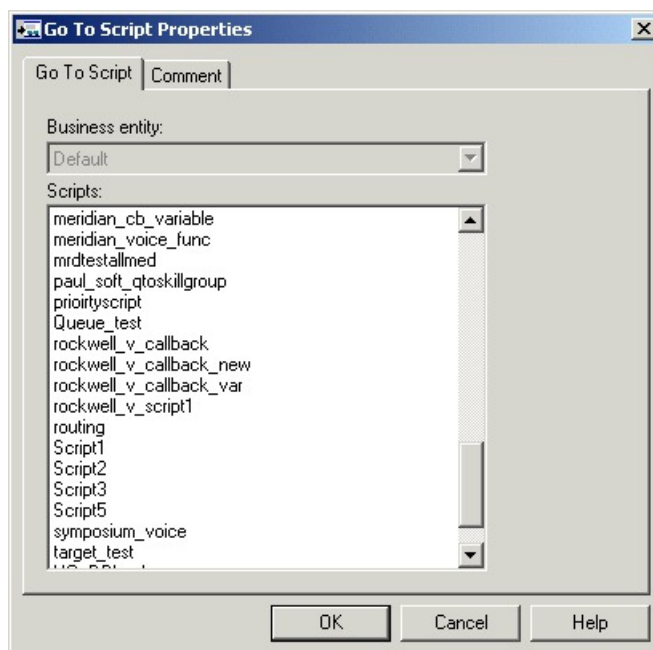
Figure 25: Go To Script Icon



For example, you might have several scripts that check for exception conditions and, if none are found, run a standard subroutine. Instead of including that subroutine as a branch from the failure output terminal of each of the exception conditions, you could use a Go To Script node pointing to a separate script containing the subroutine.

Following is the Properties dialog box of the Go To Script node:

Figure 26: Go To Script Properties



Define "Go to Script" node properties as follows:

Procedure

-
- Step 1** Select the Business entity that owns the script that the node should run. By default, Packaged CCE consists of one business entity.
 - Step 2** Select a script from the Scripts list. From within an administrative script, you can only go to another administrative script. Within a routing script, you can only go to another routing script.
 - Step 3** Optionally, add comments and connection labels.
-

Direct Script Execution to Different Branches by Percentage

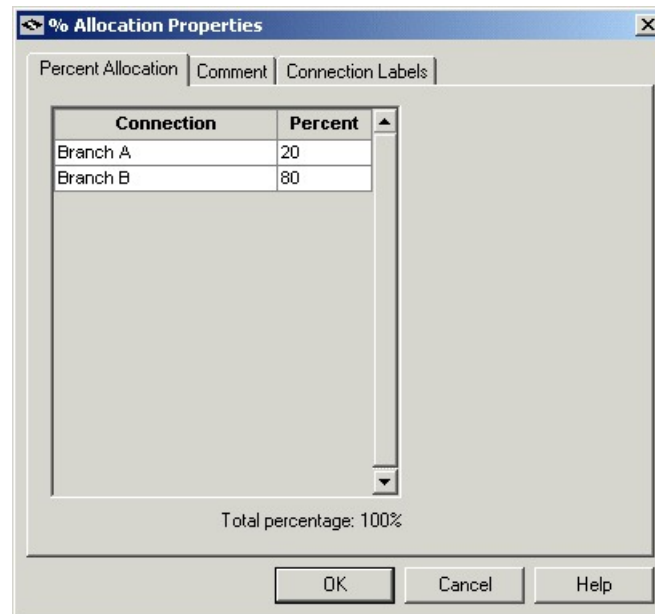
You can direct specific percentages of contacts to different branches in a script by using the Percent Allocation node (in the General tab of the Palette).

Figure 27: Percent Allocation Icon

Each branch may lead directly to a target, or may include additional processing. Because contacts are distributed by percentage and without tests of the targets' data, distributing by percentage never fails.

For example, in a geographically diverse environment, you can create a script that sends 10% of contacts to Boston, 5% to Chicago, and distributes the remaining 85% to another set of targets.

Following is the Properties dialog box of the Percent Allocation node:

Figure 28: % Allocation Properties

Define Percent Allocation node properties as follows:

Procedure

-
- Step 1** In the Percent column for each connection, enter a percent number for the percentage of contacts to process on that branch.
- Note** The percent total for all rows must equal 100.
- Step 2** Optionally, modify the Connection name. Changes appear in the connector labels when you save the properties and view the script.
- Step 3** Optionally, add comments and connection labels.
-

Categorize Contact Based on a Condition

You use the **If** node (in the General tab in the Palette) to direct script execution to one of two branches based on the result of an evaluation. You can use formulas to define the If node.

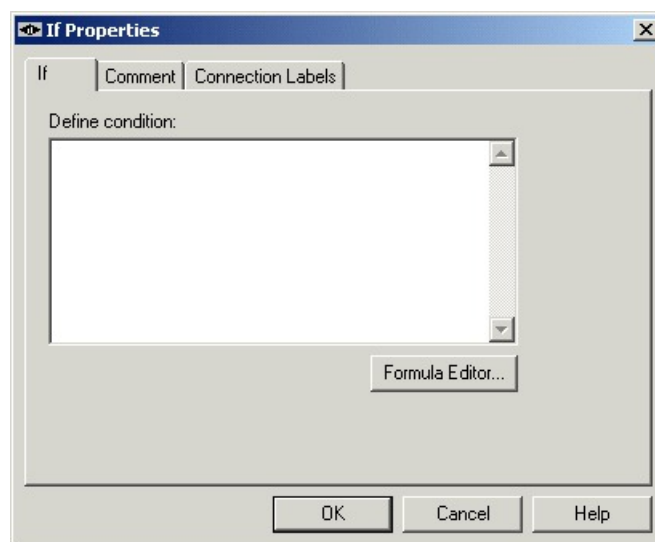
Figure 29: If Icon



When the system runs an If node, it first evaluates the condition specified in the node Properties dialog box Define condition field. If the system determines that the condition is true, control flows through the success output terminal; if it determines the condition is false, control flows through the failure output terminal.

Following is the Properties dialog box of the If node:

Figure 30: If Properties



Define If node properties as follows:

Procedure

-
- Step 1** In the Define condition field, enter a condition or use the Formula Editor to create a formula.
 - Step 2** Optionally, add comments and connection labels.
-

Categorize a Contact Based on Its Media Routing Domain

You use the Media Routing Domain node to categorize contacts based on their media routing domains. This node is described in the Universal Queue section of this document.

Categorize by External Applications

You can categorize a contact based on data returned from an application external to Unified ICM by using the Application Gateway node (in the General tab of the Palette).

Figure 31: Gateway Icon



For example, a script that processes incoming phone calls can send the caller's account number to an external application, which returns to the script the caller's account balance. The script can then branch on the value of the account balance, providing premium service to callers with higher account balances.



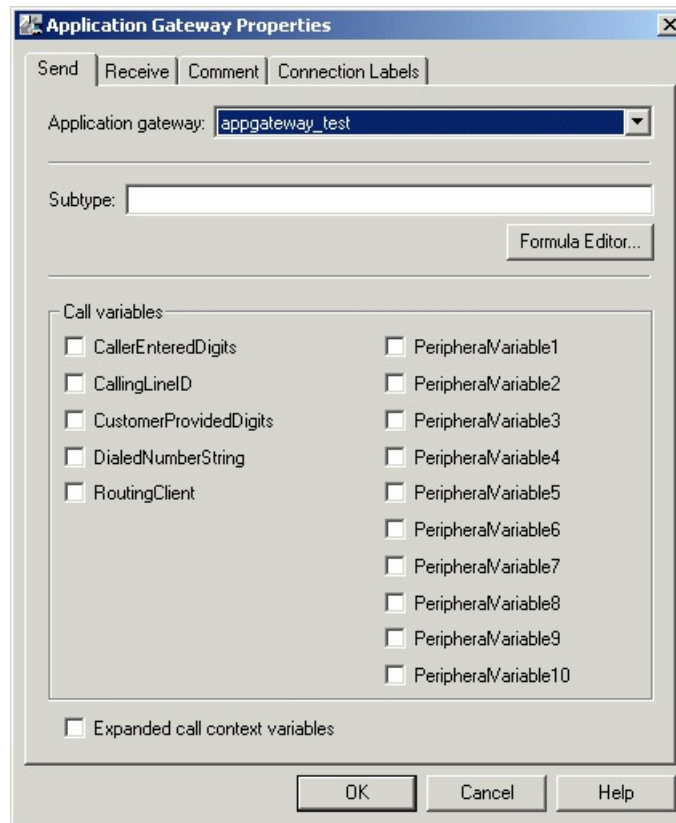
Note You must use Unified ICM Configuration Manager to define the external application. For more information, see the *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise*.

Define the Application Gateway properties as follows:

Procedure

Step 1 In the Send tab:

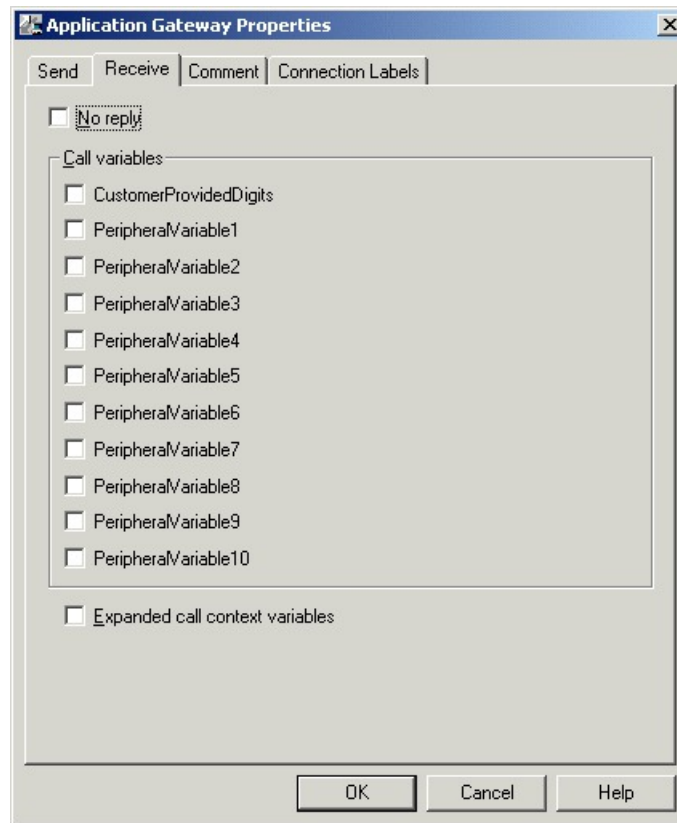
Figure 32: App Gateway Properties - Send



- Choose the gateway from the Application Gateway drop-down list.
- In the Subtype field, enter the string that is to be sent to the external application, or use the Formula Editor to write an expression that evaluates to a string.
- In the Call variables list, check the call variables to send to the external application.
- To send expanded call variables to the external application, check **Expanded call context variables**.

Step 2 In the Receive tab:

Figure 33: App Gateway Properties - Receive



- a) Select **No Reply** if the external application is not to return data to the script.

Note If you select this option, Unified ICM cannot retrieve any data from the external application.

- b) In the Call variables list, check variables that the external application may modify.
- c) Select Expanded call context variables if the external application modifies and returns values for the expanded call variables.

Step 3 Optionally, add comments and connection labels.



CHAPTER 9

Routing Target Selection

- [Routing Targets, on page 441](#)
- [Agent Routing Nodes, on page 441](#)
- [Transfer Calls from Agents to Agents, on page 441](#)
- [Nodes Used to Receive Contacts, on page 443](#)
- [Send Call to a VRU with Translation Route to VRU, on page 447](#)
- [Nodes Used to Stop Script Processing, on page 450](#)
- [Service Requested, on page 450](#)
- [Target Requery, on page 451](#)

Routing Targets

After defining how a script is used to categorize contacts, you typically use the nodes available in Script Editor to specify how the contact is to be routed to a target destination. A routing target is an entity to which the system can route a contact, including agents and skill groups. The routing target receives the contact and processes it accordingly.

Agent Routing Nodes

The following nodes are available for agent routing:

1. [Queue to Agent Node](#). For more information, see [Specify an Agent Directly, on page 475](#)
2. [Agent to Agent Node](#). For more information, see [Transfer Calls from Agents to Agents, on page 441](#)

Transfer Calls from Agents to Agents

You can transfer a call from an agent to an agent by using the Agent to Agent node in the Targets tab of the Palette.

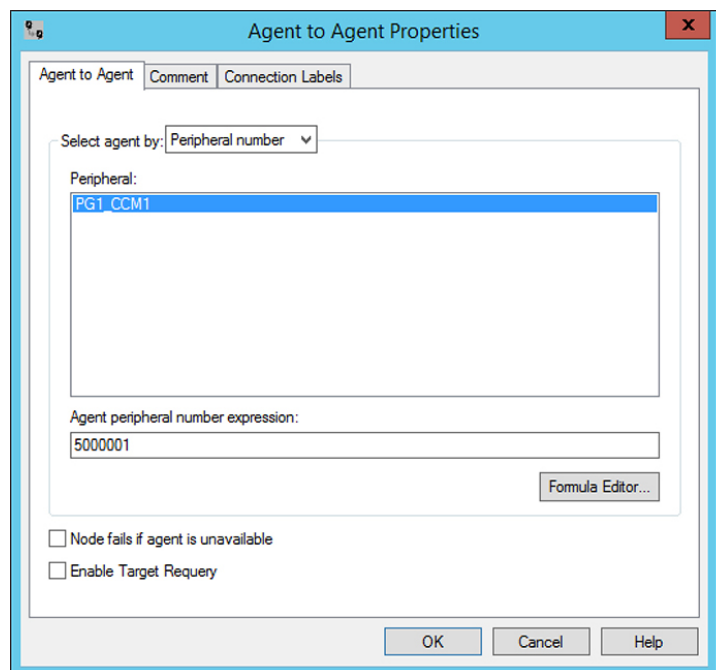
Figure 34: Agent to Agent Icon



The Agent to Agent node routes the call to the specified agent. You define the agent either by directly selecting the agent from the database or by providing an expression using a formula. The expression must translate to agent peripheral number or SkillTargetID. The router then finds a valid label for the agent. If there are no labels configured for the specified agent, the failure node of the Agent to Agent node is run.

Following is the Properties dialog box for the Agent to Agent node:

Figure 35: Agent to Agent Properties



Define Agent to Agent node properties as follows:

Procedure

-
- Step 1** Choose an option from the **Select agent by** drop-down list:
- Peripheral number - To select a peripheral and provide a formula that translates to the agent's peripheral number.
 - Enterprise Name - To select the agent from the list of configured agents.
 - Skill target ID - To select the agent by providing an expression that translates into the agent's SkillTargetID. In the supervisory case, the expression should use the call's PreferredAgentID.
- Step 2** Based on your selection in Step 1, select the peripheral or agent, or enter an expression, as necessary.
- Step 3** Optionally, check or uncheck **Fail node** if agent is unavailable:
- When checked, the success branch of the Agent to Agent node is run and the router sends the call if the router finds a valid label for the agent, the agent is available, and the agent state is Ready.
 - The failure branch of the Agent to Agent node is run if the router does not find a valid label for the agent, or the agent is not available or the agent is in TempUnavailable mode (the router has just send a call to the agent).

- c) When not checked, the success branch of the Agent to Agent node is run and the router sends the call if the router finds a valid label for the agent. The failure branch of the Agent to Agent node is run if the Router does not find a valid label for the agent.

Step 4 Optionally, add comments and connection labels.

Step 5 Optionally, check **Enable Target Requery**.

Nodes Used to Receive Contacts

Use the following nodes in Script Editor to specify how a contact is to be routed to a target.

- Enterprise Skill Group
- Enterprise Service
- Service

Define Set of Enterprise Skill Groups to Receive the Contact

You define a set of enterprise skill groups that can receive the contact by using the Enterprise Skill Group node in the Targets tab of the Palette.

Figure 36: The Enterprise Skill Group Icon



The script can determine the target enterprise skill group from the set by one of the following methods:

- Selecting the target by rules (Select node)
- Distributing contacts to targets in the set (Distribute node)
- A combination of selecting the target and distributing contacts (Route Select node)

Following is the Properties dialog box of the Enterprise Skill Group node:

Figure 37: Enterprise Skill Group Properties - Routing Tab

Enterprise Skill Group Properties

Routing Target | Connection Labels

Business Entity: Default

Enterprise target: enterprise_sg

	Skill Group	Route	Translation Route
1	m2pg7_1.Cisco_Voice.damon		

Allow connection for each target

Validate

Move

OK Cancel Help

Define Enterprise Skill Group node properties as follows:

Procedure

-
- Step 1** From the Business Entity drop-down list, select the business entity for the enterprise skill groups.
- Step 2** From the Enterprise target drop-down list, select the enterprise target for the enterprise skill groups.
- Step 3** For each enterprise skill group in the target set the following:
- In the Skill Group column, for each row used, select the enterprise skill group to which the contact can be routed.
 - In the Route column, select the route that maps to a specific target at the peripheral.
 - Optionally, in the Translation Route column, select a translation route.
- Step 4** Optionally, check **Allow connection for each target** to have an output terminal appear to the right of each individual target defined in the node. Control passes through this terminal when the associated target is chosen. When the script terminates, the route for the selected enterprise skill group is still used.
- Step 5** Click **Validate** to check whether the targets you defined are valid. Correct any errors that are flagged.
- Step 6** Optionally, add connection labels.
-

Define Set of Enterprise Services to Receive the Contact

You define a set of enterprise services that can receive the contact by using the Enterprise Service node in the Targets tab of the Palette.

Figure 38: The Enterprise Service Icon



The script can determine the target enterprise service from the set by one of the following methods:

- Selecting the target by rules (Select node)
- Distributing contacts to targets in the set (Distribute node)
- A combination of selecting the target and distributing contacts (Route Select node)

Following is the Properties dialog box of the Enterprise Service node:

Figure 39: Enterprise Service Properties - Routing Target tab

	Service	Route	Translation Route
1	m2pg7_1._serv	serv_route	

Define Enterprise Service node properties as follows:

Procedure

- Step 1** From the Business Entity drop-down list, select the business entity for the enterprise services.
- Step 2** Choose the enterprise target for the enterprise services from the Enterprise target drop-down list.

- Step 3** For each enterprise service in the target set the following:
- In the Service column, for each row used, select the enterprise service to which the contact can be routed.
 - In the Route column, select the route that maps to a specific target at the peripheral.
 - Optionally, in the Translation Route column, select a translation route.
- Step 4** Optionally, check **Allow connection for each target** to have an output terminal appear to the right of each individual target defined in the node. Control passes through this terminal when the associated target is chosen. When the script terminates, the route for the selected enterprise service is still used.
- Step 5** Click **Validate** to check whether the targets you defined are valid. Correct any errors that are flagged.
- Step 6** Optionally, add connection labels.
-

Define Set of Services to Receive the Contact

You define a set of services that can receive the contact by using the Service node in the Targets tab of the Palette.

Figure 40: The Service Icon

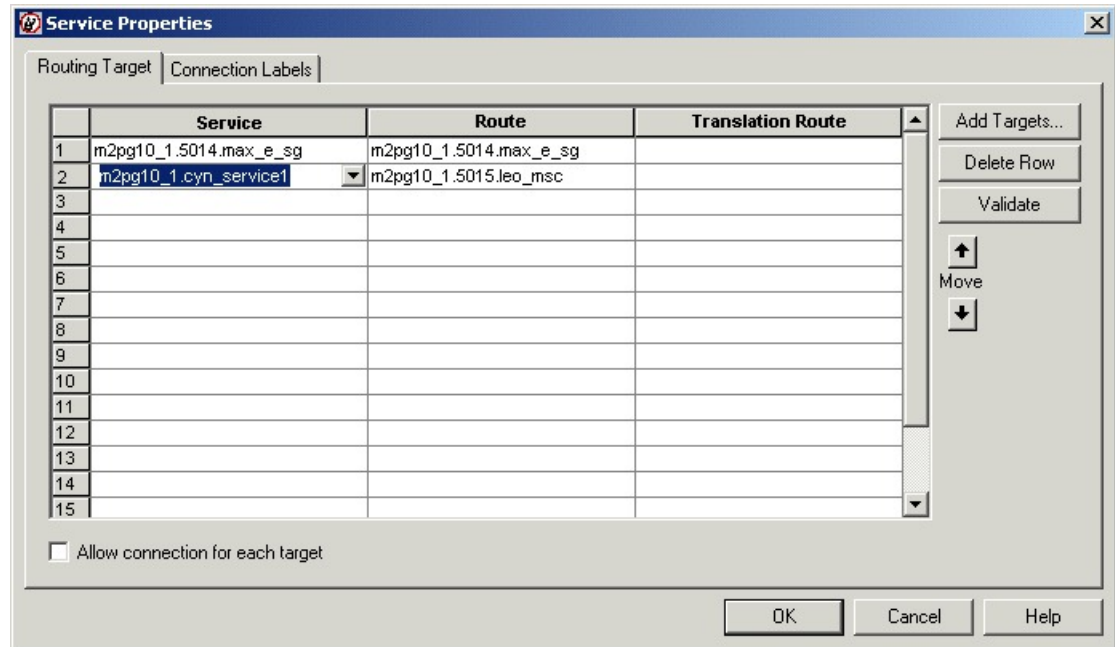


The script can determine the target service from the set by one of the following methods:

- Selecting the target by rules (Select node)
- Distributing contacts to targets in the set (Distribute node)
- A combination of selecting the target and distributing contacts (Route Select node)

Following is the Properties dialog box of the Service node:

Figure 41: Service Properties - Routing Target Tab



Define Service node properties as follows:

Procedure

-
- Step 1** For each service in the target set the following:
- In the Service column, for each row used, select the service to which the contact can be routed. You can use the drop-down list for each table cell, or select multiple services by clicking **Add Targets** and using the dialog box that opens to select multiple services.
 - In the Route column, select the route that maps to a specific target at the peripheral.
 - Optionally, in the Translation Route column, select a translation route.
- Step 2** Optionally, check **Allow connection for each target** to have an output terminal appear to the right of each individual target defined in the node. Control passes through this terminal when the associated target is chosen. When the script terminates, the route for the selected service is still used.
- Step 3** Click **Validate** to check whether the targets you defined are valid. Correct any errors that are flagged.
- Step 4** Optionally, add connection labels.
-

Send Call to a VRU with Translation Route to VRU

Before you begin

The translation route to CVP from other sites, CCE instance, or Avaya PG require translation route to VRU node to be used in the Routing script. To transfer a call to CVP using the Translation Route scheme, you must

use the *Command Execution Pane* to configure DNIS numbers in the CVP call server. You must replicate the DNIS configurations in all the CVP call servers configured in the same site.



Note The DNIS configuration in CVP is erased when you perform a full sync from the **Inventory** page of **Packaged CCE Administration**. To reconfigure the DNIS number in the CVP call server, use the *Command Execution Pane*.

For more information, see the [Command Execution Pane, on page 227](#).

Following is the Properties dialog box for the Translation Route to VRU node:

Figure 42: Translation Route to VRU Properties

	Service	Consider If	Select Min Value Of	Route	Translation Route
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					

Define Translation Route to VRU node properties as follows:

Procedure

Step 1

To change the type of target:

- Click **Change**. The Select Type dialog box opens.
- Choose the Target Type (Enterprise Service, Service, or Service Array).
- If you selected Enterprise Service, select a **Business Entity** and **Enterprise target**.
- Specify whether the Translation Route to VRU node is to act like a Select or Distribute node.

- **Distribute Among Targets.** The Translation Route to VRU node is to act like a Distribute node, distributing calls among the targets based on the relative values.
- **Select Most Eligible Target.** (Radio button.) The Translation Route to VRU node is to act like a Select node.

If you select this option, you:

- Define whether to pick the target with the maximum value or the minimum value.
- Define a formula that determines which target is to be accepted.
- Define the type of target search.

Step 2 To add targets, click **Add Targets**. The Add Targets dialog box opens. Use the Available Targets list and the Add button to select targets.

Note If you choose Enterprise Service as a target type, you can select just one item from the list. If you choose Service or Service Array, you can select one or more items from the list.

Step 3 Click **OK** to close the Add Targets dialog box. The target members you selected appear in the Properties dialog box.

Step 4 Continue defining Target information for each target:

- **Consider If** (Optional.) A formula that must evaluate to true for the target when the Packaged CCE initiates the Translation Route to VRU node, or that target is not considered.
- **Select Max/Select Min Value of A** A formula that determines which of the targets is selected.
- (Drop-down list.) The route on which to send the call if you select this target. (The list contains all routes associated with the target.)
- **Translation Route** (Drop-down list.) The route to send the call for initial VRU processing if you select this target. (The list contains all translation routes associated with the same peripheral as the target.)

Note You must specify a value for this field. When a call is sent to a translation route, the PG retrieves the final route from the Packaged CCE and coordinates the other processing with the VRU.

- **Per-node success connection** (Radio button.) Select this option to attach one success output terminal to the node. This terminal is used regardless of which target you select.
- **Per-target success connection** (Radio button.) Select this option to attach a success output terminal to each target in the node.

Note This option is useful in situations where you want to use different scripts depending on the selected target for a call.

Step 5 Optionally, click **Validate** to validate the node properties.

Step 6 Optionally, add connection labels.

Nodes Used to Stop Script Processing

You can use the following nodes to stop script processing:

- End Node
- Termination Node
- Release Call Node

End Node

You can terminate the script by using the End node in the General tab of the Palette.

Figure 43: End Icon



If the script reaches the End node, it has failed to find a target for the contact. Packaged CCE then uses the default route for the Dialed Number.

Several End nodes can appear in the same script. The End node is never required; a script can terminate with any node.

You do not define any properties for the End node. You can optionally add comments.

Release Call Node

You can terminate the script and disconnect the caller by using the Release Call node in the Targets tab of the Palette.

Figure 44: Release Call Icon



You can use a Release Call node in situations where the caller needs no further service after executing several Unified CVP scripts.

You do not define any properties for the Release Call node. You can optionally add comments.

Service Requested

ServiceRequested is a call variable available in Script Editor. It provides more details regarding the routing request. The field is currently only set for multichannel routing (Task Routing), voice callback (Agent Request) and Pick/ Pull routing, otherwise it is set to 0. Based on the value of this field, the script can take different actions.

ServiceRequested Variable

Service Requested Variable	Description
0 = ROUTE_SERVICE_REQUEST_NONE	No service requested.
1 = ROUTE_SERVICE_REQUEST_VOICE_CALLBACK	Caller is requesting a voice callback.
2 = ROUTE_SERVICE_REQUEST_TRANSFER	Transfer a task that is already assigned to an agent back to a queue.
3 = ROUTE_SERVICE_REQUEST_RONA	A task is being rerouted on no answer (RONA).

Target Requery

Target Requery is a script node feature that you can use to handle routing failures, for example due to No Answer or Busy responses, or for unreachable targets caused by transient failures in the network (such as network congestion). If the determined destination for a contact is available but not reachable, Target Requery attempts to find a different valid destination.

You need Target Requery to address the following failures:

- Failure to deliver a call to an agent.
- Failure of the outbound leg of a blind-mode Network Transfer.
- Target Requery works on a per call basis; that is, the routing information for one call does not affect the state for other calls. If the first target selected for the contact was not reachable, the target is not eliminated from the potential routing destinations for other contacts.



Note You can enable the Target Requery feature for CVP, ICM to ICM gateway, and a subset of the supported carrier NICs. You cannot use the requery feature with any of the multimedia requests because the MR PG does not support requery mechanism.

Target Requery Functionality

In the system, when queried, the CallRouter returns a label to the routing client. The routing client then routes the call to the destination specified by the label. If the destination is not reachable (for example, because of a busy signal or no answer), the call is routed to the default destination.

With Target Requery in a Label, Route Select, or Select node, if the router fails to route to a target node, a second attempt is made. If the failure occurs a second time, then the router continues from the failure path in the node.



Note In a Queue node, just one target is used. If the router fails to route to the target node, the failure path of the node is taken immediately. To implement requery in a Queue node, you can create a script that increases the priority and requeries the call from the failure path to the same queue.

In the event of a failure, you can handle requerying in the scripting environment, as you deem appropriate.

Target Requery does not require different definitions for different failure cases. However, you can choose to handle different failures differently.

Test of the RequeryStatus Variable

You can test the error path of these script nodes using Target Requery to determine the specific network cause of failure and conditionally retry the attempt as necessary. You can accomplish this using an If node to check the value of the call variable RequeryStatus. The decision path for the script is then determined by the value of the RequeryStatus variable.

The following are possible values for the RequeryStatus variable:

Table 30: RequeryStatus Variables

Requery Status Variable	Description
REQUERY_ANSWER (0)	Script ends. The call was successfully sent to the chosen target. Note This variable is used internally by the CallRouter. You cannot test for this variable in an IF node.
REQUERY_ROUTE_SELECT_FAILURE (1)	Routing client generated an error code from ReRouteReq msg indicating a Route Select failure.
REQUERY_CALLED_PARTY_BUSY (2)	Routing client generated error code from ReRouteReq msg indicating the called party is busy.
REQUERY_NO_ANSWER (3)	Routing client generated an error code from ReRouteReq msg indicating no answer.
REQUERY_ERROR (4)	CallRouter generated an error code. The attempt to send the call to target failed because the target was not reachable (i.e., busy, ring no answer).
REQUERY_ABORTED (5)	The attempt to send the call to a target failed because the caller abandoned before the call could be delivered to its destination. In the case of ABANDON and DISCONNECT, the CallRouter assumes the call has ended and ends the script. The RequeryStatus value is set to 5, indicating REQUERY_ABORTED. Note This variable is used internally by the CallRouter. You cannot test this variable in an IF node.

Requery Status Variable	Description
REQUERY_TIMED_OUT (6)	<p>The call attempt failed because the routing client did not respond to the router within the DivertOnBusyCallTimeout period (180 seconds by default). If the target node has Router Requery enabled, when DivertOnBusyCallTimeout period expires, the Router closes the Router Requery with REQUERY_TIMED_OUT .</p> <p>Note This variable is used internally by the CallRouter. You cannot test this variable in an IF node.</p>

Nodes That Support Target Requery

The following nodes support Target Requery:

- Label
- Queue
- Queue to Agent
- Precision Queue
- Route Select
- Select
- Agent to Agent

Use Target Requery

You define nodes to enable Target Requery. For the Queue, Queue to Agent, Agent to Agent, and Route Select nodes:

Procedure

-
- Step 1** Open the node properties.
- Step 2** Click **Change**. A dialog box opens.
- Step 3** Check **Enable target requery**.
- Step 4** Click **OK** to close the dialog box.
- Step 5** Click **OK** to close the properties dialog box.
- Step 6** For the Label, Select and Precision Queue nodes:
- For Select nodes:
- a) Open the node properties.
 - b) Check **Enable Target Requery**.
 - c) Click **OK** to close the properties dialog box.
-



CHAPTER 10

Network VRUs

- [VRU Functionality, on page 455](#)
- [Access to VRU Scripts in Packaged CCE Routing Scripts, on page 455](#)
- [Send Call to a VRU with Send to VRU Node, on page 455](#)
- [Run External Scripts, on page 456](#)
- [VRU Errors, on page 458](#)
- [Call Queuing at VRUs, on page 459](#)
- [Place a Call in Queue, on page 460](#)
- [Precision Queue Script Node, on page 462](#)
- [Adjust Priority of a Call in a Queue, on page 465](#)
- [Remove Call from a Queue, on page 466](#)
- [Temporarily Halt Script Execution, on page 467](#)

VRU Functionality

You can use routing scripts to divert a call to a Network VRU for additional call processing.

A VRU, or Voice Response Unit, is a telecommunications device, also called an Interactive Voice Response Unit (IVR), that plays recorded announcements and responds to caller-entered touch-tone digits. Cisco Unified Customer Voice Portal (CVP) is the supported VRU for Packaged CCE. A VRU can also be equipped with Automatic Speech Recognition (ASR) or Text-to-Speech (TTS) capabilities.

Access to VRU Scripts in Packaged CCE Routing Scripts

You can write routing scripts that send calls to the VRU, queue the call, and invoke specific VRU scripts. VRU scripts are configured using the Network VRU Scripts tool in the Unified CCE Administration tool.

Related Topics

[Add and Maintain Network VRU Scripts, on page 350](#)

Send Call to a VRU with Send to VRU Node

You can send a call to Unified CVP for further processing by using the Send to VRU node (in the Queue tab of the Palette).

Figure 45: The Send to VRU Icon

When Packaged CCE runs a Send to VRU Node, it looks up the call's Dialed Number, the Dialed Number's Customer, and the Customer's Network VRU. If that fails to retrieve a Network VRU, the router uses the system default Network VRU.

There are two failure cases:

- If the label does not exist, script execution continues with control flowing through the nodes failure output terminal.
- If Packaged CCE does not receive confirmation, execution continues with control flowing through the nodes failure output terminal.

In all other cases script execution continues with control flowing through the nodes success output terminal.

Notes:

- If the Run External Script, Play, Menu, Collect Data, or Queue node is used in a script before a Send To VRU node, an implicit Send To VRU node is assumed. You do not have to use the Send To VRU node. However, include the node in routing scripts as a visual aid if you ever need to troubleshoot the script.
- If the call is delivered to the Unified CVP but then abandoned, script execution ends. In monitor mode, a special label on the Send To VRU node accounts for these cases.

You do not need to set properties for the Send to VRU node. However, you can optionally add comments or connection labels.

Run External Scripts

You can instruct a Unified CVP to run a specific script by using the Run External Script node (in the Queue tab of the Palette).

Figure 46: The Run External Script icon

You can use multiple Run External Script nodes to run a series of scripts on the Unified CVP.

The execution of Packaged CCE routing script waits for the external script to finish:

- If the external script runs successfully, control then passes through the success branch of the Run External Script node.
- If the external script does not run successfully for any reason, then control passes through the failure branch of the Run External Script node.

**Note**

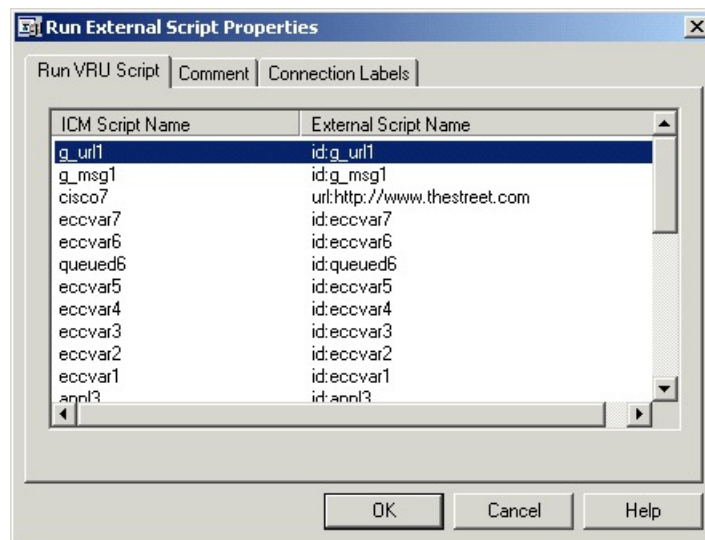
- If the current call is not at a Unified CVP when the Run External Script node is run, Packaged CCE sends the call to the associated Network VRU, as run a Send to VRU node.
- Design scripts so that the Failure branch of a Run External Script Node contains a test for the Call.VRUStatus variable. If the value is 2, the VRU is likely to be not functioning properly. Therefore, the script avoids executing any subsequent Run External Script nodes on this Failure branch.

**Note**

When an uninterruptible script is used in a Run External Script node, the CallRouter waits for the script result from the VRU. It then runs the next node. Calls can only be routed when they reach an interruptible node. The Wait node and interruptible Run External Script node (micro apps) are interruptible. Every other node is uninterruptible.

Following is the Properties dialog box for the Run External Script node:

Figure 47: Run External Script Properties



Define Run External Script node properties as follows:

Procedure

-
- Step 1** Select the Packaged CCE Script/External Script Name you want to run.
- Step 2** Optionally, add comments and connection labels.
-

VRU Errors

The following table lists the possible values for the VruStatus variable:

Table 31: VruStatus Variable Codes

Value	Meaning	Description
0	VRU_SUCCESS	The last VRU node was successful.
1	VRU_ERROR	The last VRU node failed because of a routing or configuration error.
2	VRU_TIMEOUT	The last Send To VRU failed because the routing client did not respond within 20 seconds or the last Run External Script node failed because the timeout limit defined for the script expired.
3	VRU_ABORTED	The last VRU node did not complete because the caller ended the call or stopped responding. (Because this causes the routing script to terminate immediately, this value is never seen.)
4	VRU_DIALOG_FAILED	The last VRU node failed because communication with the VRU ended unexpectedly.
5	VRU_SCRIPT_NOT_FOUND	The VRU failed because the referenced VRU script was not found in the Packaged CCE configuration.
6	STATUS_MAX_QUEUE_LIMIT_EXCEEDED	The last node failed because the maximum call queuing limit was exceeded.
7	STATUS_NO_VALID_EXPRESSION	The last node failed because no valid expression was found.
8	STATUS_NO_VALID_TARGET	The last node failed because no valid target was found.
10	STATUS_NO_MRD_MATCH	The last node failed because no targets matched with the Media Routing Domain on the call.

Value	Meaning	Description
11	STATUS_CONSIDER_IF_FAILED	The last node failed because the Consider If expression failed on all targets.
12	STATUS_NO_VALID_PERIPHERAL	The last node failed because none of the targets were configured on the supported peripheral.
13	STATUS_NO_ONLINE_PERIPHERAL	The last node failed because all targets are on peripherals that are offline.

Call Queuing at VRUs

You can queue a call at a Network VRU until a specific resource becomes available. A call can be queued for one or more skill groups, or a precision queue. As soon as an agent becomes available at one of the specified targets, the call is removed from the queue and sent to the target.

Specifically, you can:

- Place a call in a precision queue.
- Place the call in one or more skill groups.
- Adjust the priority of call in a queue for one or more skill groups.
- Remove the current call from any queues to which it is assigned.

Call Flow:

1. The call is first sent to the Network VRU. This step is required before you queue the call.
2. The call is queued for three skill groups.
3. If the call is successfully queued, the script cycles between a Wait node and a Run External Script node so that the caller hears an announcement every 30 seconds.

If an agent in one of the skill groups becomes available, the call is removed from queue and taken back from the Unified CVP. Routing script execution ends and the call is delivered to the target.

You could use other nodes like Queue to Skill Group or Queue to Precision Queue to queue the calls to different targets.



Caution Do not use the nodes like Route Select to queue the calls when the script cycles between a Wait node and a Run External Script node.



Note In this scenario, you would likely make the VRU script interruptible so that the routing script can retrieve the call immediately when the resource becomes available.

Place a Call in Queue

You can place a call in queue at a Unified CVP for one or more skill groups using the Queue node (in the **Queue** tab of the Palette).

Figure 48: The Queue Icon



If an agent becomes available in one of the skill groups, the call is routed to that resource.



Note If the current call is not at a Unified CVP when the Queue node runs, Packaged CCE sends the call to the associated Network VRU. (This does not apply to Type 2 VRUs, which are VRUs at customer premises.)

The Queue node includes a **Priority** field, which sets the initial queuing priority for the calls processed through this node versus other calls queued for the same target. The priority is expressed as an integer from 1 (top priority) to 20 (least priority). The default value is 5.

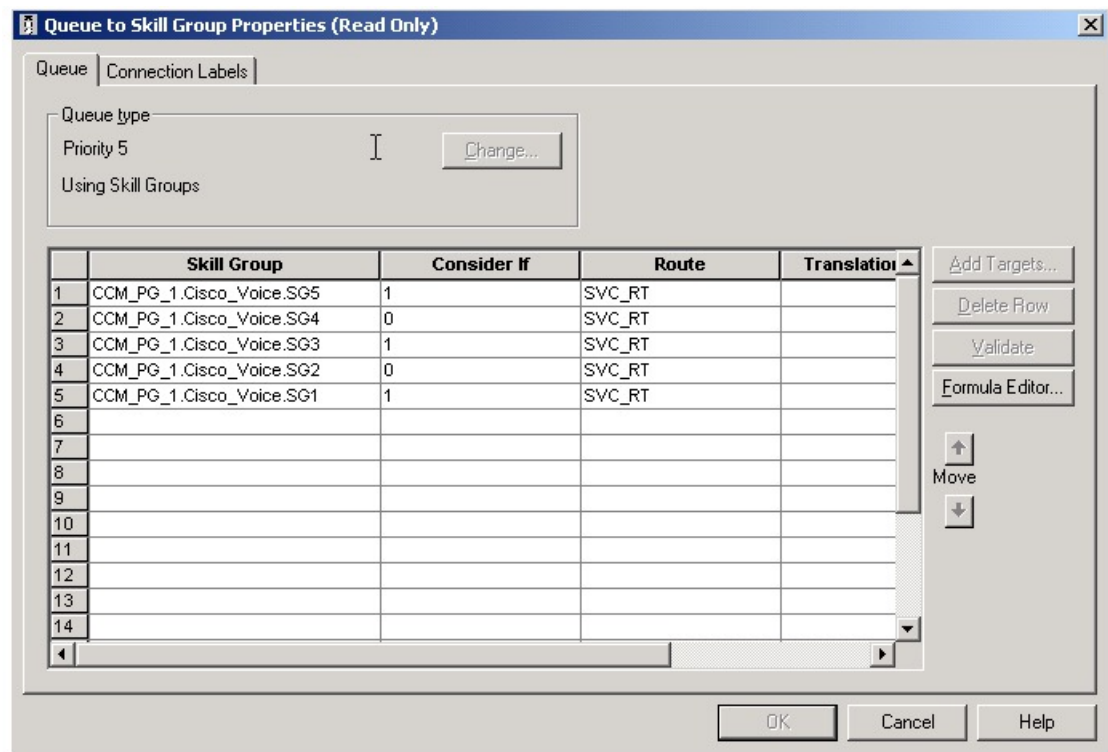
If more than one call is queued to a group when an agent becomes available, the queued call with the lowest priority number is routed to the target first. For example, assume an agent in a skill group becomes available and two calls are queued to that skill group. If one call has priority 3 and the other has priority 5, the call with priority 3, the lower value, is routed to the skill group while the other call continues to wait.



Note The Queue node does not actually result in instructions being sent to the VRU. When queuing occurs the Queue node exits immediately through the success branch and the call is assumed to be at the VRU; the script should then continue with a Run External Script node to instruct the VRU what to do while holding the call until an agent becomes available. Typically this would invoke a Network VRU script that plays music-on-hold, possibly interrupted on a regular basis with an announcement.

Following is the **Properties** dialog box for the Queue node:

Figure 49: Queue to Skill Group Properties



Define Queue node properties as follows:

Procedure

Step 1

To change the queue type:

- Click **Change**. The **Queue Type** dialog box opens.
- Select a **Target Type** (Skill Group). You cannot reference more than one type of target within a single Queue node. To queue a call to more than one target type, run multiple Queue nodes sequentially.
- Optionally, select a Priority to set the initial queuing priority for calls processed through this node versus other calls queued for the same target: 1 for top priority to 20 for least priority. (The default is 5.)
- Optionally, check **Enable Target Requery**.

Note

When Target Requery is enabled in a Queue node and a Requery happens, for example because the call is presented to an available agent, but the agent does not answer, the script continues through the failure terminal. The script can then inspect the call variable RequeryStatus to determine what to do next. The typical action in case of a No Answer would be to Queue the call again, possibly to other skill groups, and possibly increase the priority so that it is taken out of the queue before regular queued calls.

- Click **OK** to close the **Queue Type** dialog box.

Step 2

To add targets:

- Click **Add Targets**. The **Add Targets** dialog box opens, listing available targets of the type you specified.
- Use the **Available Targets** list and the **Add** button to select targets.

- c) Click **OK** to close the **Add Targets** dialog box. The target members you selected appear in the **Properties** dialog box.

Step 3 Optionally, continue defining Target Type information for the Route (Drop-down list) member. This is the route to send the call to when an agent in the target type becomes available. (The drop-down list includes all routes associated with the target.)

Step 4 Optionally, add connection labels.

What to do next



Note When processing a Queue node, the router first checks for an available target, if there is none available then the router attempts to queue the call. The call does not move to the VRU if there is an available agent.

Precision Queue Script Node

You can use the Precision Queue script node to queue a call or task based on caller requirements until agents with desired proficiency become available. This node contains multiple agent selection criterion which are separated into steps.

Figure 50: Precision Queue Script Node



A single call can be queued on multiple precision queues. If an agent becomes available in one of the precision queues, the call is routed to that resource. You cannot reference multiple precision queues with a single Precision Queue node. However, you can run multiple Precision Queue nodes sequentially to achieve this.

The Precision Queue node includes a **Priority** field, which sets the initial queuing priority for the calls processed through this node versus other calls queued to the other targets using different nodes. The priority is expressed as an integer from 1 (top priority) to 20 (least priority). The default value is 5.

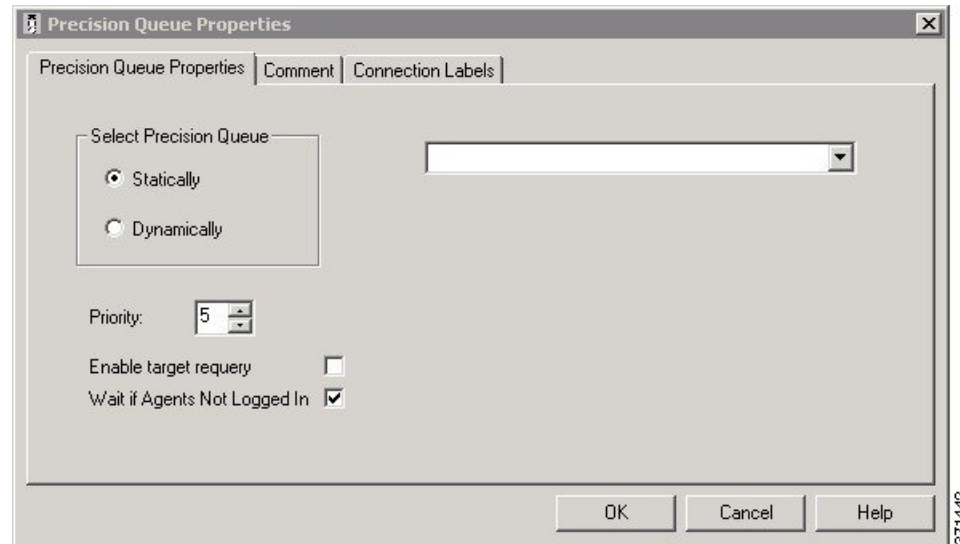
If more than one call is queued to a precision queue when an agent becomes available, the queued call with the lowest priority number is routed to the target first. For example, assume an agent in a precision queue becomes available and two calls are queued to that precision queue. If one call has priority 3 and the other has priority 5, the call with priority 3, the lower value, is routed to the precision queue while the other call continues to wait. If the priorities of the two calls are the same, then the call queued first is routed first.

VRU script instructions are not sent to the VRU. If a call enters the Precision Queue node and no resource is available, the call is queued to the precision queue and the node transfers the call to the default VRU, if the call is not already on a VRU. The script flow then exits immediately through the success branch and continues to a Run External Script node to instruct the VRU what to do while holding the call until an agent becomes available. Typically, this invokes a Network VRU script that plays music-on-hold, possibly interrupted on a regular basis with an announcement. The script flow can also use other queuing nodes to queue the same call to other targets, for example, Queue to Skill Group and Queue to Agent.

Precision Queue Properties Dialog Box - Static Precision Queue

The following list describes the **Precision Queue Properties** dialog box for a static precision queue script node.

Figure 51: Precision Queue Properties Dialog Box—Static Precision Queue



The following property is unique to static precision queues:

- **Drop-down list**—To route calls that enter this node to a static precision queue, you must select a precision queue from the list.

The following properties are common to static and dynamic precision queues:

- **Select Precision Queue** radio buttons—You can select one of the following options for each a precision queue:
 - **Statically**—Select this option to choose a single precision queue to be selected for all the calls that enter this node.
 - **Dynamically**—Select this option to select a precision queue on a call-by-call basis based on a formula.



Note The dynamic precision queue option is enabled only for System Administrators. For other users, this option is disabled.

- **Priority selection**—To select the initial queuing priority for calls processed through this node, you can select from 1 to 20. The default is 5.
- **Enable target requery check box**—To enable the requery feature for calls processed through this node, select this check box. When a requery occurs, for example if a call is presented to an available agent and the agent does not answer, the script continues through the failure terminal. The script can then inspect the call variable RequeryStatus to determine what to do next. The typical action in case of a No Answer

is to queue the call again to other precision queues, and increase the priority so that it is taken out of the queue before regular queued calls.

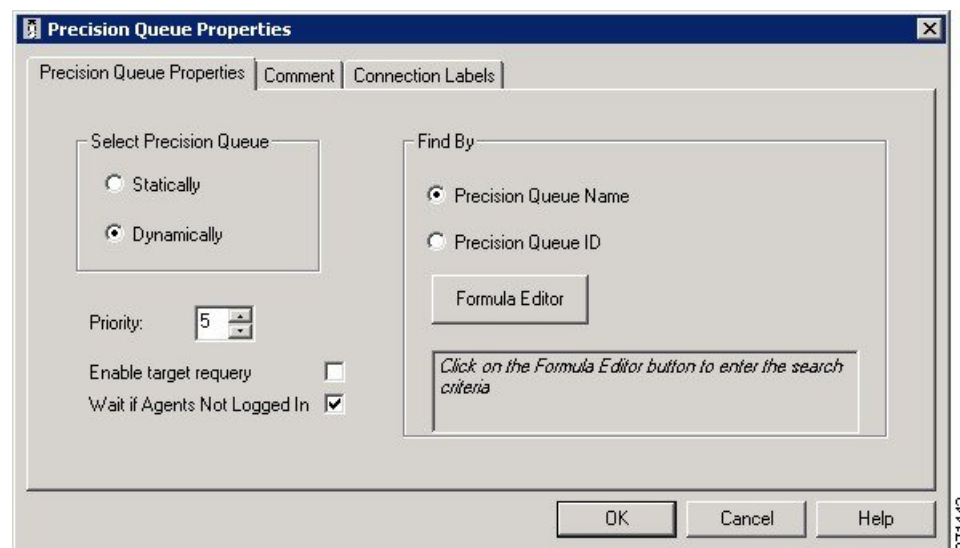
- **Wait if Agents Not Logged In check box** — When this check box is selected and the agents who are associated with a step are not logged in, then the router will wait for the time that is configured for that step. When this check box is not selected, the router will not wait on any step. However, on the last step, the router will wait indefinitely irrespective of the selection.

Precision Queue Properties Dialog Box - Dynamic Precision Queue

The following list describes the Precision Queue Properties dialog box for a dynamic precision queue script node.

Use dynamic precision queues when you want a single routing script for multiple precision queues (for example, when the overall call treatment does not vary from one precision queue to another). Dynamic precision queues can simplify and reduce the overall number of routing scripts in the system.

Figure 52: Precision Queue Properties Dialog Box—Dynamic Precision Queue



Note The dynamic precision queue option is enabled only for System Administrators. For other users, this option is disabled.

The following properties are unique to dynamic precision queues:

- **Find By radio buttons**—To dynamically route calls that enter this node to a Precision Queue name or ID, use the Find By radio buttons.
 - **Precision Queue Name radio**—Select this option to dynamically route calls that enter this node to a Precision Queue name.
 - **Precision Queue ID**—Select this option to dynamically route calls that enter this node to a Precision Queue ID.

- **Formula Editor button**—To determine to which Precision Queue name or ID to route calls that enter this node, click the Formula Editor button to create a formula. The formula is then evaluated at run time to select a precision queue by either name or by database ID. For example, you can use the formula "Call.PeripheralVariable4" to look up the Precision Queue if call variable 4 contained the Precision Queue name, as a result of a database lookup or from Unified CVP call processing.



Note The section on static precision queues describes the properties that are common to static and dynamic precision queues.

Queuing Behavior of the Precision Queue Node

Precision queues internally are configured with one or more time-based steps, each with a configured wait time. After a call is queued, the first step begins and the timer starts. This occurs although the path of the script exited the success node and a new node may be targeted (for example, Run Ext. Script).

If the timer for the first step expires, control moves to the second step (assuming one exists), and so on. As long as the call remains in queue and there are steps left to perform, the call internally continues to move between steps regardless of the path the call takes after it leaves the precision queue node. If a call is queued to two or more precision queues, the call internally walks through the steps for each precision queue in parallel. After the call reaches the last step on a precision queue, it remains queued on that step until the call is routed, abandoned, or ended.

If there is an update to the precision queue definition, then all queued calls in the precision queue are re-evaluated and are re-run from the first step.

For example, consider the wait time for an ongoing call at step 1 to be 1080 seconds, of which 1000 seconds has already elapsed. Now, suppose the wait time is changed to 900 seconds, then the wait time for this call is also reset to 900 seconds, even though only 80 more seconds are left to move to the next step.

Adjust Priority of a Call in a Queue

You can override the priority of a call in queue set by the Queue node by using the Queue Priority node (in the Queue tab of the Palette).

Figure 53: The Queue Priority Icon



For example:

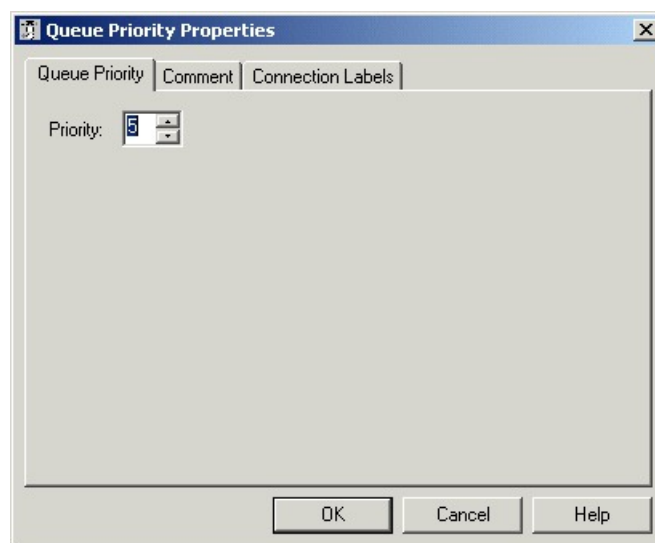
1. The original priority of the call in queue is set by the Queue to Skill Group node or the Precision Queue node.
2. The call waits in queue for 20 seconds while the caller listens to an announcement.
3. Call control passes to a second Wait node.
4. If 20 more seconds pass without an agent becoming available, the Queue Priority node is run and raises the call's priority in queue.

Notes:

- Only use the Queue Priority node after a Queue to Skill Group node or a Precision Queue node. Any subsequent use of the Queue to Skill Group node or the Precision Queue node results in setting the queue priority back to the original setting for that node.
- The Queue Priority node sets the priority for a call within all queues that the call is placed in. If a call requires the priority to be raised in one queue only, you should use a subsequent Queue to Skill Group or Precision Queue node for only that skill group/queue (with the new priority).
- Queuing priorities should be handled very carefully. Just increasing Queue priority does not get a call handled sooner. The effect depends on the other call in the queue. For example, if all calls are treated using the example above, the priority increase has no net effect. If the script above is only used for the Platinum customers while the Standard customers script leaves them at the default priority level, the effect is that all Platinum customers that have been in queue for more than 20 seconds are handled first regardless of other customers in queue. As the delay for Platinum customers is greater than 20 seconds, no Standard customers are handled ever. The solution is to increase the priority level for Standard customers as well, but only after they have been in queue for a longer period, for example 3 minutes.

Following is the Properties dialog box for the Queue Priority node:

Figure 54: Queue Priority Properties



Remove Call from a Queue

You can remove a call from any queues by using the Cancel Queuing node (in the Queue tab of the Palette).

Figure 55: The Cancel Queuing Icon



You do not have to define properties for the Cancel Queuing node. You can optionally add comments or connection labels.

Temporarily Halt Script Execution

You can halt script execution for a specified number of seconds by using the Wait node (in the Queue tab of the Palette).

Figure 56: The Wait Icon



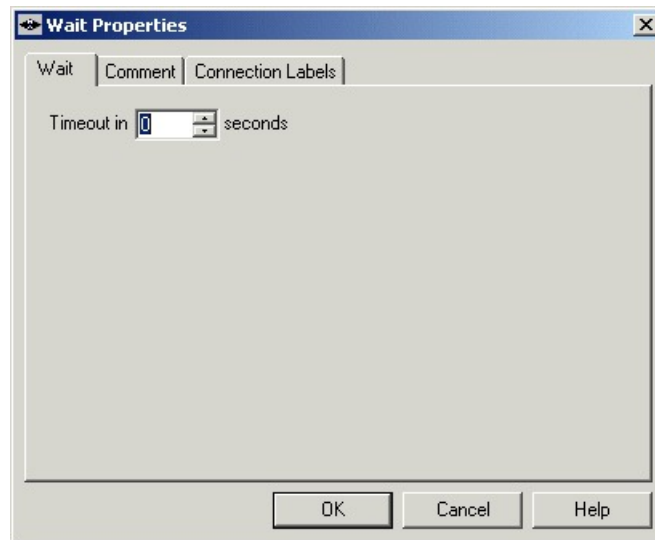
The Wait node simply stops script executing for the specified number of seconds. In the meantime, the Network VRU is waiting for instructions.



Warning You must set protocol time-out variables in Unified CVP to a value greater than the longest wait node used in the script.

Following is the Properties dialog box for the Wait node:

Figure 57: Wait Properties



Define Wait node properties as follows:

Procedure

- Step 1** In the Timeout in field, specify an interval to wait, in seconds.
- Step 2** Optionally, add comments or connection labels.



CHAPTER 11

Multichannel Routing

- [Overview of Multichannel Services, on page 469](#)
- [Enterprise Chat and Email, on page 469](#)
- [Task Routing, on page 470](#)
- [Media Routing Domains, on page 471](#)
- [Pick / Pull Node, on page 472](#)
- [Skill Group and Precision Queue Routing for Nonvoice Tasks, on page 473](#)
- [Queue to Agent Node, on page 474](#)
- [Change Queue to Agent Type, on page 474](#)
- [Specify an Agent Directly, on page 475](#)
- [Select an Agent by an Expression, on page 476](#)
- [RONA and Transfer Scripting for Task Routing, on page 478](#)
- [Estimated Wait Time Scripting for Task Routing, on page 478](#)
- [Example Universal Queue Scripts, on page 479](#)
- [Example Enterprise Chat and Email Scripts, on page 485](#)

Overview of Multichannel Services

When your system is integrated with multichannel features, you write routing scripts to route contacts that these features handle. Multichannel features include Enterprise Chat and Email, and third-party multichannel applications that use the Task Routing APIs.

Enterprise Chat and Email

You can configure CCE deployments with Enterprise Chat and Email to use independent media queues, in which an agent can handle tasks for a single media channel. You can also use Task Routing, in which an agent can handle tasks for several media channels.

Supported Route Requests for Enterprise Chat and Email

CCE supports the following types of multichannel route requests when integrated with Enterprise Chat and Email:

- **Web callback** - A web callback request is one that does not involve Enterprise Chat and Email. A customer clicks a button on a website that says, "Call me back." Then the caller and agent simply talk on the phone.
- **Text chat** - The caller and agent can conduct a text chat session when a telephone call is not desired or not possible. They can both chat and collaborate on the web.
- **E-mail message** - The customer and agent communicate using electronic mail.

Application Request Routing with Enterprise Chat and Email

Enterprise Chat and Email routes requests to the Media Routing Peripheral gateway (MR-PG). The Media Routing Peripheral Interface Manager (MR-PIM) on the MR-PG provides a generic interface to queue and route requests. The MR-PIM communicates with the CallRouter, which runs a routing script to determine how best to handle the request.

CCE uses a media class ID to identify the type of media or channel. A media class is a communication channel that is correlated to an application. Cisco_Voice is a predefined media class that is used for web and delayed callbacks requests and Packaged CCE inbound and outbound voice calls.

Each media class has at least one Media Routing Domain (MRD), which is a collection of skill groups associated with a medium. CCE uses the MRD to route a task to an agent who is associated with a skill group and a particular medium. Each MRD requires a Packaged CCE script, but it is possible to route requests from different MRDs using one script.

Synchronized Agents and Skill Groups for ECE

Agents are common across the multichannel software, but skill groups are application-specific. You can create agents using ECE or in contact center enterprise solutions and share the agents across applications. When agents or skill groups are created in ECE, they are simultaneously created in contact center enterprise solutions. If an agent is created in contact center enterprise solutions, you must enable the agent in ECE before the agent can work on those applications.

Only create, modify, or delete ECE skill groups in ECE. Skill groups are application-specific. When you create a skill group in ECE, the skill group is simultaneously created in the contact center enterprise solutions. But, you cannot enable that skill group in the core contact center enterprise applications.

Independent Media Queues for ECE

You can configure the multichannel software to route all media through independent queues that are defined by media class. You can configure agents to log in to only one media type to take either email, text chat, or voice. In this configuration, requests are queued only to agents who have signed in to the corresponding media application.

Task Routing

Task Routing describes the system's ability to route requests from different media channels to agents who work with customer contacts in multiple media. Routing scripts can send requests to agents based on business rules regardless of the media channel from which the request came. For example, based on an agent's skills

and current tasks, Unified CCE can route phone, chat, and email message requests to an agent who works with all these media. The agent can switch media on a task-by-task basis.

You can set up routing scripts so that multichannel tasks are assigned to the longest available agent in a skill group or precision queue in same Media Routing Domain as the task. You can also prioritize multichannel tasks using skill group and precision queue routing, as you would voice calls.

Media Routing Domains

Media Routing Domains (MRDs) organize how requests for each communication medium, such as voice and email, are routed to agents. For example, the Enterprise Chat and Email uses a Packaged CCE MRD to route a task to an agent who is associated with a skill group or precision queue and a particular channel.

For Enterprise Chat and Email, configure MRDs in Configuration Manager. For custom multichannel applications that use the Task Routing APIs, configure MRDs in Unified CCE Administration.

Media Routing Domains and Interruptibility

When you configure MRDs, you indicate whether tasks for the MRD are interruptible. If the MRD is not interruptible, an agent working on tasks for that MRD is not assigned tasks from other MRDs. If the MRD is interruptible, the agent may be assigned tasks from another MRD.

Typically, tasks in which the agent and customer interact synchronously, such as voice calls and chats, are not interruptible. Email messages are typically interruptible because contact with the customer is asynchronous. Therefore, an agent responding to an email message may be interrupted by a phone call or chat session.

Use Media Routing Domains to Categorize Contacts

You can categorize contacts based on the MRD of the route request.

For example, you can have different MRDs for email and chat. You can have a single script for both types of requests that branches so that it routes email messages and chats to different targets.



Note For multichannel tasks submitted by applications using the Task Routing APIs, Unified CCE determines the MRD based on the dialed number/script selector in the task request.

Use the **Media Routing Domain** node (in the Routing tab of the Palette).

Figure 58: MRD Domain Icon



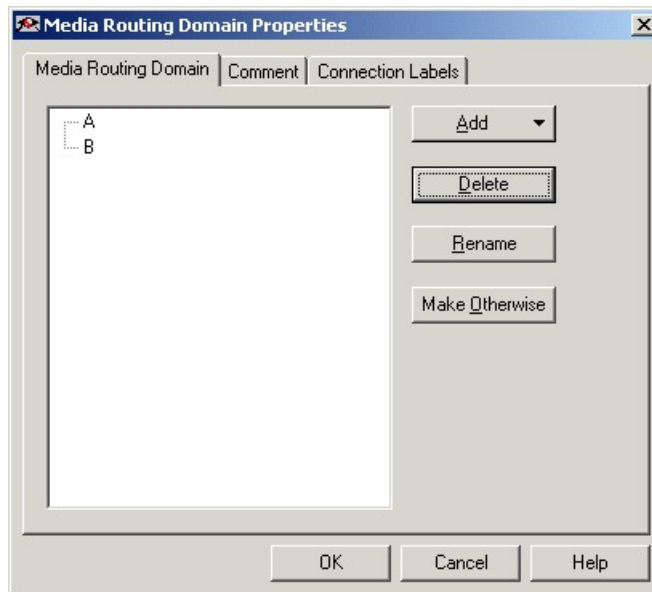
Insert targets and connections from the MRD node before you define the node's properties.



Note A branch can include multiple MRDs, but you can associate a single MRD with only one branch.

Following is the properties dialog box for the Media Routing Domain node:

Figure 59: Media Routing Domain Properties



Define Media Routing Domain node properties as follows:

Procedure

-
- Step 1** To associate an MRD with a branch, select the branch:
- a) Click **Add**.
 - b) Choose an MRD from the drop-down list.
- Step 2** To delete a branch, select it and click **Delete**.
- Step 3** To rename a branch, select it, click **Rename**, and type the new name.
- Step 4** You can define a branch as Otherwise by selecting the branch and clicking **Make Otherwise**. Execution follows this branch if none of the specified time ranges apply. You can specify only one Otherwise branch for the node.
-

Pick / Pull Node



The **Pick / Pull** node is available from the **Routing** tab **Object Palette**.

Pick / Pull node verifies that the route request is a valid pick or pull request for the specified MRD. The node checks that *serviceRequested* is one of the following:

- 4 = ROUTE_SERVICE_REQUEST_PICK_EXT_QUEUE
- 5 = ROUTE_SERVICE_REQUEST_PULL_EXT_QUEUE
- 6 = ROUTE_SERVICE_REQUEST_PICK_UCCE_AGENT

- 7 = ROUTE_SERVICE_REQUEST_TRANSFER_PICK

For these values, the script proceeds and terminates after the pick or pull is completed. For any other value of *serviceRequested*, the request flows through the node's failure branch. Check the error code in *VRUStatus*.

The node provides real-time monitoring of the following:

- Pick successes.
- Pull successes.
- Pick errors.
- Pull errors.

The following meters are applicable for the Pick/Pull node.

- Pick meter - Displays the number of nonvoice task pick requests that were successful.
- Pull meter - Displays the number of nonvoice task pull requests that were successful.
- Pick error meter - Displays the number of nonvoice task pick requests that failed.
- Pull error meter - Displays the number of nonvoice task pull requests that failed.



Note All **Pick / Pull** routing works for agents in the **Ready** or **Available** state. To be able to do this in **Not Ready** state, enable the Registry key. The Registry key that needs to be enabled on the CCE Router is `EnablePickPullWhileInNotReady`. This is located under the following registry hive on the CCE Router VM

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco  
Systems, Inc.\ICM\ucce\RouterA\Router\CurrentVersion\Configuration\Config.
```

The Registry key is dynamic and doesn't require a restart of the router, for changes to take effect. The default value is 0 or disabled. To enable the Registry key, set the value to 1.

Skill Group and Precision Queue Routing for Nonvoice Tasks

Routing to skill groups and precision queues is largely the same for voice calls and nonvoice tasks. However, the way that contact center enterprise distributes tasks has the following implications for agents who can handle multiple concurrent tasks:

- **Precision queues**—In precision queue routing, Unified CCE assigns tasks to agents in order of the precision queue steps. Unified CCE assigns tasks to agents who match the attributes for step one, up to their task limit, until all those agents are busy. Unified CCE then assigns tasks to agents who match attributes for step two, and so on. If you configure agents to handle three concurrent tasks, Unified CCE assigns three tasks to each agent in the first step. It then moves on to the second step and assigns any remaining tasks to those agents.
- **Overflow skill groups**—Routing scripts can specify a preferred skill group and an overflow skill group. Unified CCE assigns tasks to all agents in the preferred skill group, up to their task limit, before assigning any tasks in the overflow skill group. If you configure agents to handle three concurrent tasks, Unified CCE assigns three tasks to each agent in the preferred skill group. It then moves on to the overflow skill group and assigns any remaining tasks to those agents.



Note The number of available slots is an important factor in the Longest Available Agent (LAA) calculation.

The number of available slots = The maximum concurrent task limit for the MRD that an Agent has logged into - Current tasks being handled by the Agent or routed to the Agent.

If there are multiple skill groups that are part of the queue node, then the skill group that has the higher LAA is picked. Then, the agents within the picked skill group (or the Precision Queue) who have the highest number of available slots for non-voice tasks get prioritised.

Agents with the same number of available slots get prioritized based on the time in the available state or the LAA mechanism.

Related Topics

[Scripts for Precision Queues](#), on page 505

[Selection of Agents from Skill Groups](#), on page 479

[Categorization by Media Routing Domain with Skill Groups](#), on page 480

[Categorization by Media Routing Domain with Precision Queues](#), on page 481

Queue to Agent Node

You can queue a contact directly to an agent by using the **Queue to Agent** node (in the Queue tab of the Palette).



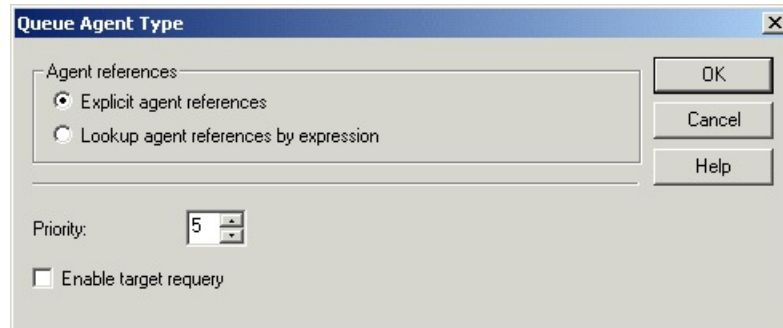
You can change the **Queue to Agent** type to:

- Specify an agent directly
- Select an agent by expression

Change Queue to Agent Type

Procedure

Step 1 In the **Queue to Agent** properties dialog box, click **Change**. The **Queue Agent Type** dialog box opens:

Figure 60: Queue Agent Type

- Step 2** To select a specific agent, select **Explicit agent references**.
 - Step 3** To select and agent by an expression, select **Lookup agent references by expression**.
 - Step 4** Select a **Priority** between 1 (the highest) and 20 (the lowest).
 - Step 5** Optionally, select **Enable target requery**.
-

Specify an Agent Directly

Following is the properties dialog box of the **Queue to Agent** node when you select to specify agents directly:

Figure 61: Agent Direct Properties

Queue to Agent Properties

Queue to Agent | Connection Labels

Queue to Agent type
Select using direct references.

	Agent	Media Routing Do	Skill Group	Route
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				

Queue if agent not logged in

Buttons: Add Target..., Delete Row, Validate, Formula Editor..., Move (up/down arrows), OK, Cancel, Help

To specify agents directly:

Procedure

-
- Step 1** If necessary, change the Queue to Agent type to **Explicit agent references**.
 - Step 2** In the **Agent** column, select an agent.
 - Step 3** In the **Media Routing Domain** column, select the media routing domain for the selected agent.
 - Step 4** In the **Skill Group** column, select the skill group for the selected agent and media routing domain.
 - Step 5** In the **Route** column, select the route for the selected agent and media routing domain.
 - Step 6** Optionally, select **Queue if agent not logged in**, to have the contact queued to the agent even if the agent is not currently logged in.
 - Step 7** To test the data you entered, click **Validate**.
 - Step 8** Optionally, modify **Connection Labels**.
-

Select an Agent by an Expression

Following is the properties dialog box of the **Queue to Agent** node when you select to use an expression:

Figure 62: Queue to Agent Properties

Queue to Agent Properties

Queue to Agent | Connection Labels

Queue to Agent type
Select using indirect references.
Target Requery Disabled

	Peripheral	Agent Expressio	Consider If	Enterprise Skill G	Enterprise Route	Route
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						

Queue if agent not logged in

Buttons: Add Target..., Delete Row, Validate, Formula Editor..., Move (up/down), OK, Cancel, Help

To specify agents by expression:

Procedure

- Step 1** If necessary, change the **Queue to Agent** type to **Lookup agent references by expression**.
- Step 2** In the **Peripheral** column, to choose an agent by Peripheral number, choose a peripheral and provide a formula in the Agent Expression that translates to the Agent's Peripheral number. If no peripheral is chosen, the agent expression should translate to the SkillTargetID or Enterprise Name of the agent.
- Step 3** In the **Agent Expression** column, provide a formula using the formula editor that translates to the agent's Peripheral number or SkillTargetID or agent Enterprise Name. To choose a peripheral (in Peripheral) and provide a formula that translates to an agent's Peripheral number.
- Note** The Peripheral column controls how the AgentExpression column is evaluated as an ICM ID. However, if you select a Peripheral from the Peripheral column, then the Agent Expression column is evaluated as an Agent Peripheral number.
- Step 4** Optionally, in the **Consider if** column, enter the formula that evaluates to true for the target when the ICM system runs the Queue to Agent node, or that target will not be selected. For help in creating a formula, put the cursor in this field and then click the **Formula Editor** button.
- Step 5** Optionally, select the **Enterprise Skill Group** that includes the appropriate skill groups to cover all media routing domain cases for the selected Agent.
- Step 6** Optionally, select the **Enterprise Route** that has an appropriate collection of routes, or the **Route**, matching the agent and media routing domain.

- Step 7** Optionally, select **Queue if agent not logged in**, to have the contact queued to the agent even if the agent is not currently logged in.
- Step 8** To test the data you entered, click **Validate**.
- Step 9** Optionally, modify connection labels.
-

RONA and Transfer Scripting for Task Routing



Note This section applies to tasks submitted by third-party multichannel applications that use the Task Routing APIs.

The *ServiceRequested* call variable is set when tasks are transferred or RONA. You can determine the value of the *ServiceRequested* call variable in an **If** node in the routing script. Based on the value of this field, the script can take different actions. For example, the script can raise the priority of the task so that it goes to the front of the queue.

The relevant *ServiceRequested* values are:

- 2: This value identifies a transferred task.
- 3: This value identifies a RONA task.

Related Topics

[RONA and Transfer Script](#), on page 482

Estimated Wait Time Scripting for Task Routing



Note This section applies to tasks submitted by third-party multichannel applications that use the Task Routing APIs.

Customers submitting a task request might want to know approximately how long they will wait for an agent. You can configure the routing script to provide the customer with an estimate of the wait time. The estimated wait time is calculated once, when the task enters the queue. The time is not updated as the position in the queue changes.

The default estimated wait time algorithm is based on a running five minute window of the rate of tasks leaving the queue. Any tasks that are routed or abandoned during the previous 5 minutes are considered as part of the rate leaving queue. For Precision Queues, the rate leaving the queue represents the rate at which tasks are delivered or abandoned from the entire precision queue, not any individual Precision Queue steps. The algorithm computes the wait time for each of the queues against which the task is queued (Skill Groups or Precision Queues) and then returns the minimum estimated wait time.



Note Queue to Agent is not supported.

While the queue builds, the small number of tasks in the queue makes the estimated wait time less accurate and the value fluctuates rapidly. As the queue operates with more tasks over time, the estimated wait time is more accurate and consistent.

Scripts for estimated wait time include:

- A **Set Variable** node, `Call.EstimatedWaitTime` to set the estimated wait time.
- A **Run External Script** node to apply a Network VRU script that returns the estimated wait time to the customer.

Related Topics

[Estimated Wait Time Script](#), on page 483

Example Universal Queue Scripts

You can design scripts to route contacts from different media in a Universal Queue environment.

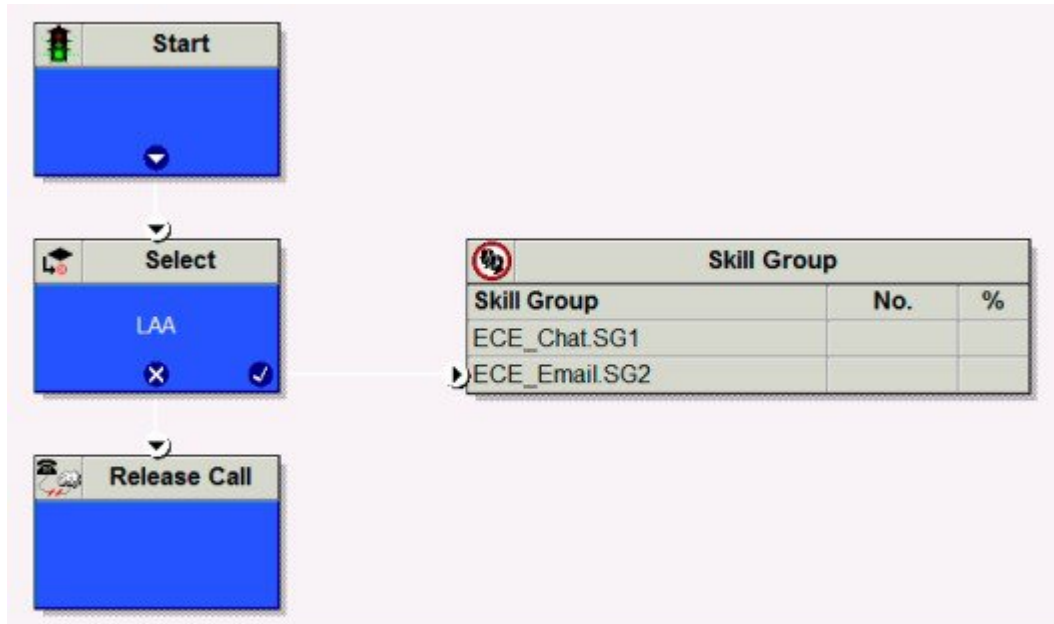
These scripts are only examples; your company's needs may differ.

For more information about Task Routing with third-party multichannel applications or Enterprise Chat and Email, see the *Cisco Packaged Contact Center Enterprise Features Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html>.

Selection of Agents from Skill Groups

The following script example shows how contacts from different channels can be routed to the Longest Available Agents in skill groups that are specific to the different channels:

Figure 63: Selecting Agents from Skill Groups

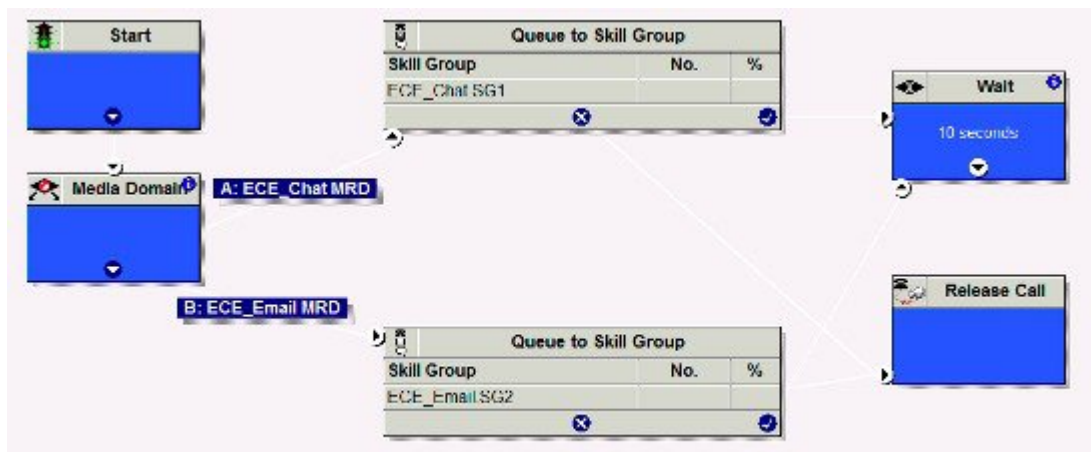


You schedule this script to run for Call Types associated with contacts from the different channels. The script then selects the Longest Available Agent from the skill group in the Media Routing Domain for that channel. The agents may be logged in to different Media Routing Domains and working with contacts from different channels; the Router determines an agent's availability across channels.

Categorization by Media Routing Domain with Skill Groups

The following script example shows how contacts can be categorized by Media Routing Domain, then queued to skill groups specific to that Media Routing Domain:

Figure 64: Categorizing by MRD with Skill Groups

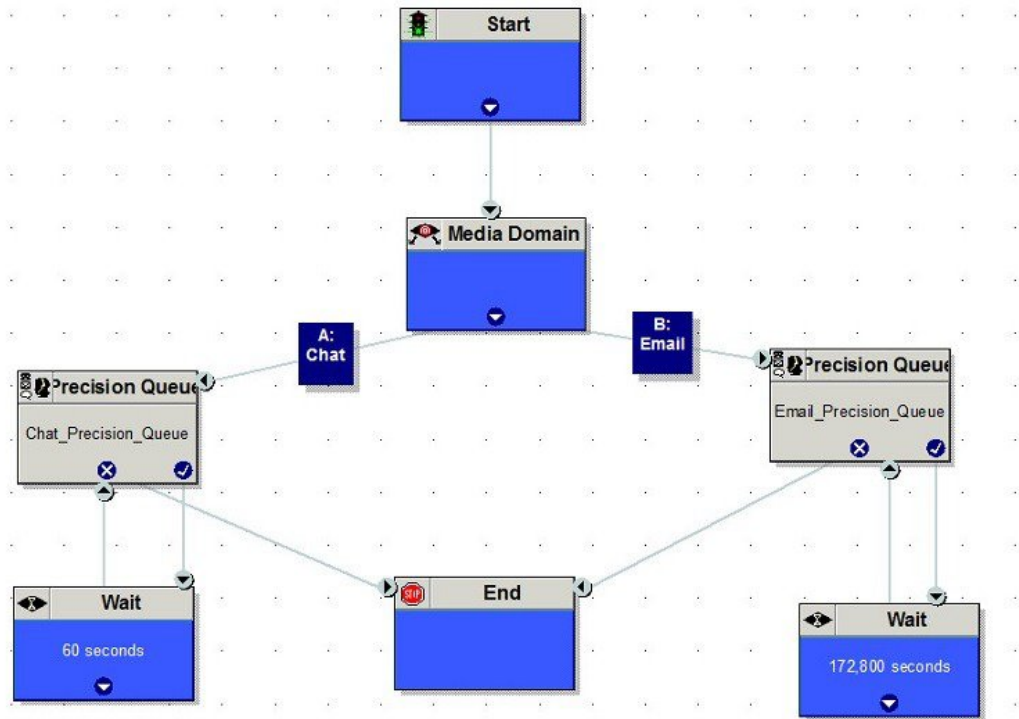


You would schedule this script to run for Call Types associated with contacts from the different channels. The script then uses the Media Routing Domain node to detect the MRD of the contact and branches to a Queue to Skill Group node that specifies skill groups specific to that MRD.

Categorization by Media Routing Domain with Precision Queues

The following script example shows how contacts can be categorized by Media Routing Domain, then queued to precision queues specific to that Media Routing Domain:

Figure 65: Categorizing by MRD with Precision Queues

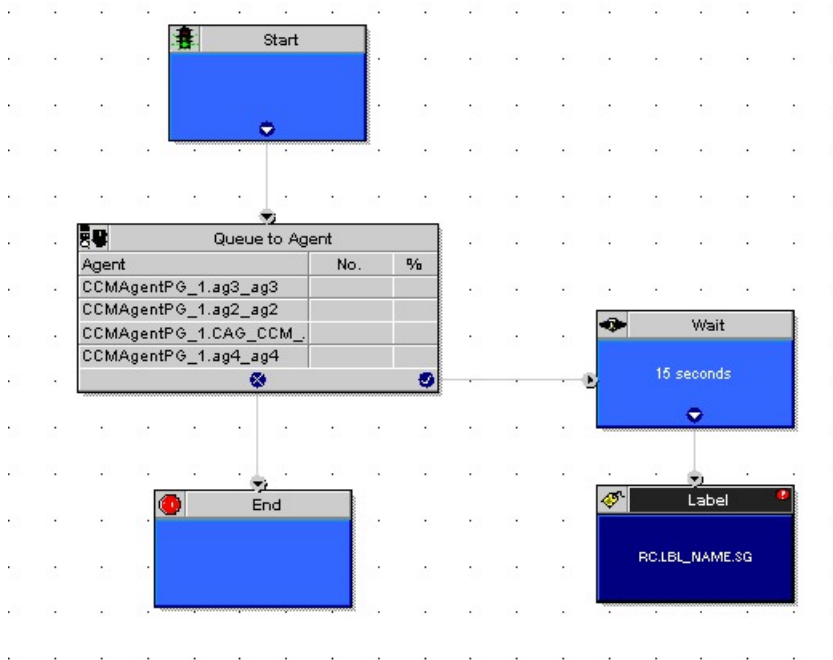


You would schedule this script to run for Call Types associated with contacts from the different channels. The script then uses the Media Routing Domain node to detect the MRD of the contact and branches to a Queue to Precision Queue node that a precision queue specific to that MRD.

Script That Queues to Agents

The following script example shows how contacts from different channels can be queued to agents:

Figure 66: Queuing to Agents

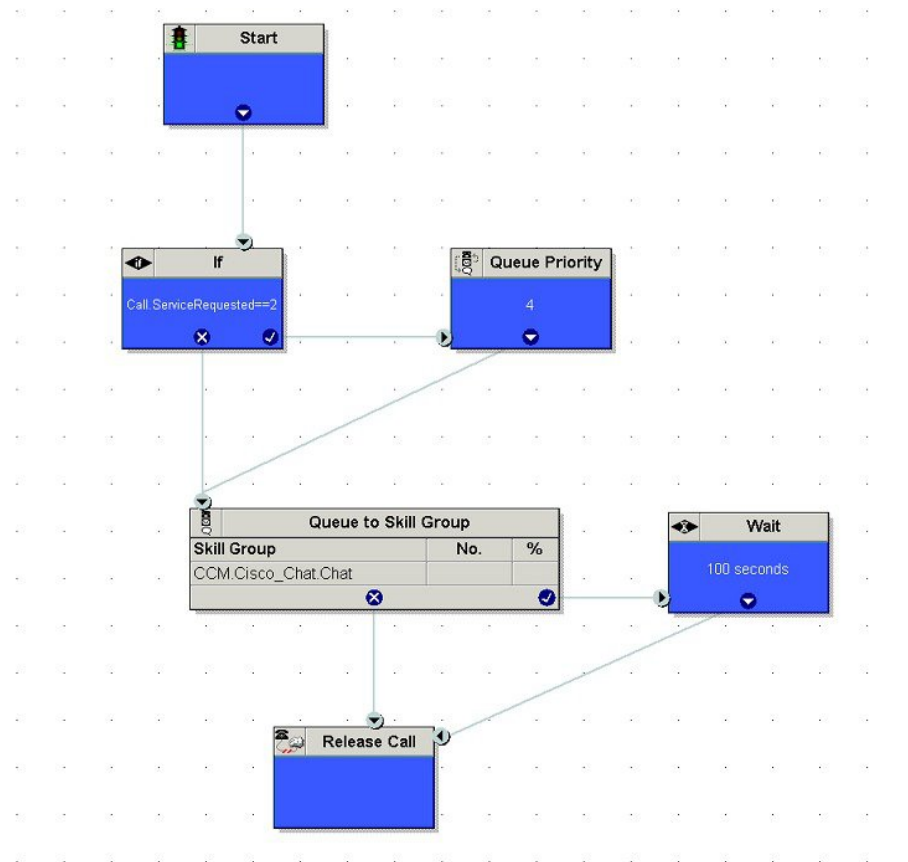


You would schedule this script to run for Call Types associated with contacts from the different channels. In the Queue to Agent node, each row defined for an agent also contains a Media Routing Domain selection. The script queues the contact to the agent with the selected MRD that matches the MRD of the contact.

RONA and Transfer Script

This example only applies to tasks submitted by third-party multichannel applications that use the Task Routing APIs. This example script shows the call priority increase if the service requested is 2 (TRANSFER).

Figure 67: Example RONA and Transfer Script



If the Call ServiceRequested call variable is set to 2 (TRANSFER) the call enters the Queue Priority node. The Queue Priority of the call is increased so that it is handled before any other calls in the queue. The Queue Priority node sends the call to the Queue to Skill Group node. If the Call ServiceRequested call variable is not set to 2 (TRANSFER), the call enters the Queue to Skill Group node.

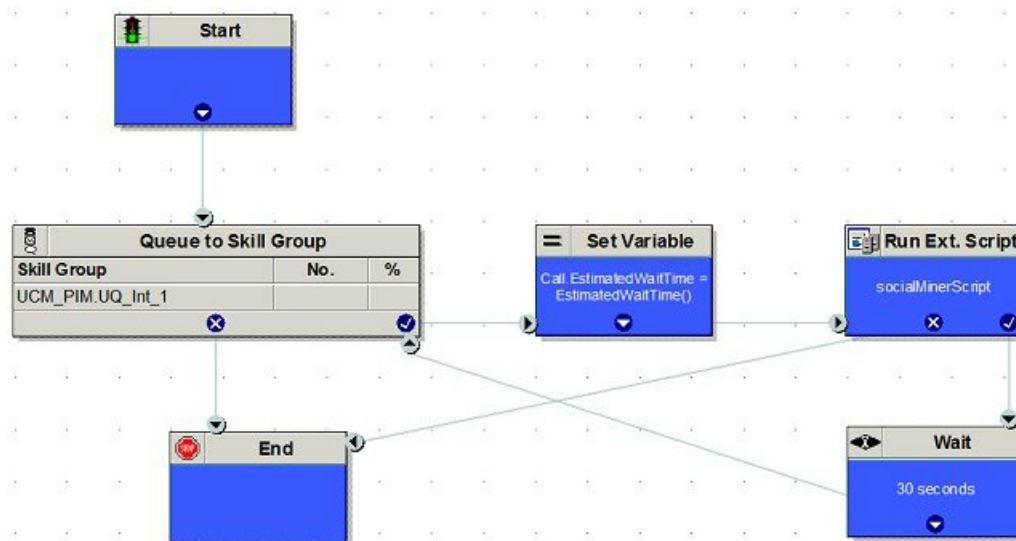
Estimated Wait Time Script

This example only applies to tasks submitted by third-party multichannel applications that use the Task Routing APIs.

Scripts for estimated wait time include:

- A Set Variable Node to set the estimated wait time.
- A Run External Script node to apply a Network VRU script that returns the estimated wait time to the customer.

Figure 68: Example Estimated Wait Time Script



Set Variable (Call.Estimated Wait Time) node: Set the estimated wait time as follows:

1. From the Set Variable node, select **Call** from the Object type drop-down menu.
2. From the Variable drop-down menu, choose **Estimated Wait Time()**.

You can then work with the Formula Editor to use the default estimated wait value or create a formula and use your own value.

3. Click **Formula Editor**, and do either of the following:
 - To use the default estimated wait value, click the Built-In Functions tab and choose EstimatedWaitTime()
 - To create a formula and use your own value, click the Variables tab and choose an entry in the Object type list and an entry in the Object list. Then double-click a variable in the Variable list.

Run Ext Script node: Apply the Network VRU script as follows:

1. Click the Queue tab.
2. Click **Run External Script**.
3. Click inside the script. A Run External Script node appears.
4. Double-click the node and choose the Network VRU script from the list; then click **OK**.

The call variable Estimated Wait Time now contains a value in the EstimatedWaitTime field and can be passed to peripherals.

Note that a Run External Script node is required to send the EstimatedWaitTime to SocialMiner.

Example Enterprise Chat and Email Scripts

For example Enterprise Chat and Email scripts, see the *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html>.



CHAPTER 12

Use of Formulas

- [Formula Usage, on page 487](#)
- [Formula Example, on page 487](#)
- [Variables, on page 487](#)
- [Operators, on page 496](#)
- [Built-in Functions, on page 499](#)
- [Custom Functions, on page 502](#)

Formula Usage

You can use formulas in many routing nodes to both categorize contacts and select routing targets.

A formula consists of one or more expressions that Packaged CCE evaluates to produce a value that it can use for subsequent script processing. You define expressions—made up of variables, constants, operators, and functions—as part of custom selection rules or distribution criteria in scripts.

Formula Example

This is an example of a simple formula:

```
CallerEnteredDigits == 1
```

In this example:

- The left value, *CallerEnteredDigits*, is a variable. More specifically, it is a call control variable.
- The operator is the "Equal To" equality operator.
- The right value is the number 1.

If the value of *CallerEnteredDigits* is 1, the formula returns true; otherwise, the formula returns false.

Variables

A variable is a named object that holds a value. You use variables in formulas to select targets and help in call tracking.

Variable Syntax

Following is the syntax for using a variable in a formula:

object-type.object-name.variable-name

Where:

- The object-type is an object category, such as SkillGroup.
- The object-name is the name of an object contained in Packaged CCE database, such as the name of a skill group (for example, BosSales).
- The variable-name is the name of an object that can hold a value, such as call information for the skill group; for example, (CallsInProgress).
- Each component in the variable is separated by a period (.).



Note Passing of internationalized characters through Media Routing interface is not supported. The application that interacts with ICM through the Media Routing interface must send any call related data in English only.

Single-Target Variables

A single-target variable examines data for one specified routing target. For example, the variable:

SkillGroup.BosSales.CallsInProgress: Examines the number of calls in progress for the BosSales skill group.

Multiple-Target Variables

A multiple-target variable examines data across multiple routing targets. For example, the function:

Max(SkillGroup..LongestAvailable)*: Finds the skill group, from all skill groups defined in the target set for the script node that calls the function, with the longest available agent.

You use an asterisk (*) as the object-name value to indicate that the variable is to examine data across multiple targets.

Call Control Variables

Call control variables provide information about the current contact that is being routed by the script. Call control variables include information about where the route request came from, contact classification data, and data to be passed to the peripheral that receives the contact.

Variable	Data Type	Description	Can be Set by the User
CallerEnteredDigits	String	Digits caller entered in response to prompts.	Yes
CallingLineID	String	Billing telephone number of the caller.	No
DialedNumberString	String	Telephone number dialed by the caller.	No

Variable	Data Type	Description	Can be Set by the User
ExpCallVarName	String	Expanded Call Context (ECC) variable value assigned in scripts and passed with contact.	Yes
PeripheralVariable1- PeripheralVariable10	String	Values passed to and from the peripheral.	Yes
RequeryStatus	Integer	Provides the ability to test the error path of the Label, Queue, RouteSelect, and Select nodes to determine the specific network cause of failure and conditionally retry the attempt as necessary.	No
RouterCallDay	Integer	An encoded value that indicates the date on which Packaged CCE processes the call.	No
RouterCallKey	Integer	A value that is unique among all calls Packaged CCE has processed since midnight. RouterCallDay and RouterCallKey combine to form a unique call identifier.	No
RoutingClient	String	The name of the routing client that made the route request.	No
TimeInQueue	Integer	Number of seconds a call has been queued.	No
UserToUserInfo	String	ISDN private network User to User information	Yes
VruStatus	Integer	Indicates the result of a previous VRU node.	No
CallGUID	varchar (32)	Globally unique call identifier.	No
LocationParamName	varchar(50)	Location name.	No
PstnTrunkGroupID	varchar(32)	The Trunk Group ID on which the call arrived on IOS Gateway.	No
PstnTrunkGroupChannelNumber	Integer	The Trunk Group Channel Number on which the call arrived on IOS Gateway.	No
SIPHeader	varchar(255)	Specific header information extracted from a SIP call that arrives at Unified CVP (or VRU).	Yes



Note The Call Variables can be used in a "SET" node in an Admin Script as temporary placeholders for complex calculation. However, because any call context is only existent as long as the call itself, the Variables cease to exist after the Route Request (a.k.a Call) is complete (be it by virtue of a successful Routing Script Execute Completion or an Administrative Script Execute Completion). They cannot be used to store values, so as to be re-used in Routing Scripts, as the Routing Scripts themselves will have a new set of CallVariables created for the Route Request.



Note When comparing two Call Variables of Numeric string, you must use the Built-In Function "value()" in the IF Node to perform Numeric comparison, otherwise there is a String comparison. Example: `value(Call.PeripheralVariable1)>=value(Call.PeripheralVariable2)` where Call.PeripheralVariable1 and Call.PeripheralVariable2 are given as Numeric string.

Expanded Call Variables

Expanded call variables store values associated with the contact.

Expanded call values are written to Termination Call Detail records only if, and when, an ECC value is explicitly set. You can set the variables in several ways, such as using a script, a Unified CVP, CTI, and so on. This applies to null values as well as non-null values.

If an expanded call variable is defined, but never assigned a value, it does not have a row in the Termination Call Variable table when a Termination Call Detail record is written.

The Latin 1 Character set is supported for expanded call context variables and peripheral call variables when used with Unified CVP, Cisco Finesse, and Cisco SocialMiner, among others.

The use of multi-byte character sets is also supported in limited usage for ECC and peripheral call variables, when:

- Setting them in the Script Editor using double quotes.
- Stored in Termination Call Variables with an appropriate SQL collation.
- Setting and receiving them through CTI OS desktops.

Expanded call values are generally passed from leg to leg on the call. After a value is assigned, the value is recorded in the Termination Call Variable for every Termination Call Detail Segment. However, this depends on how each new call segment is created.

The solution comes with some predefined expanded call variables. You can create others through the Unified CCE Administration tool.

ECC Payloads

You can define as many ECC variables as necessary. But, you can only pass 2000 bytes of ECC variables on a specific interface at any one time. To aid you in organizing ECC variables for specific purposes, the solution has *ECC payloads*.

An ECC payload is a defined set of ECC variables with a maximum size of 2000 bytes. You can create ECC payloads to suit the necessary information for a given operation. You can include a specific ECC variable in multiple ECC payloads. The particular ECC variables in a given ECC payload are called its *members*.



Note For ECC payloads to a CTI client, the size limit is 2000 bytes plus an extra 500 bytes for the ECC variable names. Unlike other interfaces, the CTI message includes ECC variable names.

In certain cases, mainly when using APIs, you might create an ECC payload that exceeds the CTI Server message size limit. If you use such an ECC payload in a client request, the CTI Server rejects the request. For an OPC message with such an ECC payload, the CTI Server sends the message without the ECC data. In this case, the following event is logged, “CTI Server was unable to forward ECC variables due to an overflow condition.”

You can use several ECC payloads in the same call flow, but only one ECC payload has scope at a given moment. TCDs and RCDs record the ID of the ECC payload that had scope during that leg of the call. The *Call.ECCPayloadID* variable contains the ID of the ECC payload which currently has scope.

In solutions that only use the default ECC payload, the system does not create an ECC variable that exceeds the 2000-byte limit for an ECC payload or the 2500-byte CTI Message Size limit.



Note Packaged CCE 2000 Agent deployment allows you to use only the default ECC payload for the Network VRU.

If you create another ECC payload, the system no longer checks the 2000-byte limit when creating ECC variables. The system creates the ECC variables without assigning them to an ECC payload. Assign the new ECC variable to an appropriate ECC payload yourself through the ECC Payload Tool.

You can create and modify ECC payloads in the **Configuration Manager > List Tools > Expanded Call Variable Payload List** tool. In Packaged CCE 4000 Agent and 12000 Agent deployments, you can assign an ECC payload to Network VRU using the Network VRU Explorer tool in Configuration Manager.

Default ECC Payload

The solution includes an ECC payload named "Default" for backward compatibility. If your solution does not require more ECC variable space, you only need the Default payload. The solution uses the Default payload unless you override it.

If your solution only has the Default payload, the solution automatically adds any new ECC variables to the Default payload until it reaches the 2000-byte limit.



Note You cannot delete the Default payload. But, you can change its members.



Important During upgrades, when the system first migrates your existing ECC variables to the Default payload, it does not check the CTI message size limit. The member names might exceed the extra 500 bytes that is allocated for ECC payloads to a CTI client. Manually check the **CTI Message Size** counter in the **Expanded Call Variable Payload List** tool to ensure that the Default payload does not exceed the limit. If the Default payload exceeds the limit, modify it to meet the limit.

In a fresh install, the Default payload includes the predefined system ECC variables. In an upgrade, the Default payload's contents depend on whether the starting release supports ECC payloads:

- **ECC payloads not supported**—During the upgrade, a script adds your existing ECC variables to the Default payload.
- **ECC payloads are supported**—The upgrade brings forward the existing definition of your Default payload.



Note If your solution includes PGs from a previous release that does not support ECC payloads, the Router always sends the Default payload to those PGs. Those PGs can properly handle the Default payload.

ECC Payload Node

The **ECC Payload** node is available from the **General** tab on the **Object Palette**:

Figure 69: Payload icon



Use this node to change the ECC payload that has scope for the following part of your script. Once you select an ECC payload, it has scope for all non-VRU operations until changed. You can select the ECC payload either statically or dynamically by the payload's EnterpriseName or ID.

Persistent vs. Non-persistent Call Variables

When Packaged CCE writes call data records to its historical database, it can store the values of all call variables. Storing excessive call variable data can degrade historical database performance. When you define a call variable (using the Expanded Call Variables gadget in the Unified CCE Administration web tool), you can tag it as either *persistent* or *non-persistent*. Only persistent call variables are written to the historical database. You can use non-persistent variables in routing scripts, but they are not written to the database.

User Variables

User variables are variables you create to serve as temporary storage for values you can test with an **If** node. For example, you could create a user variable called `usertemp` to serve as a temporary storage area for a string value used by an If node.

You create user variables through the Unified CCE Administration tool.

Each user variable must:

- Have a name that begins with `user`.
- Be associated with an object type, for example, skill group. (This enables the Packaged CCE to maintain an instance of that variable for each object of that type in the system.)
- Store a value up to 40 characters long.

After you have define a variable, you can use the Formula Editor to access the variable and reference it in expressions, just as you would with a built-in variable.

Set Variable Node Usage

Figure 70: Set Properties Window

You can set the value of a variable with the Set Variable node:

- Object type - Choose the type of object the variable is associated with.
- Object - Choose the specific object the variable is associated with.



Note If you choose Call as the Object Type, this field does not apply.

- Variable - The specific variable you want to set.



Note The variables that are available are determined by the value you choose in the Object Type field.



Note Define all integer fields in tables accessed by a Set Variables node as NOT NULL.

- Array index - Enter an integer or an expression that evaluates to an integer. For example, if the Array Index expression evaluates to 2, then the Set Variable node sets the second element of the variable array.



Note This field is only available if you select an array variable in the Variable field.

- Value - Enter the value to assign to the variable. The value can be:
 - A constant
 - A reference to another variable
 - An expression

SkillGroup.Avail and SkillGroup.ICMAvailable Variables

When the Packaged CCE system includes only the voice channel, the value of the SkillGroup.Avail variable is the number of agents in the available state, meaning that the agents are able to accept new calls.

However, when the web or e-mail channel is used with non-voice Media Routing Domains and agents log in to multiple domains, the value of the SkillGroup.Avail variable is calculated differently. There is also a SkillGroup.ICMAvail variable.

The following table describes the difference between the SkillGroup.Avail and the SkillGroup.ICMAvail variables:

Case	SkillGroup.Avail	SkillGroup.ICMAvailable
Only voice domain is used	Number of agents in the Available state.	Same
Multiple Domains are used	Number of agents in the Available state, regardless of what they may be doing in this or other domains.	Number of agents who can actually handle an additional task or call in the domain.

SkillGroup.ICMAvailable Variable

The value of the SkillGroup.ICMAvailable variable is the actual number of agents logged in to the skill group who can take new calls or tasks. Such agents must meet all the following criteria:

1. They are routable in the domain.
2. The agent's state in the domain is something other than "Not-Ready".
3. The agent is below the maximum task limit.



Note For most domains (that is, if the agent is not a Enterprise Chat and Email Multi-session agent), the maximum task limit is 1, and an agent is below the maximum only when the agent is not working on any call or task.

4. The agent is not working on another task in a non-interruptible domain.

SkillGroup.Avail Variable

SkillGroup.Avail is the number of agents in the skill group who are not doing anything in the domain. An agent who is logged in to two domains can be counted as Avail in one domain even though that agent is handling a task in another non-interruptible domain. An agent in a domain that handles multiple tasks (such

as chat) is not counted as Avail if that agent is handling a task, even though the agent has additional capacity for more tasks.

The following table shows some possible values for these variables. Assume three agents are logged in to a voice skill group, and the same three agents are also logged in to another non-interruptible domain, such as a chat domain. This table shows the voice skill group states and the number of agents available in that state.

Case	SkillGroup.Avail	SkillGroup.ICMAvailable
Initial state	3	3
First agent handles a call	2	2
Second agent handles a chat session	2 (because there are two agents doing nothing in the domain)	1 (because there is only one agent left to handle voice calls)
Voice call ends	3	2
Chat ends	3	3

If a routing script needs to check the number of available agents, using SkillGroup.Avail produces effective results as it uses an extrapolation mechanism in determining the available agent.

Following is another example showing agents handling non-interruptible chat tasks. Assume three agents are logged in to a chat skill group, each allowed to handle two chats. This table shows states for the chat skill group.

Case	SkillGroup.Avail	SkillGroup.TalkingIn	SkillGroup.ICMAvailable
Initial state	3	0	3
First agent handles a chat session	2 (because the agent is now in the talking state)	1	3 (because all three agents can still handle additional chats)
Second agent handles a chat session	1	2	3
Third agent handles a chat session	0	3	3
First agent handles second chat session	0	3 (even though a total of 4 chats are in progress, only 3 agents are doing the work)	2 (because only the second and third agents can handle an additional chat)

By default, Script Editor shows the ICMAvailable value instead of Avail value when displaying skill group real-time data.

Closed Variables

Closed variables are available for use for skill groups, peripherals, and Media Routing Domains. Closed variables allow administration scripts to turn dequeuing to these objects on and off. The Closed variables

default to 0, meaning that the object is open. A script (usually an administration script) can change the state of the Closed variables.

If a Closed flag is set to a non-zero integer, then calls are not dequeued to affected agents, regardless of their state.

When closed variables are set to zero, the queued calls do not go to the available agents immediately, and continue to be in the queue. When the agent state changes from "Not Ready" to "Ready" state, the new calls are sent to the available agents (agents in the "Ready" state) only, and not the queued calls.

Operators

Operator Precedence

The following table shows the order in which operators are evaluated.



Note The operators with priority 1 are evaluated first, then those with priority 2, and so on. The order of evaluation within each priority level can also be important. Prefix operators are evaluated from right-to-left in an expression. Assignment operators are also evaluated from right-to-left. In all other cases where operators have equal priority, they are evaluated left-to-right.

Priority	Operator type	Operators
1	Prefix (unary)	+ - ! ~
2	Multiplication and division	* /
3	Addition and subtraction	+ -
4	Shift right and shift left	>> <<
5	Relational	< > <= >=
6	Equality	== !=
7	Bitwise And	&
8	Bitwise exclusive Or	^
9	Bitwise inclusive Or	
10	And	&&
11	Or	
12	Conditional	?
13	Sequential	,

Prefix Operators

The Prefix Operators in the following table take a single operand:

Operator	Meaning	Comments/Examples
+	Positive	Numeric values are positive by default, so the positive operator (+) is optional. Example: 2 and +2 represent the same value.
-	Negative	The negative operator (-) changes the sign of a value. Example: 2 represents a positive value; -2 represents a negative value.
!	Logical negation	A logical expression is any expression that evaluates to true or false. The logical negation operator (!) changes the value of a logical expression. Note: Numerically, a false value equates to 0 and a true value equates to a non-zero value. Example: If the current value of SkillGroup.Sales.Avail is 3, then SkillGroup.Sales.Avail > 0 is true and (SkillGroup.Sales.Avail > 0) is false.
~	One's complement	Operates on a bit value, changing each 1 bit to 0 and each 0 bit to 1. Note: This operator is rarely used.

Arithmetic Operators

The Arithmetic Operators in the following table take two operands:

Operator	Meaning	Comments/Examples
*	Multiplication	Arithmetic operators perform the basic operations of addition, subtraction, multiplication and division. You can use them in making calculations for a skill group, service, or route. Note: Multiplication (*) and division (/) operators are evaluated before addition (+) and subtraction (-) operators.
/	Division	
+	Addition	
-	Subtraction	

Equality Operators

The Equality Operators in the following table take two operands:

Operator	Meaning	Comments/Examples
==	Equal to	Equality operators allow you to determine whether two values are equivalent or not.
!=	Not Equal To	

Relational Operators

The Relational Operators in the following table take two operands:

Operator	Meaning	Comments/Examples
>	Greater than	Relational operators allow you to perform a more sophisticated comparison than the equality operators.
<	Less than	
>=	Greater Than or Equal To	
<=	Less Than or Equal To	

Logical Operators

The Logical Operators in the following table take two operands. Logical operators examine the values of different logical expressions:

Operator	Meaning	Comments/Examples
&&	And	The expression is true if both of the operands are true. If either is false, the overall expression is false.
	Or	The expression is true if either or both of the operands is true. If both are false, the overall expression is false.



Note The equality (==) and relational (>) operators are evaluated before the logical operators (&& and ||).

Bitwise Operators

The Bitwise Operators in the following table take two operands.

Operator	Meaning	Comments/Examples
&	And	The & Bitwise Operator turns specific bits in a value on or off.
	Inclusive Or	Inclusive Or and Exclusive Or differ in the way they handle the case where bits in both values are 1: Inclusive Or evaluates the result as true and sets a 1 bit in the result. Exclusive Or evaluates the result as false and sets a 0 bit in the result. (An Exclusive Or applies the rule "one or the other, but not both").
^	Exclusive Or	

Miscellaneous Operators

The following table lists miscellaneous operators:

Operator	Meaning	Comments/Examples
?	Conditional	The conditional operator (?) takes three operands and its syntax is as follows: The Packaged CCE evaluates the expression by first examining the logical expression condition and then tests the following condition: If the result is true, then the overall expression evaluates to the value of the expression true-result. If the result is false, then the overall expression evaluates to the expression false-result.
&	Concatenation	The concatenation operator (&) joins two strings end-to-end. returns the value.
,	Sequential	The sequential or comma operator (,) takes two operands, each of which is an expression. Packaged CCE evaluates the left expression first and then the right expression. The value of the overall expression is the value of the right expression. The first expression typically affects the valuation of the second.
<< >>	Shift left Shift right	The shift left (<<) and shift right (>>) operators shift the bits within a value.

Built-in Functions

Date and Time Functions

The following table lists the built-in date and time functions:

Function	Data Type	Return Value/Example
date [(date)]	Integer	Returns the current system date or the date portion of a given date-time value. The given date can be a floating point value (as returned by the now function), a string of the form mm/dd/yy, or three integers: yyyy, mm, dd. date (with no arguments) returns the current date. For example, = date (2001, 7, 15) tests whether the current date is July 15, 2001. Note Do not use the slash (/) character in defining a date function. Because it is the division operator, the function would not return the results you are looking for. You can enclose the argument within a string.
day [(date)]	Integer	Returns the day of month (1-31) for the current date or a given date. The given date must be an integer or a floating-point value, as returned by the date or now function.
hour [(time)]	Integer	Returns the hour (0-23) of the current time or a given time. The given time must be a floating-point value, as returned by the now function.
minute [(time)]	Integer	Returns the minutes (0-59) of the current time or a given time. The given time must be a floating-point value as returned by the time function.

Function	Data Type	Return Value/Example
month [(date)]	Integer	Returns the month (1-12) of the current month or a given date. The given date must be a floating-point value, as returned by the date or now function.
now	Float	Returns the current date and time, with the date represented as an integer and the time represented as a fraction. Note: You can use the date or time functions without any arguments to return just the current date or time. This function is useful for comparing the current date and time to a specific point in time.
second [(time)]	Integer	Returns the seconds (0-59) of the current time or a given time. The given time must be a floating-point value, as returned by the time function.
time [(time)]	Float	Returns the current system time or the time portion of a date-time value. The given time can be a floating point value, a string of the form hh:mm:ss, or two or three numeric values: hh, mm [, ss]. (with no arguments) returns the current time. For example, = time (20:05:00) tests whether the current time is 08:05:00
weekday [(date)]	Integer	Returns the current day of week (Sunday=1, Monday=2, etc.) of the current date or given date. The given date must be an integer or floating-point value, as returned by the date or now function.
year [(date)]	And	Returns the year of the current year or given date. The given date must be a floating-point value, as returned by the date or now function.

Mathematical Functions

The following table lists the built-in mathematical functions:

Function	Data Type	Return Value/Example
abs(n)	Floating Point or Integer	Returns the absolute value of n (the number with no sign).
max(n1, n2 [,n3] . . .)	Floating Point or Integer	Returns the largest of the operands. Each operand must be numeric.
min(n1, n2 [,n3] . . .)	Integer	Returns the smallest of the operands. Each operand must be numeric.
mod(n1,n2)	Floating Point or Integer	Returns the integer remainder of n1 divided by n2.
random()	Floating Point or Integer	Returns a random value between 0 and 1.
sqrt(n)	Floating Point or Integer	Returns the square root of n. (The operand n must be numeric and non-negative).

Function	Data Type	Return Value/Example
trunc(n)	Floating Point or Integer	Returns the value of n truncated to an integer.

Miscellaneous Functions

The following table lists the built-in miscellaneous functions:

Function	Data Type	Return Value/Example
after(string1,string2)	String	That portion of string2 following the first occurrence of string1. If string1 does not occur in string2, the null string is returned. If string1 is the null string, string2 is returned.
before(string1,string2)	String	That portion of string2 that precedes the first occurrence of string1. If string1 does not occur in string2, string2 is returned. If string1 is the null string, the null string is returned.
CallTypeSurvey	String	Returns the format required for CVP to run the post call survey.
ClidInRegion	Logical	Indicates whether the CLID for the current contact is in the geographical region specified by string. The value string must be the name of a defined region. You can use the Name variable of a region to avoid entering a literal value.
concatenate(string1,string2, . . .)	String	Returns the concatenation of the arguments. The function takes up to eight arguments.
EstimatedWaitTime	Integer	Returns the minimum estimated wait time for each of the queues against which the call is queued (skill group(s) or precision queue(s)). Queue to Agent(s) is not supported. If no data is available, returns -1. The estimated wait time is calculated once, when the call enters the queue. The default estimated wait time algorithm is based on a running five minute window of the rate of calls leaving the queue. Any calls which are routed or abandoned during the previous 5 minutes are taken into account as part of the rate leaving queue. For precision queues, the rate leaving queue represents the rate at which calls are delivered or abandoned from the entire precision queue, not any individual precision queue steps.
find(string1, string2 [,index])	Integer	Returns the starting location of string1 within string2. If you specify an index value, searching starts with the specified character of string2.

Function	Data Type	Return Value/Example
if(condition,true-value,false-value)	Logical	Returns a value of true-value if the condition is true; false-value if the condition is false. Returns the current hour in 12-hour format rather than 24-hour format.
isPickPullRequest()	Logical	Whether the current service requested is for pick or pull type.
isPickPullRequest()	Logical	Whether the current service requested is for pick or pull type.
left(string,n)	String	Returns the left-most n characters of the string.
len(string)	Integer	Returns the number of characters in the string.
mid(string,start,length)	String	Returns a substring of the string, beginning with the specified start character and continuing for the specified number of characters.
result	Floating Point or Integer	Returns the result of the current Select node. (This function is valid only in a Select node.) If you are using the LAA rule in the Select node, the result function returns the number of seconds the selected agent has been available.
right(string,n)	String	Returns the right-most n characters of the string.
substr(string,start [, length])	String	Returns a substring of the string, beginning with the specified start character and continuing for the specified number of characters.
text(n)	String	Converts a numeric value into a string.
valid(variable)	Logical	Returns whether the variable has a valid value.
ValidValue(variable,value)	String	If the variable has a valid value, returns that value; otherwise, returns "value". Returns either a name from the database or the string value None.
value(string)	Floating Point or Integer	Converts a string into a numeric value.

Custom Functions

Custom functions are those functions you create for use within scripts, as opposed to built-in functions.

Add Custom Functions

Procedure

- Step 1** In Script Editor, from the **Script** menu, choose **Custom Functions**. The Custom Functions dialog box opens, listing all the custom functions currently defined.
- Step 2** Click **Add** to open the Add Custom Function dialog box.
- Step 3** Specify the following:
- Function name. All custom function names must begin with user.
 - Number of Parameters. The number of parameters to be passed to the function. A function may take 0, 1, or more parameters.
 - Function definition. The expression to be evaluated when the function is called. When entering the function definition, keep the following in mind:

The parameters to a function are numbered beginning with 1. To reference a parameter within the expression, surround it with percent signs (%). For example, %3% is a reference to the third parameter.

The lower portion of the dialog box is just like the Formula Editor. You can use it to help build the expression.
- Step 4** When finished, click **Test**. The Test Function dialog box opens.
- Step 5** Test the function by entering an example of how you might reference the function. Include a specific value for each parameter.
- Step 6** Click **Evaluate** to see how the Script Editor interprets the function call and click **Close** to return to the Add Custom Function dialog box.
- Step 7** Use one of the Validate buttons to validate the scripts that reference a selection function. (The Validate All button lets you validate all the scripts that reference any custom function.)
- Step 8** When finished, click **OK** to apply changes and to close the dialog box.
-

Import Custom Functions

Procedure

- Step 1** In Script Editor, from the **Script** menu, choose **Custom Functions**. The Custom Functions dialog box opens, listing all the custom functions currently defined.
- Step 2** Click **Import**. The Import Custom Function dialog box opens.
- Step 3** Choose a file name with an ICMF extension (.ICMF) and click **Open**. The Script Editor examines the file for naming conflicts. If a conflict is found, a dialog box appears listing options for resolving the conflict.
- Step 4** Choose one of the options and click **OK**.

Note If you choose to rename the function, the new name must begin with user.

The Script Editor performs automapping and the following happens:

- If all imported objects were successfully auto-mapped, a message window appears prompting you to review the mappings. Click **OK** to access the Object Mapping dialog box.
- If some imported objects were not successfully auto-mapped, the Object Mapping dialog box appears, with all unmapped objects labeled Unmapped.

The Object Mapping dialog box contains three columns:

- Object Types. The type of imported objects.
 - Imported Object. Name of imported object.
 - Mapped To. What this imported object will be mapped to.
- (Optional.) Click an Imported Object value. The Mapped To column displays all the valid objects on the target system.
- (Optional.) Choose an object from the Mapped To columns drop-down list on the target system that you want to map the imported object to.



Note Multiple objects may be mapped to the same target. Objects may be left unmapped; however, the resulting custom function are not valid until all objects are mapped.

When the mapping is complete, click **Apply** and **Finish**.

Export Custom Functions

Procedure

- Step 1** In Script Editor, from the **Script** menu, choose **Custom Functions**. The Custom Functions dialog box opens, listing all the custom functions currently defined.
- Step 2** Choose the custom function(s) from the list and click **Export**. The Export Custom Function dialog box opens.
- Note** If you selected a single function, that functions name appears in the File Name field. If you selected more than one function, the File Name field is blank.
- Step 3** (Optional.) Change the File Name.
- Note** You cannot change the file type; you can save the script only in .ICMF format.
- Step 4** Click **Save**. If the file name already exists, the system prompts you to confirm the save.
- Step 5** If prompted, click **OK**. The custom function(s) are saved to the specified file in text format.
-



CHAPTER 13

Scripting Specifics in a Packaged CCE Environment

- [Call Priority, on page 505](#)
- [Check for Available Agents, on page 505](#)
- [Scripts for Precision Queues, on page 505](#)
- [Cancel Queuing Node, on page 508](#)
- [End Node, on page 508](#)
- [Agent to Agent Node, on page 508](#)
- [Unified CVP as a queue point, on page 509](#)

Call Priority

When a call is queued to a skill group because there are no agents available, the Queue to Skill Group node sets the call's priority. The Queue Priority node can then promote the call's priority based on time the caller has waited. The call can be queued to multiple skill groups with the same or different priorities.

If there are calls in the agent's skill group queues when an agent becomes available, the agent is presented with the highest priority (1-20 with 1 being the highest priority) call that has waited the longest within the skill group(s) that the agent is assigned to.

Check for Available Agents

A script that routes to Packaged CCE agents needs to check for an available agent within a skill group. If an agent is not available, then the script should use a Queue to Skill Group node. The script execution ends when an agent becomes available or when the caller disconnects.

Scripts for Precision Queues

To implement Precision Routing in your contact center, you must create scripts.

You can create and use configured (static) and dynamic precision queue nodes in your scripts.

- Static precision queue nodes target a single, configured precision queue. When the script utilizes a single precision queue, use static precision queues.

- Dynamic precision queue nodes are used to target one or more previously configured precision queues. Use dynamic precision queues when you want a single routing script for multiple precision queues (for example, when the overall call treatment does not vary from one precision queue to another). Dynamic precision queues can simplify and reduce the overall number of routing scripts in the system.

Precision Queue Script Node

Use the Precision Queue script node to queue a call based on caller requirements until an agent with desired proficiency become available. This node contains multiple agent selection criteria which are separated into steps.

A single call can be queued on multiple precision queues. If an agent becomes available in one of the precision queues, the call is routed to that resource. You cannot reference multiple precision queues with a single Precision Queue node. However, you can run multiple Precision Queue nodes sequentially to achieve this.

The Precision Queue node includes a Priority field, which sets the initial queuing priority for the calls processed through this node versus other calls queued to the other targets using different nodes. The priority is expressed as an integer from 1 (top priority) to 10 (least priority). The default value is 5.

If more than one call is queued to a precision queue when an agent becomes available, the queued call with the lowest priority number is routed to the target first. For example, assume an agent in a precision queue becomes available and two calls are queued to that precision queue. If one call has priority 3 and the other has priority 5, the call with priority 3, the lower value, is routed to the precision queue while the other call continues to wait. If the priorities of the two calls are same, then the call queued first is routed first.

VRU (voice response unit) script instructions are not sent to the VRU. If a call enters the precision queue node and no resource is available, the call is queued to the precision queue and the node transfers the call to the default VRU, if the call is not already on a VRU. The script flow then exits immediately through the success branch. The script should then continue with a run external script node to instruct the VRU what to do while holding the call until an agent becomes available. Typically, this invokes a network VRU script that plays music-on-hold, possibly interrupted on a regular basis with an announcement. The script flow can also use other queuing nodes to queue the same call to other targets, for example, Queue to Skill Group and Queue to Agent.



Note Non-voice tasks can also be picked or pulled out of turn from queues, not necessarily based on the priority of the call. Such non-voice tasks that are picked or pulled by a specific agent, require a Pick/Pull node to be used in the ICM script. However, the agents belonging to other skill groups or precision queues can also pick tasks that may be queued in Skill Groups or Precision Queues other than their own. These are denoted by **Picked by another Skillgroup/PQ** or **Pulled by another Skillgroup/PQ** monitor labels, when viewing the scripts in monitor mode.

Configure a Static Precision Queue

Procedure

- Step 1** In the **Precision Queue Properties** dialog box, select the **Statically** option.
- Step 2** From the list, select a precision queue to which to route all calls that enter this node.

- Step 3** In the **Priority selection** box, select the initial queuing priority for calls processed through this node. You can select from 1 - 10. The default is 5.
- Step 4** Check the **Enable target requery** check box to enable the requery feature for calls processed through this node.
- Step 5** Check the **Wait if Agents Not Logged In** check box.
If this check box is selected and the agents associated with this step are not logged in, then the router waits for the time that is configured for that step. Whereas, if this check box is not selected, the router does not wait on any step.
- Note** The router waits indefinitely on the last step, irrespective of the selection of this check box.
- Step 6** To edit a precision queue, select a precision queue from the list, and then click **Edit Precision Queue**.
-

Configure a Dynamic Precision Queue

Procedure

- Step 1** In the **Precision Queue Properties** dialog box, select the **Dynamically** option.
- Step 2** In the **Priority selection** section, select the initial queuing priority for calls processed through this node. You can select from 1 - 10. The default is 5.
- Step 3** Check the **Enable target requery** check box to enable the requery feature for calls processed through this node.
- Step 4** Check the **Wait if Agents Not Logged In** check box.
If this check box is selected and the agents associated with this step are not logged in, then the router waits for the time that is configured for that step. Whereas, if this check box is not selected, the router does not wait on any step.
- Note** The router waits indefinitely on the last step, irrespective of the selection of this check box.
- Step 5** Select a queue option:
- To dynamically route calls that enter this node to a precision queue name, select the **Precision Queue Name** option.
 - To dynamically route calls that enter this node to a precision queue ID, select the **Precision Queue ID** option.
- Step 6** Click **Formula Editor** to create a formula that determines the precision queue name or ID to which to route calls.
-

Queuing Behavior of the Precision Queue Node

Precision queues internally are configured with one or more time-based steps, each with a configured wait time. After a call is queued, the first step begins and the timer starts. This occurs although the path of the script exited the success node and a new node may be targeted (for example, Run Ext. Script).

If the timer for the first step expires, control moves to the second step (assuming one exists), and so on. As long as the call remains in queue and there are steps left to perform, the call internally continues to move between steps regardless of the path the call takes after it leaves the precision queue node. If a call is queued to two or more precision queues, the call internally walks through the steps for each precision queue in parallel. After the call reaches the last step on a precision queue, it remains queued on that step until the call is routed, abandoned, or ended.

If there is an update to the precision queue definition, then all queued calls in the precision queue are re-evaluated and are re-run from the first step.

For example, consider the wait time for an ongoing call at step 1 to be 1080 seconds, of which 1000 seconds has already elapsed. Now, suppose the wait time is changed to 900 seconds, then the wait time for this call is also reset to 900 seconds, even though only 80 more seconds are left to move to the next step.

Cancel Queuing Node

If the call needs to be taken out of a skill group, then use the Cancel Queuing node. The Cancel Queuing node takes the call out of all the skill groups it is queued to.

End Node

The End node either tries default routing, or if there is no default label, it sends an error (dialog fail) to the routing client.

Agent to Agent Node

You can use the Agent to Agent node for agent to agent transfers; the router checks agent availability before sending the call to the agent. If the agent is not available, the script queues the call to a skill group. You can also use the Agent to Agent node to send a call to the agent: the "caller" is not required to be an agent.

For a transfer to a specific target agent, the initiating agent enters the target agent ID. The DNP entry matching the dialed number (agent ID) must have a DNP type of PBX. For this DNP type, the PIM enters the dialed number (agent ID) into the Caller-Entered Digits (CED) field while sending the route request to the Router. To have the Router handle the call properly, specify the CED field as the location of the agent ID in the Agent to Agent node.

Agent IDs must not match any of the extensions on the Unified Communications Manager cluster. If you make all agent IDs of the same length and begin with the same number, a generic wildcard string can match all agent IDs. With that wildcard string, you need only one entry in the DNP for agent-to-agent routing.

The agent-to-agent node requires that you specify the PIM. If your environment has multiple PIMs, use an agent ID number plan to determine which PIM contains an agent. Agent IDs are associated with a specific PIM and are not unique by themselves. You can set up a consistent agent ID assignment plan (such as, all agent IDs on PIM 1 begin with 1, and so on). That pattern enables you not to repeat agent IDs across the enterprise. Then, you can parse the CED field in the script editor to determine which PIM contains a specific agent.

Unified CVP as a queue point

Packaged CCE relies on the Unified CVP to queue the call while it is waiting for an available agent.

The Packaged CCE sends the call to the Unified CVP port for queuing:

- To provide the call with a termination point that allows the VoIP Gateway to return the correct signals or messages back to the PSTN.
- Provide announcements or music or expected wait time or initial position in queue to the caller while they are waiting for an agent. Allow the caller an option to leave a message if the caller does not want to wait for an agent.
- To obtain further information from the caller that is not sent from the network

The Unified CVP lets Packaged CCE know when the caller disconnects through the Event Report Message with an Event Type of either DISCONNECT or ABANDON. When an agent becomes available, Packaged CCE automatically instructs Unified CVP to route the call to the agent through the Connect message.

Interruptible vs. Non-interruptible

If the VRU script is collecting digits from the customer to ascertain information regarding the caller that is crucial for a screen pop or call routing, put the VRU script in a non-interruptible mode.

If a call was queued to a skill group through a Queue to Skill Group node and then sent to VRU to hear a non-interruptible VRU script, if during the time that the caller is interacting and listening to the non-interruptible VRU script, an agent becomes available, the call will not be connected to the agent. The Packaged CCE only looks for available agents for that call when the VRU script is finished and the call runs an interruptible node such as a Wait node or a Run External Script node for a VRU script that is interruptible. The call does, however, maintain its place in the queue so when the call does become available for an agent, it is answered before calls that came in afterward it (assuming the same priority).

For announcement and music type of treatments, put the VRU Scripts in interruptible mode. This allows the call to be connected to the first available agent even while the caller is listening to a VRU script.

You set the interruptibility of a VRU script through the Network VRU Scripts gadget in the Unified CCE Administration Web tool. Neither the VRU or the Packaged CCE script can overwrite this setting.



CHAPTER 14

Utility Nodes

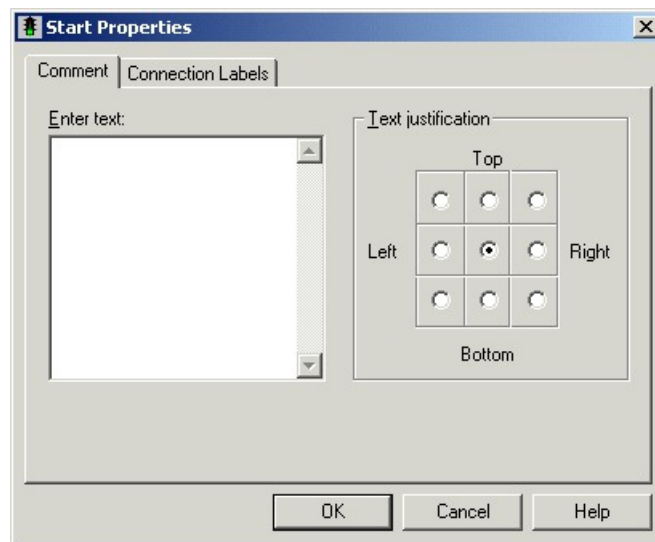
- [Start Node](#), on page 511
- [Comment Node](#), on page 511
- [Line Connector Node](#), on page 512

Start Node

The Start node marks the beginning of a script. The Script Editor automatically inserts the Start node when you create a new script; a script must have one and only one Start node.

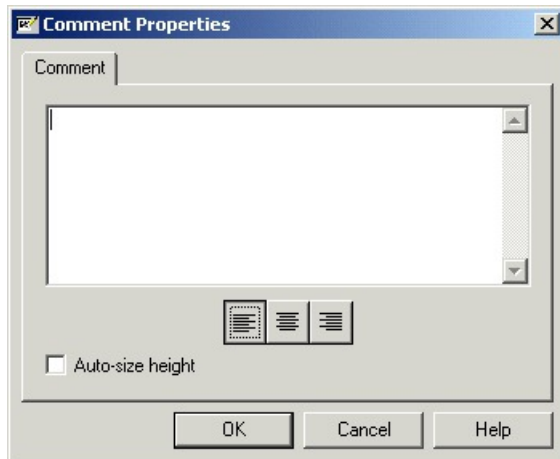
You do not define any properties for the Start node. However, you can add comments and connection labels:

Figure 71: Start Properties



Comment Node

Use the Comment node (in the General tab of the Palette) to include a block comment in a script. A block comment provides general documentation for a script or section of a script:

Figure 72: The Comment Icon**Figure 73: Comment Properties**

For example, you might add a comment describing the purpose of the script.

You can move and resize the comment box within the script.



Note If you choose the Auto-Size Height option, you cannot adjust the height of the comment.

Line Connector Node

Use the Line Connector node (in the General tab of the Palette) to make routing and administrative scripts clear and understandable.

Figure 74: The Line Connector Icon

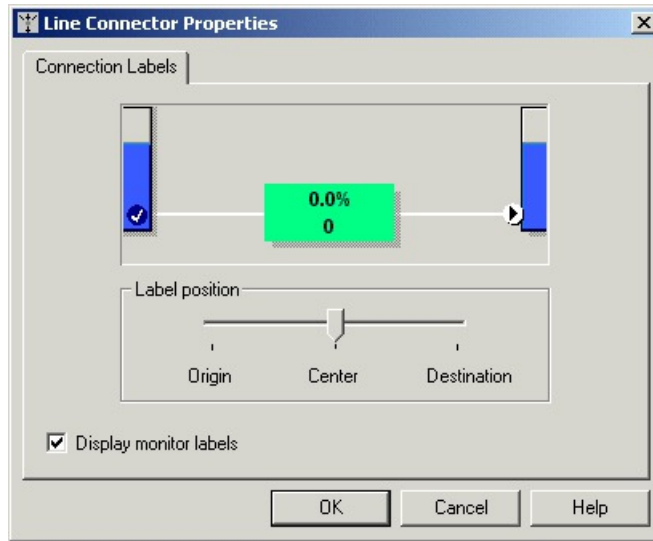
A script can be difficult to understand and the call flow hard to follow if:

- The connecting lines between nodes are too long.
- The connecting lines go in different directions.
- The connecting lines run over other nodes and other connection lines.

The Line Connector node allows you to break and reconnect lines using one or more of its multiple input connections and single output connection. Any request coming into this node (on any one of the multiple inputs) goes to the single output connection of the line connector node.

For the Line Connector node, you define the connection labels:

Figure 75: Line Connector Properties





CHAPTER 15

Unified CVP Scripting

- [Writing Scripts for Unified CVP, on page 515](#)
- [Before You Begin, on page 515](#)
- [Scripts to Access Unified CVP from Packaged CCE, on page 516](#)
- [Invoke Unified CVP Micro-applications Through Routing Scripts, on page 516](#)
- [Unified CVP Call Studio Scripting, on page 516](#)
- [Scripting for Unified CVP with Packaged CCE , on page 517](#)
- [Writing Packaged CCE Applications for Unified CVP, on page 526](#)
- [Unified CVP Micro-applications, on page 526](#)
- [Scripting for Unified CVP with Call Studio, on page 568](#)

Writing Scripts for Unified CVP

This section discusses using Packaged CCE configuration and script editing to access the Unified CVP solution.

It includes information about how to:

- Set up Packaged CCE to interact with Unified CVP
- Write applications for Unified CVP



Note This section contains important information for Unified CVP application developers. It also may be of interest to Call Center Managers, Unified CVP System Managers, and Packaged CCE system managers.

Before You Begin

This chapter makes the following assumptions:

- The information in this chapter assumes that you are already familiar with using the Unified CCE Administration and Script Editor tools for call center operations and management.
- When creating Script Editor applications that interact with Unified CVP, only use alphanumeric characters for application, element, and field names; *do not* use special characters such as periods, asterisks or brackets. Following this practice will avoid potential issues with data transfer between different systems.

Scripts to Access Unified CVP from Packaged CCE

Both Packaged CCE and Unified CVP use scripts to invoke their features. In fact, Packaged CCE references Unified CVP scripts from *within* its own scripts. This method of invoking Unified CVP from within Packaged CCE enables Packaged CCE to take advantage of the features of Unified CVP.

Packaged CCE and Unified CVP provide two service creation (scripting) environments. Each environment is used for different purposes:

- **Script Editor.** Use this scripting tool to develop agent routing scripts and to invoke the Unified CVP **micro-applications**: Play Media, Get Speech, Get Digits, Menu, Play Data, and Capture. These applications are the basic building blocks of a voice interaction design.
- **Call Studio.** Use Call Studio to develop sophisticated Unified CVP applications.



Note For more information, refer to [Scripting for Unified CVP with Call Studio, on page 568](#).

Invoke Unified CVP Micro-applications Through Routing Scripts

The Script Editor is used to develop agent routing scripts, and to invoke Unified CVP micro-applications - basic building blocks of a voice interaction design. The Unified CVP micro-applications are: Play Media, Get Speech, Get Digits, Menu, Play Data, and Capture. These applications are combined and customized in the Packaged CCE routing script to produce a viable voice interaction with the caller.

Instead of developing full scale Unified CVP applications using micro-applications, use Unified CVP scripts developed using Call Studio to create the Unified CVP applications. Micro-application-based scripts are primarily used for initial prompt and collection operations, as well as for directing the playing of .wav files while calls are in queue.

In an environment where routing script works with Call Studio script (the 2-script implementation for Unified CCE-integrated models described here), the routing script remains in control (and receives control back), even while it *delegates* the more complex self-service activity to the Call Studio script. Data can be passed from one script to the other and back through ECC variables.

Unified CVP Call Studio Scripting

Sophisticated Unified CVP applications can be developed using Call Studio which is an Eclipse-based service creation environment whose output is an intermediary file describing the application flow. That file gets loaded onto the VXML Server for execution. To invoke a VXML Server application, the script writer includes a Get Speech (GS) micro-application via the Run External Script node in the Packaged CCE routing script. This micro-application instructs the VoiceXML Gateway to interact with the VXML Server directly to run the application. The final results are passed back to Packaged CCE.

Some of the Call Studio scripting environment features include:

- A drag-and-drop interface with a palette of Unified CVP functions

- The ability to do database queries
- Extensibility with Java code written to perform any task a Java application can perform



Note Packaged CCE does not support using the *MicroApp* nodes that are available in the Script Editor. All MicroApp implementation must be done using the *Run External Script* node in Script Editor. Refer to [Writing Packaged CCE Applications for Unified CVP, on page 526](#) for detailed information about setting Unified CVP-specific parameters in this node for each Unified CVP micro-application.



Note For more information about creating scripts, refer to [Writing Packaged CCE Applications for Unified CVP, on page 526](#).

Scripting for Unified CVP with Packaged CCE

The sections that follow include:

- A discussion of micro-applications.
- A sample Packaged CCE script.
- A discussion of how Packaged CCE and Unified CVP exchange information.

Micro-applications

Micro-applications are a set of specific Unified CVP functions that can be invoked by Packaged CCE, enabling communication with the caller.

There are six Unified CVP micro-applications:

- **Play Media.** Plays a message to the caller.
- **Play Data .** Retrieves data from a storage area and plays it to the caller in a specific format called a data play back type.
- **Get Digits.** Plays a media file and retrieves digits from the caller.
- **Menu.** Plays a media menu file and retrieves a single telephone keypad entry from the caller.
- **Get Speech.** Runs a Call Studio script on VXML Server.
- **Capture.** The Capture (CAP) micro-application enables you to trigger the storage of current call data at multiple points in the Packaged CCE routing script.

Micro-applications are interpreted by the Unified CVP Service, which resides on the Unified CVP Call Server. The Unified CVP Service sends VoiceXML code to the VoiceXML Gateway Voice Browser.



Note Using ASR/TTS(speech) through micro-applications is not supported. You have to use Call Studio scripts for any caller interaction that requires use of ASR/TTS (speech).

Simple Example Script: Welcome to XYZ Corporation

Suppose you want to create a script that has an example call flow as follows.

This simple script performs the following functions:

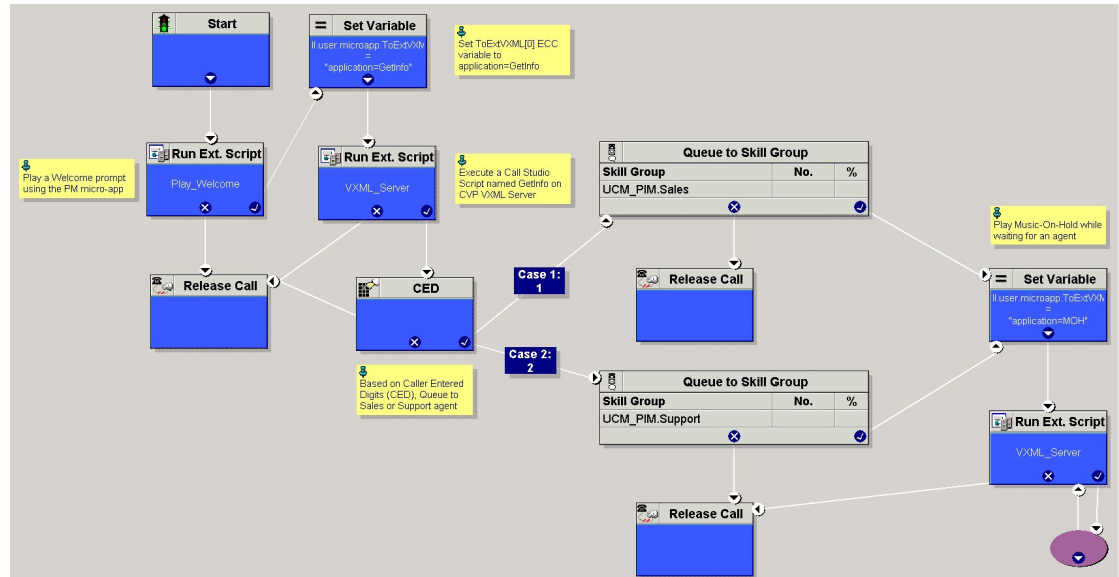
- Runs the GetInfo Call Studio script on the VXML Server to collect some caller input based on the example callflow.
- Based on caller input, queues for a sales or support agent .
- If an agent is not available, runs the MOH Call Studio script which will play music-on-hold to the caller until an agent becomes available.

Procedure

- Step 1** A call arrives at Packaged CCE and runs a Packaged CCE script.
- Step 2** The caller hears a welcome prompt.
- Step 3** The script sends the call to Unified CVP for collecting some information from the caller before queuing the call for an agent. For example, a menu is offered such as "press 1 for sales and 2 for support," as well as entering an account number.
- Step 4** If the caller is an existing customer, the caller-entered account number is used to retrieve additional information about the caller from an external database.
- Step 5** Caller-entered digits and the additional information about the caller are returned back to the Packaged CCE script to be shown a screen pop to the agent, when an agent becomes available.
- Step 6** The call is then queued waiting for an agent in a particular skill group, based on the caller selection of the type of service.
- Step 7** If an agent is available, the caller is connected to that agent. The agent desktop displays the caller information collected via caller input as well as database lookup.
- Step 8** If an agent is not available, the call is sent back to Unified CVP for playing music-on-hold while the caller waits for an agent to become available.
- Step 9** The information collected from the caller is preserved as call context on the call until the agent becomes available.

You can create a script such as the one shown in the following figure.

Figure 76: Packaged CCE Script with Call Flow



This simple script performs the following functions:

- Runs the GetInfo Call Studio script on the VXML Server to collect some caller input based on the example callflow.
- Based on caller input, queues for a sales or support agent.
- If an agent is not available, runs the MOH Call Studio script which will play music-on-hold to the caller until an agent becomes available.

Note In a “real life” application, any Packaged CCE script you create would include error checking to ensure that micro-applications instructions are properly performed.

Packaged CCE Unified CVP Micro-app Connection

Before the Unified CVP can be accessible through the Script Editor’s Run External Script node, you must first set up Packaged CCE with special Unified CVP parameters using the Unified CCE Administration tool.

Begin by using the Unified CCE Administration Network VRU Script tool to define Unified CVP parameters. See [Network VRU Scripts, on page 349](#)



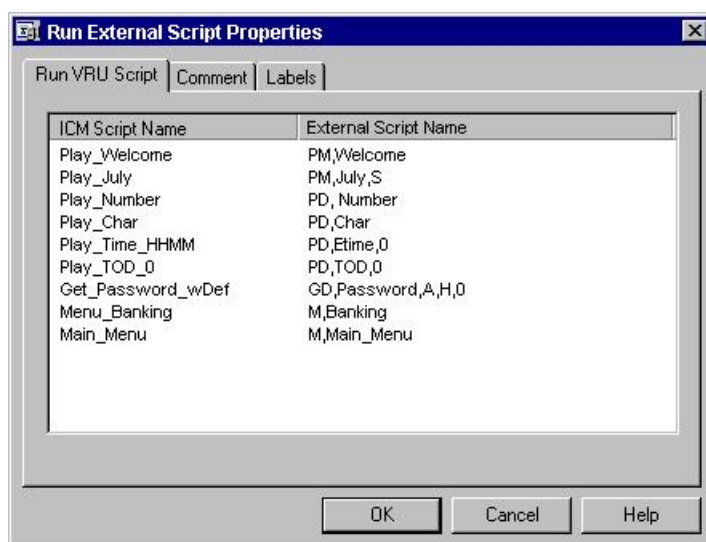
Note As shown in the two columns of the following table, certain entries for the VRU Script Name and Configuration Param fields are case-sensitive.

Attribute	Allowed Values	Applies to	Case-Sensitive?
Attribute: VRU Script Name (for example, PM, GD).	PM, GD	All micro-applications	N
Attribute: Media Library Type (A, S, V)	A, S, V	All micro-applications	N
Barge-in Allowed	Y/N	All micro-applications	N
Data playback type	Number, Char	PlayData (PD)	N
Time Format	HHMM, HHMMSS, HHMMAP	PlayData (PD)	N
Timeout Message Override	Y/N	Get Digits (GD), Get Speech (GS), Menu (M)	N
Invalid Entry Message Override	Y/N	Get Digits (GD), Get Speech (GS), Menu (M)	N
DTMF Termination Key	N	All micro-applications	N
Media File Name		All micro-applications	Y

Once the network VRU script configuration settings have been saved, the information is available to the Script Editor. When you place a Run External Script node in the Script Editor workspace and open the Properties dialog box, it displays all the script names defined in the system.

The Run External Script node below shows that the ICM Script Name Play_Welcome was selected.

Figure 77: Run External Script Node



Information Exchange Between Packaged CCE and Unified CVP

When Packaged CCE processes a Run External Script node, parameters are sent to Unified CVP.

These parameters contain instructions about how to interact with a caller, such as:

- What micro-application to use.
- The location of the media files to be played to the caller.
- Timeout settings to be used during caller digit entry.

Some Unified CVP parameters are passed to Unified CVP through Expanded Call Context (ECC) variables and/or Call.Peripheral variables. Other parameters are sent in the usual VRU messaging interface (Packaged CCE /Unified CVP Service Control Interface).

Packaged CCE Data Handling

In defining scripts, you might specify strings, numbers, or formulas to be sent to Unified CVP. When passing numbers to Unified CVP, always enclose them in quotes so that they will be processed as a string.

This is especially important if:

- Leading 0's are significant to the data type (times, character), enter the number as a quoted string (example: "031524").
- Trailing 0's after a decimal point are significant to the data type (number, character, currency), enter the number as a quoted string (examples: "42.00" or "42.10").
- The number is very large (example: a number typically expressed through exponential notation).

Unified CVP Script Error Checking

Unified CVP uses the **user.microapp.error_code** ECC variable to return information regarding problems encountered while running a script.

Unified CVP software tests for the following conditions when processing Packaged CCE scripts:

ASR error

Failure of an Advanced Speech Recognition component.

General error

General error occurred.

Invalid configuration param

Data passed from Packaged CCE to the Unified CVP Service is not consistent with what the micro-application requires for processing.

Invalid variable data

The variable data passed was not valid for the script type being processed.

Invalid VRU script name format

VRU Script Name data passed from Packaged CCE to the Unified CVP Service does not contain the expected components (micro-application name, media file name, media file type, uniqueness value).

Locale

Locale was not supported. (Only applies to Play Data micro-applications that use .wav files. Does not apply to Play Data micro-applications that use TTS, or to Play Media, Get Digits, Menu, Get Speech, or Capture micro-applications.)

Misconfigured ECC variable

An ECC variable was set to a value the Unified CVP Service did not recognize. ECC variable definitions must be the same in Packaged CCE and Unified CVP.

Network error

Failure of an IP network connection.

Reached maximum invalid tries

Caller was unsuccessful in entering digits during each of the tries allowed by the micro-application. (Only applies to Get Digits, Menu, and Get Speech micro-applications.)

Reached maximum number entry tries

Caller did not enter digits in response to the prompt for each of the tries allowed by the micro-application. (Only applies to Get Digits and Get Speech micro-applications.)

Semantic-runtime

Semantic error occurred while running a micro-application.

System error

Unexpected failure of a Unified CVP component.

Timed out

Caller did not enter digits in response to the prompt in the time allowed by the micro-application.

TTS error

Failure of a Text-to-Speech component.

Unavailable media file

Media file name passed from Packaged CCE to the Unified CVP Service did not exist on the Media Server.

Unknown micro-application

Micro-application name passed from Packaged CCE to the Unified CVP Service did not exist on the Unified CVP Service.

Unsupported locale

The VoiceXML Interpreter (that is, gateway) did not recognize the locale passed from the Unified CVP Service.

Unsupported VoiceXML element

The VoiceXML Interpreter (that is, gateway) did not recognize a VoiceXML element passed from the Unified CVP Service, VXML Server, or media server.

Unsupported VoiceXML format

The VoiceXML Interpreter (that is, gateway) did not recognize a VoiceXML format passed from the Unified CVP Service, VXML Server, or media server.

Each Unified CVP micro-application has individualized settings for **user.microapp.error_code**, as shown in the following table.

Table 32: Possible user.microapp.error_code ECC Variable Settings for Non-Video

Error Code	Play Media	Play Data	Get Digits	Menu	Get Speech	Capture
0	No error	No error	No error	No error	No error	No error
1	Caller Hangup	Caller Hangup	Caller Hangup	Caller Hangup	Caller Hangup	N/A
2	Network Error	Network Error	Network Error	Network Error	Network Error	N/A
3	System Error	System Error	System Error	System Error	System Error	System Error
5	Unknown micro-application	Unknown micro-application	Unknown micro-application	Unknown micro-application	Unknown micro-application	Unknown micro-application
6	Invalid VRU Script Name format	Invalid VRU Script Name format	Invalid VRU Script Name format	Invalid VRU Script Name format	Invalid VRU Script Name format	N/A
7	Invalid Configuration Param	Invalid Configuration Param	Invalid Configuration Param	Invalid Configuration Param	Invalid Configuration Param	N/A
8	Misconfigured ECC variable	Misconfigured ECC variable	Misconfigured ECC variable	Misconfigured ECC variable	Misconfigured ECC variable	N/A
9	One of the following: <ul style="list-style-type: none"> Media file does not exist. Invalid URL for Media file. 	One of the following: <ul style="list-style-type: none"> Media file does not exist Invalid URL for Media L file 	One of the following: <ul style="list-style-type: none"> Media file does not exist Invalid URL for Media L file 	One of the following: <ul style="list-style-type: none"> Media file does not exist Invalid URL for Media L file 	One of the following: <ul style="list-style-type: none"> Media file does not exist Invalid URL for Media file 	N/A
10	Semantic-Runtime Error	Semantic-Runtime Error	Semantic-Runtime Error	Semantic-Runtime Error	Semantic-Runtime Error	N/A
11	Unsupported VoiceXML format	Unsupported VoiceXML format	Unsupported VoiceXML format	Unsupported VoiceXML format	Unsupported VoiceXML format	N/A
12	Unsupported VoiceXML element	Unsupported VoiceXML element	Unsupported VoiceXML element	Unsupported VoiceXML element	Unsupported VoiceXML element	N/A

Error Code	Play Media	Play Data	Get Digits	Menu	Get Speech	Capture
13	N/A	Variable data is invalid	N/A	N/A	N/A	N/A
14	N/A	Location of variable data is empty	N/A	N/A	N/A	N/A
15	N/A	Time format is invalid	N/A	N/A	N/A	N/A
16	N/A	N/A	Reached Maximum Invalid Tries	Reached Maximum Invalid Tries	Reached Maximum Invalid Tries	N/A
17	N/A	N/A	Reached Maximum No Entry Tries	Reached Maximum No Entry Tries	Reached Maximum No Entry Tries	N/A
20	N/A	Data value out of range	N/A	N/A	N/A	N/A
23	No answer	No answer	No answer	No answer	No answer	N/A
24	Busy	Busy	Busy	Busy	Busy	N/A
25	General transfer error	General transfer error	General transfer error	General transfer error	General transfer error	N/A
26	Invalid extension	Invalid extension	Invalid extension	Invalid extension	Invalid extension	N/A
27	Called party ended the call	Called party ended the call	Called party ended the call	Called party ended the call	Called party ended the call	N/A
28	Error after transfer established	Error after transfer established	Error after transfer established	Error after transfer established	Error after transfer established	N/A
30	Unsupported locale	Unsupported locale	Unsupported locale	Unsupported locale	Unsupported locale	N/A
31	ASR error	ASR error	ASR error	ASR error	ASR error	N/A
32	TTS error	TTS error	TTS error	TTS error	TTS error	N/A
33	General ASR/TTS error	General ASR/TTS error	General ASR/TTS error	General ASR/TTS error	General ASR/TTS error	N/A
34	Unknown error	Unknown error	Unknown error	Unknown error	Unknown error	N/A
40	VXML Server system unavailable	N/A	N/A	N/A	VXML Server system unavailable	N/A

Error Code	Play Media	Play Data	Get Digits	Menu	Get Speech	Capture
41	VXML Server application error	N/A	N/A	N/A	VXML Server application error	N/A
42	VXML Server application used hangup element instead of subdialog return element	N/A	N/A	N/A	VXML Server application used hangup element instead of subdialog return element	N/A
43	VXML Server application is suspended	N/A	N/A	N/A	VXML Server application is suspended	N/A
44	VXML Server session error (for example, application has not yet been loaded)	N/A	N/A	N/A	VXML Server session error (for example, application has not yet been loaded)	N/A
45	VXML Server encounters a bad fetch error (for example, media or grammar file not found)	N/A	N/A	N/A	VXML Server encounters a bad fetch error (for example, media or grammar file not found)	N/A
46	Audio streaming error	N/A	N/A	N/A	N/A	N/A



Note `user.microapp.error_code` is always zero, indicating success, if control proceeds out the Checkmark (success) branch of the Run External Script node. Usually, if control proceeds out the X (failure) branch, Unified CVP sets this variable to one of the codes listed here. (Set up your routing script to always test the error code after an X branch is taken.)



Note However, if a configuration error, or a network or component failure of some sort, prevents the micro-application from being run at all, then Unified CVP does not get a chance to set this variable at all. Such cases can be identified by using a Set node to pre-set `user.microapp.error_code` to some known invalid value such as -1, and then to test for that value using an If node, following the X branch of the Run External Script node.

Writing Packaged CCE Applications for Unified CVP

Once Packaged CCE-to-Unified CVP initial setup is complete, you can create Packaged CCE applications to access Unified CVP micro-applications.

You do this using two Packaged CCE software tools:

- Unified CCE Administration
- Packaged CCE Script Editor

Use Unified CCE Administration to configure Unified CVP Network VRU scripts. The following section describes using the Script Editor to access Unified CVP micro-applications.

Related Topics

[Add and Maintain Network VRU Scripts](#), on page 350

Run External Script Node That Accesses a Unified CVP Micro-application

Procedure

Step 1 Within Script Editor, place the Run External Script object in the workspace, right-click, and open the Properties dialog box.

The Run External Script Properties dialog box lists all Network VRU scripts currently configured

Note The ICM Script Name column reflects the values defined through the Name field in ICM Configuration Manager's Scripts tool.

Step 2 Select the **ICM Script/VRU Script Name** you want to run.

Step 3 Modify the Comments tab as needed.

Step 4 Modify the Labels tab as needed.

Step 5 When finished, click **OK** to submit the changes and close the dialog box.

Unified CVP Micro-applications

The sections that follow describe the parameters that can be defined through Unified CCE Administration for each of the six Unified CVP micro-applications.

Keep the following in mind as you configure each Network VRU Script to be used with Unified CVP:

- Each micro-application parameter in fields of the Network VRU Script's Attributes tab must be separated by a comma.
- If a parameter value is not specified, the micro-application uses its default.

Dynamic Audio File Support for Micro-applications

Unified CVP lets you use a single micro-application and specify the prompt using call variables and the Packaged CCE formula editor.

To provide dynamic audio file capability, set the second VRU script parameter to a numeric value, 1-10, prefixed by a dash. You then set the Media Library to either “A”, “S”, or “V”. Unified CVP looks in the corresponding Call.PeripheralVariable for the name of the audio file to play.

When you set the Media Library to “A” or “S”, Unified CVP plays the audio file specified by the Call Variable after the “-(number)”. For example, if the second VRU Script Parameter is set to “-4”, it plays the audio file specified in Call.PeripheralVariable4. This functionality is added for Play Media, Menu, and Get Digits micro-applications.



Note When A is specified as the Media Library, it means Unified CVP looks for the media file under the C:\inetpub\wwwroot\en-us\app folder by default and when S is specified, it looks under the C:\inetpub\wwwroot\en-us\sys folder by default.

Second VRU Script Parameter	Corresponding Call Variable
-1 to -10	Call.PeripheralVariable (1 to 10)

For an example of how to use a dynamic audio file, see the following table.

VRU Script Parameter Example	Definition
PM, -3,A	<p>PM - Uses the Play Media micro-application.</p> <p>-3 - Plays the file specified in Call.PeripheralVariable3.</p> <p>A - Acquires the file from the application media files folder (for example, C:\inetpub\wwwroot\en-us\app).</p>

Notes

- If you do not specify a file extension for the file name in the Call.PeripheralVariable, the default media file extension is applied (for example, .wav for audio files).
- If you set the second VRU script parameter to a value prefixed with a dash and don't specify a file name in the corresponding Call.PeripheralVariable, the Unified CVP Service creates a VoiceXML that does not contain a media prompt.
- You can only specify the name of a single file in the Peripheral Variable. You cannot set this value to a name/value pair.

For more information, refer to the sections on individual micro-applications in this chapter.

Default Media Server for Micro-applications

You can specify a media server for a micro-application was to use the ECC variable `user.microapp.media_server`.

The global default media server can be specified in **Unified CCE Administration > Overview > Infrastructure Settings > Device Configuration > CVP Server > IVR** tab. The default media server is used by the micro-applications if the ECC variable `user.microapp.media_server` is missing or empty in the Packaged CCE script.

The following list specifies the order in which the micro-application tries to resolve which media server to use:

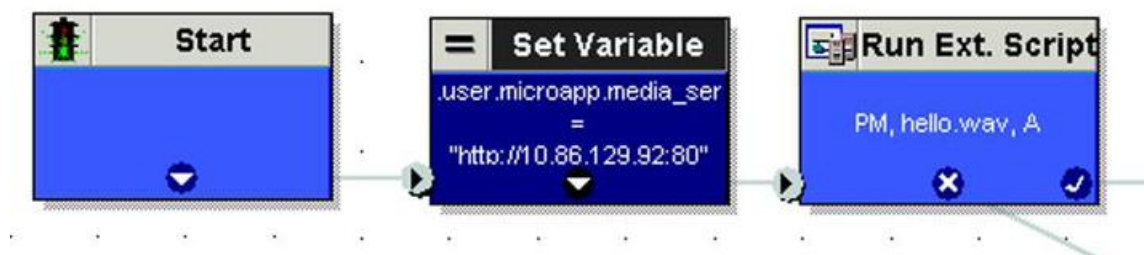
1. Media server is specified by the ECC variable: `user.microapp.media_server`
2. Global default media server is specified

The first non-empty media server value encountered in the above order is used by the micro-application. This applies to all micro-applications including

- Play Media (PM)
- Play Data (PD)
- Get Digits (PD)
- Menu (M)

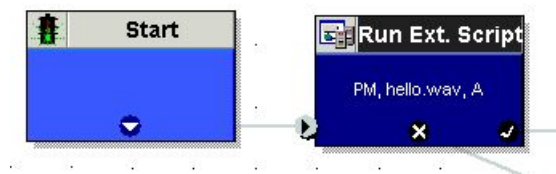
The following screen shot shows the Packaged CCE script where Play Media micro-application plays a media file using the ECC variable `user.microapp.media_server`.

Figure 78: Packaged CCE Script with Play Media Using ECC Variable



The following screen shot shows the Packaged CCE script where Play Media micro-application plays a media file using a default media server.

Figure 79: Packaged CCE Script with Play Media Using Default Media Server



Capture Micro-application

The Capture (CAP) micro-application allows you to trigger the storage of current call data at multiple points in the Packaged CCE routing script. The CAP micro-application must be configured as a VRU script, and it is run using a RunExternalScript node, just as with any other Unified CVP micro-application. The VRU Script

Name value is "CAP" or "CAP,xxx," where "xxx" is any arbitrary string to be used if necessary for uniqueness purposes. There is no VRU Script Config string.

Executing a Capture micro-application causes the Packaged CCE PG to produce an intermediate termination record. Specifically, it writes a record in the Termination_Call_Detail (TCD) table which includes all current call variables (not the VRUProgress variable), router call keys, date and time, and caller entered digits. Together with the TCD record, the Capture micro-application writes a set of records to the Termination_Call_Variable (TCV) table which includes the current values of all ECC variables.

Packaged CCE provides no standard reporting templates for TCD and TCV records. These tables are large and minimally indexed, and are optimized for writing rather than querying, to minimally impact call handling throughput. If you plan to report on this data, create off-hours extract processes which copy rows in their raw format into a database which is external to Packaged CCE. From there you can organize the tables in the way that best supports your querying requirements.

Information you need about these records includes:

- TCD records for a given call may be identified because they contain the same RouterCallKeyDay and RouterCallKey. Successive TCD records are ordered by incrementing RouterCallKeySequenceNumber.
- Intermediate TCD records may be identified because they contain a CallDisposition of 53, "PartialCall". Only the last TCD record for the call contains the actual disposition.
- TCV records corresponding to a particular TCD record may be obtained by joining on TCV.TCDRecoveryKey. This key matches the RecoveryKey value in the TCD record.
- The TCD record's CallTypeId is also populated for VRU peripherals. This means you can determine the call's current CallType at each Capture micro-application invocation, and at the end of the call.
- In Unified CVP Comprehensive call flow models, these records are associated with the VRU leg peripheral. If you are doing VRU application reporting, you can filter for TCD records which contain the PeripheralID of the Unified CVP VRU leg.

The Capture micro-application places a heavy demand on Packaged CCE resources. Each time you use it, Packaged CCE writes one TCD record and multiple TCV records. Though it can conveniently capture the information you need, it can also capture extra information which you do not require. If you overuse this micro-application, it can place a heavy load on Packaged CCE in terms of processing time and disk space, which despite the minimal indexing, may impact Packaged CCE's ability to handle the expected call load. Carefully choose where you need to capture information in your scripts. Spread data items into as many call variables as possible to maximize the usefulness of each invocation.

Play Media Micro-application

The Play Media (PM) micro-application can be configured to play a message that is contained in a media file or streaming audio file.

Configure Network VRU Script for Play Media

Use Packaged CCE Administration's Network VRU Scripts tool to specify parameters.

Procedure

-
- Step 1** Configure VRU Script field parameters:

- **Micro-application type.** For Play Media, valid options are: **PM** or **pm**.
- **Media File Name.** Name of the media file to be played (that is, the prompt file) or the name of the external VoiceXML file.
The valid options are:
 - A file name (for instance, a .wav file).
 - **null** - (default) If this field is empty, no prompt is played.
 - **-(number 1-10)** - Unified CVP plays the file in the corresponding Call.PeripheralVariable file. For example, a value of 2 instructs Unified CVP to look at Call.PeripheralVariable2.
 - **-a** - Unified CVP automatically generates the media file name for agent greeting when this option is specified. The file name is based on GED-125 parameters received from Packaged CCE .
- **Media Library Type.** Flag indicating the location of the media files to be played.
The valid options are:
 - **A** - (default) Application
 - **S** - System
- **Uniqueness value.** Optional. A string identifying a VRU Script Name as unique.

Step 2 Configure the Configuration Param field parameters:

- **Barge-in Allowed.** Specifies whether barge-in (digit entry to interrupt media playback) is allowed.
The valid options are:
 - **Y** - (default) barge-in allowed
 - **N** - barge-in not allowed

Note Voice barge-in is not supported by Play Media and Play Data micro-applications. However, Dual Tone Multifrequency (DTMF) barge-in is supported for these micro-applications.
For more information about barge-in, see [How Unified CVP Handles Barge-In, on page 531](#).
- **RTSP Timeout.** Specifies the Real-time Streaming Protocol (RTSP) timeout - in seconds - when RTSP is used.
The valid range is 0 - 43200 seconds (default is 10 seconds). If the value is set to 0 or a timeout value is not provided, the stream does not end.
See [Configure Play Media Micro-application to Use Streaming Audio, on page 531](#) for more details.
- **Type-ahead Buffer Flush.** The Cisco VoiceXML implementation includes a type-ahead buffer that holds DTMF digits collected from the caller. When the VoiceXML form interpretation algorithm collects user DTMF input, it uses the digits from this buffer before waiting for further input. This parameter controls whether the type-ahead buffer is flushed after the prompt plays out. A false value (default) means that the type-ahead buffer is not flushed after the prompt plays out. If the prompt allows barge-in, the digit that barges in is not flushed.

The valid options are

- **Y** - flush the type-ahead buffer
- **N** - (default) do not flush the type-ahead buffer

Note This parameter is usually used when two or more PM and/or PD microapps are used in a loop in the Packaged CCE script (such as while in queue for an agent). If the PM and/or PD microapps are enabled for barge-in, one would set this parameter to **Y** to prevent an uncontrolled looping in the Packaged CCE script when the user barges in.

How Unified CVP Handles Barge-In

Unified CVP deals with barge-in as follows:

- If barge-in is not allowed, the gateway continues prompt play when a caller starts entering digits.
- If barge-in is allowed, the gateway discontinues prompt play when the caller starts entering digits. See [Get Speech and External VoiceXML, on page 561](#)

Configure Play Media Micro-application to Use Streaming Audio

Use the Script Editor to configure Play Media (PM) micro-application to play .wav files from a streaming audio server.

Cisco does not sell, OEM, or support any Media Servers. The IOS gateway only supports μ -law wav files in 8-bit format. Media Servers such as RealNetwork's Helix™ Server will serve RTSP broadcast audio streams in the μ -Law format.



Note The IOS gateway only supports μ -law wav files in 8-bit format.

You must enclose the stream URL and stream name values in quotation marks.

Procedure

Step 1 Add a Set Node in the script to configure the media_server ECC variable.

- On the Set Variable tab of the Set Properties dialog box, select **Call** from the Object Type drop down and then set the Variable to user.microapp.media.server.

The screenshot shows the 'Set Properties (Read Only)' dialog box with the following configuration:

- Object type:** Call
- Object:** (No selection)
- Variable:** user.microapp.media_server
- Array index:** (empty)
- Value:** "rtsp://10.86.129.250:554/broadcast"

- In the Value field, specify the URL up to, but not including, the stream name.

Note The URL must begin with an *rtsp://* prefix (Real-time Streaming Protocol) to stream audio over the network. A trailing forward slash is not permitted in the URL.

- Click **OK**.

Step 2 Add another Set Node in the script to configure the stream name.

- On the Set Variable tab of the Set Properties dialog box, select Call from the Object Type drop down and set the Variable to **PeripheralVariable<1>**.

The range for standard Peripheral Variables is PeripheralVariable1 through PeripheralVariables10.

The screenshot shows the 'Set Properties (Read Only)' dialog box with the following configuration:

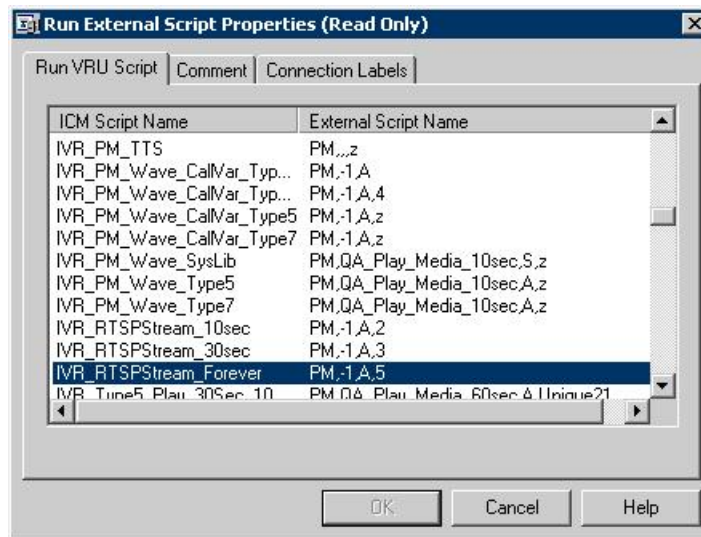
- Object type:** Call
- Object:** (No selection)
- Variable:** PeripheralVariable1
- Array index:** (empty)
- Value:** "african.rm"

- In the Value field, specify the stream name and click **OK**.

Note Stream names are case-sensitive.

Step 3 Add a Run External Script node to the workspace and double-click Run External Script.

The Run External Script Properties dialog box lists all of the Network VRU scripts that are currently configured.



Note In the example above, the Unified CVP_RTSPStream_Forever script's external script name contains four parameters: PM, -1, A, 5. The second parameter, **-1**, instructs Unified CVP to play the stream name declared in **PeripheralVariable1** (shown in Step 2). Configure streaming audio following the steps outlined so that you may easily change the stream name within the Script Editor, if necessary.

You can also use the Run External Script node in the CCE Script Editor to configure CCE to failover to a new streaming server. For example, if you want to point to an alternate streaming server (IP address), use the X-path out of the Run External Script node to redefine the media_server ECC variable. In a failover situation, the script is run and the stream plays from the targeted streaming server and proceeds generally.

Step 4 From the Run VRU Script tab, select the Script Name desired and click **OK**.

Step 5 Optionally, you can use the Packaged CCE Administration's Network VRU Scripts tool to configure the timeout value for the stream.

Configure the Configuration Param field parameter:

- In the RTSP Timeout field, enter a timeout value (in seconds).
 - The valid range is 0 - 43200 seconds.
 - If the value is set to 0 or a timeout value is not provided the stream does not end.

Step 6 Access the IOS device in global configuration mode and use the **rtsp client timeout connect** command to set the number of seconds the router waits before it reports an error to the Real-time Streaming Protocol (RTSP) server.

The range is 1 to 20. The standard value is 10 seconds.

If the SIP Call with Unified CVP Service is Terminated with **Reason Code: Q.850;Cause=38** then be sure that the network interface configuration is as follows:

```
ip route-cache same-interface
ip route-cache cef
ip route-cache
ip mroute-cache
no cdp enable
```

If specified, remove the following line from the network interface:

```
keepalive 1800
```

This issue arises if the Unified CVP loses network connectivity, then the VXML Server Gateway is not able to get information from the CVP Service, and as a result a code 38 rejection is generated in the Gateway logs.

Related Topics

[Configure Custom Streaming Ringtones](#), on page 534

Configure Custom Streaming Ringtones

You can configure custom ringtone patterns that enable you to play an audio stream to a caller in place of the usual ringtone. Customized streaming ringtones are based on the dialed number destination and, when configured, play an in-progress broadcast stream to the caller while the call is transferred an agent.

Play Media Examples: Play Welcome Message

The following table shows some Network VRU Script configuration examples for Play Media.

Table 33: Network VRU Script Configuration Examples

Example	Field Name	Field Contents	Tells Unified CVP...
1	VRU Script Name	PM,Welcome	To use the Play Media (PM) micro-application to play the "Welcome.wav" Media file and accept the defaults for remaining settings. Note If no file extension is specified, .wav is assumed.
	Configuration Param	N	That Barge-in <i>is not</i> allowed.
2	VRU Script Name	pm,July,S	To use the Play Media (PM) micro-application to play the "July.wav" Media file, using the System (S) Media library.
	Configuration Param	Null (Accept default.)	That Barge-in <i>is</i> allowed.

Example	Field Name	Field Contents	Tells Unified CVP..
3	VRU Script Name	PM,WebSite,,0	To use the Play Media (PM) micro-application to play the "Website.wav" Media file, using the default Media Type (Application library), and setting 0 as the Uniqueness value. Note A , (comma) indicates a skipped parameter. When a parameter is skipped, Unified CVP applies its default.
	Configuration Param	Null (Accept default.)	That Barge-in <i>is</i> allowed.
4	VRU Script Name	PM,WebSite,,1	To use the Play Media (PM) micro-application to play the "Website.wav" Media file, using the default Media Type (Application library), and setting 1 as the Uniqueness value.
	Configuration Param	N	That Barge-in <i>is not</i> allowed.
5	VRU Script Name	PM, -3, A	To use the Play Media (PM) micro-application, using the file listed in Call.PeripheralVariable3, acquiring the file from the Application (A) media library.
	Configuration Param	N	That Barge-in <i>is not</i> allowed.
6	VRU Script Name	PM, stream.rm	To use the Play Media (PM) micro-application to play "stream.rm" from a streaming audio server and accept the defaults for remaining settings.
	Configuration Param	N, 30	That Barge-in <i>is not</i> allowed, and the stream is configured to stop playing in 30 seconds.



Note Play Media sets the ECC variable `user.microapp.error_code` to zero, indicating success, if control proceeds out the Checkmark (success) branch of the Run External Script node. If control proceeds out the X (failure) branch, Play Media typically sets this variable to one of the codes listed in [Unified CVP Script Error Checking, on page 521](#).

Play Data Micro-application

The Play Data micro-application retrieves data from a storage area and plays it to the caller in a specific format, called a data play back type.

Some possible sources of the data to be played back:

- Information retrieved from a database look-up

- Information entered by the caller

Play Data and Data Storage

Before this micro-application can be called, you must specify the location of the play back data. You do this with a Script Editor Set node that points to one of the following storage areas:

- One of the standard Packaged CCE Peripheral Variables (PeripheralVariable1 through PeripheralVariables10).
- The `user.microapp.play_data` elements.

Configure Network VRU Script Settings for Play Data Micro-application

Use the Unified CCE Administration Network VRU Script tool's Attributes tab to specify parameters.



Note Voice barge-in is not supported by Play Media and Play Data micro-applications. However, DTMF barge-in is supported for these micro-applications.

If you are using integers that are larger than nine digits, enclose the value in quotation marks, so it will be treated as a string.

Before you begin

Procedure

Step 1 Configure VRU Script field parameters:

- **Micro-application type.** For Play Data, valid options are: **PD** or **pd**.
- **Data Playback Type.** The type of the data to be returned (“played”) to the caller. The valid options are:
 - **Number**
 - **Char** (character)
 - **Date**
 - **Etime** (elapsed time)
 - **TOD** (Time of Day)
 - **24TOD** (24-hour Time of Day)
 - **DOW** (Day of Week)
 - **Currency**

Note 24TOD and DOW data play back types are not supported when using TTS. Currency other than US dollar (USD) is not supported.

For more information about each of these playback types, including input format and output examples, see [Play Back Types for Voice Data, on page 538](#).

- **Uniqueness value.** Optional. A string identifying a VRU Script Name as unique.

Step 2 Configure the Configuration Param field parameters:

- **Location of the data to be played .** The valid options are:
 - *null* (default) - If you leave this option empty, uses the ECC variable **user.microapp.play_data**.
 - A **number** representing a Call Peripheral Variable number (for example, a 1 to represent Call.PeripheralVariable1).

Note For more information on data location, see [Play Data and Data Storage, on page 536](#).

- **Barge-in Allowed.** Specifies whether barge-in (digit entry to interrupt media playback) is allowed.

The valid options are:

- **Y** - (default) barge-in allowed
- **N** - barge-in not allowed

Note Voice barge-in is not supported by Play Media and Play Data micro-applications. However, DTMF barge-in is supported for these micro-applications.

For more information about barge-in, see [Play Data and Data Storage, on page 536](#).

- **Time Format**

Valid only for the time Data Playback types (Etime, TOD, 24TOD).

The available formats are:

- *null* - leave this option empty for non-time formats
- **HHMM** - default for time formats
- **HHMMSS** - includes seconds
- **HHMMAP** - includes am or pm; valid only for TOD

- **Type-ahead Buffer Flush .** The Cisco VoiceXML implementation includes a type-ahead buffer that holds DTMF digits collected from the caller. When the VoiceXML form interpretation algorithm collects user DTMF input, it uses the digits from this buffer before waiting for further input. This parameter controls whether the type-ahead buffer is flushed after the prompt plays out. A false value (default) means that the type-ahead buffer is not flushed after the prompt plays out. If the prompt allows barge-in, the digit that barges in is not flushed.

The valid options are:

- **Y** - flush the type-ahead buffer
- **N** - (default) do not flush the type-ahead buffer

- Note** This parameter is only applicable when using the Cisco IOS gateway with DTMF barge-in. This parameter is generally used when two or more PM and/or PD microapps are used in a loop in the CCE script (such as while in queue for an agent). If the PM and/or PD microapps are enabled for barge-in, one would set this parameter to **Y** to prevent an uncontrolled looping in the CCE script when the user barges in.
-

Play Back Types for Voice Data

Configuring how voice data is presented to a caller is an important part of setting up your Unified CVP. The "Data Play Back Types" table below describes each type, along with sample valid values and formats for the supported locales when **not** using TTS:

- **en-us**. English (United States)
- **en-gb**. English (Great Britain)
- **es-mx**. Spanish (Mexico)
- **es-es**. Spanish (Spain)

Locale is selected by setting the **user.microapp.locale** variable.

Any string of characters typically used in the language may need to be spoken back character by character (this includes special keyboard symbols and numbers). If a particular symbol is not used by a particular language, a string containing that symbol may be spelled out with a Play Data with Char data type.

For example, assume that a Unified CVP application in the US (a locale of **en-us**) queries a database for an account owner's name and spells the name back to the caller. If the name pulled from the database was "Hänschen Walther," the media files that would need to be pulled from the Media Server would have been derived from a URL including the **en-us** locale. The symbol **ä** has a decimal value of 228, which is different than the symbol **a** which has a value of 97. It is the translator's task to record the proper word(s) for each symbol to be supported. For detailed information on character translation, refer to [System Media Files, on page 541](#).

Table 34: Data Play Back Types

Data Play Back Type	Description	Input Format	Output Examples (When Not Using TTS)
Number	Play the stored data as a number.	<p>#####.#####</p> <p>The leading minus (-) is optional and is played as “minus.”</p> <p>The whole number portion of the string can contain a maximum of 15 digits (for a maximum value of 999 trillion, 999 billion and so on).</p> <p>The decimal point is represented as a period (.) and played as “point.” It is optional if there is no floating portion.</p> <p>The floating point portion of the number is optional and can contain a maximum of six digits.</p> <p>Trailing zeros are played.</p>	<p>en-us and en-gb typical spoken form:</p> <ul style="list-style-type: none"> • -123 = “minus one hundred twenty three” • 35.67 = “thirty five point six seven” • 1234.0 = “one thousand, two hundred, thirty four point zero” <p>es-mx and es-es typical spoken form:</p> <ul style="list-style-type: none"> • -120 = “menos ciento veinte” • 10.60 = “diez coma seis cero” • 1,100 = “mil cien”
Char	Play the stored data as individual characters.	<p>All printable American National Standards Institute (ANSI) characters are supported.</p> <p>Note Code Page 1252 is ANSI standard. It contains ASCII (characters 0-127) and extended characters from 128 to 255</p>	<p>en-us and en-gb typical spoken form:</p> <ul style="list-style-type: none"> • abc123= “A, B, C, one, two, three” <p>es-mx and es-es typical spoken form:</p> <ul style="list-style-type: none"> • abc123 = “A, B, C, uno, dos, tres”

Data Play Back Type	Description	Input Format	Output Examples (When Not Using TTS)
Date	Play the stored data as a date.	YYYYMMDD, regardless of locale. YYYY options: the range of 1800 through 9999. MM options: the range of 01 through 12. DD options: the range of 01 through 31. Note The software does not validate the date (for example, 20000231 is valid and played accordingly). However, a failure occurs if any bounds are broken (for example, 34 for month).	en-us typical spoken form: <ul style="list-style-type: none"> • MMDDYYYY format: 20000114 = “January fourteenth, two thousand” en-gb typical spoken form: <ul style="list-style-type: none"> • DDMMYYYY format: 20000114 = “Fourteenth of January, two thousand” es-mx and es-es typical spoken form: <ul style="list-style-type: none"> • DDMMYYYY format: 20001012 = "doce octubre dos mil" Note All spoken forms use the proper grammar for the locale.
Etime (elapsed time)	Play the stored data as an amount of elapsed time.	HHMM or HHMMSS Maximum 99 hours, 59 minutes, 59 seconds Leading zeros are ignored.	en-us and en-gb typical spoken form: <ul style="list-style-type: none"> • HHMM format: 0830= “eight hours thirty minutes” • HHMMSS format: 083020= “eight hours, thirty minutes, twenty seconds” es-mx and es-es typical spoken form: <ul style="list-style-type: none"> • HHMM format: 0205 = “dos horas cinco minutos” • HHMMSSS format: 020101 = “dos horas un minuto un segundo”

Data Play Back Type	Description	Input Format	Output Examples (When Not Using TTS)
TOD (Time of Day)	Play the stored data as a time of day.	HHMM or HHMMSS 24 hour time HH options: 00 - 24 MM options: 00 - 59 SS options: 00 - 59	en-us and en-gb typical spoken form: <ul style="list-style-type: none"> • HHMM format: 0800 = “eight o’clock” 0830 = “eight thirty” 1430 = “two thirty” • HHMMSS format: 083020 = “eight thirty and twenty seconds” • HHMMAP format: 1430 = “two thirty p.m.” es-mx and es-es typical spoken form: <ul style="list-style-type: none"> • HHMM format: 0100 = “una a.m.” • HHMMAP format: 1203 = “doce y tres p.m.” • HHMMSS format: 242124 = “doce veintiuno a.m.”
DOW (Day of Week)	Play the stored data as a day of week.	An integer from 1 through 7 (1 = Sunday, 2 = Monday, et cetera). Note The DOW data play back type is not supported when using TTS.	en-us and en-gb typical spoken form: <ul style="list-style-type: none"> • 7 = “Saturday” es-mx and es-es typical spoken form: <ul style="list-style-type: none"> • 7 = “Sabado”

System Media Files

The following tables describe the English System Media Files installed by Unified CVP. These system media files are intended as samples only. It is the Customer/Media Administrator’s responsibility to record all the system prompts for all the locales.

The table that follows lists the System Media File information for cardinal numbers.

Table 35: System Media Files, Cardinal Numbers

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		point	point	Number
		minus	minus	Number
0	48	0	zero	All except DOW
1	49	1	one (masculine version), uno (es-mx and es-es)	All except DOW
2	50	2	two	All except DOW
3	51	3	three	All except DOW
4	52	4	four	All except DOW
5	53	5	five	All except DOW
6	54	6	six	All except DOW
7	55	7	seven	All except DOW
8	56	8	eight	All except DOW
9	57	9	nine	All except DOW
		10	ten	Same for the rest of all the numbers
		11	eleven	
		12	twelve	
		13	thirteen	
		14	fourteen	
		15	fifteen	
		16	sixteen	
		17	seventeen	
		18	eighteen	
		19	nineteen	
		20	twenty	
		21	twenty-one	
		22	twenty-two	

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types /When Media File Is Used
		23	twenty-three	
		24	twenty-four	
		25	twenty-five	
		26	twenty-six	
		27	twenty-seven	
		28	twenty-eight	
		29	twenty-nine	
		30	thirty	
		31	thirty-one	
		32	thirty-two	
		33	thirty-three	
		34	thirty-four	
		35	thirty-five	
		36	thirty-six	
		37	thirty-seven	
		38	thirty-eight	
		39	thirty-nine	
		40	forty	
		41	forty-one	
		42	forty-two	
		43	forty-three	
		44	forty-four	
		45	forty-five	
		46	forty-six	
		47	forty-seven	
		48	forty-eight	
		49	forty-nine	

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		50	fifty	
		51	fifty-one	
		52	fifty-two	
		53	fifty-three	
		54	fifty-four	
		55	fifty-five	
		56	fifty-six	
		57	fifty-seven	
		58	fifty-eight	
		59	fifty-nine	
		60	sixty	
		61	sixty-one	
		62	sixty-two	
		63	sixty-three	
		64	sixty-four	
		65	sixty-five	
		66	sixty-six	
		67	sixty-seven	
		68	sixty-eight	
		69	sixty-nine	
		70	seventy	
		71	seventy-one	
		72	seventy-two	
		73	seventy-three	
		74	seventy-four	
		75	seventy-five	
		76	seventy-six	

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		77	seventy-seven	
		78	seventy-eight	
		79	seventy-nine	
		80	eighty	
		81	eighty-one	
		82	eighty-two	
		83	eighty-three	
		84	eighty-four	
		85	eighty-five	
		86	eighty-six	
		87	eighty-seven	
		88	eighty-eight	
		89	eighty-nine	
		90	ninety	
		91	ninety-one	
		92	ninety-two	
		93	ninety-three	
		94	ninety-four	
		95	ninety-five	
		96	ninety-six	
		97	ninety-seven	
		98	ninety-eight	
		99	ninety-nine	
		oh	oh	24TOD, Date
		hundred	hundred	Number, 24TOD, Date, Currency

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		thousand	thousand	Number, Date, Currency
		million	million	Number, Currency
		billion	billion	Number, Date, Currency
		trillion	trillion	Number, Currency

The table that follows lists the System Media File information for ordinal numbers.



Note If ordinal system prompts are to be used in a script for a purpose other than dates, they should be recorded as application prompts with the true ordinal values.

Table 36: System Media Files, Ordinal Numbers

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		1ord	first	Date
		2ord	second	Date for all ordinal numbers
		3ord	third	
		4ord	fourth	
		5ord	fifth	
		6ord	sixth	
		7ord	seventh	
		8ord	eighth	
		9ord	ninth	
		10ord	tenth	
		11ord	eleventh	
		12ord	twelveth	
		13ord	thirteenth	
		14ord	fourteenth	

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		15ord	fifteenth	
		16ord	sixteenth	
		17ord	seventeenth	
		18ord	eighteenth	
		19ord	nineteenth	
		20ord	twentieth	
		21ord	twenty-first	
		22ord	twenty-second	
		23ord	twenty-third	
		24ord	twenty-fourth	
		25ord	twenty-fifth	
		26ord	twenty-sixth	
		27ord	twenty-seventh	
		28ord	twenty-eighth	
		29ord	twenty-nineth	
		30ord	thirtieth	
		31ord	thirty-first	

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

Table 37: System Media Files, Measurements

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
$\frac{1}{2}$	189	one_half	one half	Char
$\frac{1}{4}$	188	one_quarter	one quarter	Char
$\frac{3}{4}$	190	three_quarters	three quarters	Char
A, a	65,97	a	A	Char
B,b	66,98	b	B	Char

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
C, c	67,99	c	C	Char
D, d	68,100	d	D	Char
E, e	69,101	e	E	Char
F, f	70,102	f	F	Char
G, g	71,103	g	G	Char
H, h	72,104	h	H	Char
I, I	73,105	I	I	Char
J, j	74,106	j	J	Char
K, k	75,107	k	K	Char
L, l	76,108	l	L	Char
M, m	77,109	m	M	Char
N, n	78,110	n	N	Char
O, o	79,111	o	O	Char
P, p	80,112	p	P	Char
Q, q	81,113	q	Q	Char
R, r	82,114	r	R	Char
S, s	83,115	s	S	Char
T, t	84,116	t	T	Char
U, u	85,117	u	U	Char
V, v	86,118	v	V	Char
W, w	87,119	w	W	Char
X, x	88,120	x	X	Char
Y, y	89,121	y	Y	Char
Z, z	90,122	z	Z	Char
Œ, œ	140,156	oe_140_156	Ligature OE	Char
À,à	192,224	a_192_224	A grave	Char

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
Á,á	193,225	a_193_225	A acute	Char
Â,â	194,226	a_194_226	A circumflex	Char
Ã,ã	195,227	a_195_227	A tilde	Char
Ä,ä	196,228	a_196_228	A umlaut	Char
Å,å	197,229	a_197_229	A with ring above	Char
Æ,æ	198,230	ae_198_230	Ligature AE	Char
È,è	200,232	e_200_232	E grave	Char
É,é	201,233	e_201_233	E acute	Char
Ê,ê	202,234	e_202_234	E circumflex	Char
Ë,ë	203,235	e_203_235	E umlaut	
Ì,ì	204,236	i_204_236	I grave	Char
Í,í	205,237	i_205	I acute	Char
Î,î	206,238	i_206	I circumflex	Char
Ï,ï	207,239	i_207	I umlaut	Char
Ð	208	char_208	character 208	Char
ð	240	char_240	character 240	
Ò,ò	210,242	o_210_242	O grave	Char
Ó,ó	211,243	o_211_243	O acute	Char
Ô,ô	212,244	o_212_244	O circumflex	Char
Õ,õ	213,245	o_213_245	O tilde	Char
Ö,ö	214,246	o_214_246	O umlaut	Char
x	215	multiply	multiplication sign	Char
Ø,ø	216,248	o_216_248	oh stroke	Char
Ù,ù	217,249	u_217_249	U grave	Char
Ú,ú	218,250	u_218_250	U acute	Char
Û,û	219,251	u_219_251	U circumflex	Char
Ü,ü	220,252	u_220_252	U umlaut	Char

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
Ÿ,ÿ	221,253	y_221_253	Y acute	Char
Ɔ	222	char_222	character 222	Char
ß	223	ss	double s	Char
÷	247	divide	division sign	Char
Ɔ	254	char_254	character 254	Char
Ÿ,ÿ	159,255	y_159_255	character 159 or 255	Char

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

Table 38: System Media Files, Months

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		January	January	Date
		February	February	Date
		March	March	Date
		April	April	Date
		May	May	Date
		June	June	Date
		July	July	Date
		August	August	Date
		September	September	Date
		October	October	Date
		November	November	Date
		December	December	Date

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

Table 39: System Media Files, Days

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		Sunday	Sunday	DOW
		Monday	Monday	DOW
		Tuesday	Tuesday	DOW
		Wednesday	Wednesday	DOW
		Thursday	Thursday	DOW
		Friday	Friday	DOW
		Saturday	Saturday	DOW

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

Table 40: System Media Files, Time

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		hour	hour	Etime, 24TOD per locale, TOD per locale
		hours	hours	Etime, 24TOD per locale, TOD per locale
		minute	minute	Etime
		minutes	minutes	Etime
		second	second	Etime, 24TOD
		seconds	seconds	Etime, 24TOD
		on	on	per locale (unused for en-us)
		at	at	per locale (unused for en-us)
		am	am	TOD
		pm	pm	TOD
		oclock	oclock	TOD

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



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

Table 41: System Media Files, Currency

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		currency_minus	minus	Currency
		currency_and	and	Currency
\$	36	USD_dollar	dollar	Currency
		USD_dollars	dollars	Currency
		Note Unified CVP uses the USD_dollar.wav and USD_dollars.wav media files; the dollar.wav and dollars.wav used by ISN Version 1.0 are no longer installed.		
\$	36	CAD_dollar	dollar	Currency
		CAD_dollars	dollars	Currency
		HKD_dollar	dollar	Currency
		HKD_dollars	dollars	Currency
¢	162	cent	cent	Currency
		cents	cents	Currency
		euro	euro	Currency
£	163	GBP_pound	pound	Currency
		GBP_pounds	pounds	Currency
		penny	penny	Currency
		pence	pence	Currency
		MXN_peso	peso	Currency
		MXN_pesos	pesos	Currency
		centavo	centavo	Currency
		centavos	centavos	Currency

The table that follows lists the System Media File information for gaps of silence and miscellaneous phrases.

Table 42: System Media Files, Silence, and Miscellaneous Phrases

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		silence_.1_sec	(.1 second of silence)	Used for pauses where needed
		silence_.25_sec	(.25 second of silence)	Used for pauses where needed
		silence_.5_sec	(.5 second of silence)	Used for pauses where needed
		silence_1_sec	(1 second of silence)	Used for pauses where needed
		and	and	Etime,TOD,25TOD

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

Table 43: System Media Files, ANSI Characters

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
	32	space	space	Char
!	33	exclamation_mark	exclamation mark	Char
"	34	double_quote	double quote	Char
#	35	pound	pound	Char
%	37	percent	percent	Char
&	38	ampersand	ampersand	Char
'	39	apostrophe	apostrophe	Char
(40	open_parenthesis	open parenthesis	Char
)	41	close_parenthesis	close parenthesis	Char
*	42	asterisk	asterisk	Char
+	43	plus	plus	Char
,	44	comma	comma	Char
-	45	hyphen	hyphen	Char

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
.	46	period	period	Char
/	47	slash	slash	Char
:	58	colon	colon	Char
;	59	semicolon	semicolon	Char
<	60	less_than	less than	Char
=	61	equal	equal	Char
	62	greater_than	greater than	Char
?	63	question_mark	question mark	Char
@	64	at_symbol	at	Char
[91	left_square_bracket	left square bracket	Char
\	92	backslash	backslash	Char
]	93	right_square_bracket	right square bracket	Char
^	94	caret	caret	Char
_	95	underscore	underscore	Char
`	96	single_quote	single quote	Char
{	123	open_brace	open brace	Char
	124	pipe	pipe	Char
}	125	close_brace	close brace	Char
~	126	tilde	tilde	Char
'	130	char_130	low single quote	Char
<i>f</i>	131	char_131	F with hook	Char
”	132	low_double_quote	low double quote	Char
...	133	ellipsis	ellipsis	Char
†	134	char_134	character 134	Char
‡	135	char_135	character 135	Char
^	136	char_136	character 136	Char
‰	137	per_mille	per mile	Char

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
Š	138	char_138	character 138	
<	139	left_pointing_angle	left pointing angle	Char
‘	145	left_single_quote	left single quote	Char
’	146	right_single_quote	right single quote	Char
“	147	left_double_quote	left double quote	Char
”	148	right_double_quote	right double quote	Char
·	149	bullet	bullet	Char
–	150	en_dash	en dash	Char
—	151	em_dash	em dash	
~	152	small_tilde	small tilde	Char
™	153	trade_mark	trade mark	Char
š	154	char_154	character 154	Char
›	155	char_155	character 155	Char
¡	161	exclamation_mark_inverted	inverted exclamation mark	Char
⌘	164	char_164	character 164	Char
⏪	166	broken_pipe	broken pipe	Char
§	167	section	section	Char
¨	168	char_168	character 168	Char
©	169	copyright	copyright	Char
ª	170	char_170	character 170	Char
«	171	left_double_angle_quote	left double angle quote	Char
¬	172	not	not	Char
-	173	char_173	character 173	Char
®	174	registered	registered	Char
—	175	char_175	character 175	Char
°	176	degree	degree	Char

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
±	177	plus_minus	plus or minus	Char
²	178	superscript_2	superscript two	Char
³	179	superscript_3	superscript three	Char
´	180	acute_accent	acute accent	Char
μ	181	micro	micro	Char
¶	182	paragraph	paragraph	Char
·	183	middle_dot	middle dot	Char
¸	184	cedilla	cedilla	Char
¹	185	superscript_1	superscript one	Char
°	186	char_186	character 186	Char
»	187	right_double_angle_quote	right double angle quote	Char
¿	191	question_mark_inverted	inverted question mark	Char

Play Data Configuration Examples

The following table shows several configuration examples for Play Data.

Table 44: Play Data Configuration Examples

If the VRU Script Name field setting is...	It means...	If the Configuration Param field is...	It means...
PD,Number Note If you are using integers that are larger than nine digits, enclose the value in quotation marks, so it will be treated as a string.	PD - Use the Play Data micro-app. Number - Play back the data as a number.	empty	Play the data in the default ECC, user.microapp.play_data , as a number.
PD, Char	pd - Use the Play Data micro-app. Char - Play back the data as individual characters.	1	1 - Play the data in Call PeripheralVariable 1 as a character.

If the VRU Script Name field setting is...	It means...	If the Configuration Param field is...	It means...
PD,Etime,0 Note If you are using integers that are larger than 9 digits, enclose the value in quotation marks, so it will be treated as a string.	PD - Use the Play Data micro-app. Etime - Play back the data as a Time.	1,,HHMM	1 - Play the data in Call PeripheralVariable 1 as an elapsed time. , - (Skipped parameter) Accept default setting (Y) HHMM - Play the time in HHMM format (for example, 8 hours, 30 minutes).
PD,Date	PD - Use the Play Data micro-app. Date - Play back the data as a Date.	1,N	1 - Play the data in Call Variable 1 as a date. N - No barge-in allowed.
PD,Currency	PD - Use the Play Data micro-app. Currency - Play back the data as a Currency.	4,N	4 - Play the data in Call Variable 4 s currency. N - No barge-in allowed.



Note Play Data sets the ECC variable **user.microapp.error_code** to zero, indicating success, if control proceeds out the Checkmark (success) branch of the Run External Script node. If control proceeds out the X (failure) branch, Play Data typically sets this variable to one of the codes listed in [Unified CVP Script Error Checking, on page 521](#).

Get Digits Micro-application

The Get Digits (GD) micro-application plays a media file and retrieves digits. For example, you could use Get Digits in an application that prompts a caller to enter a password.

Unified Customer Voice Portal passes the retrieved digits back to Packaged CCE for further processing using the Caller-Entered Digits (CED) field in the CCE/Unified CVP Messaging interface. (This is available in the Packaged CCE script through the variable Call.CallerEnteredDigits).

Configure Network VRU Script Settings for Get Digits Micro-application

Use the Unified CCE Administration Network VRU Script tool to specify parameters.

Procedure

- Step 1** Configure VRU Script field parameters:
- **Micro-application type.** For Get Digits, valid options are: **GD** or **gd**.

- **Media File Name.** Name of the media file to be played (that is, the prompt file). The valid options are:
 - A file name (for instance, a .wav file).
 - Note** The file name is case-sensitive.
 - **null** - (default) If this field is empty, no prompt is played.
 - **-(number 1-10)** - Unified CVP plays the file in the corresponding Call.PeripheralVariable file. For example, entering -2 causes Unified CVP to look at Call.PeripheralVariable2.
- **Media Library Type** . Flag indicating the location of the media files to be played. The valid options are:
 - **A** - (default) Application
 - **S** - System
- **Uniqueness value.** Optional. A string identifying a VRU Script Name as unique.

Step 2 Configure the Configuration Param field parameters:

- **Minimum Field Length.** Minimum number of digits expected from the caller. The valid options are: **1-32** (the default is **1**)
- **Maximum Field Length.** Maximum number of digits expected from the caller. The valid options are: **1-32** (the default is **1**).
 - Note** For information about Maximum Field Length and the DTMF Termination Key, see [Get Digits and Digit Entry Completion, on page 561](#).
- **Barge-in Allowed** . Specifies whether barge-in (digit entry to interrupt media playback) is allowed. The valid options are:
 - **Y** - (default) barge-in allowed
 - **N** - barge-in not allowed

For more information about barge-in, see [How Unified CVP Handles Barge-In, on page 531](#).

 - Note** Unified CVP deals with barge-in as follows: If barge-in *is* not allowed, the SIP/Gateway continues prompt play when a caller starts entering digits. If barge-in *is* allowed, the Gateway discontinues prompt play when the caller starts entering digits. See [Get Speech and External VoiceXML, on page 561](#).
- **Inter-digit Timeout** . The number of seconds the caller is allowed between entering digits. If exceeded, the system times-out. The valid options are: **1-99** (the default is **3**).
- **No Entry Timeout** . The number of seconds a caller is allowed to begin entering digits. If exceeded, the system times-out. The valid options are: **0-99** (the default is **5**).
- **Number of No Entry Tries.** Unified CVP repeats the “Get Digits” cycle when the caller does not enter any data after the prompt has been played. (Total includes the first cycle.) The valid options are: **1-9** (the default is **3**).

- **Number of Invalid Tries.** Unified CVP repeats the “Get digits” cycle when the caller enters invalid data (total includes the first cycle). The valid options are: **1-9** (default is **3**).
- **Timeout Message Override** . The valid options are:
 - **Y** - override the system default with a pre-recorded Application Media Library file
 - **N** - (default) do not override the system default
- **Invalid Entry Message Override.** The valid options are:
 - **Y** - override the system default with a pre-recorded Application Media Library file.
 - **N** - (default) do not override the system default

Note For more information about Timeout and Invalid Entry Messages, see [System Media Files, on page 541](#).

- **DTMF Termination Key.** A single character that, when entered by the caller, indicates that the digit entry is complete. The valid options are:
 - **0-9**
 - ***** (asterisk)
 - **#** (pound sign, the default)
 - **N** (No termination key)

Note For information about Maximum Field Length and the DTMF Termination Key, see [Get Digits and Digit Entry Completion, on page 561](#).

- **Incomplete Timeout.** The amount of time after a caller stops speaking to generate an invalid entry error because the caller input does not match the defined grammar. The valid options are: **0-99** (the default is **3**).

Note If the value is set to 0, the Unified CVP Service treats the NoEntry Timeout as NoError.

Get Digits Configuration Examples

The following table shows several configuration examples for Get Digits for an application that prompts using .wav files and retrieves input through DTMF.

Table 45: Get Digits Configuration Examples for .wav Files

If the VRU Script Name field setting is...	It means...	If the Configuration Param field setting is...	It means...
GD>Password,A,0	<p>GD - Use the Get Digits micro-app.</p> <p>Password - Play the Media file named "Password.wav."</p> <p>A - Application Media Library.</p> <p>0 - Uniqueness value.</p>	6,12	<p>6 - Minimum field length</p> <p>12 - Maximum field length</p> <p>Accept defaults for all other settings.</p>
GD>Password,A,1	<p>gd - Use the Get Digits micro-app.</p> <p>Password - Play the Media file named "Password.wav."</p> <p>A - Application Media Library.</p> <p>1 - Uniqueness value.</p>	6,12,N,3,5,2,2,N,Y,#	<p>6 - Minimum field length</p> <p>12 - Maximum field length</p> <p>N - No barge-in allowed</p> <p>3 - Inter-digit Timeout (seconds)</p> <p>5 - No Entry Timeout (seconds)</p> <p>2 - Number of no entry tries</p> <p>2 - Number of invalid tries</p> <p>N - Timeout Msg Override</p> <p>Y - Invalid Entry Msg Override</p> <p># - DTMF Termination key</p>
Note	The two examples above both play the Password.wav file ("Please enter your password followed by the pound sign.") and collect digits. They differ in that the first example accepts most of the default settings available through the Configuration Param field; the second field does not.		
GD,ssn	<p>GD - Use the Get Digits micro-app.</p> <p>ssn - Play the Media file named "ssn.wav."</p>	9,9,	<p>9 - Minimum field length</p> <p>9 - Maximum field length</p> <p>Accept defaults for all other settings.</p>
Note	Type-ahead can only be used with the Get Digits micro-application when <code>user.microapp.input_type</code> is set to D . See Get Speech and External VoiceXML, on page 561 .		
GD, -4, S	<p>gd - Use the Get Digits micro-app</p> <p>-4 - Calls the file specified in Call.PeripheralVariable4</p> <p>S - Acquires the file from the System media library</p>	6,12,	<p>6 - Minimum field length</p> <p>12 - Maximum field length</p> <p>Accept defaults for all other settings</p>

Get Speech and External VoiceXML

You can use the Get Speech micro-application to pass information to and from an external VoiceXML file. The following table describes how to set the Get Speech script to use external VoiceXML.

To set up the Get Speech micro-application to use external VoiceXML, set the Media Library Type to "V". The Unified CVP Service creates VoiceXML that calls the external VoiceXML that is specified in the external VoiceXML file name. The URL to the external VoiceXML is formed from a combination of the media_server, locale, App_Media_Lib and external VoiceXML file name. If the VoiceXML file name does not contain a file extension, the default "*.VoiceXML" is used.

If the external VoiceXML is used, the only GetSpeech VRU Script parameters that are used are:

- "Number of Invalid Entry" errors, and
- "Number of No Entry" errors.

The Unified CVP Service "NoEntry" and "InvalidEntry" retry logic are used if the external VoiceXML returns a <noinput> or <nomatch> event.

Error Handling

Error handling

The error handling for an external VoiceXML called from the Get Speech micro-application includes the following:

- If you set the "Media Library Type" to "V" and you do not set an "External VoiceXML Name" parameter, an "Invalid VRU Script Name" error is returned to Packaged CCE .

Get Digits and Digit Entry Completion

Unified CVP tests GD digit entry input against several conditions to determine whether digit entry is complete.

Unified CVP considers digit entry to be complete if the caller enters any of the following:

- The maximum allowable number of digits (when terminator key is not used).
- The maximum number of digits, excluding a terminator key.
- Less than the maximum number of digits, followed by the terminator key.
- Less than the maximum number of digits and exceeding the inter-digit timeout.
- Nothing and reaching the no entry timeout.



Caution It is important that you set up your Packaged CCE script to test for all the scenarios mentioned below.

If Digit Entry Input Is Complete

After digit-entry input is complete, Unified CVP validates the digit string to determine if it is >= (greater than or equal to) the minimum length and <= (less than or equal to) the maximum length.

In variable-length data entry, the Maximum Field Length value does not accommodate the termination key. For example, if a GD micro-application is configured to accept a password that is between 6 and 12 digits

long and digit-entry completion is indicated through a termination key (or a timeout), the Minimum Field Length setting would be 6, the Maximum Field Length setting would be 12, and the DTMF Termination Key is defined as a single character.

Before passing the result back to the Unified CVP Service, SIP Service discards the termination key (only the password digits are included in the CED returned to Packaged CCE).



Note In this example, if the 13th digit is entered without reaching the interdigit timeout and the 13th digit is not the terminator key, the extra digits are buffered by the gateway VXML browser and will be consumed by the next digit collecting node (for example: GD or Menu micro-app).

This type-ahead behavior is described online in the Type-ahead Support section of the [Cisco VoiceXML Programmer's Guide](#).

After validating the digit string, Unified CVP does the following:

- If the string is valid, Unified CVP stores the digit string (not including the terminator key) in the Call.CallerEnteredDigits variable, exits the node through the Checkmark (success) branch, and returns control to Packaged CCE software.
- If the string is not valid, Unified CVP considers it an invalid entry and does the following:
 - If the Number of Invalid Entry Tries value is not reached, Unified CVP plays an error message and re-plays the original prompt.
 - If the Number of Invalid Entry Tries value is reached, Unified CVP stores the last-entered digit string in the Call.CallerEnteredDigits variable, exits the node through the X (failure) branch, sets the **user.microapp.error_code** ECC variable to **16** (Reached Maximum Invalid Tries), and returns control to Packaged CCE .

If No Entry Timeout Occurs

If the caller does not enter input and No Entry Timeout period is exceeded, the following happens:

- If the Number of No Entry Tries value has not been reached, Unified CVP plays the “no entry” error message and re-plays the original prompt.
- If the Number of No Entry Tries value has been reached, Unified CVP exits the node through the X (failure) branch, sets the Call.CallerEnteredDigits variable to NULL, the **user.microapp.error_code** ECC variable to **17** (Reached Maximum No Entry Tries), and returns control to Packaged CCE .

Menu Micro-application

This micro-application plays a menu media file and retrieves a defined digit. (Menu is similar to the Get Digit micro-application except that it only accepts one digit, which it checks for validity.)

Unified CVP passes the retrieved digit back to Packaged CCE for further processing using the Caller-Entered Digits (CED) field in the Packaged CCE / Unified CVP Messaging interface.

Configure Network VRU Script Settings for the Menu Micro-application

Use the Packaged CCE Administration Network VRU Script tool to specify parameters.

Procedure

Step 1

Configure VRU Script field parameters:

- **Micro-application type** . For Menu, valid options are: **M** or **m**.
- **Media File Name**. Name of the media file to be played (that is, the prompt file). The valid options are
 - A file name (for instance, a .wav file)
 - Note** The file name is case-sensitive.
 - **null** - (default) If this field is empty, Unified CVP examines the contents of the **user.microapp.inline_tts** ECC variable. If this ECC variable contains a value, Unified CVP prompts using TTS. If the ECC is empty, no prompt is played.
 - **-(number 1-10)** - Unified CVP plays the file in the corresponding Call.PeripheralVariable file. For example, entering -2 causes Unified CVP to look at Call.PeripheralVariable2.
- **Media Library Type** . Flag indicating the location of the media files to be played. The valid options are:
 - **A** - (default) Application
 - **S** - System
- **Uniqueness value**. Optional. A string identifying a VRU Script Name as unique.

Step 2

Configure the Configuration Param field parameters:

- A list of **menu choices** . The valid options are:
 - **0-9**
 - ***** (asterisk)
 - **#** (pound sign)

Formats allowed include:

- Individual options delimited by a / (forward slash)
- Ranges delimited by a - (hyphen) with no space
- **Barge-in Allowed** . Specifies whether barge-in (digit entry to interrupt media playback) is allowed.

The valid options are:

- **Y** - (default) barge-in allowed
- **N** - barge-in not allowed

For more information about barge-in, see [How Unified CVP Handles Barge-In, on page 531](#).

- **No Entry Timeout** . The number of seconds a caller is allowed to begin entering digits. If exceeded, the system times-out. The valid options are: **0-99** (the default is **5**).

- **Number of No Entry Tries.** Unified CVP repeats the "Menu" cycle when the caller does not enter any data after the prompt has been played. (Total includes the first cycle.) The valid options are: **1-9** (the default is **3**).
- **Number of Invalid Tries .** Unified CVP repeats the prompt cycle when the caller enters invalid data. (Total includes the first cycle.) The valid options are: **1-9** (the default is **3**).
- **Timeout Message Override.** The valid options are:
 - **Y** - override the system default with a pre-recorded Application Media Library file
 - **N** - (default) do not override the system default
- **Invalid Entry Message Override .** The valid options are:
 - **Y** - override the system default with a pre-recorded Application Media Library file
 - **N** - (default) do not override the system default

Note For more information about Timeout and Invalid Entry Messages, refer to [System Media Files, on page 541](#)

Menu Configuration Examples

The following table shows several configuration examples for Menu for use in an application where input type is DTMF.

Table 46: Menu Configuration Example - DTMF Application

If the VRU Script Name field setting is...	It means...	If the Config Param setting is...	It means...
M, Banking	<p>M - Use the Menu micro-app.</p> <p>Banking - Play the Media file named "Banking.wav."</p> <p>Note This file may contain a message such as: "For Checking, press 1. For Savings, press 2. For Money Market, press 3."</p>	1-3	1-3 - Accept numbers 1, 2, 3. Accept all other defaults (No Entry Timeout, Number of no entry tries, Number of invalid tries, Timeout Msg Override, Invalid Entry Msg Override).

If the VRU Script Name field setting is...	It means...	If the Config Param setting is...	It means...
M,Main_Menu	<p>M - Use the Menu micro-app.</p> <p>Main_Menu - Play the Media file called "Main_Menu.wav."</p> <p>Note This file may contain a message such as: "For information or transactions on checking, press 1. For savings or club accounts, press 2. For other information, press 0. If you know your party's extension, press 9."</p>	0-2/9,,4,2,2	<p>0-2/9 - Accept numbers 0, 1, 2, and 9.</p> <p>, (Skipped parameter) - Accept the default barge-in setting (Y).</p> <p>4 - No Entry Timeout value (in seconds).</p> <p>2 - Number of no entry tries allowed.</p> <p>2 - Number of invalid tries allowed.</p> <p>Accept all other defaults (Timeout Msg Override, Invalid Entry Msg Override).</p>
M,-2,S	<p>M - Use the Menu micro-app.</p> <p>-2 - Plays the file specified in Call.PeripheralVariable2.</p> <p>S - Acquires the file from the System media library.</p>	1-3	<p>1-3 - Accept numbers 1, 2, 3. Accept all other defaults (No Entry Timeout, Number of no entry tries, Number of invalid tries, Timeout Msg Override, Invalid Entry Msg Override).</p>



Note Menu sets the ECC variable **user.microapp.error_code** to zero, indicating success, if control proceeds out the Checkmark (success) branch of the Run External Script node. If control proceeds out the X (failure) branch, Menu typically sets this variable to one of the codes listed in [Unified CVP Script Error Checking, on page 521](#).

Menu and Digit Entry Completion

Unified CVP tests Menu digit entry input against two conditions to determine whether digit entry is complete:

- If a caller enters a digit, Unified CVP checks whether the digit is within the set of valid digits for this menu.
- If a caller does not enter a digit, Unified CVP checks whether the No Entry Timeout value has been reached.



Caution It is important that you set up your Packaged CCE script to test for all the scenarios mentioned below.

Digit Entry Completion

After a caller enters a digit, Unified CVP validates the digit against the list of valid menu options that were defined through CCE Configuration Manager. Then Unified CVP does the following:

- If the digit is valid, Unified CVP stores the digit in the `Call.CallerEnteredDigits` variable, exits the node through the Checkmark (success) branch, and returns control to Packaged CCE .
- If the digit is not valid, Unified CVP considers it an invalid entry and does the following:
 - If the Number of Invalid Entry Tries value *has not* been reached, Unified CVP plays the "invalid message" file and re-plays the menu prompt.
 - If the Number of Invalid Entry Tries value has been reached, Unified CVP stores the last-entered invalid digit in the `user.microapp.caller_input` variable, exits the node through the X (failure) branch, sets the `user.microapp.error_code` ECC variable to **16** (Reached Maximum Invalid Tries), and returns control to Packaged CCE .

If No Entry Timeout Occurs

If the caller does not enter a digit within the No Entry Timeout period:

- If the Number of No Entry Tries value is reached, Unified CVP plays the "no entry" error message and re-plays the menu prompt.
- If the Number of No Entry Tries value has been reached, Unified CVP exits the node through the X (failure) branch, sets the `Call.CallerEnteredDigits` variable to NULL, the `user.microapp.error_code` ECC variable to **17** (Reached Maximum No Entry Tries), and returns control to Packaged CCE .

Get Speech Micro-application

The Get Speech (GS) micro-application is used to run a Call Studio script on VXML Server.

Configure Network VRU Script Settings for the Get Speech Micro-application

Use the Packaged CCE Administration's Network VRU Script tool to specify parameters.



Note By default a pre-configured network VRU script called `VXML_Server` has already been configured in Packaged CCE. This should be used in all Run External Script nodes that intend to run a Call Studio script. When using an optional feature like Courtesy Callback, you must configure additional GS network VRU scripts.

Procedure

Step 1

Configure VRU Script field parameters:

- **Micro-application type.** For Get Speech, valid options are: **GS** or **gs**.
- **Media File Name.** Only the value **Server** is supported for this field for GS.
- **Media Library Type.** Only the value **V** is supported for this field for GS.
- **Uniqueness value.** Optional. A string identifying a VRU script name as unique.

Step 2

Configure the Configuration Param field parameters:

Note Configuration parameters 1-10 are only for non-Packaged CCE deployments with Unified CVP where GS is supported with external VXML. Only the Pass FTP Information parameter (parameter 11) is configurable when using the Agent Greeting recording feature.

- **Pass FTP Information** Specifies whether to pass FTP server information to the VXML Server. This option is only useful if the VXML Server application uses the FTP_Client Element and the FTP server information is already configured. Valid options are:
 - **Y** - Pass FTP server information to the VXML Server as VXML Server session variables.
 - **N** - (default) Do not pass FTP server information.

If the **Pass FTP Information** parameter is set, the following information is passed:

- **ftpServer** - A space separated string of FTP servers. For example, `ftp_host1|21|username|password ftp_host2`. Everything is optional except the host name. See FTP_Client Element settings located in the *Elements Specifications for Cisco Unified CVP VXML Server and Cisco Unified Call Studio* guide for more information.
- **ftpPath** - A path on the FTP server. By default, this path is formed from the content of the ECC variable `user.microapp.locale` concatenated with path separator (/) and the content of the ECC variable `user.microapp.app_media_lib`. One exception is if the value of `user.microapp.app_media_lib` is `..`, then `app` is used instead. An example of a path is: `en-us/app`

Passing Information to the Call Studio Scripts Executing on VXML Server

You can pass up to 1050 characters to the Call Studio scripts executing on VXML server by using an ECC Variable array.

Table 47: To External VoiceXML ECC Variable Array

ECC Variable Name	Type	Max. Number of Elements	Max. Size of Each Element
user.microapp.ToExtVXML	Array	5	210

This variable array contains a list of semicolon delimited name/value pairs. The following is an example of the syntax:

Table 48: Sample Array Definition

Variable Name	Values
user.microapp.ToExtVXML[0]	"Company=Cisco;Job=technical writer"
user.microapp.ToExtVXML[1]	"Location=Boxborough;Street=Main"
user.microapp.ToExtVXML[2]	"FirstName=Gerrard;LastName=Thock"
user.microapp.ToExtVXML[3]	"Commute=1 hour;Car=Isuzu"

Unified CVP sends each name/value pair as a session variable on the call to VXML server (for example, a session variable named **Company** with a value of **Cisco**). The session variables are accessible in the Call Studio scripts.

Passing Data Back to Packaged CCE from the VXML Server

Unified CVP can return 840 characters from the VXML server.

The following ECC Variable array is added:

Table 49: From External VoiceXML ECC Variable Array

ECC Variable Name	Type	Max. Number of Elements	Max. Size of Each Element
user.microapp.FromExtVXML	Array	4	210

The Get Speech micro-app returns up to 840 characters by populating the **user.microapp.caller_input** variable and each element of the **user.microapp.FromExtVXML** array.



Note By default user.microapp.FromExtVXML ECC variable is pre-defined for Packaged CCE but not enabled. You can use the predefined ECC variable or update the length based on your needs.

Scripting for Unified CVP with Call Studio

You can use Call Studio to build sophisticated Unified CVP applications which can then be loaded onto a VXML Server machine for execution.

To invoke a VXML Server application, create a Packaged CCE routing script that

- Includes a user.microapp.ToExtVXML[0] ECC variable instructing the VoiceXML Gateway to interact with the VXML Server directly to run the application
- Instructs the application to pass back results to Packaged CCE

This section describes

- Call Studio and how to use it to pass data to Packaged CCE
- How to integrate Call Studio scripts with Packaged CCE scripts

- How to deploy Call Studio Scripts in Unified CVP

High-Level Configuration Instructions

This chapter presents a set of high-level instructions for configuring many of the Unified CVP call flow models (deployment models).

Each set of call flow model instructions contains:

- A brief overview of that call flow model
- High-level instructions for configuring the components in that call flow model
- References to detailed instructions (elsewhere in this guide, in online help, or in other documents) for performing each high-level task

This chapter also includes information, or pointers to information, for configuring the Gateway, Packaged CCE VRU handling and Unified CVP Call Server (including the SIP Service, Packaged CCE service, and Unified CVP Service).

Call Studio ReqICMLabel Element to Pass Data

The ReqICMLabel element allows a Call Studio script to pass caller input, Call Peripheral variables, and Expanded Call Context (ECC) variables to a Packaged CCE script. The ReqICMLabel must be inserted into a Call Studio script as a decision element. In Call Studio, the returned Packaged CCE label result can be used by other elements in the same application, such as the Transfer or Audio element. The Transfer element sends instructions to the IOS Voice Browser to transfer the caller to the desired location.

After the ReqICMLabel exits its path, you can retrieve the values set by the Packaged CCE script by selecting the Element Data tab for the ReqICMLabel element. The element data value is `{Data.Element.ReqICMLabelElement.result}`. ReqICMLabelElement is the name of the ReqICMLabel element in the Call Studio script. The default name for this element is ReqICMLabel_<n>. For example, if you changed ReqICMLabel to GetICMLabel, the value returned from Packaged CCE is `{Data.Element.GetICMLabel.result}`, where *result* is the variable of the ReqICMLabel element that contains the Packaged CCE label.

Table 50: Settings

Name (Label)	Type	Required	Single Setting Value	Substitution Allowed	Default	Notes
Call Peripheral Variables 1 - 10 (callvar1 - callvar10)	String	No	Yes	Yes		Call Peripheral variables passed by the Call Studio script to the Packaged CCE server. This setting can be a maximum of 40 characters. The Packaged CCE server returns a name-value pair for up to 10 Call Peripheral Variables in a result. Any value that is placed in callvar<n> from a Call Studio script is returned unchanged, if the Packaged CCE script does not change it.

Name (Label)	Type	Required	Single Setting Value	Substitution Allowed	Default	Notes
Call Peripheral Variables Return 1 - 10 (callvarReturn1 - callvarReturn10)	String	No	Yes	Yes		Call Peripheral variables created upon the return of the Packaged CCE Label request, regardless of whether or not these variables are filled by the Packaged CCE script. You need two sets of these variables to keep reporting to the Packaged CCE Call Peripheral Variables separate from what is returned from Packaged CCE.
FromExtVXML0 - 3 (External VXML 0 - External VXML 3)	String Array	No	Yes	Yes		Expanded Call Context (ECC) variables passed by the Call Studio script to the Packaged CCE Packaged CCE server. Each variable is a string of name-value pairs, separated by semicolons, for up to four external VoiceXML variables. This setting can be a maximum of 210 characters.
ToExtVXML0 - 4 (External VXML 0 - External VXML 4)	String Array	No	Yes	Yes		Expanded Call Context (ECC) variables received from the Packaged CCE script. The Packaged CCE server returns a string of name-value pairs, separated by semicolons, for up to five external VoiceXML variables.
Timeout	Integer	Yes	Yes	Yes	3000 (ms)	The number of milliseconds that the transfer request waits for a response from the Packaged CCE server before timing out. Note This value is increased or decreased by increments of 500 ms.
caller_input (Caller Input)	String	No	Yes	Yes		This setting can be a maximum of 210 characters. The caller_input is only passed to Packaged CCE from Call Studio.

Table 51: Element Data

Name	Type	Notes
result	String	Packaged CCE label returned from a Packaged CCE server. You can use this result as input to other Call Studio elements, such as Transfer or Audio. The element data value is {Data.Element.ReqICMLabelElement.result}.

Name	Type	Notes
callvar<n>	String	Call Peripheral variables that the Call Studio scripts passes to the Packaged CCE server. Valid Call Peripheral Variables are callvar1 - callvar10.
callvarReturn<n>	String	<p>Call Peripheral variables that the Packaged CCE script returns to the VXML Server. Valid Call Peripheral Variables are callvarReturn1 - callvarReturn10.</p> <p>For example, if a Packaged CCE script contains Call Peripheral variable 3 with the string value "CompanyName=Cisco Systems, Inc", you can access the value of CompanyName that is returned by the Packaged CCE script by using</p> <p>Data.Element.ReqICMLabelElement.callvarReturn3</p> <p>The returned value is "Cisco Systems, Inc."</p>

Table 52: Session Data

Name	Type	Notes
name	String	<p>Value for a name-value pair contained in a ToExtVXML variable returned in the Packaged CCE label. You must know which name-value pairs are set in the Packaged CCE script to retrieve the correct value from the Call Studio script.</p> <p>For example, if a Packaged CCE script contains a user.microapp.ToExtVXML0 variable with the string value "CustomerName=Mantle", specify Data.Session.CustomerName. If the same Packaged CCE script contains a user.microapp.ToExtVXML0 variable with the string value "BusinessType=Manufacturing", you can access the customer business type returned by the Packaged CCE script by using Data.Session.BusinessType.</p>

Table 53: Exit States

Name	Notes
done	The element execution is complete and the value is successfully retrieved.
error	The element failed to retrieve the value.

Studio Element Folder is "Cisco."

Integrate Call Studio Scripts with Unified CCE Scripts - Traditional Method

This section describes how to integrate the VXML Server into the Unified CVP solution in the traditional way. This process involves

- Creating a Unified CCE script with ECC variables configured for VXML Server
- Creating a VRU Script to run in the Packaged CCE script

Integrate Call Studio Scripts with Packaged CCE Scripts

The following steps describe how to integrate Call Studio scripts with Packaged CCE :

Procedure

Step 1 Set the user.microapp.ToExtVXML[0] ECC variable to application=HelloWorld.

Note This example indicates that the VXML Server runs the “HelloWorld” application. To run a different application, change the value of user.microapp.ToExtVXML[0] accordingly.

Step 2 Create a Run External Script node within the Packaged CCE script with a VRU Script Name value of GS,Server,V.

- Configure the timeout setting in the Network VRU Script to a value greater than the timeout value in the VXML Server application. (This timeout is only used for recovery from a failed VXML Server.)
- Always leave the **Interruptible** checkbox in the Network VRU Script Attributes checked. Otherwise, calls queued to a VXML Server application may stay in the queue when an agent becomes available.

Step 3 After you configure the Packaged CCE script, configure a corresponding VXML Server script with Call Studio. The VXML Server script must

- Begin with a Unified CVP Subdialog_Start element (immediately after the Call Start element)
 - Contain a Unified CVP Subdialog_Return element on all return points (script must end with a Subdialog_Return element)
 - Must include a value for the call input for the Unified CVP Subdialog_Return element
 - Must add Data Feed/SNMP loggers to enable reporting
-

Call Studio Scripts in Unified CVP

Call Studio scripts can be deployed in one of the following ways:

- In Call Studio, create and deploy the Call Studio scripts to the local machine using the **Archive** option.
- In Call Studio, use the **Deploy Remotely** option to deploy the scripts to an FTP Server.

Deploy Call Studio Scripts Using Call Studio

Procedure

Step 1 Create or modify one or more VoiceXML application scripts.

Step 2 Use Call Studio to set up the loggers using the ActivityLogger, ErrorLogger, and Admin Logger tools. Set up the Unified CVP Datafeed logger for each application.

Note Call Studio also includes CVPDatafeedLogger and CVPSNMPLLogger. Call Studio lets you change other parameters for these loggers, such as log file size, log lever, et cetera.

See the Call Studio documentation for more information.

Step 3 Deploy one or more VoiceXML application scripts to the local machine using the archive option. The archived scripts are saved as a zipped file under a user-specified directory, for example:

C:\Program Files\Cisco\CallStudio

Note The sample folder is C:\Cisco\CallStudio, which is also the default folder.



CHAPTER 16

Outbound Option Scripting

- [Outbound Option Scripting](#), on page 575

Outbound Option Scripting

Detailed scripting information for Outbound Option is available in the *Cisco Packaged Contact Center Enterprise Features Guide* at https://www.cisco.com/en/US/products/ps12586/tsd_products_support_series_home.html.



PART **III**

Database Administration

- [Database Administration, on page 579](#)



CHAPTER 17

Database Administration

- [Unified CCE Database Administration, on page 579](#)
- [Historical Data, on page 580](#)
- [Database Statistics, on page 581](#)
- [Database Administration Tool, on page 581](#)
- [Increase the size of the disk space for an existing virtual machine, on page 589](#)
- [Database Sizing Estimator Tool, on page 590](#)
- [Administration and Data Server with Historical Data Server Setup, on page 592](#)
- [Database Size Monitoring, on page 593](#)
- [System Response When Database Nears Capacity, on page 594](#)
- [Allocation of More Database Space, on page 595](#)
- [Initialize Local Database \(AWDB\), on page 595](#)
- [General Database Administration, on page 595](#)
- [Logger Events, on page 596](#)
- [Database Networking Support, on page 596](#)
- [Database Backup and Restore, on page 596](#)
- [Database Recovery Models, on page 597](#)
- [Database Comparison, on page 597](#)
- [Database Resynchronization, on page 597](#)

Unified CCE Database Administration

When you install a new Logger, you create its central database. Create an HDS database on a real-time Administration & Data Server. When you create a database, you specify the size of its data or log files. The data files must be sufficient for all the data that you expect the database to hold. The size of the central and HDS databases depend on your call center traffic and your data retention requirements.



Note For more information on how to perform a manual configuration for integrating AWDB with ECE, see the section *Integrating ECE with Unified CCE* in the [Enterprise Chat and Email Installation and Configuration Guide](#).

The local database (awdb) contains configuration and real-time data, if the Administration & Data Server role includes a real-time server. Because the real-time data in the local database (awdb) are constantly overwritten by new data, the database size remains fairly constant.

Over time, the size of your enterprise or your call volumes can change significantly. Therefore, you might need to resize the central and HDS databases to meet new requirements. You do not need to resize the local database (awdb). To resize the local database (awdb), use the ICM Database Administration (ICMDBA) tool.

The data in the central database and HDS database grow as they accumulate historical data and call detail records. The growth is directly related to the following factors:

- Size of the Unified ICM configuration; for example, how many services, skill groups, routes, and trunk groups are configured.
- Call rate; that is, how many calls per day the system software is handling.
- How long historical data is kept in the database.

The amount of configuration data directly affects the amount of historical data generated. The system software generates a new historical record every half hour for each service, skill group, route, trunk group, and so on, that is configured in the Unified ICM system.

You size and create the central and HDS databases after installing the system software. Use the Database Sizing Estimator applet for estimating the size of these databases, based on the expected usage.

If your configuration expands significantly or if you change the retention times for historical data, you might have to increase the size of the database. This increase might involve adding more disks to the system.

Historical Data

The system software initiates a purge process on the Logger once every day. By default, the purge process runs each night at 12:30 A.M. The purge process deletes records that are older than a specified number of retain days. When you set up the Logger using the Web Setup tool, you can modify the default retention time and purge schedule.

This table lists the *default* settings for retaining historical data.

Historical tables	Default retention time
Logger_Admin, Import_Rule_History, Persistent	30 days
Recovery	3650 days
All other historical tables	14 days

The following large historical tables are not purged by the system software but as a scheduled SQL Server Agent Job:

- Agent_Event_Detail
- Call_Type_SG_Interval
- Dialer_Detail
- Network_Event_Detail

- Route_Call_Detail
- Route_Call_Variable
- Termination_Call_Detail
- Termination_Call_Variable

**Caution**

SQL Server Agent Jobs are installed and enabled during the Unified CCE install and upgrade procedure. Do not stop these jobs while the system software is active. If you plan to stop the Logger and Administration & Data Server-hds component services for maintenance for more than a day, manually disable the Microsoft SQL Server jobs using the SQL Server enterprise management tool. Later, after the services are started, re-enable the jobs.

Database Statistics

Maintaining accurate, up-to-date statistical details is essential to a well-run database environment and contributes to the optimizer's efficient handling of work load. In some SQL Server-based environments, it is not unusual to see users rely on the database itself to maintain statistics by using the Auto Create Statistics and Auto Update Statistics options. Setting these options in an AW environment (with its rapid data turnover) results in a considerable effort being expended in updating statistics. For that reason, users often schedule these options to run during off-peak hours. Because the database in the AW environment is nearly empty during off-peak times, however, statistics gathered then might not be as helpful as they would be when collected at other, busier times.

Another option to consider for gathering statistics is the creation of a SQL Server Agent job that periodically runs the Microsoft stored procedure `sp_updatestats`. The `sp_updatestats` procedure updates statistics as required for all user-defined and internal tables in the current database and can be run on an hourly basis if workload and environment permit.

Database Administration Tool

Unified CCE includes the ICMDBA tool (`icmdba.exe`) in the `\icm\bin` folder. This tool provides a central utility to administer the Unified ICM databases. Use this tool to:

- Create, edit, and delete central databases, local databases, and historical databases
- Resize database files
- Recreate databases
- Import and export Unified ICM configuration data to and from databases
- View database properties

In addition to these tasks, you can start or stop a server and do some limited SQL Server configuration.



Note Before using the ICMDBA tool, install the Unified CCE software. See the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide, for information on the Unified CCE installation.



Note The ICMDBA Import /Export feature works on Unified ICM configuration data only. To import or export Unified ICM historical data, use Microsoft's SQL Server Database Backup and Database Restore utilities.

You start the ICMDBA either by double-clicking **ICMDBA** in the Unified CCE Tools folder or by selecting **Start > Run > ICMDBA**.

The main window is a tree hierarchy displaying the Unified ICM database servers in the current domain.



Note If you cannot find the server you want in the main window, you can select any computer on your local network by choosing **File > Add Computer**.

Expanding the server name displays the Unified ICM instances that have databases on the server. Expanding the Unified ICM instance displays a specific Unified ICM node or nodes (Administration & Data Server and Logger) on machines that have databases for that instance. Expanding the node displays the databases associated with the node. Expanding the node database displays a list of the individual tables in the node database. Under databases are the table groups, and the final level lists the tables in the group.

You can create databases for instances with or without configured components. When an instance does not have configured components, database creation occurs under the instance within a component placeholder on the ICMDBA tree view.

To view the properties of a table, right-click the desired table in the list and select Properties from the context menu, or double-click the table in the list.

There are two ways to access the ICMDBA tool functions:

- From the main window, select a node or database from the tree and then select a function from the menu bar menu.
- Right-click a node or database to display a context menu.

Create Database with Configured Components

Use the Create function to create a database for an Administration & Data Server or Logger. You can only create one Logger database per side.

Procedure

- Step 1** With the Unified CCE running, for the server and instance, select the node (Administration & Data Server or Logger) where you want to create the database.
- Step 2** Select **Database > Create** from the menu bar (or click the right mouse button and select **Create**). The **Create Database** window is displayed.

- Step 3** Enter the following information for the database:
- **DB Type**—Specify the type of database: **Outbound Option** for an outbound dialer, **Administration & Database Server** for a local database (awdb), or **Historical Data Server/Detail Data Server (HDS/DDS)** for Administration & Data Server machines. For a **Logger** device, the default database type is displayed (Logger side must be selected).
 - **ICM Type**—Specify whether this system is a Unified ICM or Unified CCE, Unified ICMH, or CICM (Customer ICM) system.
 - **Region**—Specify regional information where applicable.
- Step 4** Select **Add**. This button invokes the **Add Device** window.
- Use this window to create a new data file and a new log file for the selected database. Specify the disk drive letter and size in megabytes for each new file.
- Note** Move the database log file to a separate virtual drive. By default, both the log file and database data file are installed in `\MSSQL\DATA` on the virtual drive where you create the database. You can move the log file with SQL Server Management Studio.
- Note** By default, the newly created data file is set to “Automatically Grow,” if it exceeds the initially specified size. You can modify this setting, and the maximum file size, with SQL Server Enterprise Manager. Verify on the **Files** page in SQL Server Enterprise Manager that the **Autogrowth** column shows:
- Data files automatically grow in 100-MB increments.
 - Log files automatically grow in 10% increments.
- Step 5** After you complete entering information in the **Create Database** window, select **Create** to close the window and create the database.

Create Database Without Configured Components

Use the Create function to create a database for an Administration & Data Server or Logger. You can only create one Logger database per side.



Note When an instance does not have any configured components, database creation occurs under the instance within a component placeholder.

Procedure

- Step 1** With Unified CCE running, for the server and instance, select the instance where you want to create the database.
- Step 2** Select **Database > Create** from the menu bar (or click the right mouse button and select **Create**). The **Select Component** dialog appears.
- Step 3** Select the **Administration & Data Server**, **LoggerA**, or **LoggerB** component and select **OK**.

- Step 4** If you select LoggerA or LoggerB, the **Select Logger type** dialog appears, allowing you to select **Enterprise**, **CICM**, or **NAM**. Select the logger type and select **OK**.
The **Create Database** window appears.
- Step 5** Enter the following information for the database:
- **DB Type**—Specify the type of database: **Outbound Option** for an outbound dialer, **Administration & Database Server** for a local database (awdb), or **Historical Data Server/Detail Data Server (HDS/DDS)** for Administration & Data Server machines. For a **Logger** device, the default database type is displayed (Logger side must be selected).
 - **ICM Type**—Specify whether this system is a Unified ICM or Unified CCE, Unified ICMH, or CICM (Customer ICM) system.
 - **Region**—Specify regional information where applicable.
- Step 6** Select **Add**. This button invokes the **Add Device** window.
Use this window to create a new data file and a new log file for the selected database. Specify the disk drive letter and size in megabytes for each new file.
- Note** Move the database log file to a separate virtual drive. By default, both the log file and database data file are installed in \MSSQL\DATA on the virtual drive where you create the database. You can move the log file with SQL Server Management Studio.
- Note** By default, the newly created data file is set to “Automatically Grow,” if it exceeds the initially specified size. You can modify this setting, and the maximum file size, with SQL Server Enterprise Manager. Verify on the **Files** page in SQL Server Enterprise Manager that the **Autogrowth** column shows:
- Data files automatically grow in 100-MB increments.
 - Log files automatically grow in 10% increments.
- Step 7** After you have completed entering information in the Create Database window, select **Create** to close the window and create the database.

Delete a Database

Use the Delete function to delete an Administration & Data Server or Logger database.



- Note** When an instance does not have any configured components, component placeholders appear under that instance on the application tree view. If you delete the database, the component placeholders no longer appear.

Procedure

- Step 1** With Unified CCE running, for the server, instance, and node (Administration & Data Server or Logger), select the database that you want to delete.
- Step 2** Select **Database > Delete** from the menu bar.
- Step 3** The **Delete Database** prompt appears. Select **Yes** to delete the database.

- Step 4** Verify that you want to delete the database in the message box.
- Step 5** Select **Close** to exit. Check the main window to verify that the database was deleted.

Expand a Database

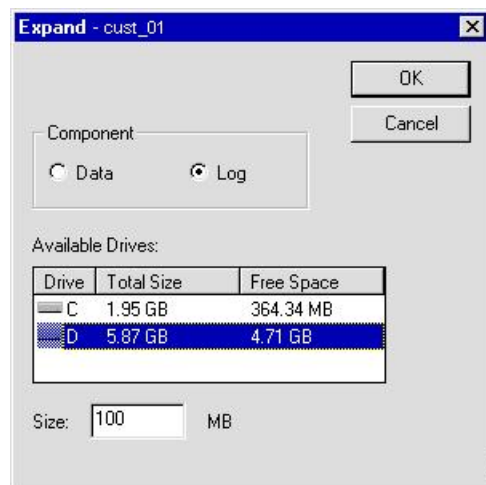
Use this function to add a new storage file.



Note ICMDBA allows a database to be expanded a maximum of 49 times (resulting in 50 segments). In the event that you reach this limit, you must either recreate the database or use SQL Enterprise Manager to modify the database.

Procedure

- Step 1** For the server, instance, and node (Administration & Data Server or Logger), select the database that you want to expand.
- Step 2** Select **Database > Expand** from the menu bar (or click the right mouse button and select **Expand**). The **Expand** window appears:



- Step 3** Use the window to adjust the size allocation on the database storage device, by completing the following fields:
- **Component**—Specifies whether the file is a data file or log file. Each database must have a file for each type of service.
 - **Available Drives**—Specify the drive on which to create the database.
 - **Size**—Specifies the size (in MB) of the storage. The field displays a default size, adjust the value as necessary.
- Step 4** Select **OK** to expand the file and exit the screen.

Recreate a Database

Use the Recreate function to recreate a database. The procedure for recreating a database is similar to the procedure for creating a database.



Caution When you recreate a database, the information currently stored in the database is deleted.



Note When an instance does not have any configured components, database creation occurs under a component placeholder on the application tree view.

Procedure

-
- Step 1** For the server, instance, and node (Administration & Data Server or Logger), select the database that you want to recreate.
 - Step 2** Select **Database > Recreate** from the menu bar. The **Recreate** window appears.
 - Step 3** Enter the database information. See the online help for a description of the fields.
 - Step 4** Select **Create** to continue. A message is displayed asking if you are sure you want to recreate the database. Select **Yes** to continue the operation.
 - Step 5** The next **Recreate Database** window appears. Select **Start** to recreate the database. After the process completes, a message appears indicating the action was successful. Select **OK** and then select **Close** to exit.
-

View Database Properties

The ICMDBA tool allows you to view the properties of specified databases.

Procedure

-
- Step 1** For the server, instance, and node (Administration & Data Server or Logger), select the database that you want to view.
 - Step 2** Select **Database > Properties** from the menu bar (or click the right mouse button and select **Properties**). The **Properties** window appears.
The screen display includes the following information:
 - Instance name
 - The database configuration
 - The size and percentage used of the files
 - Where the data and log files are stored
 - Step 3** After you finish viewing the database properties, select **Close** to exit the window.
-

View Table Properties

ICMDBA also allows you to view the properties of each table in the database.

Procedure

- Step 1** Select and expand the database to display the tables of a database.
 - Step 2** Double-click the table you want to view. The **Table Properties** window appears.
 - Step 3** After you finish viewing the table properties, select **Close** to exit the window.
-

Import and Export Data

You can use Import/Export functions to move Unified ICM configuration data from one database to another.



Note The ICMDBA Import/Export feature handles Unified ICM configuration data only. To import or export Unified ICM historical data, use Microsoft's SQL Server Database Backup and Database Restore utilities.

Procedure

- Step 1** For the server, instance, and node (Administration & Data Server or Logger), select the database from which you want to import or export data.
- Step 2** Select **Data > Import** (or Export) from the menu bar. The **Import data to** (or Export) window appears.
- Step 3** Check **Lockout Changes**, if you want to prevent changes to the database during the import or export operation.
- Step 4** Check **Truncate Config Message Log**, if you want to truncate the Config_Message_Log table in the Logger database.

Note Truncating deletes the data and does not export the Config_Message_Log table.

- Step 5** Set the **Data type** for the imported data.
 - Step 6** Indicate the path for the source/destination of the data.
 - Step 7** Select **Import** (or Export) to display the **Import** (or Export) dialog.
 - Step 8** Select **Start** to import (or export) the data. After the process completes, a message appears indicating that the action was successful. Select **OK** and then select **Close** to exit. You can select **Cancel** at any time to end the process.
-

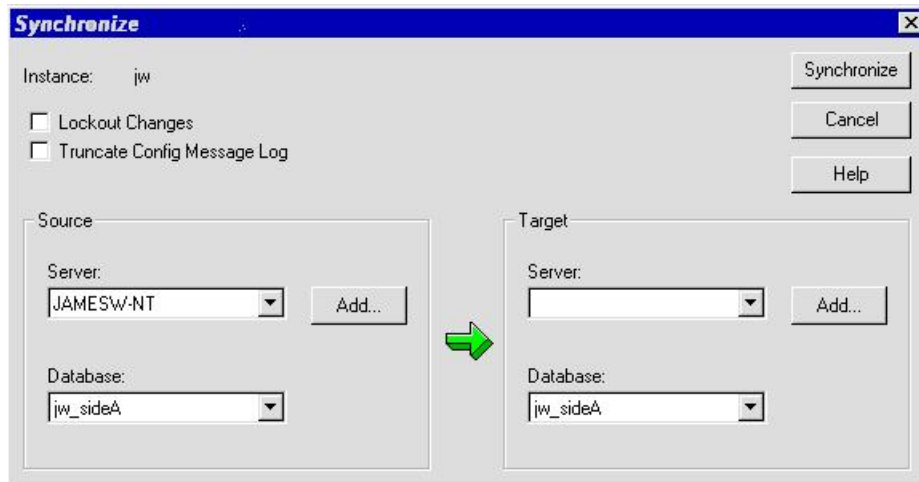
Synchronize Database Data

Use the Synchronize function to synchronize the configuration data of two Logger databases. This function does not synchronize the historical data.

Procedure

Step 1 For the server and instance, select the Logger database to synchronize.

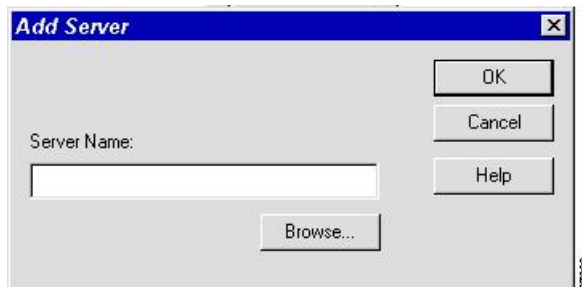
Step 2 Select **Data > Synchronize** from the menu bar. The **Synchronize** window appears:



Step 3 Check **Lockout Changes**, if you want to prevent changes to the database during the synchronize operation.

Step 4 Check **Truncate Config Message Log**, if you want to truncate the Config_Message_Log table in the Logger database.

Step 5 Select the server name and database for both source and target from the drop down lists. To select a server that is not on the drop down list, select **Add** and enter the server name in the **Add Server** box:



Step 6 Select **Synchronize**.

Step 7 A message box appears asking for confirmation. Select **OK** to continue.

Step 8 The next **Synchronize** window appears. Select **Start** to synchronize the data. After the process completes, a message appears indicating that the action was successful. Select **OK** and then select **Close** to exit. You can select **Cancel** at any time to end the process.

Configure a Database Server

ICMDBA allows you to start or stop a server and to do some limited server configuration.

To start or stop a server, select the node from the list and select **Server > Start/Stop** from the menu bar.



Note When you use the Configure option, the SQL Server, Administration & Data Server, and Logger restart automatically. However, when you use the Stop option from the Server menu, manually restart the Logger and Administration & Data Server from ICM Service Control.

Procedure

- Step 1** Select the server and select **Server > Configure** from the menu bar. The **Configure** window appears.
- Step 2** Use this window to modify the following SQL Server parameters:
- **User Connections**—Indicates the maximum number of users that can connect to SQL Server at one time.
 - **Locks**—Indicates the maximum number of available locks.
 - **Open Objects**—Indicates the maximum number of available open objects.
- Note** User Connections, Locks, and Open Objects are “dynamically allocated” by SQL Server. Unified ICM does not allow you to change these options, so they are dimmed.
- **Open Databases**—Indicates the maximum number of available open databases.
 - **Memory**—Indicates the amount of memory (in megabytes) allocated to SQL Server processing.
- Note** You can configure a specific amount of memory instead of the SQL Server default of “Dynamic.” Specifying a value of 0 sets the Memory setting to “Dynamic.”
- **Recovery Interval**—This setting controls checkpoint frequency.
 - **Max Async ID**—Indicates the maximum number of outstanding asynchronous disk input/output (I/O) requests that the entire server can issue against a file.
- Step 3** After you are finished configuring the server, select **OK** to complete the operation or select **Cancel** to end the operation without making any changes.
-

Increase the size of the disk space for an existing virtual machine

For deployments of 4000 agents or more, you can increase the size of the virtual machine's (VM) disk space on your Windows server. To increase the size of the VM's disk space for 2000 agents deployment, follow these steps:

Before you begin

Plan for a maintenance window to increase the size of the disk space.

Procedure

- Step 1** Power off the VM.
 - Step 2** Clone the VM or take a snapshot of the powered off VM.
 - Step 3** Change the size of the disk space, as required. Ensure that the disk format is set to Thick Provision Lazy Zeroed.
 - Step 4** Power on the VM.
 - Step 5** On the Windows server, go to **Server Manager > File and Storage Services > Volumes > Disks**.
 - Step 6** Modify the disk size and verify the changes.
 - Step 7** Delete the clone or snapshot of the old VM.
-

Database Sizing Estimator Tool

The Database Sizing Estimator tool enables you to perform database sizing tasks.

The Database Sizing Estimator estimates the storage requirements for a Cisco Unified ICM/CCE logger or HDS database. The tool bases the estimate on information about the configuration of the environment (for example, the number of agents, skill groups, call types, and so on) and database retention days. You can supply initial values by loading values from your local Unified ICM database.

When values are updated in the Database Sizing Estimator, the application recalculates its totals. This update enables you to immediately see the effects of each change as it is made, with the values displayed in a spreadsheet. The tool enables you to engage in what-if scenarios to see the effects that various changes have on the database sizing requirements.

The Database Sizing Estimator allows you to save the values as an XML file on your local machine. At any time, you can load the saved XML file back into the Database Sizing Estimator, so you can continue revising your estimates.

Cisco Unified ICM/CCE Database Retriever Dialog

The Cisco Unified ICM/CCE Database Retriever dialog, which you access from the Database Sizing Estimator tool, queries the existing database and registry configuration. The Database Sizing Estimator tool then uses this data to provide starting values, which you can modify.

To access the **Database Retriever** dialog, select **Load from DB** in the Database Sizing Estimator tool on your local machine.



Note Cisco Unified ICM/CCE Database Retriever can retrieve the configuration and retention information from any Unified ICM/CCE system containing a Logger or Historical Data Server (HDS) database. The Database Sizing Estimator can calculate a database size for a newer schema other than the deployment to which the Database Sizing Estimator is connected.

Start Database Sizing Estimator

The following steps describe how to start the Database Sizing Estimator.



Note For Database Sizing Estimator field-level descriptions, see the online help.

Procedure

Step 1 Open the Database Sizing Estimator tool by selecting **Database > Estimate** in the ICMDDBA tool.

Step 2 The Cisco Unified ICM/CCE Database Sizing Estimator window appears:

The screenshot shows the Database Sizing Estimator window with the following configuration options:

Configuration	Value
Agents	10
Routing Clients	10
Translation Routes	10
Application Gateways	10
Scripts	10
Trunk Groups	10
Call Types	10
Services	10
Precision Queue	10
Network Trunk Groups	10
Skill Groups	10
Precision Queue per Agent	10
Peripherals	10
Skills per Agent	10
Routes	10
Skills per Call Type	10

Buttons on the right: Load from File, Save to File, Load from DB, About..., Help.

Call and Event Data tabs: Call and Event Data, Interval Data, Five Minute Data, Outbound, Advanced.

Call and Event Data	Records Per Day	Days	MB
<input checked="" type="checkbox"/> Route Call Detail	1000	14	11.8
<input checked="" type="checkbox"/> Termination Call Detail	400	14	8.5
<input checked="" type="checkbox"/> ECC Variables Stored	# of Variables Per Call Detail: 0	Total ECC Bytes Per Call Detail: 0	Days: 14, MB: 0.0
<input checked="" type="checkbox"/> Events	10000	14	244.2

Database Size: Required: 741.5 MB

Database Version: Schema Version: 10.0(x)

Copyright © 1994-2012 Cisco Systems, Inc.

Step 3 The window displays initial default values for all fields. As you change the field values, the database size requirements update automatically. You can load values from a previous version or from the **Cisco Unified ICM/CCE Database Retriever** dialog by selecting **Load from File** to load an external XML data file.

Estimate Database Size



Note Steps 1–3 in this procedure only apply when using existing databases.

Procedure

- Step 1** Use your existing database as the starting point. Select **Load from DB** in the **Database Sizing Estimator** main window. The **Cisco Unified ICM/CCE Database Retriever** dialog appears.
- Step 2** Select the database you want to use as the starting point for your sizing estimates.
- Step 3** Select **Retrieve**.
The fields in the **Database Sizing Estimator** main window auto-populate with the information from the selected database.
- Step 4** Modify the database information depending on your scenario. As changes are made, the **Database Size Required** value changes.
- Step 5** Save your work in progress by selecting **Save to File**.
-

Administration and Data Server with Historical Data Server Setup

There are two ways to set up a Historical Data Server (HDS) VM:

- The instance is created in the domain, but not already added.
- The instance is created in the domain and is already added.

Set Up HDS and Add Instance

Procedure

- Step 1** Run the Cisco Unified ICM/Contact Center Enterprise (if you have not run it already) on the local machine.
- Step 2** Run the Web Setup tool for that machine (in a browser, from anywhere). Under **Instance Management**, select **Add** and add the instance.
- Step 3** Run the ICMDBA tool on the local machine. Create the Historical Data Server/Detail Data Server database.
- Step 4** Return to the Web Setup tool. Under **Component Management**, select **Add** on the Administration & Data Server list page, then follow the instructions in the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide. If you did not perform step 3, the Administration & Data Server **Add** wizard does not allow you to finish this procedure until you create an HDS database.
-

What to do next

Use the Database Sizing Estimator tool to determine the size of the database and then use the ICMDBA tool to create the database.



Note In 2000 Agents deployment, databases are created automatically for on-box HDS. Disk usage must be below 90%; if it exceeds the threshold, add external HDS.

Set Up HDS from Added Instance

Procedure

-
- Step 1** Run the Cisco Unified ICM/Contact Center Enterprise Installer (if you have not run it already) on the local machine.
- Step 2** In the Web Setup tool, under **Component Management**, select **Add** on the Administration & Data Server list page, then follow the instructions in the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide. If you did not perform step 1, the Administration & Data Server **Add** wizard does not allow you to finish this procedure until you create an HDS database.
-

What to do next

Use the Database Sizing Estimator tool to determine the size of the database and then use the ICMDBA tool to create the database.

Database Size Monitoring

Regularly monitor the space used by the central database and transaction logs. You can monitor database size by viewing the Logger's per-process log files. The per-process log files contain information on Logger and database activity, as this example log file illustrates:

```

C:\vicr\bin\VDUMPLOG.exe
Events from February 25, 1997:
00:38:13 Trace: 81% of the available free space is used in cus01_sideA database.
01:08:13 Trace: 76% of the available free space is used in cus01_sideA database.
02:08:15 Trace: 77% of the available free space is used in cus01_sideA database.
07:08:21 Trace: 78% of the available free space is used in cus01_sideA database.
12:08:27 Trace: 79% of the available free space is used in cus01_sideA database.
17:07:32 Trace: 80% of the available free space is used in cus01_sideA database.
22:07:38 Trace: 81% of the available free space is used in cus01_sideA database.

Events from February 26, 1997:
00:37:41 Trace: 79% of the available free space is used in cus01_sideA database.
01:07:42 Trace: 70% of the available free space is used in cus01_sideA database.
05:07:47 Trace: 71% of the available free space is used in cus01_sideA database.
09:37:52 Trace: 72% of the available free space is used in cus01_sideA database.
10:37:54 Trace: 73% of the available free space is used in cus01_sideA database.
11:07:54 Trace: 74% of the available free space is used in cus01_sideA database.
12:07:56 Trace: 75% of the available free space is used in cus01_sideA database.
13:07:57 Trace: 76% of the available free space is used in cus01_sideA database.
13:37:57 Trace: 77% of the available free space is used in cus01_sideA database.
14:37:59 Trace: 78% of the available free space is used in cus01_sideA database.
15:38:00 Trace: 79% of the available free space is used in cus01_sideA database.
37335

```

The Logger logs events and trace messages that show the percentage of space used in the database. These files are stored in a `\logfile`s subdirectory in the Logger's folder (la or lb). You can view the Logger's per-process log files by using the Unified ICM dumplog utility.

When the database becomes 80 percent full, the Logger logs an EMS warning message to the central database. The "80 percent full" warning message might also immediately be sent to your Unified ICM network management station through SNMP or SYSLOG.



Note See the [Serviceability Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise](#) for more information on using the dumplog utility.

If you decide that you need more database space, contact your Unified ICM support provider.

System Response When Database Nears Capacity

The system software has automatic checks to prevent the central database from becoming full:

- **Warning message**—When the central database begins to approach its capacity, the system software issues a warning message. By default, this warning occurs when the database is 80% full, but you can configure this value. Warning messages trigger an event that is registered in AlarmTracker, which the console window displays in an EMS trace message.
- **Purge Adjustment**—Purge Adjustment automatically deletes the oldest historical data when the database usage exceeds 80% threshold or when the central or HDS database nears its capacity. However, purge adjustment does not happen immediately. It happens at the default scheduled purge time (00:30 AM), or at the time that you have specified for the scheduled purge to happen.

By default, purge adjustment occurs when the database is 80% full, but you can specify the percentage when you set up the Logger.

If the historical databases for the Logger, AW-HDS-DDS, AW-HDS, and HDS-DDS are not adequately sized, the purge adjustment feature is activated when the database usage exceeds the threshold. Use the **Database Sizing Estimator** tool to size your database requirements.



Note The purge adjustment feature affects performance of the Unified CCE system. The high CPU and disk usage due to purge adjustment could affect component performance including failures.

See the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide for more on purging information from databases.

- **Emergency/Automatic Purge**—By default, the system automatically deletes the oldest historical data from all historical tables when the database exceeds 90% usage capacity.

The automatic purge ensures that the database can never become full. But, the purge means that you can lose older historical data.

Allocation of More Database Space

If the central database is growing too large, you can allocate more space. If you require more space in the central database, back up the primary database before you add more space. Your Unified CCE support provider might have options for allocating more space.

Initialize Local Database (AWDB)

Usually, you do not need to initialize the local database (awdb), because initialization happens automatically during its creation. If you ever need to initialize the local database after its creation, you can do so.

Procedure

- Step 1** Double-click **Initialize Local Database** within the Administration Tools folder. The **Initialize Local Database** main window appears.
 - Step 2** Select **Start** to transfer the data. As data is copied, the screen displays the number of rows processed for each table.
 - Step 3** After the transfer is complete, select **Close** to exit.
-

General Database Administration

Because Unified ICM is a mission-critical application that runs 24 hours a day, the system software takes care of many routine administration tasks automatically. In general, the system software retains control of most of the database administration functions in order to keep external interference to a minimum.

The Unified ICM administrator might perform several optional Unified ICM administration tasks:

- Setting networking options
- Monitoring Logger activity

- Backing up the central database
- Restoring the central database from a backup
- Comparing databases
- Resynchronizing databases



Note To conserve system resources, minimize all Unified ICM process windows before configuring your system.

Logger Events

You can view recent Logger activity by viewing the Logger's per-process log files. Per-process log files document events for the specific processes running on a computer. These files are useful in diagnosing problems with processes on the Logger (and on other nodes in the Unified ICM system).

You can also view Logger event data in the central database. The Event Management System (EMS) logs events to the central database. Be especially aware of Error and Warning events generated by the Logger. For example, the system software logs a Warning event when the central database becomes 80% full.

See the [Serviceability Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise](#) for more information on viewing the per-process log files and central database event data.

Database Networking Support

You can use the SQL Server Setup program to specify which network protocols the database manager supports.

The correct order and states are:

1. **Shared Memory**—Enabled
2. **Named Pipes**—Enabled
3. **TCP/IP**—Enabled
4. **VIA**—Disabled

See the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise* http://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_installation_guides_list.html for detailed information about installing SQL Server. For more information about database networking, see the Microsoft documentation for Microsoft SQL Server.

Database Backup and Restore

A database can be lost or corrupted for several reasons. Because you cannot protect against all these reasons, you must have a backup strategy in place. This backup strategy is especially important if you have a nonredundant central database configuration. However, even for a redundant system, you still need to perform backups to protect against software problems that corrupt both sides of the system.

The commonly used database backup strategies are:

- Regularly scheduled database backups
- Mirrored disk configurations
- Redundant Array of Inexpensive Disks (RAID) configurations

Although the last two strategies might decrease system performance, they have the advantage of not requiring manual intervention. However, while these configurations protect against disk drive failure and bad media, they might not protect against some software errors.

In a single database configuration, ensure protection against all types of errors. To protect your data, regularly back up the central database with the SQL Administrator tool provided with SQL Server.

When you restore a database, you can only restore up to the last backup. Any transactions after that backup are lost. In single database configurations, daily backups are required to ensure maximum data protection.



Note You must back up the entire database at each backup interval. The system software does not support the use of transaction log dumps as incremental backups.

For general information about developing a backup strategy, including the use of mirrored disks, see *Microsoft's SQL Server System Administrator's Guide*. For specific information about backing up a database using SQL Administrator, see *Microsoft's SQL Administrator User's Guide*.

Database Recovery Models

When you install a Logger, HDS, or AWDB database, the ICMDBA tool automatically sets the database recovery model to Simple. The Simple model is required for the Unified CCE data recovery mechanism.

For more information, see the Microsoft documentation.

Database Comparison

For diagnostic purposes, you can check that two databases have the same data in a specific table. For example, you can check that the ICM_Locks table contains the same data on both sides of a Central Controller. The tool `dbdiff.exe` performs this type of check. Its syntax is as follows:

```
dbdiff database1.table@host1 database2.table@host2
```

For example:

```
dbdiff cust1_sideA.ICM_Locks@geoxylgra cust1_sideB.ICM_Locks@geoxylgrb
```

The batch script `diffconfig.bat` invokes **dbdiff** for various tables to automatically compare two Unified ICM databases. Its syntax is as follows:

```
diffconfig database1 host1 database2 host2
```

For example:

```
diffconfig cust1_sideA geoxylgra cust1_sideB geoxylgrb
```

Database Resynchronization

You might occasionally need to repair corrupt configuration data on the Logger database on one side of a redundant Unified ICM by copying the configuration data on Logger database from the other side. You can synchronize the configuration data on the databases using either the DOS Command window or the ICM Database Administration (ICMDBA) tool.

The ICMDBA synchronize process involves dropping the targeted side data and copying the data from the source. For example, if you are synchronizing side B data to side A data, the side B data is replaced with the data stored in side A. For more information, see [Synchronize Database Data, on page 587](#).



Note Perform these procedures in a maintenance window.

Synchronize Configuration Data between Loggers from Command Window

Procedure

- Step 1** Stop the Logger for the target database, if that Logger is running.
 - Step 2** In a DOS Command window on the VM for that Logger, change to the `\icm` directory.
 - Step 3** Run the following command: `install\syncloggers <Source_logger_server> <Source_logger_database> <Target_logger_server> <Target_logger_database>`.
 - Step 4** When prompted, Type **Y** to continue, upon which configuration of target database will be deleted and synced with source database.
-

What to do next

When the command is complete, restart the Logger on the target server.



APPENDIX **A**

Troubleshooting

- [Packaged CCE Logs, on page 599](#)
- [Character Sets, on page 601](#)
- [System Performance During Database Updates, on page 602](#)

Packaged CCE Logs

You can download several types of Packaged CCE log files from the Unified CCE Administration interface.

System Validation Logs

When you configure your deployment, if either the server or any of the VMs do not meet requirements, you see a message indicating connection problems. This message has a link to a log file. Open this file to see whether the servers are valid and whether all VMs match the deployment profiles.

Sample log file showing summary of invalid results:

```
VM Validation Results: Wed Aug 20 08:05:36 EDT 2012
Overall: false
Valid Systems: 0 of 1
Summary:
ESX Server: sideB
ESX Server Properties Valid: true
VM Layout Valid: false.
```

The information at the top of the log is a summary of the results. This log shows that the server is valid but the VM layout is not.

Sample log showing invalid server

This shows that the server does not have the required number of CPU Cores.

```
Server Result:
Required Version: 5.0.0
Required Min CPU Cores: 20
Required Min Memory (MB): 95000
Required HD(s) (GB): [1392, 1949, 273]
Required Bios <Major version>: C260
Required Vendor: Cisco Systems Inc
Found Version: 5.0.0
Found CPU Cores: 10
Found Memory (MB): 98185
Found HD(s) (GB): [1392, 273, 1949]
```

```
Found Bios: C260.1.4.2b.0.102620111637
Found Vendor: Cisco Systems Inc
```

There are three log entries for invalid VMS:

- **Required Profiles without Matching Virtual Machines**
This means system does not have VMs present that match our requirements
- **Optional Profiles without Matching Virtual Machines**
This means that the CVP Reporting profile, which is defined as optional, does not exist on the system. This does not block validation.
- **Virtual Machines without Matching Profiles**
This means the system has VMs that do not match requirements. They might be extra VMs or incorrectly-configured VMs.

Sample log showing valid VM

```
Virtual Machines Matching Defined Profiles:
VM: BB-CCE-AW-A
Profile: Unified CCE Data Server
CPU Cores: 4
Reservation: 5100
RAM (MB): 8192
HD(s) (GB): [80, 750]
VMWare Tools Version: 8384
```

Bulk Job Logs

A log file is generated for each bulk job. The log file is retained until the bulk job is deleted and contains details about each operation that was performed, as well as a summary indicating whether the bulk job completed successfully or failed.

Follow this procedure to open the log:

1. Open the Bulk Jobs tool.
2. From the List of Bulk Jobs, click the ID to go to the View Bulk Job page.
3. Click Log File **Download**. If the job is still processing, click **Download** again to review the updates as the job progresses.

You must authenticate to open or save this file.

The **Download** button is disabled if the bulk job was created using Unified CCE Administration on an AW host that is different from the host on which the job is being viewed.

Sample log file:

```
2016-06-27T17:20:19-04:00 - Job created
2016-06-27T17:20:19-04:00 - Job started
2016-06-27T17:20:19-04:00 - Processing line 1: Header
2016-06-27T17:20:19-04:00 - Processing line 2: operation=CREATE, agentId=1000,
userName=asmith,
firstName=Agent, lastName=Smith, password=secret, loginEnabled=true, ssoEnabled=false,
description=Agent Smith,
agentStateTrace=false,agentDeskSettingsName=Default_Agent_Desk_Settings,
agentTeamName=robots, skillGroups=sg1;sg2, defaultSkillGroup=sg1, attributes=,
supervisor=false,
supervisorTeams=, departmentName=
```

```

2016-06-27T17:20:20-04:00 - Created /unifiedconfig/config/agentteam/6348
2016-06-27T17:20:20-04:00 - Created /unifiedconfig/config/skillgroup/13515
2016-06-27T17:20:21-04:00 - Created /unifiedconfig/config/skillgroup/13516
2016-06-27T17:20:21-04:00 - Created /unifiedconfig/config/agent/13517
2016-06-27T17:20:21-04:00 - Processing line 3: operation=UPDATE, agentId=,
userName=neo@cisco.com,
firstName=Mister, lastName=Anderson, password=passw0rd, loginEnabled=true, ssoEnabled=false,
description=Neo, agentStateTrace=true,agentDeskSettingsName=~, agentTeamName=~, skillGroups=,
defaultSkillGroup=~, attributes=kungFu=9; actuallyKnowsKungFu=false, supervisor=true,
supervisorTeams=team1;team2, departmentName=department1
2016-06-27T17:20:21-04:00 - Error processing line 3: agentUserName: The specified agent
userName
does not exist neo@cisco.com.
2016-06-27T17:20:21-04:00 - Processing line 4: operation=UPDATE, agentId=1001, userName=,
firstName=,
lastName=, password=, loginEnabled=, ssoEnabled=, description=,
agentStateTrace=,agentDeskSettingsName=,
agentTeamName=, skillGroups=, defaultSkillGroup=, attributes=, supervisor=, supervisorTeams=,
departmentName=
2016-06-27T17:20:21-04:00 - Error processing line 4: agentId: The specified agent Id does
not exist 1001.
2016-06-27T17:20:21-04:00 - Processing line 5: operation=DELETE, agentId=1001, userName=,
firstName=,
lastName=, password=, loginEnabled=, ssoEnabled=, description=,
agentStateTrace=,agentDeskSettingsName=,
agentTeamName=, skillGroups=, defaultSkillGroup=, attributes=, supervisor=, supervisorTeams=,
departmentName=
2016-06-27T17:20:21-04:00 - Error processing line 5: agentId: The specified agent Id does
not exist 1001.
2016-06-27T17:20:21-04:00 - Processing line 6: operation=DELETE, agentId=, userName=jsmith,
firstName=,
lastName=, password=, loginEnabled=, ssoEnabled=, description=,
agentStateTrace=,agentDeskSettingsName=,
agentTeamName=, skillGroups=, defaultSkillGroup=, attributes=, supervisor=, supervisorTeams=,
departmentName=
2016-06-27T17:20:21-04:00 - Error processing line 6: agentUserName: The specified agent
userName does not
exist jsmith.
2016-06-27T17:20:21-04:00 - Job partially completed due to errors
2016-06-27T17:20:21-04:00 - 5 lines processed, 1 succeeded, 4 failed
2016-06-27T17:20:21-04:00 - 1 agent teams created, 1 agents created, 2 skill groups created

```

Character Sets

If you installed the Language Pack, the Sign-In window includes a Language drop-down menu. The drop-down menu includes more than a dozen languages. Select any one of them to see the Unified CCE Administration interface and online help in that language.

You must enter characters that the database recognizes in the **Description** field in all tools and in the **First Name** and **Last Name** fields in the Agent tool. If you do not, you see an error message which states that “The system does not support these characters.”

System Performance During Database Updates

Saving, Editing, and Deleting

The addition, update, or deletion of any object triggers a database update. The system can process a single update at a time. When an update is already in progress, the system queues subsequent pending updates.

While updates are pending or in progress, a spinning wheel, indicating progress, appears on the window during a save or deletion.

If an update fails, you see an error message appear indicating that your record was not saved or deleted. You do not need to refresh or navigate away from the page. You can try the save or delete action again.

Validation and Capacity Checks

The system performs the following checks when you initially save or edit and when you confirm a deletion. It performs the same two checks when the transaction reaches the head of the queue and is about to be written to the database.

- Validation check. The initial validation checks if a required field is missing or if a field contains too many characters or invalid characters. The second validation ensures system integrity. For example, are you adding an agent to an agent team that was just deleted?
- Capacity check.

If the transaction fails either check, an error message alerts you to the validation error or capacity restriction.



APPENDIX B

Reference

- [Security Certificates](#), on page 603
- [Graceful Shutdown of Call Server or Reporting Server](#), on page 616
- [Unified CVP Statistics](#), on page 616
- [Unified CVP Reporting Statistics](#), on page 628

Security Certificates

Certificates are used to ensure that browser communication is secure by authenticating clients and servers on the Web. Users can purchase certificates from a certificate authority (CA signed certificates) or they can use self-signed certificates. To establish a secure communication, execute the commands in the Command Prompt as an Administrator (right click over the **Command Prompt** and select **Run as administrator**).



Note To download PEM encoded certificates, refer to the respective browser documentation for instructions.

Certificates for Live Data

You must set up security certificates for Finesse and Cisco Unified Intelligence Center with HTTPS.

You can:

- Use the self-signed certificates provided with Finesse and Cisco Unified Intelligence Center.
- Obtain and install a Certification Authority (CA) certificate from a third-party vendor.
- Produce a certificate internally.



Note As is the case when using other self-signed certificates, agents must accept the Live Data certificates in the Finesse desktop when the sign in before they can use the Live Data gadget.

Add Self-Signed Certificates for Live Data

Both Finesse and Unified Intelligence Center are installed with self-signed certificates. If you choose to work with these self-signed certificates (rather than producing your own CA certificate or obtaining a CA certificate from a third-party certificate vendor), you must first export the certificates from the Unified Intelligence Center Publisher and Subscriber. You must then import the certificates into Finesse, importing the Publisher certificate to the Finesse Primary node and the Subscriber certificate to the Finesse Secondary node.

As is the case when using other self-signed certificates, agents must accept the Live Data certificates in the Finesse desktop when they sign in before they can use the Live Data gadget.

Procedure

- Step 1** Sign in to Cisco Unified Operating System Administration on Cisco Unified Intelligence Center (<https://<hostname of Cisco Unified Intelligence Center server>/cmplatform>).
- Step 2** From the **Security** menu, select **Certificate Management**.
- Step 3** Click **Find**.
- Step 4** Do one of the following:
- If the tomcat certificate for your server is on the list, click the certificate to select it. (Ensure that the certificate you select includes the hostname for the server.)
 - If the tomcat certificate for your server is not on the list, do the following:
 - a. Click **Generate New**.
 - b. When the certificate generation is complete, restart the Cisco Tomcat service, Unified Intelligence Center Reporting service, and Cisco Live Data NGNIX service.
 - c. Restart this procedure.
- Step 5** Download the PEM encoded certificate and save the file to your desktop.
You must download the certificates that contain the hostnames Cisco Unified Intelligence Center publisher and Cisco Unified Intelligence Center subscriber.
- Step 6** Sign in to Cisco Unified Operating System Administration on the primary Finesse server (<https://FQDN of Finesse server:8443/cmplatform>).
- Step 7** From the **Security** menu, select **Certificate Management**.
- Step 8** Click **Upload Certificate**.
- Step 9** From the **Certificate Name** drop-down list, select **tomcat-trust**.
- Step 10** Click **Browse** and browse to the location of the certificate (Cisco Unified Intelligence Center publisher and subscriber certificates).
- Step 11** Click **Upload File**.
- Step 12** Restart Cisco Finesse Tomcat on the Finesse server.
-

Obtain and Upload CA Certificate for Live Data from a Third Party Vendor

You can use a Certification Authority (CA) certificate provided by a third-party vendor to establish an HTTPS connection between the Finesse and Cisco Unified Intelligence Center servers.

Follow the instructions in the TechNote *Procedure to Obtain and Upload CA Certificate from a Third-party Vendor*, available at <https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-enterprise-1101/200286-Unified-CCE-Solution-Procedure-to-Obtai.html>.

Setup CA in Windows

Set up Microsoft Certificate Server for Windows 2008 R2

This procedure assumes that your deployment includes a Windows Server 2008 R2 (Standard) Active Directory server. Perform the following steps to add the Active Directory Certificate Services role on the Windows 2008 R2 (Standard) domain controller.

Procedure

- Step 1** Click **Start**, right-click **Computer**, and select **Manage**.
 - Step 2** In the left pane, click **Roles**.
 - Step 3** In the right pane, click **Add Roles**.
The Add Roles Wizard opens.
 - Step 4** On the Select Server Roles screen, check the **Active Directory Certificate Services** check box, and then click **Next**.
 - Step 5** On the Introduction to Active Directory Certificate Services screen, click **Next**.
 - Step 6** On the Select Role Services screen, check the **Certification Authority** check box, and then click **Next**.
 - Step 7** On the Specify Setup Type screen, select **Enterprise**, and then click **Next**.
 - Step 8** On the Specify CA Type screen, select **Root CA**, and then click **Next**.
 - Step 9** Click **Next** on the Set Up Private Key, Configure Cryptography for CA, Configure CA Name, Set Validity Period, and Configure Certificate Database screens to accept the default values.
 - Step 10** On the Confirm Installations Selections screen, verify the information, and then click **Install**.
-

Set up Microsoft Certificate Server for Windows Server

This procedure assumes that your deployment includes a Windows Server Active Directory server. Perform the following steps to add the Active Directory Certificate Services role on the Windows Server domain controller.

Before you begin

Before you begin, Microsoft .Net Framework must be installed. See Windows Server documentation for instructions.

Procedure

- Step 1** In Windows, open the **Server Manager**.
- Step 2** In the **Quick Start** window, click **Add Roles and Features** .

- Step 3** In the **Set Installation Type** tab, select **Role-based or feature-based installation** , and then click **Next**.
- Step 4** In the **Server Selection** tab, select the destination server then click **Next**.
- Step 5** In the **Server Roles** tab, check the **Active Directory Certificate Services** box, and then click the **Add Features** button in the pop-up window.
- Step 6** In the **Features** and **AD CS** tabs, click **Next** to accept default values.
- Step 7** In the **Role Services** tab, verify that **Certification Authority** box is checked, and then click **Next**.
- Step 8** In the **Confirmation** tab, click **Install**.
- Step 9** After the installation is complete, click the **Configure Active Directory Certificate Service on the destination server** link.
- Step 10** Verify that the credentials are correct (for the domain Administrator user), and then click **Next**.
- Step 11** In the **Role Services** tab, check the **Certification Authority** box, and then click **Next**.
- Step 12** In the **Setup Type** tab, select **Enterprise CA**, and then click **Next**.
- Step 13** In the **CA Type** tab, select **Root CA**, and then click **Next**.
- Step 14** In the **Private Key, Cryptography, CA Name, Validity Period, and Certificate Database** tabs, click **Next** to accept default values.
- Step 15** Review the information in the **Confirmation** tab, and then click **Configure**.

Generate and Import CA Signed Certificate in AW Machine

Generate and Import the CA signed certificate to all AW Machines.

Procedure

- Step 1** Log in to the AW-HDS-DDS Server.
- Step 2** Execute the following command:


```
cd %JAVA_HOME%\bin
```
- Step 3** Remove the existing certificate by executing:


```
keytool.exe -delete -alias <certificate_name> -keystore ..\lib\security\cacerts
```
- Step 4** Enter the keystore password when prompted.
The default keystore password is **changeit**.
- Note** To change the keystore password, see [Change Java Truststore Password, on page 608](#).
- Step 5** Generate a new key pair for the alias with the selected key size by running **keytool.exe -genkeypair -alias <certificate_name> -v -keysize 1024 -keyalg RSA -keystore ..\lib\security\cacerts**.


```
Enter keystore password: <enter the keystore password>
What is your first and last name?
[Unknown]: <specify the AW host name> E.g CCE-AW-1-21
What is the name of your organizational unit?
[Unknown]: <specify OU> E.g. ccbu
What is the name of your organization?
[Unknown]: <specify the name of the org> E.g. cisco
What is the name of your City or Locality?
```



```
[Unknown]: <specify the name of the city/locality> E.g. BLR
What is the name of your State or Province?
[Unknown]: <specify the name of the state/province> E.g. KA
What is the two-letter country code for this unit?
[Unknown]: <specify two-letter Country code> E.g. 91
Is CN=CCE-AW-1-21, OU=cisco, O=ccbu, L=BLR, ST=KA, C=91 correct?
[no]: yes
```

- Step 6** Enter the keystore password when prompted.
- Step 7** Generate the CSR certificate for the alias by running `keytool.exe -alias <certificate_name> -certreq -keystore ..\lib\security\cacerts -file c:\cert\<certificate_name>.csr` and save it to a file (for example, tomcatCert.csr).
- Step 8** Enter the keystore password when prompted.
- Step 9** Copy the root CA certificate and the CA-signed certificate to `%JAVA_HOME%\bin`.
- Step 10** Install the root CA certificate by running `keytool.exe -keystore ..\lib\security\cacerts -import -v -trustcacerts -alias root -file %Path_Of_Root_Cert%\<filename_of_root_cert>`.
- Step 11** Enter the keystore password when prompted.
- Step 12** Install the signed certificate by running `keytool.exe -keystore ..\lib\security\cacerts -import -v -trustcacerts -alias <certificate_name> -file %Path_Of_Root_Cert%\<filename_of_CA_signed_cert>`.
- Step 13** Go to Services and restart Tomcat.

Generate and Import Self-signed Certificate in AW Machine

Generate and Import the self-signed certificate to all AW Machines.

Procedure

- Step 1** Log in to the AW-HDS-DDS Server.
- Step 2** Execute the following command:


```
cd %JAVA_HOME%\bin
```
- Step 3** Remove the existing certificate by executing:


```
keytool.exe -delete -alias <certificate_name> -keystore ..\lib\security\cacerts
```
- Step 4** Enter the keystore password when prompted.
The default keystore password is **changeit**.

Note To change the keystore password, see [Change Java Truststore Password, on page 608](#).
- Step 5** Generate a new key pair for the alias with the selected key size by running: `keytool.exe -genkeypair -alias <certificate_name> -v -keysize 1024 -keyalg RSA -keystore ..\lib\security\cacerts`.


```
Enter keystore password: <enter the keystore password>
What is your first and last name?
[Unknown]: <specify the AW host name> E.g CCE-AW-1-21
What is the name of your organizational unit?
[Unknown]: <specify OU> E.g. ccbu
What is the name of your organization?
[Unknown]: <specify the name of the org> E.g. cisco
What is the name of your City or Locality?
```

```
[Unknown]: <specify the name of the city/locality> E.g. BLR
What is the name of your State or Province?
[Unknown]: <specify the name of the state/province> E.g. KA
What is the two-letter country code for this unit?
[Unknown]: <specify two-letter Country code> E.g. 91
Is CN=CCE-AW-1-21, OU=cisco, O=ccbu, L=BLR, ST=KA, C=91 correct?
[no]: yes
```

Step 6 Go to Services and restart Tomcat.

Generate Self-Signed Certificate in ECE Web Server

Procedure

- Step 1** Login to the **ECE Web Server**.
- Step 2** Open the **Internet Information Services (IIS) Manager**.
- Step 3** In the left pane, under **Connections**, choose the configured <hostname>. The <hostname> **Home** page appears.
- Step 4** From the **IIS** area, click **Server Certificates**.
- Step 5** In the right pane, under **Actions**, click **Create Self-Signed Certificate**. The **Create Self-Signed Certificate** window appears.
- Step 6** In the **Specify a friendly name for the certificate** field, enter a name for the certificate.
- Step 7** From the **Select a certificate store for the new certificate** drop-down list, choose **Web Hosting**.
- Step 8** Click **OK**. The certificate is generated and appears in the Home page.
- Step 9** In the left pane, under **Connections**, navigate to **Sites > Default Web Site**. The **Default Web Site Home** page appears.
- Step 10** In the right pane, under **Actions**, click **Bindings**.
- Step 11** Click **Add**. The **Add Site Binding** window appears.
- Step 12** From the **Type** drop-down list, choose **https**.
- Step 13** From the SSL certificate drop-down list, choose the <hostname>.
- Step 14** Click **OK**.
- Step 15** In the right pane, under **Manage Website**, click **Restart**.
-

Change Java Truststore Password

This procedure explains how to change a truststore password in a Windows machine.

Procedure

- Step 1** Log in to the Windows machine.
- Step 2** Run the following command:
- ```
cd %JAVA_HOME%\bin
```
- Step 3** Change the truststore password by running the following command:
- ```
keytool.exe -storepasswd -keystore ..\lib\security\cacerts
Enter keystore password: <old-password>
New keystore password: <new-password>
Re-enter new keystore password: <new-password>
```
-

Add Principal AW certificate to all Unified CVP Servers.

Procedure

- Step 1** Download Packaged CCE webadmin self-signed certificate to %CVP_HOME%\conf\security\.
- Step 2** Import the certificate to the CVP Call Server keystore - %CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias AW_cert -file %CVP_HOME%\conf\security\<AW certificate>.
-

Import WSM CA Certificate into CVP

Procedure

- Step 1** Log in to the Call Server or Reporting Server and retrieve the keystore password from the `security.properties` file.
- Note** At the command prompt, enter the following command:
- ```
more %CVP_HOME%\conf\security.properties.

Security.keystorePW = <Returns the keystore password>
```
- Use this keystore password when prompted for, in the following steps.
- Step 2** Remove the existing certificate by running `%CVP_HOME%\jre\bin\keytool.exe -delete -alias wsm_certificate -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS`.
- Step 3** Enter the keystore password when prompted.
- Step 4** Generate a new key pair for the alias with selected key size by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias wsm_certificate -v -validity <duration in days> -keysize 2048 -keyalg RSA`.

```

Enter keystore password: <enter the keystore password>
What is your first and last name?
[Unknown]: <specify the FQDN of the CVP server. For example: cvp-1a@example.com >
What is the name of your organizational unit?
[Unknown]: <specify OU> E.g. CCBU
What is the name of your organization?
[Unknown]: <specify the name of the org> E.g. CISCO
What is the name of your City or Locality?
[Unknown]: <specify the name of the city/locality> E.g. BLR
What is the name of your State or Province?
[Unknown]: <specify the name of the state/province> E.g. KAR
What is the two-letter country code for this unit?
[Unknown]: <specify two-letter Country code> E.g. IN
Specify 'yes' for the inputs.

```

**Note** The default duration for `validity` is 90 days.

- Step 5** Generate the CSR certificate for the alias by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -certreq -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.csr` and save it to a file (for example, `wsm.csr`).
- Step 6** Enter the keystore password when prompted.
- Step 7** Download `wsm.csr` from CVP `%CVP_HOME%\conf\security\` and sign it from CA.
- Step 8** Copy the root CA certificate and the CA-signed certificate to `%CVP_HOME%\conf\security\`
- Step 9** Install the root CA certificate by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v -validity <duration in days> -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cert>`.
- Step 10** Enter the keystore password when prompted.
- Step 11** Install the signed certificate by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v -validity <duration in days> -trustcacerts -alias wsm_certificate -file %CVP_HOME%\conf\security\<filename_of_CA_signed_cert>`.
- Step 12** Enter the keystore password when prompted.
- Step 13** Restart the **Cisco CVP WebServicesManager** service.

## Import CA Certificate into AW Machines



**Note** Prior to attempting to manage the system through Unified CCE Administration, the Administration & Data Server (AW) must exchange the SSL certificates with the Customer Voice Portal (CVP), Finesse, Cisco Enterprise Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Unified Communication Manager (CUCM), Cisco Identity Service (idS), and Virtual Voice Browser (VVB) to establish a trust communication.

### Procedure

- Step 1** Log in to the AW-HDS-DDS Server.
- Step 2** Execute the following command:

```
cd %JAVA_HOME%\bin
```

**Step 3** Copy the Root or intermediate certificates to a location in AW Machine.

**Step 4** Remove the existing certificate by executing:

```
keytool.exe -delete -alias <AW FQDN> -keystore ..\lib\security\cacerts
```

**Step 5** Enter the truststore password when prompted.

The default truststore password is **changeit**.

**Note** To change the truststore password, see [Change Java Truststore Password, on page 608](#).

**Step 6** At the AW machine terminal, run the following command:

- `cd %JAVA_HOME%\bin`
- `keytool -import -file <path where the Root or intermediate certificate is stored> -alias <AW FQDN> -keystore ..\lib\security\cacerts`

**Step 7** Enter the truststore password when prompted.

**Step 8** Go to Services and restart Apache Tomcat.

---

## Add Solution Components Self-Signed Certificate to AW Machine

### Add Finesse Certificate to AW Machine

If you do not have a CA certificate, you must import a self-signed certificate from the Finesse server to an AW machine. This enables AW Machine to communicate to Finesse over a secure channel.



---

**Note** • The certificate CommonName (CN) must match the Fully Qualified Domain Name (FQDN) provided for the respective Finesse and IdS servers in the Packaged CCE Inventory.

---

#### Procedure

---

**Step 1** Sign in to the Cisco Unified Operating System Administration on the primary server (*https://<FQDN of Finesse server>:8443/cmplatform*).

**Step 2** From the **Security** menu, select **Certificate Management**.

**Step 3** Click **Find**.

**Step 4** Do one of the following:

- If the tomcat certificate for your server is not on the list, click **Generate Self-signed**. When the certificate generation is complete, reboot your server.
- If the tomcat certificate for your server is on the list, click the certificate to select it. (Ensure that the certificate you select includes the hostname for the server.)

**Step 5** Download the PEM encoded certificate and save the file to your desktop.

You must download the self-signed certificates that contain the hostname of the primary server.

**Step 6** Copy the certificate to a location in AW Machine.

**Step 7** Run the following command at the AW machine terminal:

- `cd %JAVA_HOME%`
- `keytool -import -file <path where self-signed certificate is copied> -alias <FQDN of Finesse Server> -keystore .\lib\security\cacerts`

**Step 8** Go to Services and restart Tomcat.

## Add IdS Certificate to AW Machine

If you do not have a CA certificate, you must import a self-signed certificate from the Cisco Identify Service (IdS) to an AW machine. This enables AW Machine to communicate to IdS over a secure channel.



### Note

- You must download and import the certificate from both IdS publisher and subscriber servers.
- The certificate CommonName (CN) must match the Fully Qualified Domain Name (FQDN) provided for the respective Finesse and IdS servers in the Packaged CCE Inventory.

### Procedure

**Step 1** Sign in to the Cisco Unified Operating System Administration on the primary server (*https://<FQDN of Ids server:8443>/cmplatform*).

**Step 2** From the **Security** menu, select **Certificate Management**.

**Step 3** Click **Find**.

**Step 4** Do one of the following:

- If the tomcat certificate for your server is not on the list, click **Generate Self-signed**. When the certificate generation is complete, reboot your server.
- If the tomcat certificate for your server is on the list, click the certificate to select it. (Ensure that the certificate you select includes the hostname for the server.)

**Step 5** Download the PEM encoded self-signed certificate and save the file to your desktop.

You must download the self-signed certificates that contain the hostname of the primary server.

**Step 6** Copy the certificate to a location in AW Machine.

**Step 7** Run the following command at the AW machine terminal:

- `cd %JAVA_HOME%`
- `keytool -import -file <path where self-signed certificate is copied> -alias <FQDN of IdS Server> -keystore .\lib\security\cacerts`

**Step 8** Go to Services and restart Tomcat.

---

## Add ECE Web Server Certificate to AW Machine

If you do not have a CA certificate, you must import a self-signed certificate from the ECE web server to AW machine. This will enable you to launch the ECE gadget in the Unified CCE Administration.

### Procedure

---

- Step 1** From the ECE Web Server (<https://<ECE Web Server>>), download the PEM encoded certificate, and save the file to your desktop.
- Step 2** Copy the certificate to a location in AW Machine.
- Step 3** Run the following command at the AW machine terminal:
- `cd %JAVA_HOME%\bin`
  - `keytool -import -file <path where self-signed certificate is copied> -alias <FQDN of ECE Web Server> -keystore ..\lib\security\cacerts`
- Step 4** Enter the truststore password when prompted.  
The default truststore password is **changeit**.
- Note** To change the truststore password, see [Change Java Truststore Password, on page 608](#).
- Step 5** Go to Services and restart Tomcat.
- 

## Import WSM Certificate into AW Machines



**Note** This procedure is applicable if you do not have the CA certificate.

---

When you install CVP Call Server or Reporting Server, you must import the Web Service Manager (WSM) self-signed certificate into all AW machines. This will eliminate any browser warnings and establish HTTPS connection between CVP Call Server or Reporting Server and AW machine. Use Keytool to generate a Self-Signed Certificate.



**Important** The certificate CommonName (CN) must match the Fully Qualified Domain Name (FQDN) provided for the CVP Call Server or Reporting Server in the Packaged CCE Inventory.

---

### Procedure

---

- Step 1** Log in to the CVP Call Server or Reporting Server.

**Step 2** On the command prompt, navigate to the directory where .keystore is located.

For example:

```
%CVP_HOME%\conf\security
```

**Step 3** Delete the wsm certificate from the CVP keystore using the following command:

```
%CVP_HOME%\jre\bin\keytool.exe -delete -alias wsm_certificate -keystore
%CVP_HOME%\conf\security\.keystore -storetype JCEKS
```

**Step 4** Enter the CVP keystore password.

The CVP keystore password is available at %CVP\_HOME%\conf\security.properties.

Or,

Run the following command to get the keystore password:

```
more %CVP_HOME%\conf\security.properties
Security.keystorePW = <Returns the keystore password>
```

**Step 5** Run the following command to generate the self-signed certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore
-genkeypair -alias wsm_certificate -v -validity <duration in days> -keysize 2048 -keyalg
RSA
```

**Note** The default duration for validity is 90 days.

```
Enter keystore password: <enter the keystore password>
What is your first and last name?
[Unknown]: <Specify the FQDN of the CVP server. For example: cvp-1a@example.com>
What is the name of your organizational unit?
[Unknown]: <specify OU> E.g. CCBU
What is the name of your organization?
[Unknown]: <specify the name of the org> E.g. CISCO
What is the name of your City or Locality?
[Unknown]: <specify the name of the city/locality> E.g. BLR
What is the name of your State or Province?
[Unknown]: <specify the name of the state/province> E.g. KAR
What is the two-letter country code for this unit?
[Unknown]: <specify two-letter Country code> E.g. IN
Specify 'yes' for the inputs.
```

**Step 6** Enter the key password for wsm certificate. Leave it blank to use the default keystore password.

**Step 7** Restart the CVP Call Server or Reporting Server.

**Step 8** Download the self-signed certificate from the browser (*https://FQDN of the CVP Server:8111/cvp-dp/rest/DiagnosticPortal/GetProductVersion*).

**Step 9** Copy the certificate to a location in AW Machine.

**Step 10** At the AW machine terminal, run the following command:

- cd %JAVA\_HOME%\bin
- keytool -import -file <path where self-signed certificate is copied> -alias <FQDN of the CVP Server> -keystore ..\lib\security\cacerts

**Step 11** Enter the truststore password when prompted.

The default truststore password is **changeit**.

**Note** To change the truststore password, see [Change Java Truststore Password, on page 608](#).



**Step 12** Go to Services and restart Apache Tomcat.

---

## Import VVB Self-Signed Certificate into AW Machines

Import self-signed certificate from Virtualized Voice Browser (VVB) into all AW machines. This enables the AW Machine to communicate with the component over a secure channel.



**Note**

- The certificate CommonName (CN) must match the Fully Qualified Domain Name (FQDN) provided for VVB in the Packaged CCE Inventory.

---

### Procedure

---

- Step 1** Sign in to the **Cisco Unified Operating System Administration** on the VVB server using the URL (*https://<FQDN of VVB server>:8443/cmplatform*).
- Step 2** From the **Security** menu, select **Certificate Management**.
- Step 3** Click **Find**.
- Step 4** Do one of the following:
- If the tomcat certificate for your server is not on the list, click **Generate Self-signed**. When the certificate generation is complete, reboot your server.
  - If the tomcat certificate for your server is on the list, click the certificate to select it. (Ensure that the certificate you select includes the hostname for the server.)
- Step 5** Download the PEM encoded certificate and save the file to your desktop.  
You must download the self-signed certificates that contain the hostname of the primary server.
- Step 6** Copy the certificate to a location in AW Machine.
- Step 7** Run the following command as an administrator at the AW machine terminal:
- ```
• cd %JAVA_HOME%\bin
```
- ```
• keytool -import -file <path where self-signed certificate is copied> -alias <FQDN of component Server> -keystore ..\lib\security\cacerts
```
- Step 8** Enter the keystore password when prompted.  
The default keystore password is **changeit**.
- Note** To change the keystore password, see [Change Java Truststore Password, on page 608](#).
- Step 9** Go to Services and restart Apache Tomcat.
-

# Graceful Shutdown of Call Server or Reporting Server

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

## Procedure

- 
- Step 1** Log in to the CVP Call Server box.
  - Step 2** Go to <CVP-INSTALLED-LOCATION>\Cisco\CVP\bin\ServiceController.
  - Step 3** Run the `service-controller.bat` file.
  - Step 4** Enter the administrator credentials, service name, and IP address details at the prompt:

```
CALLSERVER-IP-ADDRESS: <IP-Address of the Call Server>
CALLSERVER-USERNAME: <Username of the Call Server>
CALLSERVER-PASSWORD: <Password of the Call Server>
SERVICE-NAME: <Choose the Service name which you need to shutdown
gracefully(callserver/reportingserver)>
REPORTINGSERVER-IP-ADDRESS: <IP-Address of the REPORTING SERVER>
```

- Note**
- To shut down the Reporting Server gracefully, ensure that the CVP Call Server is up and running.
  - If you have selected the **reportingserver** service, then be sure to provide the IP address of the Reporting Server.
- 

## Unified CVP Statistics

### Call Server

#### 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.

The following table describes ICM Service call statistics.

*Table 54: ICM Service Call Statistics*

| Statistic           | Description |
|---------------------|-------------|
| Realtime Statistics |             |

| <b>Statistic</b>                          | <b>Description</b>                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Active Calls                              | 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.                                                                        |
| Active SIP Call Legs                      | 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.                                                        |
| Active VRU Call Legs                      | 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.                                                          |
| Active ICM Lookup Requests                | 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.                                                                           |
| Active Basic Service Video Calls Offered  | The current number of simultaneous basic service video calls being processed by the ICM service where video capability was offered.                                                                                                                                                                                                    |
| Active Basic Service Video Calls Accepted | The current number of simultaneous calls that were accepted as basic service video calls and are being processed by the ICM service.                                                                                                                                                                                                   |
| <b>Interval Statistics</b>                |                                                                                                                                                                                                                                                                                                                                        |
| Start Time                                | The time at which the current interval has begun.                                                                                                                                                                                                                                                                                      |
| Duration Elapsed                          | The amount of time that has elapsed since the start time in the current interval.                                                                                                                                                                                                                                                      |
| Interval Duration                         | The interval at which statistics are collected. The default value is 30 minutes.                                                                                                                                                                                                                                                       |
| New Calls                                 | 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.                                                                                                                          |
| SIP Call Legs                             | 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. |
| VRU Call Legs                             | 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.        |

| Statistic                                | Description                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ICM Lookup Requests                      | 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. |
| Basic Service Video Calls Offered        | The number of offered basic service video calls processed by the ICM service during the current interval.                                                                                                                                                                                                                                           |
| Basic Service Video Calls Accepted       | The number of basic service video calls accepted and processed by the ICM service during the current interval.                                                                                                                                                                                                                                      |
| <b>Aggregate Statistics</b>              |                                                                                                                                                                                                                                                                                                                                                     |
| Start Time                               | The time the service started collecting statistics.                                                                                                                                                                                                                                                                                                 |
| Duration Elapsed                         | The amount of time that has elapsed since the service start time.                                                                                                                                                                                                                                                                                   |
| Total Calls                              | 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.                                                                                                                                                                                            |
| Total SIP Call Legs                      | 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.                                                                                                                        |
| Total VRU Call Legs                      | 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.                                                                                          |
| Total ICM Lookup Requests                | 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.                                                      |
| Total Basic Service Video Calls Offered  | The total number of newly offered basic service video calls processed by the ICM service since system start time.                                                                                                                                                                                                                                   |
| Total Basic Service Video Calls Accepted | The total number of new basic service video calls accepted and processed by the ICM service since system start time.                                                                                                                                                                                                                                |

## 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.

The following table describes the SIP Service call statistics.

Table 55: SIP Service Call Statistics

| Statistic                                 | Description                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Realtime Statistics</b>                |                                                                                                                                                                                                                                                                                                                                                                                       |
| Active Calls                              | A real time snapshot metric indicating the count of the number of current calls being handled by the SIP service.                                                                                                                                                                                                                                                                     |
| Total Call Legs                           | 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.                                                    |
| Active Basic Service Video Calls Offered  | The number of basic service video calls in progress where video capability was offered.                                                                                                                                                                                                                                                                                               |
| Active Basic Service Video Calls Answered | The number of basic service video calls in progress where video capability was answered.                                                                                                                                                                                                                                                                                              |
| Active Agent Whisper Calls                | The number of active whisper call legs.                                                                                                                                                                                                                                                                                                                                               |
| Active Agent Greeting Calls               | The number of active greeting call legs.                                                                                                                                                                                                                                                                                                                                              |
| <b>Interval Statistics</b>                |                                                                                                                                                                                                                                                                                                                                                                                       |
| Start Time                                | The time the system started collecting statistics for the current interval.                                                                                                                                                                                                                                                                                                           |
| Duration Elapsed                          | The amount of time that has elapsed since the start time in the current interval.                                                                                                                                                                                                                                                                                                     |
| Interval Duration                         | The interval at which statistics are collected. The default value is 30 minutes.                                                                                                                                                                                                                                                                                                      |
| New Calls                                 | 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.                                                                                                                                                                                                |
| Connects Received                         | 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. |
| Avg Latency Connect to Answer             | 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.                                                                                                                                                             |

| <b>Statistic</b>                   | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Failed SIP Transfers (Pre-Dialog)  | 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. |
| Failed SIP Transfers (Post-Dialog) | 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.                                               |
| Basic Service Video Calls Offered  | The number of basic service video calls offered in the current interval.                                                                                                                                                                                                                                                                                                                                                                                 |
| Basic Service Video Calls Answered | The number of basic service video calls answered in the current interval.                                                                                                                                                                                                                                                                                                                                                                                |
| Whisper Announce Answered          | The number of calls for which whisper announcement was successful during the interval.                                                                                                                                                                                                                                                                                                                                                                   |
| Whisper Announce Failed            | The number of calls for which whisper announcement was failed during the interval.                                                                                                                                                                                                                                                                                                                                                                       |
| Agent Greeting Answered            | The number of calls for which agent greeting was successful during the interval.                                                                                                                                                                                                                                                                                                                                                                         |
| Agent Greeting Failed              | The number of calls for which agent greeting was failed during the interval.                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Aggregate Statistics</b>        |                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Start Time                         | The time the service started collecting statistics.                                                                                                                                                                                                                                                                                                                                                                                                      |
| Duration Elapsed                   | The amount of time that has elapsed since the service start time.                                                                                                                                                                                                                                                                                                                                                                                        |
| Total New Calls                    | 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.                                                                                                                                                                                                                                                                   |
| Connects Received                  | 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.                                                                                 |

| Statistic                                | Description                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Avg Latency Connect to Answer            | 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.                                                                                                                                                                                                |
| Failed SIP Transfers (Pre-Dialog)        | 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.                                                |
| Failed SIP Transfers (Post-Dialog)       | 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. |
| Total Basic Service Video Calls Offered  | The total number of basic service video calls offered since system start time.                                                                                                                                                                                                                                                                                                                          |
| Total Basic Service Video Calls Answered | The total number of basic service video calls answered since system start time.                                                                                                                                                                                                                                                                                                                         |
| Total Whisper Announce Answered          | The total number of call for which whisper announce was successful since the system start time.                                                                                                                                                                                                                                                                                                         |
| Total Whisper Announce Failed            | The total number of calls for which whisper announce failed since the system start time.                                                                                                                                                                                                                                                                                                                |
| Total Agent Greeting Answered            | The total number of calls for which agent greeting was successful since the system start time.                                                                                                                                                                                                                                                                                                          |
| Total Agent Greeting Failed              | The total number of calls for which agent greeting failed since the system start time.                                                                                                                                                                                                                                                                                                                  |

## Infrastructure Statistics

Unified CVP infrastructure statistics displays realtime, interval, and aggregate data (including Java Virtual Machine (JVM) and threadpool realtime statistics).

The following table describes infrastructure statistics.

**Table 56: Infrastructure Statistics**

| Statistic                  | Description |
|----------------------------|-------------|
| <b>Realtime Statistics</b> |             |

| <b>Statistic</b>                   | <b>Description</b>                                                                                                                                                                                                                         |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ports Available                    | 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.                                                 |
| Current Port Usage                 | 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.                                                         |
| Current Port Usage State           | The threshold level of port usage. There are four levels: safe, warning, critical, and failure.                                                                                                                                            |
| <b>Interval</b>                    |                                                                                                                                                                                                                                            |
| Start Time                         | The time the system started collecting statistics for the current interval.                                                                                                                                                                |
| Duration Elapsed                   | The amount of time that has elapsed since the start time in the current interval.                                                                                                                                                          |
| Interval Duration                  | The interval at which statistics are collected. The default value is 30 minutes.                                                                                                                                                           |
| Total New Port Usage Requests      | 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.                                         |
| Average Port Usage Requests/Minute | 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.               |
| Maximum Port Usage                 | The maximum number of ports used during this time interval.                                                                                                                                                                                |
| <b>Aggregate Statistics</b>        |                                                                                                                                                                                                                                            |
| Start Time                         | The time the service started collecting statistics.                                                                                                                                                                                        |
| Duration Elapsed                   | The amount of time that has elapsed since the service start time.                                                                                                                                                                          |
| Total New Port Usage Requests      | 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.                                                          |
| Average Port Usage Requests/Minute | 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. |
| Peak Port Usage                    | 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.               |



| Statistic                        | Description                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Total Denied Port Usage Requests | 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 57: Thread Pool Realtime Statistics**

| Statistic                  | Description                                                                                  |
|----------------------------|----------------------------------------------------------------------------------------------|
| <b>Realtime Statistics</b> |                                                                                              |
| Idle Threads               | The number of idle threads waiting for some work.                                            |
| Active Threads             | The number of running thread pool threads currently processing some work.                    |
| Core Pool Size             | The number of thread pool threads that are never destroyed, regardless of their idle period. |
| Maximum Pool Size          | The maximum number of thread pool threads that can exist simultaneously.                     |
| Largest Pool Size          | The peak number of thread pool threads simultaneously tasks with some work to process.       |

The following table describes Java Virtual Machine statistics.

**Table 58: Java Virtual Machine (JVM) Realtime Statistics**

| Statistic                  | Description                                                                                                                                                                                                          |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Realtime Statistics</b> |                                                                                                                                                                                                                      |
| Peak Memory Usage          | 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.     |
| Current Memory Usage       | The current number of megabytes of memory used by the Java Virtual Machine.                                                                                                                                          |
| Total Memory               | 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. |

| Statistic           | Description                                                                                                                                                                                                                                                                                                 |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Available Memory    | 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.                                                                                        |
| Threads in Use      | The number of threads currently in use in the Java Virtual Machine. This number includes all of the Unified CVP and thread pool threads, as well as those threads created by the Web Application Server running within the same JVM.                                                                        |
| Peak Threads in Use | 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 and thread pool threads, as well as threads created by the Web Application Server running within the same JVM. |
| Uptime              | 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.                                                                                                           |

## VXML Server

### Unified CVP VXML Server Statistics

The **Unified CVP VXML Server Statistics** displays realtime, interval, and aggregate Unified CVP VXML Server statistics.

- To view VXML Statistics, at least one deployed Unified CVP VXML Server application must be configured with the CVPDataFeed logger.

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

**Table 59: VXML Server Statistics**

| Statistic                    | Description                                                                    |
|------------------------------|--------------------------------------------------------------------------------|
| <b>Port Usage Statistics</b> |                                                                                |
| Total Ports                  | The total number of licensed ports for this Unified CVP VXML server.           |
| Port Usage Expiration Date   | The date when the licensed ports expires for this Unified CVP VXML server.     |
| Available Ports              | The number of port licenses available for this Unified CVP VXML server.        |
| Total Concurrent Callers     | The number of callers currently interacting with this Unified CVP VXML server. |
| <b>Real Time Statistics</b>  |                                                                                |

| <b>Statistic</b>            | <b>Description</b>                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Active Sessions             | The number of current sessions being handled by the Unified CVP VXML Server.                                                                                                                                                                                                                                                                        |
| Active ICM Lookup Requests  | The number of current ICM requests being handled by the Unified CVP VXML Server.                                                                                                                                                                                                                                                                    |
| <b>Interval Statistics</b>  |                                                                                                                                                                                                                                                                                                                                                     |
| Start Time                  | The time at which the current interval begins.                                                                                                                                                                                                                                                                                                      |
| Duration Elapsed            | The amount of time that has elapsed since the start time in the current interval.                                                                                                                                                                                                                                                                   |
| Interval Duration           | The interval at which statistics are collected. The default value is 30 minutes.                                                                                                                                                                                                                                                                    |
| Sessions                    | The total number of sessions in the Unified CVP VXML Server in the current interval.                                                                                                                                                                                                                                                                |
| Reporting Events            | The number of events sent to the Unified CVP Reporting Server from the Unified CVP VXML Server in the current interval.                                                                                                                                                                                                                             |
| ICM Lookup Requests         | The number of requests from the Unified CVP VXML Server to the ICM Service in the current interval.                                                                                                                                                                                                                                                 |
| ICM Lookup Responses        | 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. |
| ICM Lookup Successes        | The number of successful requests from the Unified CVP VXML Server to the ICM Service in the current interval.                                                                                                                                                                                                                                      |
| ICM Lookup Failures         | 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.                                                                                         |
| <b>Aggregate Statistics</b> |                                                                                                                                                                                                                                                                                                                                                     |
| Start Time                  | The time at which the current interval has begun.                                                                                                                                                                                                                                                                                                   |
| Duration Elapsed            | The amount of time that has elapsed since the start time in the current interval.                                                                                                                                                                                                                                                                   |
| Total Sessions              | The total number of sessions in the Unified CVP VXML Server since startup.                                                                                                                                                                                                                                                                          |
| Total Reporting Events      | The total number of reporting events sent from the Unified CVP VXML Server since startup.                                                                                                                                                                                                                                                           |

| Statistic                  | Description                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Total ICM Lookup Requests  | 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.                                                                                                                                                                                                                          |
| Total ICM Lookup Responses | 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. |
| Total ICM Lookup Successes | 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.                                                                                                                                                                                                                                      |
| Total ICM Lookup Failures  | 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 the Unified CVP VXML Server generates a failed message.                                                                                                     |

## Infrastructure Statistics

To view further details about infrastructure statistics, see section [Infrastructure Statistics](#), on page 621.

## 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.

The following table describes the IVR Service call statistics.

**Table 60: IVR Service Call Statistics**

| Statistic                       | Description                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------|
| <b>Realtime Call Statistics</b> |                                                                                   |
| Active Calls                    | The number of active calls being serviced by the IVR service.                     |
| Active HTTP Requests            | The number of active HTTP requests being serviced by the IVR service.             |
| <b>Interval Statistics</b>      |                                                                                   |
| Start Time                      | The time the system started collecting statistics for the current interval.       |
| Duration Elapsed                | The amount of time that has elapsed since the start time in the current interval. |

| <b>Statistic</b>                 | <b>Description</b>                                                                                                                                                                                                                                                                                                 |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interval Duration                | The interval at which statistics are collected. The default value is 30 minutes.                                                                                                                                                                                                                                   |
| Peak Active Calls                | Maximum number of active calls handled by the IVR service at the same time during this interval.                                                                                                                                                                                                                   |
| New Calls                        | 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.                                                                                                                               |
| Calls Finished                   | 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.                                         |
| Average Call Latency             | The average amount of time in milliseconds it took the IVR Service to process a New Call or Call Result Request during this interval.                                                                                                                                                                              |
| Maximum Call Latency             | 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.                                                                                                                           |
| Minimum Call Latency             | 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.                                                                                                                                |
| Peak Active HTTP Requests        | 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.                         |
| Total HTTP Requests              | The total number of HTTP Requests received from a client by the IVR Service during this time interval.                                                                                                                                                                                                             |
| Average HTTP Requests/second     | The average number of HTTP Requests the IVR Service receives per second during this time interval.                                                                                                                                                                                                                 |
| Peak Active HTTP Requests/second | 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. |
| <b>Aggregate Statistics</b>      |                                                                                                                                                                                                                                                                                                                    |
| Start Time                       | The time the service started collecting statistics.                                                                                                                                                                                                                                                                |

| Statistic                 | Description                                                                                                                                                                                                                                                                                                      |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Duration Elapsed          | The amount of time that has elapsed since the service start time.                                                                                                                                                                                                                                                |
| Total New Calls           | 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. |
| Peak Active Calls         | The maximum number of simultaneous calls processed by the IVR Service since the service started.                                                                                                                                                                                                                 |
| Total HTTP Requests       | Total HTTP Requests is a metric that represents the total number of HTTP Requests received from all clients. This metric is the total number of HTTP Requests received by the IVR Service since system startup.                                                                                                  |
| Peak Active HTTP Requests | Active HTTP Requests is a metric that indicates the current number of simultaneous HTTP requests processed by the IVR Service. Maximum number of active HTTP requests processed at the same time since the IVR service started. This is also known as high water marking.                                        |

## Unified CVP Reporting Statistics

### Reporting Statistics

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

The following table describes the Unified CVP Reporting Server statistics.

**Table 61: Unified CVP Reporting Server Statistics**

| Statistic                  | Description                                                                                                                                                                              |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Interval Statistics</b> |                                                                                                                                                                                          |
| Start Time                 | The time the system started collecting statistics for the current interval.                                                                                                              |
| Duration Elapsed           | The amount of time that has elapsed since the start time in the current interval.                                                                                                        |
| Interval Duration          | The interval at which statistics are collected. The default value is 30 minutes.                                                                                                         |
| VXML Events Received       | 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. |

| <b>Statistic</b>            | <b>Description</b>                                                                                                                                                                                                 |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SIP Events Received         | 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.                             |
| IVR Events Received         | 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.                                  |
| Database Writes             | The total number of writes to the database made by the Unified CVP Reporting Server during the interval. For each write to the database by the Unified CVP Reporting Server, this metric will be increased by one. |
| <b>Aggregate Statistics</b> |                                                                                                                                                                                                                    |
| Start Time                  | The time the service started collecting statistics.                                                                                                                                                                |
| Duration Elapsed            | The amount of time that has elapsed since the service start time.                                                                                                                                                  |
| VXML Events Received        | 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.                      |
| SIP Events Received         | 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.                        |
| IVR Events Received         | 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.                        |
| Database Writes             | 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.       |

## Infrastructure Statistics

To view further details about infrastructure statistics, see section [Infrastructure Statistics](#) , on page 621.







## INDEX

- A**
- accessing micro-application by specifying Run VRU Script Node **526**
  - adding **40, 241, 260, 263, 322, 326, 342, 346, 350, 359, 391**
    - attributes **260**
    - bucket intervals **359**
    - bulk jobs **391**
    - call types **342, 346**
    - data sources **40**
    - desk settings **322**
    - ECC variables **346**
    - Media Routing Domains **326**
    - Network VRU Scripts **350**
    - precision queues **263**
    - supervisors **241**
  - agent desk settings **88**
    - configuring **88**
  - agent trace **324**
  - agents **236–238, 382**
    - bulk jobs **382**
    - reskill **236**
    - reskill multiple **237–238**
  - attributes **259–261**
    - adding **260**
- B**
- bucket intervals **358–359**
    - adding **359**
    - reporting **358**
  - built-in functions **499**
    - date and time functions **499**
  - bulk jobs **377, 382, 388–389, 391, 599**
    - adding **391**
    - agents **382**
    - call type **388**
    - logs **599**
    - review details **391**
    - skill group **389**
- C**
- call statistics **616, 618, 626**
    - ICM Service **616**
    - IVR service **626**
  - call statistics (*continued*)
    - SIP Service **618**
  - Call Studio **569, 571–572**
    - deploying scripts **572**
    - integrating scripts (simplified with Unified ICME scripts) **572**
    - integrating scripts with Unified ICME scripts **571**
    - using ReqICMLabel **569**
  - call type **388**
    - bulk jobs **388**
  - call type reporting **342**
  - call types **342, 346, 421**
    - adding **342, 346**
    - and scripts **342**
    - categorization **342**
    - default call type **421**
  - Capture micro-application error code settings **521**
  - categorizing contacts **425, 428–430, 432–433**
    - by branching **433**
    - by call type qualifiers **428**
    - by dialed number **429**
    - by the day of week **432**
    - by time **430**
    - by time and date **430**
    - through scheduling scripts by call type **425**
  - CG **81**
    - Private Interfaces **81**
    - Visible Interfaces **81**
  - configuration parameters **529**
    - Play Media micro-application **529**
  - creating **526**
    - Unified CCE applications **526**
  - CTI Server **79, 81**
    - Adding **79**
      - adding a component **79**
      - completing setup **81**
      - setting Network Interface Properties **81**
      - setting properties **79**
  - custom functions **503–504**
    - adding custom functions **503**
    - exporting custom functions **504**
    - importing custom functions **503**
  - CVP scripting **515–517, 521, 528–529, 535, 557, 562, 566, 568**
    - about **516**
    - Capture micro-application **528**
    - considerations for ICM Enterprise **515**

CVP scripting (*continued*)

- data handling [521](#)
- error checking [521](#)
- Get Digits (GD) micro-application [557](#)
- Get Speech (GS) micro-application [566](#)
- information exchange [521](#)
- Menu (M) micro-application [562](#)
- micro-applications [517](#)
- Play Data (PD) micro-application [535](#)
- Play Media (PM) micro-application [529](#)
- with Call Studio [568](#)
- with ICM Enterprise [517](#)

**D**

- data handling in scripting [521](#)
- data sources [40](#)
  - adding [40](#)
- data storage for Play Data micro-application [536](#)
- Default Media Server [527](#)
  - for Micro-applications [527](#)
- deleting [397](#)
  - permanently [397](#)
- deploying scripts [572](#)
  - with Call Studio [572](#)
- desk settings [322](#)
  - adding [322](#)
- dialed number [422](#)
- dialed numbers [327](#)
- digit entry completion [561, 565](#)
  - Get Digits micro-application [561](#)
  - Menu micro-application [565](#)
- dynamic audio file capability [527](#)

**E**

- ECC variables [346, 349](#)
  - adding [346](#)
  - sizing [349](#)
- end node [450](#)
- enterprise services [445](#)
- enterprise skill groups [443](#)
- error checking [521](#)
  - in scripting [521](#)
- error code settings [521](#)
  - Capture micro-application [521](#)
  - Get Digits micro-application [521](#)
  - Get Speech micro-application [521](#)
  - Menu micro-application [521](#)
  - Play Data micro-application [521](#)
  - Play Media micro-application [521](#)
  - user.microapp.error\_code ECC variable for non-video [521](#)
  - user.microapp.error\_code ECC variable for video [521](#)
- error codes [521](#)
  - user.microapp.error\_code ECC [521](#)

- examples [527, 534, 556, 560, 564](#)
  - Get Digits micro-application configuration [560](#)
  - Menu micro-application configuration [564](#)
  - Play Data micro-application configuration [556](#)
  - Play Media micro-application configuration [534](#)
  - using a dynamic audio file [527](#)
- external VoiceXML [561, 567–568](#)
  - error handling, Get Speech micro-application [561](#)
  - Get Speech micro-application [561](#)
  - passing data back to Unified ICME [568](#)
  - passing information [567](#)

**F**

- formulas [487](#)
  - formula example [487](#)

**G**

- Get Digits micro-application [521, 560–561](#)
  - configuration examples [560](#)
  - digit entry completion [561](#)
  - error code settings [521](#)
  - if no entry timeout occurs [561](#)
- Get Speech micro-application [521, 561](#)
  - error code settings [521](#)
  - external VoiceXML [561](#)

**H**

- Helix Server [534](#)
  - streaming ringtones [534](#)
- high-level configuration steps for call flow models [569](#)
- how to [471, 474–476, 493](#)
  - change the queue to agent type [474](#)
  - select an agent by an expression [476](#)
  - set variable values with the set variable node [493](#)
  - specify an agent directly [475](#)
  - use MRD to categorize contacts [471](#)

**I**

- ICM Service [616](#)
  - statistics [616](#)
- ICM user accounts [248](#)
- information exchange [521](#)
  - in scripting [521](#)
- infrastructure statistics [621](#)
  - descriptions [621](#)
- integrating scripts [572](#)
  - Call Studio and ICME [572](#)
- integrating scripts - traditional [571](#)
  - Call Studio and ICME [571](#)
- internet script editor (ISE) [408–409](#)
  - starting ISE [408](#)

internet script editor (ISE) (*continued*)  
 upgrading ISE [409](#)  
 IVR Service [626](#)  
 statistics [626](#)

## K

keyboard shortcuts [159](#)

## L

licensing [621](#)  
 statistics [621](#)  
 logs [599](#)  
 bulk jobs [599](#)  
 system validation [599](#)

## M

mathematical Functions [500](#)  
 media routing domain [471](#)  
 Media Routing Domains [326](#)  
 adding [326](#)  
 Media Server [527](#)  
 specify in Operations Console [527](#)  
 Menu micro-application [521, 564–565](#)  
 configuration examples [564](#)  
 digit entry completion [565](#)  
 error code settings [521](#)  
 if no entry timeout occurs [565](#)  
 micro-applications [517, 526–529, 535, 557, 562, 566](#)  
 accessing [526](#)  
 Capture [528](#)  
 dynamic audio file support [527](#)  
 Get Digits (GD) [557](#)  
 Get Speech (GS) [566](#)  
 Menu (M) [562](#)  
 Play Data (PD) [535](#)  
 Play Media (PM) [529](#)  
 specifying Run External Script Node to access [526](#)  
 using for scripting [526](#)  
 Micro-applications [527](#)  
 Default media server [527](#)  
 miscellaneous functions [501](#)  
 MR PG [147](#)  
 setting up [147](#)  
 multichannel scripting [471](#)

## N

Network VRU Scripts [350–353, 356](#)  
 adding [350](#)  
 configuration parameters [353](#)  
 sample configuration values [356](#)  
 sample VRU Script Names [352](#)

Network VRU Scripts (*continued*)  
 VRU Script Name Parameters [351](#)  
 node [472](#)  
 pick / pull [472](#)  
 Node Manager [81](#)  
 nodes [450](#)  
 end [450](#)  
 release call [450](#)

## O

operators [496–498](#)  
 arithmetic operators [497](#)  
 bitwise operators [498](#)  
 equality operators [497](#)  
 logical operators [498](#)  
 miscellaneous operators [498](#)  
 operator precedence [496](#)  
 prefix operators [497](#)  
 relational operators [497](#)

## P

param elements, using [567](#)  
 parameter element, URL [567](#)  
 PG [81](#)  
 Private Interfaces [81](#)  
 play back types for voice data [538](#)  
 Play Data micro-application [538](#)  
 Play Data micro-application [521, 536, 538, 556](#)  
 configuration examples [556](#)  
 data storage [536](#)  
 error code settings [521](#)  
 play back types for voice data [538](#)  
 Play Media micro-application [521, 534](#)  
 configuration example, play welcome message [534](#)  
 error code settings [521](#)  
 precision queues [259, 261–263, 265, 267, 465, 505–507](#)  
 adding [263](#)  
 attributes [259, 261](#)  
 Consider If [261, 265, 267](#)  
 dynamic [507](#)  
 expressions [261, 265](#)  
 or skill groups [262](#)  
 precision queues [259](#)  
 terms [259](#)  
 queuing behavior [465, 507](#)  
 scripting [505–507](#)  
 static [506](#)  
 steps [265](#)  
 terms [261](#)  
 Wait for [265](#)  
 Private Interfaces [81](#)

**R**

- report templates [40](#)
  - locating [40](#)
- Reporting Server [628](#)
  - statistics [628](#)
- ReqICMLabel [569](#)
  - using to pass data [569](#)
- requirements [568](#)
  - VoiceXML [568](#)
- reskilling agents [236](#)
- reskilling multiple agents [237–238](#)

**S**

- Script Execution [433](#)
- scripting for CVP [515–517, 521, 528–529, 535, 557, 562, 566, 568](#)
  - about [516](#)
    - Capture micro-application [528](#)
    - considerations for ICM Enterprise [515](#)
    - data handling [521](#)
    - error checking [521](#)
    - Get Digits (GD) micro-application [557](#)
    - Get Speech (GS) micro-application [566](#)
    - information exchange [521](#)
    - Menu (M) micro-application [562](#)
    - micro-applications [517](#)
    - Play Data (PD) micro-application [535](#)
    - Play Media (PM) micro-application [529](#)
    - with Call Studio [568](#)
    - with ICM Enterprise [517](#)
  - scripting for Packaged CCE precision queues [505](#)
  - service creation environments (script editors) [516](#)
    - Call Studio [516](#)
    - ICM Script Editor [516](#)
- services [446](#)
- SIP Service call statistics [618](#)
- skill group [389](#)
  - bulk jobs [389](#)
- skill groups [256, 262](#)
  - and Cisco Unified Intelligence Center reporting [256](#)
  - or precision queues [262](#)
- specifying Run External Script Node to access Unified CVP
  - micro-applications [526](#)
- statistics [616, 618, 621, 624, 626, 628](#)
  - ICM service [616](#)
  - infrastructure [621](#)
  - IVR Service [626](#)
  - licensing [621](#)
  - Reporting Server [628](#)
  - SIP Service [618](#)
  - thread pool [621](#)
  - VXML Server [624](#)
- stopping script processing [450](#)
- streaming ringtones [534](#)
  - Helix Server [534](#)

- supervisor assist [249](#)
- supervisors [241, 249](#)
  - adding [241](#)
  - and teams [249](#)
- system statistics [621](#)
  - licensing [621](#)
  - thread pool [621](#)
- system validation [599](#)
  - logs [599](#)

**T**

- target requery [451](#)
- teams [249](#)
- thread pool statistics [621](#)
- timezones [40](#)
  - and data sources [40](#)

**U**

- Unified CCE [516, 526](#)
  - creating applications to access Unified CVP
    - micro-applications [526](#)
  - scripting [516](#)
- Unified CVP report templates [40](#)
  - obtaining [40](#)
- Unified ICME [568](#)
  - passing data back with external VoiceXML [568](#)
- Unified Intelligence Center [40](#)
  - data sources [40](#)
- user interface [159](#)
  - keyboard shortcuts [159](#)
- using [567](#)
  - param elements [567](#)
- utility nodes [511–512](#)
  - comment [511](#)
  - line connector [512](#)
  - start [511](#)

**V**

- variables [488, 490, 492, 495](#)
  - call control variables [488](#)
  - closed variables [495](#)
  - ECC variables [490](#)
  - multi-target variables [488](#)
  - single-target variables [488](#)
  - user variables [492](#)
  - variable syntax [488](#)
- videos [521](#)
  - error code settings for Full Video [521](#)
- Visible Interfaces [81](#)
- voice data, play back types [538](#)
- VoiceXML [516, 561, 567–568](#)
  - error handling, Get Speech micro-application [561](#)

VoiceXML (*continued*)

- external, Get Speech micro-application [561](#)
  - passing data back to Unified ICME with external [568](#)
  - passing information to the external [567](#)
  - requirements [568](#)
  - scripting [516](#)
- VRU [526, 531](#)
- Run VRU Script node [526, 531](#)
- VRUs [455, 458–459](#)
- accessing VRU scripts [455](#)
  - checking for VRU errors [458](#)
  - queuing calls at VRUs [459](#)
- VXML Server [624](#)
- statistics [624](#)

