



Cisco Unified Contact Center Enterprise Features Guide, Release 12.6(2)

First Published: 2023-04-28

Americas Headquarters

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

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)

© 1994–2023 Cisco Systems, Inc. All rights reserved.



Preface

- [Change History](#), on page iii
- [About This Guide](#), on page iv
- [Audience](#), on page v
- [Related Documents](#), on page v
- [Communications, Services, and Additional Information](#), on page v
- [Field Notice](#), on page v
- [Documentation Feedback](#), on page vi
- [Conventions](#), on page vi

Change History

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

Change	See	Date
Added the URL of the Webex Connect datacenter in Canada.	Integrate Cloud Connect with Webex Connect	07 August, 2023
Updated integration URL with production URL for U2C port 443.	Virtual Agent-Voice	20 July, 2023
Overview of Partial Response included and reference to the article link provided.	Virtual Agent-Voice	26 June, 2023

Change	See	Date
Initial Release of Document for Release 12.6(2)		April, 2023
A new chapter has been added that has information about how to provision and work with digital channels.	Digital Channels Integration using Webex Connect	
The VPN-less Access to Finesse Desktop section that was in the Mobile Agent chapter has been made into a separate chapter with additional details added.	VPN-less Access to Finesse Desktop	
A new chapter has been added that provides information about how to set up and use the Virtual Agent-Voice Call Transcription feature.	Virtual Agent–Voice Call Transcription	
The Virtual Agent-Voice and the Virtual Agent–Voice for Dialogflow CX chapters have been combined into one chapter. This chapter also includes information about cloud-based connectors.	Virtual Agent-Voice	
Cisco IdS now supports an asymmetric key encryption for signing the tokens generated for authentication.	Single Sign-On	
A new appendix has been added. This appendix replaces the Reverse-Proxy Configuration appendix.	Reverse Proxy Automated Installer	
A new appendix has been added that has guidelines for custom reverse proxy deployment.	Guidelines for Custom Reverse Proxy Deployment	

About This Guide

This guide explains features you can use in conjunction with Cisco Unified Contact Center Enterprise. For each feature, there is a description, procedures for initial setup, and details on the functionality the feature provides.

Audience

This guide is prepared for Contact Center administrators who configure and run the contact center, manage agents, and address operational issues.

Related Documents

Subject	Link
Design considerations and guidelines for deploying a Unified CCE solution, including its various components and subsystems.	<i>Solution Design Guide for Cisco Unified Contact Center Enterprise</i> at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.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</i> font	<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: <pre><html><title>Cisco Systems, Inc. </title></html></pre>
< >	<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.



CONTENTS

PREFACE

Preface	iii
Change History	iii
About This Guide	iv
Audience	v
Related Documents	v
Communications, Services, and Additional Information	v
Field Notice	v
Documentation Feedback	vi
Conventions	vi

CHAPTER 1

Agent Answers	1
Introduction	1
Prerequisites	1
Important Considerations	2
Contact Center AI Services Task Flow	3
Contact Center AI Configuration	4
Associate Contact Center AI Configuration with All Call Types	4
View Contact Center AI Configuration	5
Reset Contact Center AI Global Configuration	5
Associate Contact Center AI Configuration with a Call Type	5
View Contact Center AI Configuration	5
Update Associate Contact Center AI Configuration	5
Reset Contact Center AI Configuration	6
Enable or Disable Contact Center AI Services for Agents	6
Enable or Disable Contact Center AI Services for an Agent	6
Enable or Disable Contact Center AI Services for Multiple Agents	6

Enable or Disable AnswersContact Center AI Services for Agents using Bulk Job 7

Create a SIP Profile at the Dial-Peer Level in CUBE 8

Import or Verify WebSocket Connector Certificate to CUBE 8

Reconfigure Agent Answers after Upgrade to Unified CCE 12.6 9

CHAPTER 2

Agent Greeting 11

Capabilities 11

 Agent Greeting Phone Requirements (for Local Agents Only) 11

 Agent Greeting Functional Limitations 12

 Whisper Announcement with Agent Greeting 12

Initial Setup 12

 Configuration Requirements 12

 Deploy Agent Greeting 13

 Agent Greeting Deployment Tasks 13

 Agent Greeting Scripts 25

Reporting 32

 Greeting Call Statistics 32

 Peripheral Call Types for Agent Greeting 32

Serviceability 32

CHAPTER 3

Agent Request 33

Agent Request Feature Description 33

 Agent Request Prerequisites 34

 Agent Request Call Flow 34

 Agent Request Scenarios 35

Configure Unified CCE for Agent Request 36

 Configuration Manager 36

 Configure Network VRU and Network VRU Script 36

 Configure the Media Routing PG and PIM 36

 Configure Call Type 37

 Configure Dialed Number/Script Selector 37

 Configure ECC Variables 37

 Set up the Media Routing PG and PIM 37

Configure Customer Collaboration Platform for a Voice Callback Agent Request 38

Create Feed	38
Create Campaign	39
Create Notification	39
Agent Request Script	40
Create Agent Request Script	41
Use the Sample Code to Create a Customer Callback Request	42
Agent Request Reporting	43

CHAPTER 4
Business Hours 45

Business Hours Overview	45
Business Hours Use Cases	46
Set the Principal AW for Business Hours	46
Business Hours Set Up Workflow	47

CHAPTER 5
Call Transcription 51

Introduction	51
Prerequisites	51
Contact Center AI Services Task Flow	52
Enable or Disable Contact Center AI Services for Agents	53
Enable or Disable Contact Center AI Services for an Agent	53
Enable or Disable Contact Center AI Services for Multiple Agents	53
Enable or Disable AnswersContact Center AI Services for Agents using Bulk Job	54
Bulk Contact Center AI Services Content File	54

CHAPTER 6
Digital Channels Integration Using Webex Connect 57

Overview	57
Prerequisites	57
Redaction of sensitive data	58
Workflow for enabling and managing digital channel interactions	59
Generate public key certificate using Cisco IdS	63
Regenerate public key certificate using Cisco IdS	63
Reverse proxy configuration for digital channel interaction	64
Reverse proxy deployment model	64
Workflow to configure reverse proxy using automated installer	65

- Add Proxy IP 66
- Configure reverse proxy host verification 67
- Custom reverse proxy configuration 68
- ECC Variables for Digital Routing Tasks 68
- Manage digital channels 70
 - Set up media channels 71
 - Configure queue settings 72
 - Synchronize CCE agents to Webex Engage 73
 - Important considerations for agent synchronization 73
 - Enable agents for digital channels 74
 - Configure SQL user account for digital channels 74
 - Configure User Sync 74
 - Define ECC variables 77
 - Integrate Cloud Connect with Webex Connect 77
 - Manage connection between Cloud Connect and MR PG 78
- Disposition codes for digital channel interaction 79
- Agent Request or Web Callback using Webex Connect 84
 - Configure Web Callback 85
- Reporting 88
 - Webex Connect reporting 88
 - Digital Routing reporting 88

CHAPTER 7

- Call Transcript 91**
 - Feature Overview 91
 - Capabilities 91
 - Getting Started 91
 - Prerequisites 92
 - Configuration Task Flow 92
 - Documentation Resources 92

CHAPTER 8

- Contact Sharing 95**
 - Contact Sharing Overview 95
 - Contact Sharing Call Flow 96
 - Failover for Contact Sharing 97

Contact Director Installation and Setup	97
Install Unified CCE	98
Application Gateway Access Between Systems	99
Install Cisco Unified Intelligence Center (Optional)	102
Install Unified CVP	102
Set Up Contact Sharing	102
Set Up a Contact Sharing Node	102
Set up Contact Sharing Machine Inventory	103
Add and Maintain Rules	104
Add a New Rule by Copying an Existing Rule	104
Add and Maintain Groups	105
Scripting for Contact Sharing	106
Expression Formula for Contact Sharing	106
About Contact Sharing Expression Formula	106
Contact Sharing Expression Format	106
Contact Sharing Expression Examples	106
Contact Sharing Expression Reference	108
Routing and Scripting for Contact Sharing	111
Error Handling for Contact Sharing	112
Other Scripting Considerations	112
<hr/>	
CHAPTER 9	Mobile Agent 115
Mobile Agent	115
Capabilities	115
Cisco Unified Mobile Agent Description	115
Feature Requirements	120
Supported Unified CCE Features	121
Important Considerations	122
Unified Mobile Agent Call Flows	124
Unified Mobile Agent Reporting	130
Initial Setup	130
Summary of Unified Mobile Agent System Configuration Tasks	130
Unified CM CTI Port Configuration and Mapping for Unified Mobile Agent	131
Maximum Call Duration Timer Configuration	134

- Agent Desk Setting Configuration for Unified Mobile Agent 134
- Device Configuration for Unified Mobile Agent 135
- Media Termination Points Configuration 135
- Enabled Connect Tone Feature 139
- Enable Mobile Agent Connect Tone 139
- Administration and Usage 140
 - Cisco Finesse 140
 - Serviceability 142

CHAPTER 10

Post Call Survey 145

- Post Call Survey 145
 - Post Call Survey Use Case 145
 - Post Call Survey Design Impacts 145
- Configure Post Call Survey in CVP 146
- Configure Unified CCE 146
 - Configure ECC Variable 146

CHAPTER 11

Precision Queue 149

- Capabilities 149
 - Precision Queues 149
 - Skill Groups or Precision Queues? 150
 - Attributes 151
 - Precision Queue Call Flow Example 152
 - Scripts for Precision Queues 152
 - Precision Queue Script Node 153
 - Queuing Behavior of the Precision Queue Node 153
 - Dynamic Limits for Skill Groups and Precision Queues Per Agent 154
- Initial Setup 155
 - Add Attributes 155
 - Search for Agents 156
 - Assign Attributes to Agents 156
 - Add Precision Queue 157
 - Consider If Formula for Precision Queue 159
 - Build Precision Queue Steps 159

- Configure a Static Precision Queue 161
- Configure a Dynamic Precision Queue 162

CHAPTER 12**Single Sign-On 163**

- Single Sign-On 163
 - Contact Center Enterprise Reference Design Support for Single Sign-On 164
 - Coresidency of Cisco Identity Service by Reference Design 165
 - Single Sign-On Support and Limitations 165
- Single Sign-On Configuration Flow 166
- Configure an Identity Provider (IdP) 166
 - Install and Configure Active Directory Federation Services 167
 - Authentication Types 167
 - Integrate Cisco IdS with AD FS 167
 - Enable Signed SAML Assertions 171
 - Multi-Domain Configuration for Federated ADFS 171
 - Federated ADFS Configuration 172
 - Primary ADFS Configuration 172
 - Kerberos Authentication (Integrated Windows Authentication) 172
 - Optionally Customize the AD FS Sign-In Page in Windows Server to Allow User ID 172
- Set the Principal AW for Single Sign On 174
- Set Up the System Inventory for Single Sign-On 174
- Configure the Cisco Identity Service 175
 - Install Certification Authority (CA) Certificate 177
- Register Components and Set Single Sign-On Mode 178
- Hostname or IP Address Change 179
- Single Sign-On and the Agent Tool 179
- Migration Considerations Before Enabling Single Sign-On 179
 - Administrator User and Single Sign-On in Unified Intelligence Center 179
 - Browser Settings and Single Sign-On 180
- Migrate Agents and Supervisors to Single Sign-On Accounts 181
- Allowed Operations by Node Type 182
- Configure SAML Certificate Secure Hash Algorithm from SHA-1 to SHA-256 183
- Access Public Key Signing Certificate 183
- Single Sign-On Log Out 184

CHAPTER 13

Task Routing 185

- Task Routing **185**
 - Task Routing Deployment Requirements **187**
 - Supported Functionality for Third-Party Multichannel Tasks **187**
 - Plan Task Routing Media Routing Domains **188**
 - Plan Dialed Numbers **191**
 - Skill Group and Precision Queue Routing for Nonvoice Tasks **192**
 - Agent State and Agent Mode **192**
 - Customer Collaboration Platform and Finesse Task States **193**
- Control SocialMiner Application Access **194**
 - utils whitelist admin_ui list **194**
 - utils whitelist admin_ui add **195**
 - utils whitelist admin_ui delete **195**
- Task Routing API Request Flows **196**
 - Task Routing API Basic Task Flow **196**
 - Task Routing API Agent Transfer Flow **200**
 - Task Routing API RONA Flow **200**
 - Task Routing API Agent Sign Out with Tasks Flows **201**
- Failover and Failure Recovery **203**
- Task Routing Setup **206**
 - Initial Setup **206**
 - Configure Finesse with the AW **208**
 - Configure Network VRU and Network VRU Scripts **209**
 - Configure the Media Routing PG and PIM **209**
 - Set up the Media Routing PG and PIM **210**
 - Add Customer Collaboration Platform as an External Machine **210**
 - Unified CCE Administration and Configuration Manager Tools **211**
 - Increase TCDTimeout Value **213**
 - Create Routing Scripts for Task Routing **213**
- Sample Code for Task Routing **213**
 - Sample Customer Collaboration Platform HTML Task Application **214**
 - Sample Finesse Code for Task Routing **214**
- Task Routing Reporting **215**

CHAPTER 14	Unified Communications Manager Extension Mobility	217
	Capabilities	217
	Configuration	218

CHAPTER 15	Virtual Agent–Voice	219
	Feature Overview	219
	Onboarding Experience	220
	VAV via Cloud-Based Connector	220
	Overview	220
	Important Considerations	221
	Prerequisites	222
	Configuration Task Flow	224
	Hybrid IVR with VAV via Cloud-Based Connector	224
	Configure Hybrid IVR	225
	VAV via Premise-Based Connector	226
	Documentation Resources	237
	Regional Media Data Center Region Mapping	238

CHAPTER 16	Virtual Agent–Voice Call Transcription	243
	VAV Transcript Overview	243
	Prerequisites	244
	Configuration Task Flow	244

CHAPTER 17	VPN-less Access to Finesse Desktop	247
	VPN-less access to Finesse desktop	247
	Prerequisites	247
	Supported Reverse-Proxy Deployment Models	248
	Load balancer, WAF, and proxy support for reverse-proxy deployments	249
	Authentication	252
	Host-Mapping file for network translation	255
	DNS Configuration for Finesse, IdS, and CUIC servers	257
	Reverse-Proxy selection and configurations	258
	Performance and Hardware Recommendations	258

- Determine Scale and Hardware for Proxy 258
- Determine Gadget Compatibility 259
- Finesse URL 261
- VPN-less Finesse configurations 261
 - Populate Network Translation Data 262
 - Host the Mapping File 264
 - Add Proxy IP by Using CLI 265
 - Configure Reverse-Proxy Host Verification 266
 - Configure Proxy Mapping by Using CLI 267
 - Configure CORS and Frame-Ancestors 268
 - Configure SSO 268
- Serviceability 269
 - Monitor Connected Agents and Supervisors 269
 - API Modifications to Support Reverse-Proxy Deployments 270
- HTTP Return codes returned by the reverse-proxy 270
- Historical and Real Time Gadgets 271
- Security Guidelines 272
- Caveats 272

CHAPTER 18

- Webex Experience Management Integration 275**
 - Experience Management Overview 275
 - Experience Management Voice Survey 276
 - Experience Management Task Flow 276
 - Provision Experience Management Service on Cloud Connect 278
 - Configuration Changes in Webex Experience Management 278
 - Configure Unified CCE for Experience Management Voice, SMS and Email Survey 279
 - Configure Expanded Call Variables 279
 - Configure POD.ID 280
 - Upload Audio Files for Questions in Experience Management 281
 - Configure Dialed Number and Call Type 281
 - Associate Survey to Call Type in Unified CCE Admin 282

CHAPTER 19

- Webex Experience Management Digital Channel Survey 283**
 - Overview 283

Digital Channel Survey	283
Digital Channel Survey Task Flow (Email/Chat)	284
Provision Cloud Connect for Digital Channel Survey	285
Configure Unified CCE for Digital Channel Survey	285
Configure Expanded Call Variables	285
Configure POD.ID	286
Configure Call Type, Dialed Number, and Survey Association	287
Associate Survey to Call Type in Unified CCE Admin	287
<hr/>	
CHAPTER 20	Whisper Announcement 289
Capabilities	289
Functional Limitations	289
Deployment Tasks	290
Create Whisper Announcement Audio Files	290
Deploy Whisper Announcement Audio Files to Media Server	291
Using a Default Media Server	291
Configure Whisper Service Dialed Numbers	291
Configure Dialed Numbers	292
Configure Ringtone Dialed Number	292
Add Whisper Announcement to Routing Scripts	292
Specify WhisperAnnouncement Call Variable	293
Specify Unified CVP Media Server Information	293
Test Whisper Announcement File Path	295
Other Script Settings That Are Required for Whisper Announcement	295
Fail-Safe Timeout for Whisper Announcement in Unified CCE	295
Whisper Announcement Sample Scripts	296
WA.ICMS Script	296
WA_AG.ICMS Script	296
Import Sample Whisper Announcement Scripts	297
How Whisper Announcement Works	297
Whisper Announcement Audio File	297
While a Whisper Announcement Is Playing	297
Whisper Announcement with Transfers and Conference Calls	298
Whisper Announcement Call Flow	298

Reporting and Serviceability 299

APPENDIX A

Reverse Proxy Automated Installer 301

Introduction 301

Prerequisites 301

Requirements 301

Components Used 302

Background Information 302

Reverse-Proxy Installer 303

Upgrade notes for 12.6(1) ES01-7 based reverse proxy configurations 306

Install and Operations 306

Setup reverse-proxy 306

Proxy Hardware requirements 307

Prepare Host 307

Install the reverse proxy Installer package 308

Configure Host OS 308

Configure proxy hardware resources and other critical runtime options 309

Configure SSL certificates 309

Configure the Mapping File 313

Configure deployment environment configurations 315

Starting the reverse-proxy 318

Serviceability 319

Bootstrap checks or validations 319

Launcher logs 320

Access and error logs 321

IP blocking logs 321

Syslogs 321

Reloading configuration and clearing cache 322

Static file hosting 322

Reverse-proxy caching 322

Use configurations with custom NGINX installation 323

Upstream component configuration specifics 324

Verifying Reverse-Proxy Configuration 324

Finesse 324

Cisco Unified Intelligence Center and LiveData	324
Cisco Identity Service	324
Security	325
Authentication	325
Validating unauthenticated static resources	326
Brute Force attack prevention	326
Attack Detection Parameters	326
Logging	327
Caching CORS headers	327
Install and configure Fail2ban	327
Frequently Asked Questions	329
Environment Files	329
Installer env properties	330
Core properties	335
Directory (DIR) properties	347
Common Properties	348
Common SSL-Related Properties	348
Cisco Finesse Properties	351
<hr/>	
APPENDIX B	Guidelines for Custom Reverse Proxy Deployment
	375
Reverse proxy selection and configuration for digital channel interactions	375
Minimum and additional requirements	375
Configure custom reverse proxy	376
Host header configuration	376
Reverse proxy selection and configuration for VPN-less access to Finesse Desktop	377
Minimum and additional requirements	377
Configure Reverse-Proxy	379
Host Header Configuration	379



CHAPTER 1

Agent Answers

- [Introduction, on page 1](#)
- [Prerequisites, on page 1](#)
- [Important Considerations, on page 2](#)
- [Contact Center AI Services Task Flow, on page 3](#)
- [Contact Center AI Configuration, on page 4](#)
- [Create a SIP Profile at the Dial-Peer Level in CUBE, on page 8](#)
- [Import or Verify WebSocket Connector Certificate to CUBE, on page 8](#)
- [Reconfigure Agent Answers after Upgrade to Unified CCE 12.6, on page 9](#)

Introduction

Unified CCE leverages Artificial Intelligence (AI) and Natural Language Understanding (NLU) to provide services that assist agents. These services are available for the agents in the Cisco Finesse desktop gadgets.

Agent Answers feature provides relevant suggestions and recommendations in real time for the agent to consider. The suggestions and recommendations are based on the ongoing conversation between the caller and the agent.

More often than not, agents lack the depth of knowledge about the products and services of the business they serve. Agent Answers enhances the customer experience because the timely suggestions improve the ability of the agent to respond. Businesses can cut down on training costs and time.

Prerequisites

The prerequisites for configuring Agent Answers are:

- Ensure Agent Answers is configured on a supported CUBE platform. For more details on supported CUBE platforms and configuration, see the *WebSocket-Based Media Forking for Cloud Speech Services* chapter in the *Cisco Unified Border Element Configuration Guide - Cisco IOS XE 17.6 Onwards* at <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/websocket-forking-for-cube.html>.
- The following components must be on release 12.6(2): CCE components (Router, Logger, PG, and AW), Cisco Finesse, Cisco Unified CVP, and Cloud Connect.

- Ensure that your Unified ICM AW server has 443/8443 ports opened and is able to access the following websites:
 - *.wbx2.com
 - *.ciscoocservice.com
- Ensure that CUBE has access to the following websites:
 - *.cisco.com
 - *.ciscopark.com
 - *.rtmsprod.net
 - *.wbx2.com
- Ensure that Unified CCE AW, Unified CCE OAMP, Cloud Connect, CUBE, and Agent Desktop components have access to Webex services to use the Agent Answers.

Important Considerations

Consider the following before configuring the Agent Answers services:

- Agent Answers services are supported on calls that originate from CVP routing clients. Calls originating from routing clients other than CVP or calls that are sent using the translation route to CVP do not support the Agent Answers services.
- The following failover scenarios don't support Agent Answers services:
 - CCE components running in maintenance modes switch to the peer side, passing the call context to the other side. If the call context (required to trigger the Agent Answers services) is lost, Agent Answers services may not work as expected.
 - Agent Answers services is supported during VRU PG failovers before and after the transfer. However, Agent Answers services aren't supported when the transfer is in progress.
 - Agent Answers services aren't supported during Agent PG failovers.
- Agent Answers services aren't supported in the following call scenarios:
 - Direct Extension calls
 - Outbound campaign calls and agent-initiated outbound calls.
 - Calls routed to agents on non-CUCM Peripheral Gateways such as the TDM PG and System PG
 - Transfer and conference calls
- Agent Answers services are supported only with G.711 μ law.
- A CUBE instance can support either WebSocket-based forking or Network-based Recording (NBR) forking. However, you cannot enable both types of forking on the same instance of CUBE.

Contact Center AI Services Task Flow

- Step 1** Create a CCAI configuration in Cisco Webex Control Hub at <https://admin.webex.com>. A CCAI configuration leverages CCAI Connectors to invoke the CCAI services.
For details, see the [Create a Contact Center AI Configuration](#) article.
- Step 2** Ensure that the Cloud Connect publisher and subscriber are installed.
For more information, see the *Install Cloud Connect* section in *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html>.
- Step 3** Configure Cloud Connect in the CVP Operations Console (OAMP). For details see the section *Configure CVP Devices for Cloud Connect* in the *Administration 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>.
- Step 4** Register Cloud Connect in the Unified CCE Administration console to establish a secure and trusted communication channel between the Cisco Contact Center on-premises deployment and cloud services.
For details, see the *Cloud Connect Integration* section in the *Administration Guide for Cisco Unified Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-maintenance-guides-list.html>.
- Step 5** Import the Cloud Connect certificate to the CVP Server.
For details, see the section *Import Cloud Connect Certificate to Unified CVP Keystore* in the *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>.
- Step 6** In the Unified CCE Administration console, do the following with the CCAI configuration (created in step 1):
a) To view and sync the Contact Center AI configuration which is associated with all call types as a global configuration.
b) To view, update, or delete the Contact Center AI configuration associated with a specific call type.
- Step 7** Provision Cloud Connect on Cisco Finesse.
For more information, see the *Cloud Connect Server Settings* topic in the *Cisco Finesse Administration Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html>.
- Step 8** Do the following in the Cisco Finesse Administration console.
- To enable CCAI services in Cisco Finesse, see the *AI Services Configuration* section in the *Cisco Finesse Administration Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html>.
 - To add the Agent Answers gadget to the Cisco Finesse desktop layout, see the *Contact Center AI Gadgets* section in the *Cisco Finesse Administration Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html>.

Once enabled, the Agent Answers gadget appears on the Home tab and displays relevant articles and suggestions during an incoming call. For details on how to use the gadget, see the *Contact Center AI Gadgets Guide*.

Note Gadget auto-hide/un-hide and notifications capability is available only if the gadget is configured as a multi-tab gadget in Cisco Finesse. For more details, see *Configure Multi-Tab Gadget Layout* section in the *Cisco Finesse Administration Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html>.

Step 9 To add the Agent Answers gadget to the Cisco Finesse desktop layout:

a) Enable the Agent Answers gadget in Cisco Finesse Administration.

For details, see the *Manage Desktop Layout* section in the [Cisco Finesse Administration Guide](#).

b) Enable the Agent Answers service in Unified CCE Administration for an agent or multiple agents together.

Once enabled, the Agent Answers gadget appears on the Home tab and displays relevant articles and suggestions during an incoming call. For details on how to use the gadget, see the *Contact Center AI Gadgets User Guide for Cisco Contact Center Enterprise*.

Note Gadget auto-hide/un-hide and notifications capability is available only if the gadget is configured as a multi-tab gadget in Cisco Finesse. For more details, see *Configure Multi-Tab Gadget Layout* section in the *Cisco Finesse Administration Guide*.

Step 10 Perform the following steps to configure WebSocket-based forking in CUBE.

a) Create a SIP profile and associate it at the dial-peer level in CUBE. For details, see *Importing Cube Certificate*.

b) Import the WebSocket Connector certificate to CUBE. For details, see *Importing Cube Certificate*.

c) Configure WebSocket-based forking in CUBE. For details, see the *WebSocket-Based Media Forking for Cloud Speech Services* chapter in the *Cisco Unified Border Element Configuration Guide - Cisco IOS XE 17.6 Onwards*.

CUBE uses a WebSocket connection to fork the media streams of the agent and the caller towards the Webex CCAI Orchestrator service. For more details, see the Contact Center AI Services Considerations section in the *Solution Design Guide for Cisco Unified Contact Center Enterprise*.

Step 11 To use the regionalised media support, see the [Regional Media Data Center Region Mapping, on page 238](#) section.

Contact Center AI Configuration

In the Unified CCE Administration console, the Contact Center AI (CCAI) feature tab allows administrators to associate the CCAI configuration (created in the Control Hub at <https://admin.webex.com/>) with all the call types (global configuration) or with a specific call type. Upon associating a CCAI configuration with the call type, the global configuration (if any) gets overridden for the specific call type.



Note To access this feature, add Cloud Connect to the inventory and register it in the Unified CCE Administration console.

Associate Contact Center AI Configuration with All Call Types

You can view, update, or reset the Contact Center AI configuration, which is associated with all call types.

View Contact Center AI Configuration

In the **Unified CCE Administration**, navigate to **Overview > Features > Contact Center AI**. The **Contact Center AI Configuration** search box displays the name of the CCAI configuration that was previously associated with all call types.

Reset Contact Center AI Global Configuration

This procedure explains how to reset the Contact Center AI configuration. Upon reset, the previously associated configuration is cleared from the search box.

-
- Step 1** In the **Unified CCE Administration**, navigate to **Overview > Features > Contact Center AI**.
 - Step 2** In the **Contact Center AI Configuration** search box, next to the configuration name, click the **x** icon.
 - Step 3** Click **Save**.
-

Associate Contact Center AI Configuration with a Call Type

You can view, update, or delete the Contact Center AI configuration associated with a specific call type.

View Contact Center AI Configuration

In the **Unified CCE Administration**, navigate to **Overview > Call Settings > Route Settings > Call Type**. The **Contact Center AI Configuration** search box displays the name of the CCAI configuration that was previously associated with the call type.

Update Associate Contact Center AI Configuration

You can create a Call Type using the **Configuration Manager** tool. However, you can use the **Unified CCE Administration** to associate a Contact Center AI configuration with a call type. This procedure explains how to update the Contact Center AI configuration associated with a call type.



Note Only one configuration can be associated with a call type.

-
- Step 1** In the **Unified CCE Administration**, navigate to **Overview > Call Settings > Route Settings**.
 - Step 2** Click the **Call Type** tab and select the call type for which Contact Center AI configuration has to be associated.
 - Step 3** Click the **Contact Center AI** tab.
 - Step 4** In the **Contact Center AI Configuration** search box, click the search icon. A pop-up window displays a list of CCAI configurations.
 - Step 5** Select the required configuration and click **Save**.
-

Reset Contact Center AI Configuration

This procedure explains how to reset the Contact Center AI configuration. Upon reset, the previously associated configuration with the call type is cleared from the search box.

-
- Step 1** In the **Unified CCE Administration**, navigate to **Overview > Call Settings > Route Settings**.
- Step 2** Click the **Call Type** tab.
- Step 3** In the **Contact Center AI Configuration** search box, next to the configuration name, click the **x** icon.
- Step 4** Click **Save**.
-

Enable or Disable Contact Center AI Services for Agents

Contact Center AI Services can be configured for each agent. Administrators and supervisors can enable or disable the services for an agent or multiple agents together.

Enable or Disable Contact Center AI Services for an Agent

This procedure explains how to enable or disable Contact Center AI Services for an agent.

-
- Step 1** In **Unified CCE Administration**, choose **Users > Agents**.
- Step 2** Click on the agent row whose services are to be modified.
- Step 3** Click the **Contact Center AI** tab.
Displays a list of services enabled or disabled for the agent.
- Step 4** To enable or disable the required Contact Center AI Services, check or uncheck the check boxes corresponding to the services.
- Step 5** Click **Save**.
-

Enable or Disable Contact Center AI Services for Multiple Agents

Administrators and supervisors can enable or disable Contact Center AI Services for multiple agents.

All agents must belong to the same site and the same department, or all agents must be global agents. The **Edit** button is disabled if:

- Agents from different sites, departments, or peripheral sets are selected.
- A mix of global and departmental agents are selected.

-
- Step 1** In **Unified CCE Administration**, choose **Users > Agents**.
- Step 2** Check the check box corresponding to each agent whose services you want to edit.
- Step 3** Click **Edit > Contact Center AI**.
The Edit Services dialog displays a list of services that are the service that is enabled or disabled.
- If the service is enabled for all the agents selected for editing, the check box is checked.

- If the service is disabled for all the agents selected for editing, the check box is unchecked.
- If the service is enabled for some agents and disabled for the others, the check box has a dash (—).

Step 4 To enable or disable the Contact Center AI Services, check or uncheck the check boxes corresponding to the services.

Step 5 Click **Save**, and then click **Yes** to confirm the changes.

Enable or Disable AnswersContact Center AI Services for Agents using Bulk Job

Step 1 Navigate to **Unified CCE Administration > Overview > Bulk Import**.

Step 2 Click **Templates**.

The **Download Templates** popup window opens.

Step 3 Click the **Download** icon for the Contact Center AI template you want to use.

Step 4 Click **OK** to close the **Download Templates** popup window.

Step 5 Open the `.csv` template in Microsoft Excel.

Step 6 Populate the file as described in the [Bulk Contact Center AI Services Content File, on page 7](#).

Step 7 Save the populated file to the local machine.

Step 8 Navigate to **Unified CCE Administration > Overview > Bulk Import**.

Step 9 Click **New**.

Step 10 In the optional **Description** field, enter up to 255 characters to describe the bulk job.

Step 11 In the **Content file** field, choose the file to upload, and then click **Save**.

Bulk Contact Center AI Services Content File

The content file for Contact Center AI bulk job contains the fields given in the following table. Enter the values appropriately in the given fields to enable or disable Contact Center AI Services for the agents.



Note Bulk job is available for administrators only when Cloud Connect is added in the inventory and registered on the Control Hub.

Field	Required?	Description
agentId	Agent ID or Username	Existing agentId for which you want to enable or disable the Contact Center AI Services. You must provide either an agentId or the userName. If both are provided, agentId takes precedence over the userName. If the agentId value is left blank, the userName will reference an existing agent.

Field	Required?	Description
userName	Username or Agent ID	Username of the agent for which you want to enable or disable the Contact Center AI Services. If no agent is found with the given username, the Contact Center AI Services association fails.
agentServices	Yes (to enable Contact Center AI Services)	The type of Contact Center AI Services to be associated with the agent. Supported values are AgentAnswers and Transcript. To associate more than one services, separate the values using semicolon (;). If the value is updated, any existing enabled service gets overwritten. If the value is left empty, no service gets associated with the agent.

Create a SIP Profile at the Dial-Peer Level in CUBE

Run the following CLI commands on the CUBE terminal to create a SIP profile and associate that profile at the dial-peer level. These commands add a SIP header to the SIP profile configuration, allowing CVP to identify which CUBE device can receive the forking request.

```
voice class sip-profiles <SIP-profile-identifier-a>
request INVITE sip-header Call-Info add "X-Cisco-Forking: supported"
dial-peer voice <SIP-profile-identifier-b> voip
voice-class sip profiles <SIP-profile-identifier-a>
```

Example:

```
voice class sip-profiles 104
request INVITE sip-header Call-Info add "X-Cisco-Forking: supported"
dial-peer voice 4445 voip
voice-class sip profiles 104
```

Import or Verify WebSocket Connector Certificate to CUBE

By default, the trust pool bundle includes the **IdenTrust Commercial** certificate. This certificate is required for validating the **WSConnector** certificate during the TLS connection establishment of the **WebSocket Connector**.

Step 1 Run the command to verify if the certificate is included.

```
show crypto pki trustpool | include IdenTrust
cn=IdenTrust Commercial Root CA 1
o=IdenTrust Inc
```

```
cn=IdenTrust Commercial Root CA 1
o=IdenTrust Inc
```

Step 2 If **IdenTrust** certificates are not present, add the certificates to CUBE.

- Open the following URL <https://www.cisco.com/security/pki/>.
- Locate the **Cisco Trusted Core Root Bundle** under the **Trusted Root Stores**.
- Select the **Cisco Trusted Core Root Bundle**, right click, and then select **Copy link**. The URL for the bundle is copied to your clipboard.
- Run the following command in CUBE terminal:

```
CUBE# configure terminal
CUBE(config)# crypto pki trustpool import clean URL <URL copied in step 2(c)>
```

Example:

```
CUBE(config)# crypto pki trustpool import clean URL
http://www.cisco.com/security/pki/trs/ios_core.p7b
```

Output

```
Reading file from http://www.cisco.com/security/pki/trs/ios_core.p7b
Loading http://www.cisco.com/security/pki/trs/ios_core.p7b
% PEM files import succeeded.
```

The **IdenTrust** certificates are added to CUBE. To verify the addition, run the following command **show crypto pki trustpool | include IdenTrust**. The output will display the **IdenTrust** certificates as shown in Step 1.

Reconfigure Agent Answers after Upgrade to Unified CCE 12.6

Before you begin

In Unified CCE 12.6, the CCAI services include the following enhanced capabilities when compared to 12.5:

- Reporting:** The Agent Answers Analytics report compares an agent's handle time when the Agent Answers service was enabled vs. when the service was disabled. The report helps you understand the impact of the Agent Answers services on an agent's performance.
- Transfers and Conference Calls Support:** The Agent Answers and Call Transcript services continue during call transfers or call conferences.
- Enable the CCAI Configuration for Specific Call Types:** The CCAI Configuration can be enabled for all or specific call types.
- Enable the CCAI Services for Specific Agents:** The CCAI Services can be configured for each agent. Administrators and supervisors can enable or disable the services for an agent or multiple agents.

If you used the CCAI Services on Unified CCE 12.5, you've already completed most of the configurations that are required for the Agent Answers and Call Transcript services to work in Unified CCE 12.6. No changes are required to the existing Google CCAI, CUBE, or Cloud Connect configurations.

While configuring the CCAI services in Unified CCE 12.5, you enabled Cisco Finesse 12.6 to display the CCAI gadgets to all the agents by running the `enableCustomAgentServices` CLI command.

Once you complete the agent configurations (at Step 3 in the following procedure) and run the `enableCustomAgentServices` CLI command to disable the gadgets for all the agents (at Step 4), Cisco Finesse relies on agent-specific configuration in Unified CCE Administration to display the gadgets.

Follow these steps to complete the CCAI configuration in Unified CCE 12.6 and leverage the enhanced capabilities listed above:

-
- Step 1** In Control Hub, set a CCAI configuration as the default configuration for all calls. For more details, see Step 7a at <https://help.webex.com/en-us/npbt02j/Configure-Contact-Center-AI>.
- Step 2** In the Unified CCE Administration console, do one of the following:
- To view and sync the Contact Center AI configuration that is associated with all call types as a global configuration, see [Associate Contact Center AI Configuration with All Call Types, on page 4](#).
 - To view, update, or delete the Contact Center AI configuration that is associated with a specific call type, see [Associate Contact Center AI Configuration with a Call Type, on page 5](#).
- Step 3** In the Unified CCE Administration console, enable or disable CCAI Services for an agent or multiple agents. For more details, see [Enable or Disable Contact Center AI Services for Agents, on page 6](#).
- Step 4** Undo these CCAI settings configured when Unified CCE was in 12.5:
- Delete the "call.user.configid" ECC variable you created for the Answers feature and remove the association of this variable with the CCE script.

For more details, see the *Contact Center AI Services Task Flow* section in the *Cisco Unified Contact Center Enterprise Features Guide, Release 12.5* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html>.
 - In Cisco Finesse, run the following CLI command to disable the CCAI services from all the Cisco Finesse clusters:

```
utils finesse set_property webservices enableCustomAgentServices false
```


For more details, see the *AI Services Configuration* topic in the *Cisco Finesse Administration Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html>.
-



CHAPTER 2

Agent Greeting

- [Capabilities, on page 11](#)
- [Initial Setup, on page 12](#)
- [Reporting, on page 32](#)
- [Serviceability, on page 32](#)

Capabilities

The Agent Greeting feature lets an agent record a message that plays automatically to callers when they connect to the agent. The greeting message can welcome the caller, identify the agent, and include other useful contextual information. With Agent Greeting, each caller can receive a clear, well-paced, language-appropriate, and enthusiastic introduction. Another benefit is that it saves the agent from having to repeat the same introductory phrase for each call. It also gives the agent a moment to review the desktop software screen popups while the greeting plays.

The process of recording a greeting is much the same as recording a message for voicemail. Depending on how the call center is set up, agents may be able to record different greetings that play for different types of callers. For example, agents can record an English greeting for English speakers or an Italian greeting for Italian speakers.

Agent Greeting Phone Requirements (for Local Agents Only)

Agent Greeting is available to agents and supervisors who use IP Phones with Built-In Bridge (BIB). These agents are typically located within a contact center. Phones used with Agent Greeting must meet these requirements:

- The phones must have the BIB feature.



Note If you disable BIB, the system attempts to use a conference bridge for Agent Greeting call flow and raises a warning event.

- In an IPv6-enabled environment, Agent Greeting may require extra Media Termination Points (MTPs).

See the *Contact Center Enterprise Compatibility Matrix* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html> for the list of supported Cisco Unified Call Center phone models.

Agent Greeting Functional Limitations

Agent Greeting is subject to these limitations.

- Agent Greeting does not support outbound calls made by an agent. The announcement plays for inbound calls only.
- Only one Agent Greeting file plays per call.
- Supervisors cannot listen to agent recorded greetings.
- Agent Greetings do not play when the router selects the agent through a label node.
- Agent Greeting supports Unified CM based Silent Monitoring with this exception: Supervisors cannot hear the greetings themselves. If a supervisor tries to start a silent monitoring session while a greeting is playing, a message displays stating that a greeting is playing and to try again shortly.

Whisper Announcement with Agent Greeting

You can use Agent Greeting with the Whisper Announcement feature. Here are some things to consider when using them together:

- On the call, the Whisper Announcement always plays first.
- To shorten your call-handling time, use shorter Whisper Announcements and Agent Greetings than if you were using either feature by itself. A long Whisper Announcement followed by a long Agent Greeting equals a long wait before an agent actively handles a call.
- If you use a Whisper Announcement, your agents probably handle different types of calls: for example, “English-Gold Member-Activate Card,” “English-Gold Member-Report Lost Card,” “English-Platinum Member-Account Inquiry.” Therefore, you may want to ensure that greetings your agents record are generic enough to cover the range of call types.

For more information about Whisper Announcement, see [Whisper Announcement, on page 289](#)

Initial Setup

This section is intended for system administrators responsible for installing and configuring Unified CCE. It describes the one-time tasks required to set up Agent Greeting.

Configuration Requirements

The following configuration components must be in place to deploy Agent Greeting.

Where	What
Unified Communications Manager	For phones that use Agent Greeting, you must set the Built-in-Bridge option to On or De Administration, select Device > Phone > Built in Bridge .
Unified CCE	<p>Agent Greeting is supported with Type 10 Network VRUs only. (Type 10 is required to al is not configured for a Type 10 VRU, you must modify it accordingly.</p> <p>Agent Greeting requires at minimum three expanded call variables.</p> <ul style="list-style-type: none"> • <code>user.microapp.ToExtVXML</code>: This is used twice in an Agent Greeting record script: application; the second time is to tell the recording application where to save greetin • <code>user.microapp.app_media_lib</code>: This is required in Agent Greeting record and play scr greeting audio files are stored. Maximum Length - 100 and Enabled. • <code>user.microapp.input_type</code>: This is required in Agent Greeting record scripts to limit th <p>No other ECC (Expanded Call Variable) are needed if you serve your files from the Unif default locale directory ("<code><web_server_root>\en-us\app</code>"). However, if you store your fil the ECC in the next row in your scripts.</p>
Unified CCE (optional variables, used to override defaults)	<p>To make these variables available to your script authors, confirm that they are defined in ECC variables for CVP, see the <i>Administration Guide for Cisco Unified Customer Voice Po</i> unified-customer-voice-portal/tsd-products-support-series-home.html.</p> <ul style="list-style-type: none"> • <code>user.microapp.media_server</code>: Use to identify the Unified CVP media server if it is o • <code>user.microapp.locale</code>: Use to specify the name of the locale directory on the media s • <code>user.microapp.UseVXMLParams</code>: Required in your record script if you include the recording script to use the name/value pair of the application that you pass in the us
Unified CVP	Unified CVP Server must be installed and configured, as described in the <i>Cisco Unified</i> https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-en

Deploy Agent Greeting

Agent Greeting Deployment Tasks

-
- Step 1** Ensure that your system meets the baseline requirements for software, hardware, and configuration described in the System Requirements and Limitations section.
- Step 2** Configure one or more servers to act as media servers. Configuration requirements include IIS and FTP.
- Step 3** In Unified CVP, add media servers, configure FTP connection information, and deploy the media servers.
- Step 4** Configure a Unified CVP media server, if you have not already done so. See [Configure Media Server for Agent Greeting, on page 14](#).
- Step 5** In Unified CVP, republish the VXML Gateway.tcl scripts with updated Agent Greeting support. See [Republish the tcl scripts to VXML Gateway, on page 18](#) for Agent Greeting support.

- Step 6** Set the cache size on the VXML Gateway. See [Set Cache Size on VXML Gateway, on page 18](#).
- Step 7** Record the voice prompts to play to agents when they record a greeting and to deploy the audio files to your media server. See [Create Voice Prompts for Recording Greetings, on page 18](#).
- Step 8** Configure call types to record and play agent greetings. See [Configure Call Types, on page 19](#).
- Step 9** Configure dialed numbers to record and play agent greetings. See [Configure Dialed Numbers, on page 20](#).
- Step 10** [Schedule the Script, on page 20](#).
- Step 11** [Define Network VRU Scripts for Agent Greeting, on page 20](#).
- Step 12** In Script Editor:
- To use the installed scripts to record and play agent greetings, see [Import Example Agent Greeting Scripts, on page 22](#).
 - To create your own scripts, see [Agent Greeting Scripts, on page 25](#).
- Step 13** [Modify the Unified CCE call routing scripts to use Play Agent Greeting script, on page 23](#).
-

Configure Media Server for Agent Greeting

Agent Greeting uses the Unified CVP media server. If you previously configured and deployed one or more Unified CVP media servers for other features, you do not have to configure any additional servers for Agent Greeting. You can optionally add additional media servers.

Agent Greeting uses the Unified CVP media server to store and serve the following types of files:

- Prompt files, prepared by Administrators. These files supply the prompts that agents hear when they record their greetings. The Administrator must manually add the prompt files to all the media servers that their Agent Greeting scripts will query to retrieve those files.
- Greeting files, recorded by agents. These files are the actual greetings that play to callers. They are recorded by individual agents. The system handles the storage of these files as follows:
 - A greeting file is named using the convention *PersonID_AgentGreetingType*. For more about *AgentGreetingType*, see [Specify AgentGreetingType Call Variable, on page 24](#).
 - When a greeting is first recorded, it is stored temporarily on the Unified CVP Server, where an agent can listen to it before confirming its use.
 - When the agent confirms the greeting, the file is transferred, using FTP, to all media servers that are deployed and are configured with FTP enabled. Make sure that an FTP server is installed and configured for the correct version of IIS on the media server. For instructions, consult your Microsoft documentation (<http://microsoft.com>).
 - To satisfy a request for the greeting to play to a caller, the greeting file is copied from the media server to the VXML Gateway, where it is cached. The cached copy is used to satisfy subsequent requests for the greeting. Content expires in the cache based on the cache timeout period defined on the media server.

The routing scripts look for the prompt and greeting files either on the configured default Unified CVP media server or on a specific server identified in the script. Some typical scripting scenarios for retrieving files for Agent Greeting include:

- All files are retrieved from the default server.
- All files are retrieved from the default server if available; otherwise, a redundant server is queried.

- For security, the prompt files are retrieved from one server and the greetings files are retrieved from a different server.
- For load balancing, the greetings files are dispersed among several servers and retrieved based on tests in the script.

Media Server Hardware and Network Requirements

Ensure the server is accessible to CVP, Unified CCE, and your agent desktops.

Prepare a Media Server

1. Ensure that IIS is properly configured and running on the server. It must be listening on port 80.
2. Ensure the server is accessible to CVP, Unified CCE, and your agent desktops.
3. Perform the following steps:
 - a. On the taskbar, click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
 - b. In the **Server Manager** hierarchy pane, expand **Roles**, and then click **Web Server (IIS)**.
 - c. In the **Web Server (IIS)** pane, scroll to the **Role Services** section, and then click **Add Role Services**.
 - d. On the **Select Role Services** page of the **Add Role Services** wizard, expand **FTP Server**.
 - e. Select **FTP Service**.



Note To support ASP.NET membership or IIS Manager authentication for the FTP service, you need to select **FTP Extensibility**.

- f. Click **Next**.
- g. On the **Confirm Installation Selections** page, click **Install**.
- h. On the **Results** page, click **Close**.
- i. In the sites section, click **Add FTP Site**. Provide a site name and path to the same location as the http directory c:\inetpub\wwwroot.
- j. Select your desired binding method, specify to start automatically, select **No SSL** and click **Next**.
- k. On the **Authentication and Authorization** section select the type of authentication required. If using basic, note the name and password of the account.
- l. Select the authorization; for anonymous select **Anonymous users**.
- m. Set the read and write permissions.



Note Make note of your FTP connection information -- connection type, user name, password, and port number.

4. Make sure that the FTP and the IIS share the same root directory, because the recording application writes the file to the media server directory structure, and the greeting playback call uses IIS to fetch the file. The `en-us/app` directory should be under the same root directory for FTP and IIS.
5. Create a dedicated directory on the server to store your greeting files. This lets you specify a lower cache timeout of 5 minutes for your agent greeting files that does not affect other more static files you may be serving from other directories. By default, the Record Greeting application posts the `.wav` file to the `en-us/app` directory under your `web/ftp` root directory. You may create a dedicated directory such as `ag_gr` under the `en-us/app` directory, and then indicate this in the Unified CCE script that invokes the recording application. Use the array for the ECC variable `call.user.microapp.ToExtVXML` to send the `ftpPath` parameter to the recording application. Make sure the ECC variable length is long enough, or it may get truncated and fail.
6. In IIS Manager, set the cache expiration for the dedicated directory to a value that allows re-recorded greetings to replace their predecessor in a reasonable amount of time, while minimizing requests for data to the media server from the VXML Gateway. The ideal value varies depending on the number of agents you support and how often they re-record their greetings. Two minutes may be a reasonable starting point.
7. Also find the site you are using, go to the agent greeting folder you created (`ag_gr`), and then select **HTTP Response Headers**.
8. Select **Add**, then **Set Common Headers**.
9. Select **Expire Web Content** and set your desired value.



Note After specifying the cache timeout, it is a good idea to clear the cache on the VXML Gateway. This ensures the gateway requests the latest files from the media server. You need only clear the gateway cache once. Open a command prompt on the CVP VXML Gateway, log into IOS, and enter the following commands:

```
my_server# conf t
my_server(config)# clear http client cache
my_server(config)# exit
my_server(config)# wr
```



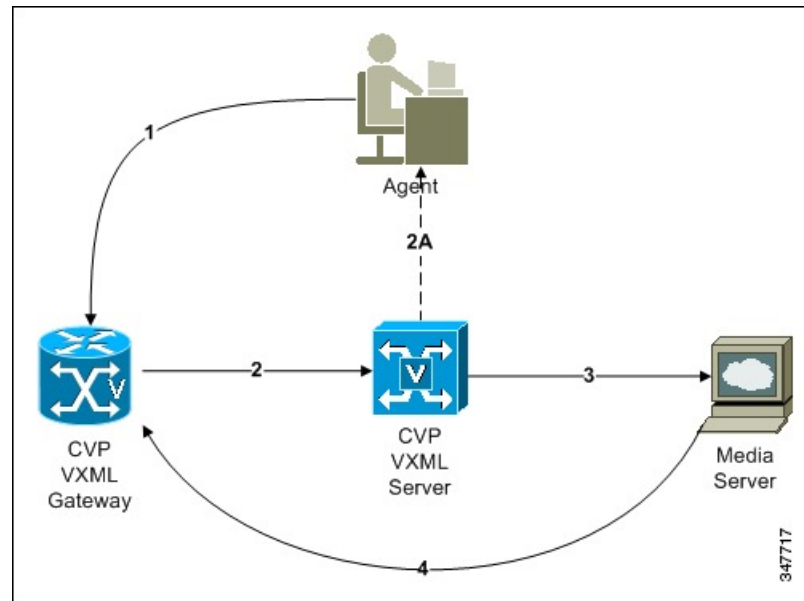
Note The HTTP client response timeout setting on the gateway must be greater than the time it takes to complete the largest anticipated FTP file transfer. If an FTP file transfer takes longer than the configured duration in seconds for HTTP client response timeout, the FTP transfer completes correctly, but the call drops as soon as the configured timeout duration is met. To change the HTTP client response timeout setting, open a command prompt on the CVP VXML Gateway, log into IOS, and enter the following commands:

```
my_server# conf t
my_server(config)# http client response timeout <new value in seconds>
my_server(config)# exit
my_server(config)# wr
```

By default, the HTTP client response timeout value for CVP is 30 seconds.

How Greeting Files Are Recorded and Served

Following is an illustration of how Greeting files are recorded and served, followed by a step by step description.



1. An agent initiates a greeting recording session and records a greeting.
2. The VXML Gateway passes the recorded (but unsaved) greeting file to the VXML Server.
3. The agent asks to listen to the greeting before saving it. The file is played from the VXML Server.
4. The agent saves the greeting. The file is named (based on the Person ID + AgentGreetingType) and stored on the media server.
5. Requests for the greeting file come in through the VXML Gateway. The VXML Gateway examines its web server cache for the file. If the file is present and not expired, the cached version is served. If the file is not present, or if its timestamp exceeds the cache expiration, the file is retrieved from the media server and cached again.

Add and Configure Media Servers in CVP

You can add one or more servers to CVP to act as media servers. If you add multiple media servers, note the following:

- CVP automatically propagates files that are added to one media server out to all media servers in the list that have FTP enabled. To enable FTP on a media server, use the following procedure.
- You can designate one media server as the default. If a default media server is defined, requests for files are automatically sent to that server without your having to specify that server in your routing scripts.

1. Access the CVP Operations Console by typing **https://<OAMP_server_IP>:9443/oamp**.
2. At the CVP Operations Console, select **Device Management > Media Server**.
3. Add a server to the list of CVP media servers.
4. Select **FTP Enabled**.

5. Configure the credentials and port settings that will permit CVP to write files to the server using FTP.
6. Optionally, you can designate one of your media servers as the Default Media Server.
7. Click the **Deploy** button to deploy the list of media servers to your CVP Servers.

Note: If you deploy the list of media servers and then designate a default, you must redeploy the list.

Republish the tcl scripts to VXML Gateway

The .tcl script files that ship with Unified CVP include updates to support Agent Greeting. You must republish these updated files to your VXML Gateway.

Republishing scripts to the VXML Gateways is a standard task in CVP upgrades. You must republish the scripts before you can use Agent Greeting.

-
- Step 1** In the Unified CVP Operation Console, select **Bulk Administration > File Transfer > Scripts and Media**.
 - Step 2** Set Device to Gateway.
 - Step 3** Select the gateways you want to update. Typically you would select all of them unless you have a specific reason not to.
 - Step 4** Select **Default Gateway Files**.
 - Step 5** Click **Transfer**.
-

Set Cache Size on VXML Gateway

To ensure adequate performance, set the size of the cache on the VXML Gateway to the maximum allowed. The maximum size is 100 megabytes; the default is 15 kilobytes. Failure to set the VXML Gateway cache to its maximum can result in slowed performance to increased traffic to the media server.

Use the following Cisco IOS commands on the VXML Gateway to reset the cache size:

```
conf t
http client cache memory pool 100000
exit
wr
```

For more information about configuring the cache size, see the *Configuration Guide for Cisco Unified Customer Voice Portal* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html>.

Create Voice Prompts for Recording Greetings

You must create audio files for each of the voice prompts that agents hear as they record a greeting. The number of prompts you require can vary, but a typical set can consist of:

- A welcome followed by a prompt to select which greeting to work with (this assumes you support multiple greetings per agent)
- A prompt to select whether they want to hear the current version, record a new one, or return to the main menu
- A prompt to play if a current greeting is not found.

To create voice prompts for recording greetings:

-
- Step 1** Create the files using the recording tool of your choice. When you record your files:
- The media files must be in `.wav` format. Your `.wav` files must match Unified CVP encoding and format requirements (G.711, CCITT A-Law 8 kHz, 8 bit, mono).
 - Test your audio files. Ensure that they are not clipped and that they are consistent in volume and tone.
- Step 2** After recording, deploy the files to your Unified CVP media server. The default deployment location is to the `<web_server_root>\en-us\app` directory.
- Step 3** Note the names of the files and the location where you deployed them on the media server. Your script authors need this information for the Agent Greeting scripts.
-

Built-In Recording Prompts

The Unified CVP Get Speech micro-application used to record Agent Greetings includes the following built-in prompts:

- A prompt that agents can use to play back what they recorded
- A prompt to save the greeting, record it again, or return to the main menu
- A prompt that confirms the save, with an option to end the call or return to the main menu

You can replace these `.wav` files with files of your own. For more information, see the Unified Customer Voice Portal Call Studio documentation at <https://www.cisco.com/c/en/us/support/unified-communications/unified-call-studio/tsd-products-support-series-home.html>.

Example Record Greeting Prompts

Unified CCE includes three example record greeting audio prompts. These are installed on each ICM server at `<icm_root>\wav`. These example files are referenced in the example recording script that are included with ICM. If you plan to deploy the example script, copy the audio prompts to the `<web_server_root>en-us\app` directory on your media server.

Configure Call Types

To record and play agent greetings, create the following call types: `RecordAgentGreeting` and `PlayAgentGreeting`.

- Step 1** From the Configuration Manager, select **Tools > List Tools**.
- Step 2** Select **Call Type List**.
- Step 3** Click **Retrieve**.
- Step 4** Click **Add**.
- Step 5** Create a call type to record agent greetings and use the name `RecordAgentGreeting`. Then click **Save**.
- Step 6** Create a call type to play agent greetings and use the name `PlayAgentGreeting`. Then click **Save**.
-

Configure Dialed Numbers

To record and play agent greetings, create the following dialed numbers: RecordAgentGreeting and PlayAgentGreeting.

-
- Step 1** From the Configuration Manager, select **Tools > List Tools**.
- Step 2** Select **Dialed Number/Script Selector List**.
- Step 3** Click **Retrieve**.
- Step 4** Click **Add**.
- Step 5** On the **Attributes** tab, do the following:
- Create a dialed number to record agent greetings; use the name RecordAgentGreeting. (The name must match exactly and is case-sensitive.) Set the **Media routing domain** to **Cisco_Voice**, and then click **Save**.
 - Create a dialed number to play agent greetings; use the name PlayAgentGreeting. (The name must match exactly and is case-sensitive.) Set the **Media routing domain** to **Cisco_Voice**, and then click **Save**.
- Step 6** On the **Dialed Number Mapping** tab, do the following:
- Click **Add** and map the RecordAgentGreeting dialed number to its call type; click **OK**.
 - Click **Add** and map the PlayAgentGreeting dialed number and its call type; click **OK**.
-

Schedule the Script

-
- Step 1** In the **Script Editor**, select **Script > Call Type Manager**.
- Step 2** From the Call Type Manager screen, select the **Schedules** tab.
- Step 3** From the Call type drop-down list, select the call type to associate with the script; for example, PlayAgentGreeting.
- Step 4** Click **Add** and select the script you want from the Scripts box.
- Step 5** Click **OK** twice to exit.
-

Define Network VRU Scripts for Agent Greeting

For Agent Greeting record and play scripts to interact with Unified CVP, Network VRU scripts are required. The number of VRU scripts that you require and how you configure them depends on how you choose to script Agent Greeting.

To create these scripts, use the Network VRU Script List Tool found in Configuration Manager.

The following table lists an example set of Agent Greeting Network VRU scripts based on the example Agent Greeting scripts that are included with the software.



Note If you require the following example VRU scripts, you must manually create them.

- The Network VRU must be a Type10
- The default timeout 180 is acceptable
- Leave Overridable unchecked

Table 2: Agent Greeting Network VRU Scripts

Name / VRU Script Name	Configuration Parameter	Interruptible (Y/N)	What it does
AgentGreeting PM, -a	null	N	Causes a saved greeting audio file to play. The -a parameter automatically generates the file name by concatenating the Person ID with the AgentGreetingType variable value set in your routing scripts that target an agent.
GreetingMenu_1_to_9 M,press_1_thru_9_greeting,A	1-9	Y	During a recording session, play an audio file that presents a voice menu prompting the agent to press the number corresponding to the greeting he or she wants to record. The 1-9 configuration parameter defines the range of allowable keys. So this value also determines the number of concurrent greetings agents can have. The A parameter specifies that the file is in the (default) Application directory on the Unified CVP Server.
GreetingSubMenu M,press1-press2-press3,A	1-3	Y	During a recording session, play an audio file that prompts the agent to press 1 to listen to a greeting, 2 to record, or 3 to go to the main menu.
Greeting_Not_Found PM,no_greeting_recorded,A	Y	Y	During a recording session, if an agent tries to play back a greeting that does not exist, play the no_greeting_recorded audio file. The Y configuration parameter in this instance allows barge-in (digit entry to interrupt media playback).
T10_GS_AUDIUM GS,Server,V, FTP	,,,,,,,,,Y	Y	This starts the external VXML application that records the greeting. The VRU script name must be specified exactly as shown and is case-sensitive. The Y parameter in the eleventh position of the Configuration Parameter is required. It allows the script to pass FTP connection information to the VXML server. The VXML server then uses this information to make an FTP connection to the media server when saving greeting files.
GreetingReview PM, -a,A	Y	Y	This script allows the agent to review the recorded greeting audio file.



Note For descriptions of VRU Script Name parameters and detailed instructions on creating Network VRU scripts for CVP micro-applications, see the [Configuration and Administration Guide for Cisco Unified Customer Voice Portal](#).

Import Example Agent Greeting Scripts

To view or use the example Agent Greeting scripts, you must first import them into Script Editor. To import the scripts:

Step 1 Launch Script Editor.

Step 2 Select **File > Import Script** and select a script to import.

The scripts are located in the `icm\bin` directory on the Unified CCE AW-HDS-DDS.

Note When you import the example scripts, Script Editor maps objects that are referenced in the scripts. Some of the objects, such as the external Network VRU scripts, skill groups, route to skill group, or precision queue, do not map successfully. You must create these manually or change these references to point to existing scripts, skill groups, and precision queues in your system.

What to do next

In addition to importing the scripts, you may need to modify the following items. For more information, see [Agent Greeting Scripts, on page 25](#).

- If you do not use a default media server, you must modify the media server specification.
- If you do not use the default values for application and locale (`en-us/app`), you must modify the path name of greeting files.
- Using the Unified CCE Administration tool, enable all expanded call variables referenced by the following sample scripts.

Agent Greeting Example Routing Scripts

The example routing script files in the `icm\bin` directory include:

- **AG.ICMS**—This script sets up an Agent Greeting by setting the greeting type to be used on the call and then queuing the call to a skill group or precision queue. Once an agent is selected from the skill group or precision queue and the call routed to the agent, the `PAG.ICMS` script is invoked. It requires that you define an `AgentGreeting VRU` script (described in [Define Network VRU Scripts for Agent Greeting, on page 20](#)) and a skill group.
- **PAG.ICMS**—This script causes an Agent Greeting to play. It is invoked by the `PlayAgentGreeting` dialed number that you configured earlier in the configuration process. This number must be associated with a call type that then runs the script. It requires that you define an `AgentGreeting VRU` script, described in [Define Network VRU Scripts for Agent Greeting, on page 20](#).
- **RECORD_AG.ICMS**—This script lets agents record a greeting. It is called from the agent desktop when an agent clicks the Record Agent Greeting button. It prompts the agent to select which greeting to play or record. This script is invoked by the `RecordAgentGreeting` dialed number that you configured earlier in this configuration process. It requires that you define all five VRU scripts described in [Define Network VRU Scripts for Agent Greeting, on page 20](#).
- **WA_AG.ICMS**—This script plays a Whisper Announcement and an Agent Greeting together on the same call flow. It requires that you define an `AgentGreeting VRU` script (described in [Define Network VRU Scripts for Agent Greeting, on page 20](#)) and a skill group.



Note The PAG.ICMS and RECORD_AG.ICMS example scripts assume that a default media server is configured in Unified CVP, and the greeting files are stored in a dedicated directory named ag_gr directory. The WA_AG.ICMS script does not include a dedicated directory.



Note For greeting, the initial script sets up the call between caller and agent, and a different script plays the greeting to the agent after the caller is connected. If the initial Unified CCE script overrides the default media server with a SET node, the call context of expanded call variables is preserved on the greeting playback call as well, and the Default Media Server may be overridden. In this case, modify the greeting playback script to use a SET node with the correct media server.

Test Agent Greeting File Path

When an agent records a greeting, the greeting file is saved with a system-generated name as follows:

- The Person ID number is prepended to the starting string. For example, an agent with a Person ID of 5050 would have greeting files named 5050_1 or 5050_French.
- The filename ends with the value of the Call.AgentGreetingType variable associated with the choice the agent made when recording the greeting. For example, if the agent selected the first option, and the Agent Greeting record script sets the first option to "1," then the greeting filename is appended with _1. As another example, if descriptive strings were implemented, and the first option is associated with the string "French," then the greeting filename is appended with _French.

The greeting file is saved in a directory whose path is determined by the following variables in the Agent Greeting record script:

- A specific media server, or the default media server. (The file is later pushed to all FTP-enabled media servers.)
- A specific application directory, or the default application directory.
- A specific locale directory, or the default locale directory.

To test the path you defined to the greeting file in your script variables, plug the complete URL into a browser. The .wav file should play. For example:

- If your script uses a default media server whose IP is *192.1.1.28 + the default locale + an application directory named greet + 5050_im1.wav*, then the generated URL should be `http://192.1.1.28/en-us/app/greet/5050_1.wav`. Entering this URL into a browser should cause this agent's greeting to play.
- If your script includes: *http://my_server.my_domain.com + the default locale + an application directory app/greet + 5050_1.wav*, then the path should be `http://my_server.my_domain.com/en-us/app/greet/5050_1.wav`.

Modify the Unified CCE call routing scripts to use Play Agent Greeting script

For an Agent Greeting play script to run, you must add an AgentGreetingType Set Variable node to your existing Unified CCE call routing scripts: This variable's value is used to select the audio file to play for the

greeting. Set the variable before the script node that queues the call to an agent (that is, the Queue [to Skill Group or Precision Queue], Queue Agent, Route Select, or Select node).

Specify AgentGreetingType Call Variable

To include Agent Greeting in a script, insert a Set Variable node that references the AgentGreetingType call variable. The AgentGreetingType variable causes a greeting to play and specifies the audio file it should use. The variable value corresponds to the name of the greeting type for the skill group or Precision Queue. For example, if there is a skill group or Precision Queue for Sales agents and if the greeting type for Sales is '5', then the variable value should be 5.

You can use a single greeting prompt throughout a single call type. As a result, use one AgentGreetingType set node per script. However, as needed, you can set the variable at multiple places in your scripts to allow different greetings to play for different endpoints. For example, if you do skills-based routing, you can specify the variable at each decision point used to select a particular skill group or Precision Queue.



Note Only one greeting can play per call. If a script references and sets the AgentGreetingType variable more than once in any single path through a script, the last value to be set is the one that plays.

Use these settings in the Set Variable node for Agent Greeting:

- Object Type: Call.
- Variable: Must use the AgentGreetingType variable.
- Type: Must use the PersonID_AgentGreetingType type.
- Value: Specify the value that corresponds to the greeting type you want to play. For example: “2” or “French”
 - You must enclose the value in quotes.
 - The value is not case-sensitive.
 - The value cannot include spaces or characters that require URL encoding.

Scripting Agent Greeting for Multiple Customers

In the out-of-box method for deploying Agent Greeting, Unified CCE uses the customer information from the built-in “PlayAgentGreeting” dialed number to choose the correct network VRU to play the greeting. If your deployment has multiple customers configured within your Unified CCE instance and you want to use Agent Greeting with all of them, you must configure things differently to work around customer associations.

Configure Custom Dialed Number for Agent Greeting Play

To play Agent Greetings for multiple customer instances, configure the built-in PlayAgentGreeting dialed number for each Unified CM routing client, but do not associate it with a specific customer. The Unified CM peripheral uses this number to initiate Agent Greeting play. If you want your greetings to be played from a different network VRU, use the TranslationRouteToVRU node in your routing scripts to explicitly choose the network VRU.

Configure Custom Dialed Number for Agent Greeting Record

To record Agent Greetings when you have multiple customers, you must create your own custom dialed number for recording. You may want to create different dialed numbers for different customers. As with Agent Greeting play, if you want to use different network VRUs to record Agent Greetings for different customers, use the TranslationRouteToVRU node in your routing script to explicitly select the network VRU.

Create your own custom button or have your agents enter the record dialed number using the dial pad on their desktops.

Agent Greeting Scripts

Agent Greeting requires two call routing scripts: one that agents can use to record greetings and one to play a greeting to callers. Examples of these scripts are included in your installation. This section describes the elements in the installed example scripts, including optional features and other modifications that you can make. To create scripts from scratch, use this section to understand the required elements in Agent Greeting scripts.



Note If you plan to use the installed example scripts out of the box, you can ignore this section.

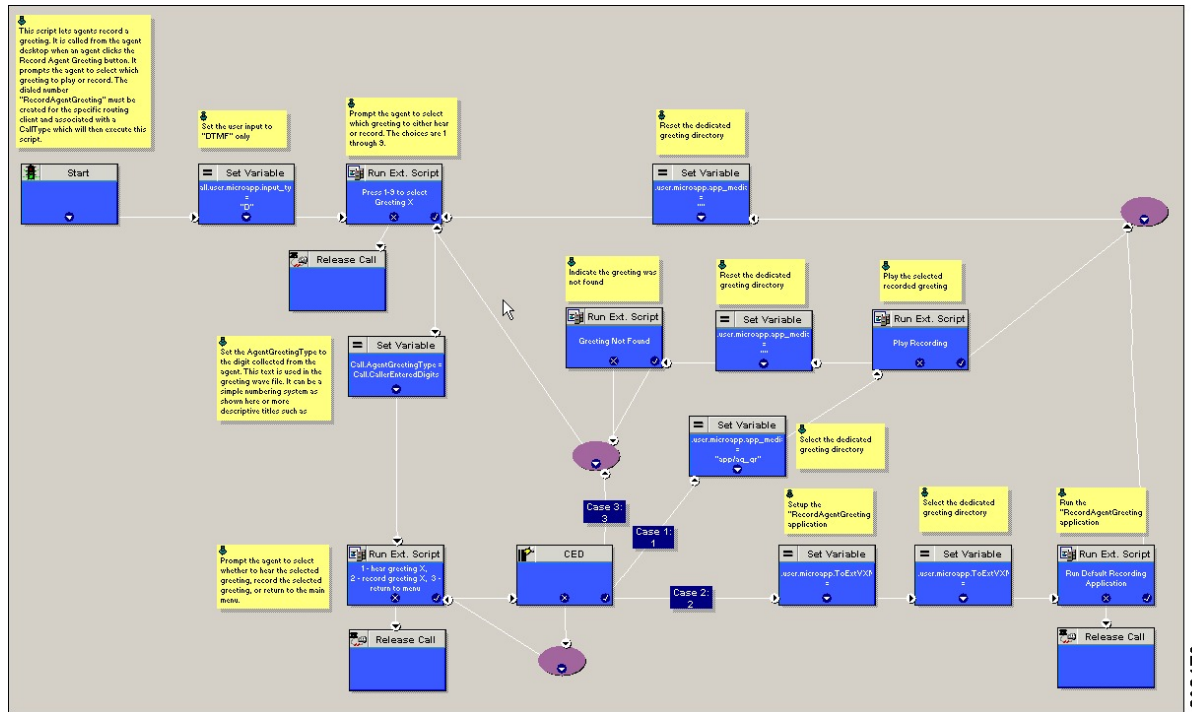
Agent Greeting Recording Script

The Agent Greeting recording script is a dedicated routing script that allows agents to record greetings. You can use the installed example scripts or create your own.

In the example script shown here, the agent is first prompted to select one of nine possible greeting types. After selecting a greeting type, the agent chooses whether to 1) listen to the existing greeting for that type; 2) record a new greeting for that type, or 3) return to the main menu. If the agent selects the option to listen, the name of the application directory on the media server is set and the external VRU script that plays the greeting is triggered. Then the agent is returned to the main menu. If the agent selects the option to record, the Unified CVP recording application is called. The recording application contains its own built-in audio prompts that step the agent through the process of recording and saving a greeting. At the end, the agent is returned to the main menu.

There are several other behaviors in the script to note. An agent may select to listen to a greeting type for which no greeting exists. In that event, a VRU script that plays an error message is called. Also, in two places in the script, the path to the application directory is reset to the default. This is because (in this example) that is where the files for the audio files reside. The only files that reside outside of the default directory are the greetings themselves.

Figure 1: Agent Greeting Record Script



302476

RecordAgentGreeting Micro-application

Unified CVP includes a dedicated micro-application -- RecordAgentGreeting -- for recording agent greetings. The application lets agents record, review, re-record, and confirm the save of a greeting. It includes audio files to support each of these functions. If an agent is not satisfied with a greeting, it can be re-recorded up to three times. Upon confirmation of a save, the application FTPs the saved file to the media server.

Built-in error checking includes checks for the data required to name the file (*Person ID + AgentGreetingType* variable value), media server specification, valid menu selections made by the agent, and successful FTP of the greeting file.

Agent Greeting Record Script Nodes

Using the example script as a reference, here are descriptions of the functions its nodes perform.

Table 3: Script Node Functions for Agent Greeting

Node	Value	What it does
Variable:Call:user.microapp.input_type	D	Sets the allowable input type to DTMF (touch tone).
RunExtScript:Press 1-9 to Select Greeting X	M,press_1_thru_9_greeting,A	Runs the VRU script that defines which digits are valid to select an AgentGreetingType and plays a voice prompt describing the options.

Node	Value	What it does
Variable:Call:AgentGreetingType	Call CallerEnteredDigits	Sets the AgentGreetingType to the digit the agent pressed. This text is used in the greeting wave file. It can be a simple numbering system or more descriptive titles such as "English."
RunExtScript: 1 - hear greeting X, 2 - record greeting X, 3 - return to menu	M,press1-press2-press3,A	Runs the VRU script that defines which digits are valid to select a desired action and plays a voice prompt describing the options.
CED	1,2,3	Tells the script how to handle the caller entered digits in response to the 1,2,3 external script.
Variable:Call: user.microapp.app_media_lib	Set three times: <ul style="list-style-type: none"> • Once to "app/ag_gr" • Twice to "" (an empty string; that is, the default) 	Defines the path to the application directory on the Unified CVP media server. Prior to playing the greeting file, it is set to the dedicated greeting file directory (in this example, app/ag_gr). After the greeting file plays, it is reset to the default application directory where (in this example) the files for voice prompts are stored. If the voice prompts were stored in the same directory as the greeting files, there would be no need to reset the path.
RunExtScript: Play Recording	PM,-a,A	Runs the VRU script that plays the selected Agent Greeting.
RunExtScript:Greeting Not Found	PM,no_greeting_recorded,A	Runs the VRU script that plays an error message if the Agent Greeting selected to play does not exist.

Node	Value	What it does
Variable: Call:user.microapp. ToExtVXML[]	Array Index: 2 Value: "ftpPath=<path_to_dedicated/directory>" For example: "ftpPath=en-us/app/ag_gr"	Specifies the FTP information that the VXML server uses to write greeting files to the media server. The information must match the FTP information configured for the media server in the Unified CVP Operations Console. The value for array index must be 2. The value consists of: <ul style="list-style-type: none"> • ftpPath= to set the path to the dedicated directory for agent greeting files. • The path must begin with the locale directory. To view additional setting options, see CVP documentation .
Variable: Call:user.microapp. ToExtVXML[]	Array Index: 0 Value: "application=RecordAgentGreeting"	Identifies the external Unified CVP micro-application (RecordAgentGreeting) that is used to record the greeting. The value for array index must be 0.
RunExtScript: Run Default Recording Application	GS, Server, V	Runs the VRU script that launches the Get Speech micro-application on the VXML server.

Specify Media Server in Routing Scripts

When you configure media servers in CVP, you can specify a default media server. The benefit to specifying a default media server is that your scripts do not need a Set Variable node to access the default media server. For this to work, you must make sure that the files a script requests are stored on the default server.

If you do not define a default media server, or if you define a default but the files that your script requires are not stored on the default, then the script must include a Set Variable node to identify a media server.

To specify a media server that stores the files required by your script, use the following settings in the Set Variable node:

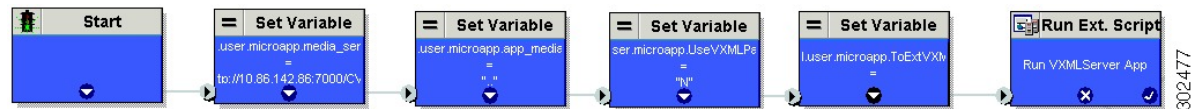
- Object Type: Call.
- Variable: Must use the user.microapp.media_server expanded call variable.
- Value: Specify the HTTP path to the server. For example: "http://myserver.mydomain.net." You must enclose the path in quotes.
- Alternately you can specify an IP address in place of a hostname.

In scripts that invoke an external VXML application (as the Agent Greeting record script does), if you explicitly set a variable for the media server (`user.microapp.media_server`), then you must also set the following variables:

- The path to the media server application directory (`user.microapp.app_media_lib`)
- The CVP UseVXMLParams value to N. (`user.microapp.UseVXMLParams`)

See the following example.

Figure 2: Additional Required Variables When Specifying a Media Server



Specify Greeting File Locale and Application Directories in Routing Scripts

CVP uses a default storage directory for media files: `<web_server_root>/en-us/app`. To take advantage of this, Unified CCE call routing scripts automatically add `en-us/app` to the server name when constructing HTTP requests for media files. For example:

- If the script node that defines the media server has a value of “`http://myserver.mydomain.com`,” and
- The script node that defines which audio file to play has a value of “`5050_1.wav`” (for an agent with a Person ID of 5050), then
- The HTTP request for the file is automatically constructed as
`http://myserver.mydomain.com/en-us/app/5050_1.wav`

If your greeting audio files are stored in a different locale directory, you must add a Set Variable node to your script that identifies the locale directory. As you must store your greeting files in a dedicated subdirectory under the locale, you must always add a Set Variable node that identifies that directory.

Use these settings in the Set Variable node to specify your locale directory:

- Object Type: Call.
- Variable: Must use the `user.microapp.locale` expanded call variable.
- Value: Specify the directory name. For example: “`pt-br`” (Portuguese-Brazil). You must enclose the path in quotes.

Use these settings in the Set Variable node to specify your application directory:

- Object Type: Call.
- Variable: Must use the `user.microapp.app_media_lib` expanded call variable.
- Value: Specify the directory name. For example: to use a directory “`greet`” in place of the default directory “`app`”, enter “`greet`”. To use a sub-directory “`greet`” under “`app`” enter “`app/greet`”. You must enclose the path in quotes.

Verify Length for Media Server Locale and Application Directory Variables

If you include Set Variable nodes for the media server, locale, and/or application directories, make sure that the values you set for them do not exceed the Maximum Length settings for their corresponding expanded call variables.

For example, if you include a Set Variable node for the media server with a value of “http://mysubdomain.mydomain.co.uk”, the string is 33 characters long. Therefore, the Maximum Length setting for the user.microapp.media_server expanded call variable must be 33 or greater. Otherwise, the server name is truncated in the HTTP request for the file and the file is not found.

To configure ECC variables, use the Unified CCE Configuration Manager. Select **List Tools > Expanded Call Variables List**.

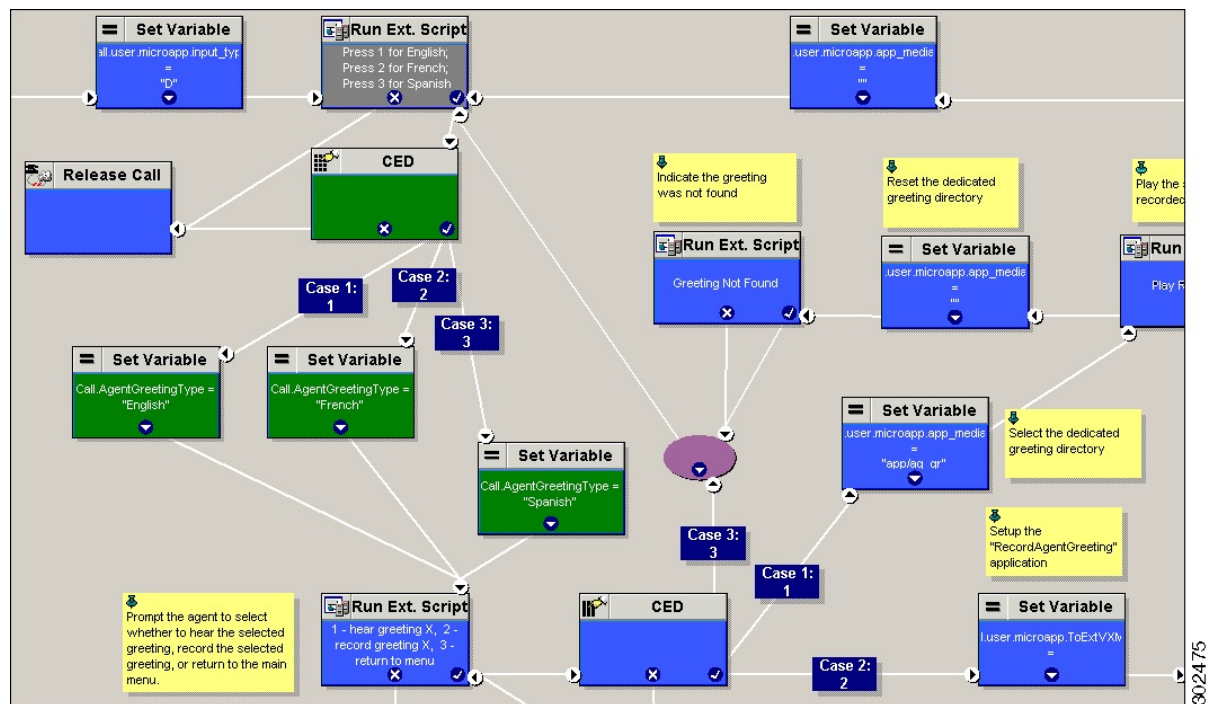
Descriptive Agent Greeting Type Strings

The previous Agent Greeting record script example stores Agent Greeting Type values as numbers (although in string format). But suppose you prefer more descriptive string names. For example, “English,” “French,” and “Spanish.” Or “Sales,” “Billing,” and “Tech Support.”

Descriptive names can make it easier to understand at a glance what different numeric key selections in your scripts correspond to. Note that they also affect how greeting files are named (for example, for an agent whose Person ID is 5050, 5050_English.wav as opposed to 5050_1.wav).

The following script example is almost identical to the previous record script, except that it includes four additional nodes (highlighted in green). They consist of an additional CED node that maps the keys 1, 2, and 3 to language names. The Run Ext Script node (in gray) was modified for the new options. The rest of the script is the same with no other changes required. Note that your routing scripts require a corresponding mapping of numeric keys to language names.

Figure 3: Script with Descriptive Greeting Type Strings



Agent Greeting Play Script

The Agent Greeting feature requires a dedicated routing script that causes the agent greeting to play. This script is invoked by the PlayAgentGreeting dialed number.

The Play script must contain at least two and possibly four specific nodes, depending on other factors.

You always need the following nodes:

- A Run External Script node that calls the VRU script that plays the greeting.
- A Set Variable node that sets the directory path to your greeting files.

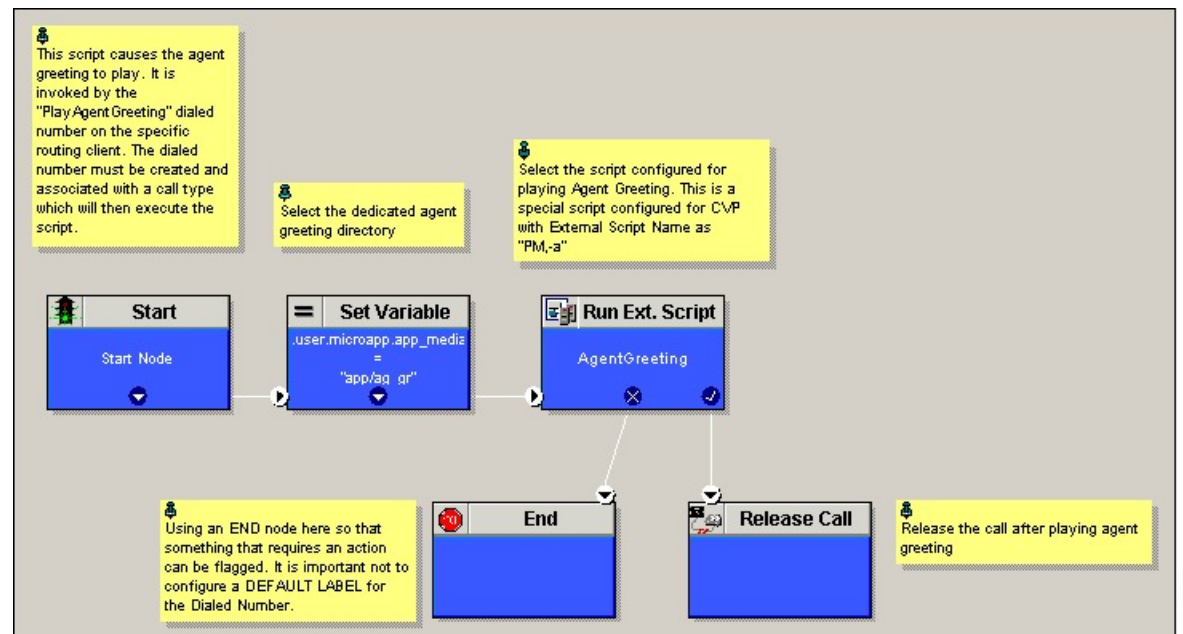
You may also need to include in your scripts Set Variable nodes that:

- Specify the Media Server: Unified CVP lets you specify a default media server. If you are not serving your audio files from the default media server, your scripts must include a variable that identifies the server where your audio files are stored.
- Specify the Locale Directory: Additionally, if you are not storing your files in the default locale directory `en-us` on the media server, you must include a variable that specifies the name of the locale directory where the files are stored.



Note The Locale Directory set variable node is optional. It is needed only if you decide to use a directory other than the default one.

Figure 4: Agent Greeting Play Script Example



On a Mobile Agent callflow, CUCM may return a 404 error due to the absence of Agent Greeting, leading to call failure. To fix this issue, do the following:

1. Add a new Run External Script node with its backup media mapped to the agent greeting.
2. Add the Run External Script node between the failure path of the AgentGreeting Run External Script node and the End node.
3. Connect the Run External Script node's success path to the existing Release call node and failure path to the existing end node.

Adding the Run External Script node may add a short delay of one to two seconds to the call flow.

Reporting

In agent, skill group, and precision queue reports, greeting time is not specifically broken out. The period during which the greeting plays is reported as talk time. Record time is counted as an internal call by the default skill group.

Calls that involve Agent Greeting consist of two call legs: the inbound call from the customer and the call to Unified CVP for the greeting. Both of these legs have the same RouterCallKeyDay and RouterCallKey values in the TCD and RCD tables in the database. You can use these values to link the two legs together for reporting purposes.

Greeting Call Statistics

To view greeting call statistics, create a separate call type and associate it with the routing script that plays agent greeting. New Cisco Unified Intelligence Center templates for the agent greeting call type are created based on the data in the existing Call_Type_Real_Time and Call_Type_Interval table in the database.

Peripheral Call Types for Agent Greeting

There are two peripheral call types specific to Agent Greeting that you can use to track and report on the feature.

- Call Type 39: Play Agent Greeting. Route request to play an Agent Greeting.
- Call Type 40: Record Agent Greeting. Agent call for recording an Agent Greeting.

Extra TCDs and RCDs are generated for the agent greeting call leg, and they can be linked to the first call leg by the same RouterCallKeyDay and RouterCallKey.

Serviceability

Serviceability for Agent Greeting includes SNMP events captured by your Network management software that indicate reasons for greeting failures and counters to track the number of failed greeting events.



Note There is no counter for the number of failed agent greeting calls.

When system components fail, Agent Greeting may be impacted. For example, if a requested greeting audio file cannot be found for any reason, the call proceeds without the Agent Greeting.



CHAPTER 3

Agent Request

- [Agent Request Feature Description, on page 33](#)
- [Configure Unified CCE for Agent Request, on page 36](#)
- [Configure Customer Collaboration Platform for a Voice Callback Agent Request, on page 38](#)
- [Agent Request Script, on page 40](#)
- [Use the Sample Code to Create a Customer Callback Request, on page 42](#)
- [Agent Request Reporting, on page 43](#)

Agent Request Feature Description

The Agent Request feature allows a customer to initiate a request on the web that results in a call from an agent.

To use Agent Request, your solution requires the Cisco Customer Collaboration Platform optional component. Cisco Customer Collaboration Platform works in a Contact Center Enterprise (Unified CCE) solution to process the request from its inception through the delivery of the callback.



Important The Agent Request feature can be used only if the customer or a partner develops a custom application. There is sample code on DevNet (formerly Cisco Developer Network) that you can use to understand how to start building your custom application to submit callback requests to Customer Collaboration Platform.

Customer Collaboration Platform and Agent Request

Customer Collaboration Platform provides the Callback API used by a custom application to request a phone call from a contact center agent.

The API works in conjunction with Customer Collaboration Platform callback feeds, campaigns, and notifications to pass callback requests to the contact center for routing.

The Callback API:

- Allows custom applications to initiate a callback.
- Forwards the callback request and callback details to Unified CCE using a notification mechanism (the Connection to Unified CCE notification type) through a Media Routing (MR) connection.

- Allows custom applications to retrieve the state of the callback as well as the estimated wait time (EWT) until an agent becomes available.
- Allows custom applications to cancel a requested callback.

The Callback API supports the use of Call variables and ECC variables for callback requests. Call variables and ECC variables send customer-specific information with the request. When you create a callback contact, the social contact associated with the callback contact includes all of the specified variables as extension fields.

Unified CCE and Agent Request

When it receives an Agent Request, Unified CCE performs these tasks:

- Process the callback request.
- Route the callback request to an agent and place a call from the agent's phone to the customer.
- Notify Customer Collaboration Platform that the agent has been selected.

Agent Desktops and Agent Request

Cisco Finesse supports Agent Request.

Enterprise Chat and Email and Agent Request

To configure prefixes and filters for dialed numbers in Enterprise Chat and Email, you must use the Unified CCE Script Editor.

Unsupported Environments

Agent Request is not supported:

- In a Parent/Child deployment
- With Mobile Agents
- In a hybrid deployment

Agent Request Prerequisites

Install and configure Customer Collaboration Platform before implementing Agent Request. Customer Collaboration Platform must be geographically colocated with one side of the Media Routing Peripheral Gateway (MR PG).

The customer or partner must build a custom application for the Agent Request feature. See [Use the Sample Code to Create a Customer Callback Request, on page 42](#).

Customer Collaboration Platform is always deployed in a DMZ. Remember to open the port you have configured for the MR PG. See [Set up the Media Routing PG and PIM, on page 37](#).

Agent Request Call Flow

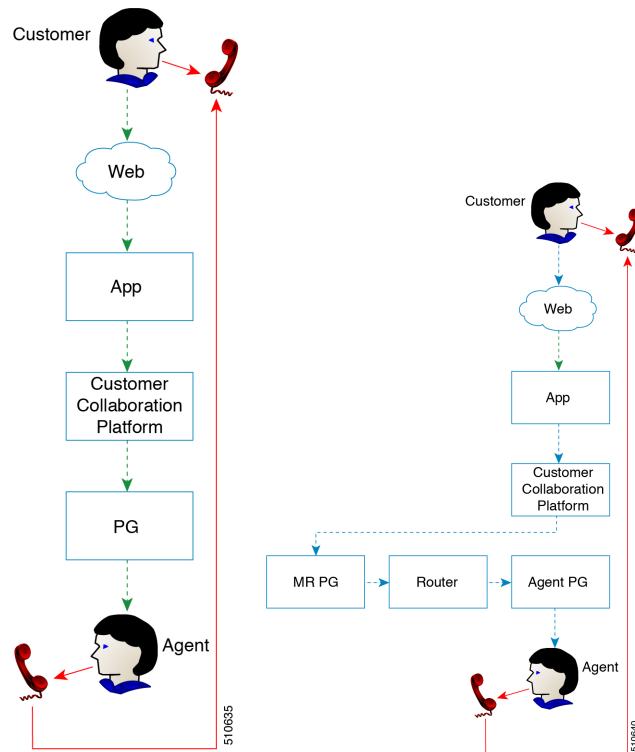
The flow proceeds as follows:

1. The customer application initiates an agent request by requesting a callback.
2. Customer Collaboration Platform sends the request to the Media Routing PG.
 - a. The Media Routing PG sends the request to the Router.
 - b. The Router sends the request to the Agent PG.
 - c. The Agent PG sends the request to the agent.
3. A call is initiated from the agent's phone, on behalf of the agent, dialing the customer's phone number.



Note The agent does not control when the call is placed.

Figure 5: Agent Request Call Flow



Agent Request Scenarios

1. From the web, the customer requests to speak to an agent.
2. The customer receives feedback that the request is accepted.
3. The customer receives feedback that the call is queued and the estimated wait time.
4. The customer receives feedback that a call is on its way.

5. The agent's phone places an outbound call.
6. The agent is presented with call context.

If	Then
The customer is available	The customer receives and answers the call, and speaks to the agent
The customer is busy when the callback occurs	The agent receives a busy tone
The customer does not answer when the callback occurs	The agent hears ringing
The customer cancels the callback before an agent is selected	There is no impact on the agent

Configure Unified CCE for Agent Request

The following information describes how to configure Agent Request for a Unified CCE deployment.



Important Configure Unified CCE before you configure Customer Collaboration Platform.

Configuration Manager

Use these Configuration Manager tools and procedures to configure Agent Request.

Configure Network VRU and Network VRU Script

-
- Step 1** In the Configuration Manager, use the Network VRU Explorer tool to configure and save a type 2 VRU. The Network VRU is used to queue voice callback tasks if an agent is not available to handle them.
- Step 2** In the Configuration Manager, use the Network VRU Script List tool to add a Network VRU Script that references the Network VRU that you configured in Step 1.
The Network VRU Script is used for Estimated Wait Time.
-

Configure the Media Routing PG and PIM

-
- Step 1** In Configuration Manager, open the PG Explorer tool to configure a media routing PG.
- Step 2** Create a media routing PIM and routing client for Customer Collaboration Platform.
Write down the Logical Controller ID and the Peripheral ID. You will use them when you set up the PG.
- Step 3** On the Peripheral tab in the PG Explorer tool, check the **Enable post routing** check box.

- Step 4** On the Routing Client tab in the PG Explorer tool, select the **Multichannel** option from the **Routing Type** drop-down list box.
- Step 5** On the Advanced tab in the PG Explorer tool, select the type 2 Network VRU that you created.

Configure Call Type

Open the Call Type List tool, and create a call type to handle calls from an agent request voice callback.

Configure Dialed Number/Script Selector

- Step 1** Open the Dialed Number/Script Selector List tool, and create a script selector on the routing client that you configured. Customer Collaboration Platform uses this script selector to request agents for voice callback. (The script selector configured here must be the same as the one entered in the Customer Collaboration Platform notification.)
- Step 2** On the Attributes tab, select **Cisco_Voice** from the **Media routing domain** drop-down list box.
- Step 3** On the **Dialed Number Mapping** tab, map the script selector to the call type you created.

Configure ECC Variables

- Step 1** Open the **Expanded Call Variable List** tool.
- Step 2** Add one or more ECC Variables for the callback request.

Note Arrays are not supported with the Agent Request feature.

CCE solutions support the Latin 1 character set only for Expanded Call Context variables and Call variables when used with CVP, Finesse, and Customer Collaboration Platform. CCE also supports the use of multi-byte character sets in limited usage for ECC and call variables when setting them in Script Editor using double quotes.

Set up the Media Routing PG and PIM

- Step 1** From Cisco Unified CCE Tools, select **Peripheral Gateway Setup**.
- Step 2** On the Components Setup screen, in the Instance Components panel, select the PG Instance component. If the PG does not exist, click **Add**. If it exists, click **Edit**.
- Step 3** In the Peripheral Gateways Properties screen, click **Media Routing**. Click **Next**.
- Step 4** Click **Yes** at the prompt to stop the service.
- Step 5** From the Peripheral Gateway Component Properties screen, click **Add**, select the next PIM, and configure with the Client Type of Media Routing as follows.
- Check **Enabled**.

- b) In the **Peripheral Name** field, enter **MR**.
- c) For **Application Hostname (1)**, enter the hostname or IP address of Customer Collaboration Platform.

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.

- d) By default, Customer Collaboration Platform accepts the MR connection on **Application Connection Port** 38001. The Application Connection Port setting on Customer Collaboration Platform must match the setting on the MR PG; if you change the port on one side of the connection, you must change it on the other side.
- e) Leave the **Application Hostname (2)**, field blank.
- f) Keep all other values.
- g) Click **OK**.

Step 6 On the Peripheral Gateway Component Properties screen, enter the Logical Controller ID that you recorded when you configured the Media Routing PG and PIM.

Step 7 Accept defaults and click **Next** until the Setup Complete screen opens.

Step 8 At the Setup Complete screen, check **Yes** to start the service. Click **Finish**.

Step 9 Click **Exit Setup**.

Step 10 Repeat from Step 1 for Side B.

Step 11 Navigate to **Unified CCE Administration > Infrastructure Settings > Inventory**.

Step 12 Add Customer Collaboration Platform as an external machine.

- a) Click **Add**.
- b) Select Customer Collaboration Platform from the drop-down list.
- c) Enter the required information.
- d) Click **Save**.

The system automatically enables and completes the **CCE Configuration for Multichannel Routing** settings in Customer Collaboration Platform Administration, including the **Application Connection Port** you specified.

Configure Customer Collaboration Platform for a Voice Callback Agent Request

To support a callback request, Customer Collaboration Platform must be configured with:

- A callback feed
- A campaign
- A Connection to CCE notification configured for the campaign mentioned above that will be triggered by incoming callback requests with a matching tag.

Create Feed

Step 1 Sign in to Customer Collaboration Platform.

Step 2 Click **Configuration**.

- Step 3** On the **Manage Feeds** panel, click **New**.
- Step 4** For **Type**, select **Callback**.
- Step 5** Name the feed.
- Step 6** For **Reply Template**, retain the default, *No reply template*.
- Step 7** Configure the feed to automatically tag all callback requests that come in on that feed. For example, autotag with 'sendtocontactcenter'.
Make a note of the tag. It is used to trigger the notification to CCE.
- Step 8** Click **Save**.
-

Create Campaign

- Step 1** Sign in to Customer Collaboration Platform.
- Step 2** Click **Configuration**.
- Step 3** On the **Manage Campaigns** panel, click **New**.
- Step 4** Name the campaign.
- Step 5** Enter an optional description.
- Step 6** Make no selection in the **Chat Invitation Feed** drop-down list.
- Step 7** Locate the Callback feed in the **Available** panel and move it to **Selected**.
- Step 8** Click **Save**.
-

Create Notification

- Step 1** Sign in to Customer Collaboration Platform.
- Step 2** Click **Administration**.
- Step 3** On the **Manage Notifications** panel, click **New**.
- Step 4** For **Type**, select **Connection to CCE**.
- Step 5** Name the notification.
- Step 6** From the **Campaigns** drop-down list, select the campaign that you created for the callback.
- Step 7** In the **Tags** field, enter the tag that is automatically applied to callback requests by the feed. In our example 'sendtocontactcenter'.
- Step 8** For **Request Type**, select **Callback**.
- Step 9** In the **Dialed Number/Script Selector** field, enter the dialed number string that you have configured.
See [Configure Dialed Number/Script Selector, on page 37](#).
- Step 10** Click **Save**.
-

Agent Request Script

The Agent Request Script is used to implement an optional dial-plan, queue a call to the skill group node, and calculate the estimated wait time for a voice callback to a customer.

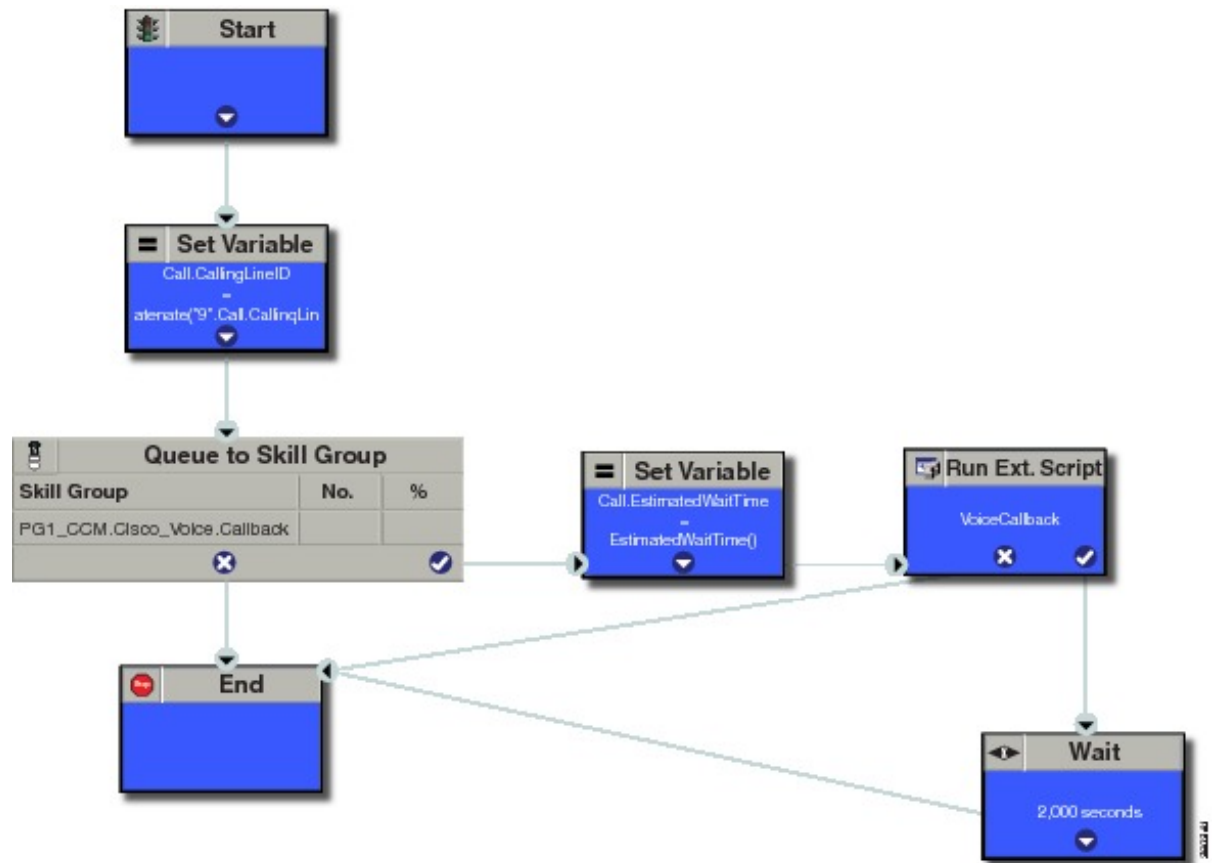
A customer who requests a voice callback might want to know approximately how long it will be before the call is returned. You can configure voice callback to provide an estimate of the wait time back to the customer. The estimated wait time is calculated once, when the call enters the queue. The time 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 calls leaving the queue. Any calls that are routed or abandoned during the first five 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. The algorithm computes the wait time for each of the queues against which the call is queued (Skill Groups or Precision Queues) and then returns the minimum estimated wait time. Queue to Agent is not supported.

While the queue builds, the small number of calls in the queue makes the estimated wait time less accurate and the value fluctuates rapidly. As the queue operates with more calls over time, the estimated wait time is more accurate and consistent.



Note The built-in function also applies to inbound calls that queue.



Create Agent Request Script

To create a Agent Request script:

-
- Step 1** **Start node:** Create the **Start** node by selecting a new Routing Script from the Script Editor.
- Step 2** **Set Variable (Call.Calling Line ID) node:** (optional). If required, you can set the CallingLineID (CLID/ ANI) variable to implement a "dial-plan," pre-pending a set of digits to the phone number provided by the customer so that it can be correctly routed. For example, it is often necessary to add 9 to the phone number to reach an outside line. In other cases, more pre-pended digits may be required to reach the end customer.
- You can also set up Unified Communications Manager Route Patterns to respond to a certain set of digits by routing the call to an outside line with a specified area code. To implement a dial-plan, add a Set Variable node before the queue, as shown in this example. In this case, a 9 is pre-pended to the customer phone number using the built-in concatenate function.
- Step 3** **Queue to Skill Group node:** The Agent Request call can be queued against one or more Skill Groups, Precision Queues, or a queue-to-agent node. In the example script, the call is queued against a single skill group.
- Step 4** **Set Variable (Call.Estimated Wait Time) node:** Set the Call Wait time as follows:
- From the Set Variable node, select **Call** from the **Object type** drop-down menu.
 - 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.

- c) Click **Formula Editor**. You can either use the default estimated wait value, by clicking the **Built-In Functions** tab and choosing **EstimatedWaitTime()**. Or to create a formula and use your own estimated time value, click the **Variables** tab, and choose an entry in the **Object type** list and **Object** list. Then double-click a variable in the **Variable** list.

Step 5 **Run Ext Script node:** Apply the **Network VRU** script as follows:

- a) Click the **Queue** tab.
- b) Click **Run External Script**.
- c) Click inside the script. A Run External Script node appears.
- d) Double-click the node and choose the Network VRU script from the list and 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 Customer Collaboration Platform.

Step 6 **Wait node:** The wait period for an agent becomes available.

Step 7 **End node:** The script ends if no agent becomes available.

Use the Sample Code to Create a Customer Callback Request

Cisco Systems has made sample callback application code available to use as a baseline in building your own application. This sample includes retrieving and displaying the estimated wait time, assuming it has been configured in Unified CCE. You can find the sample code on DevNet.



Note You cannot copy and paste this code to achieve a working application. It is a only a guideline.

For more information about how to use the Callback API, see the [Cisco Customer Collaboration Platform Developer Guide](#).

Step 1 Retrieve the feed id by entering this URL in a browser: **https://<Customer Collaboration Platform_Hostname_or_Ip>/ccp-webapp/ccp/feed**.

In the example output below, note that the value in the <name> field is "Callback." Look for the number of the feed id identified at the end of the refURL path (in this case, it is 100000) just before the </refURL> tag. Copy this number.

```
<feeds>
<Feed>
<changeStamp>0</changeStamp>
<name>Callback</name>
<pushFeedURL>https://128.107.81.27/ccp/callback/feed/100000</pushFeedURL>
<refURL>https://128.107.81.27/ccp-webapp/ccp/feed/100000</refURL>
<status>1</status>
<tags>
<tag>trial</tag>
</tags>
<type>10</type>
</Feed>
</feeds>
```

Step 2 Access the sample application from DevNet: <https://developer.cisco.com>.

Step 3 Enter values in the fields:

- **Title:** A title or subject for the callback request.
- **Author:** The name of the person submitting the callback request.
- **Phone:** The phone number to call back.
- **Feed Id:** The value from the refURL above.

Step 4 Click **Call me back**.

Agent Request Reporting

Cisco Unified Intelligence Center CCE reports include data for Agent Requests



Note Agent requests that fail before being routed to CCE will not be included in the CCE solution-level reports. The Customer Collaboration Platform search function can be used to identify these requests.

Call Type and Call Type Skill Group Metrics

- **Calls Offered** — Incremented when Call Type is entered (through Script Selector or Call Type node).
- **Calls Abandoned in Queue** — Incremented when a Queued Callback request is canceled by the customer prior to when an Agent is selected to handle the Voice Callback call.
- **Calls Answered** — Incremented if the call is placed from the agent and represents work accepted by the agent.
- **Calls Handled** — Incremented if the customer answers the call. Calls Answered minus Calls Handled indicates how many calls failed to reach the intended customer.
- **Service Level Offered** — Incremented for all routed calls, including voice callback calls initiated through the agent request API.
- **ServiceLevelCalls** — Incremented if the call is presented to the agent within a service level.
- **Answer Intervals (1 - 10)** — The appropriate bucket is incremented based on how long the call was in the queue.

Skill Group Metrics

Call Type Skill Group and Skill Group metrics are not counted in the same way. The skill group metric treats each call as agent-initiated; therefore, Calls Answered and Calls Handled are not incremented. AgentOutCallsTime, AgentOutCalls, AgentOutCallsTalkTime, AgentOutCallsOnHold, and AgentOutCallsOnHoldTime are incremented.

Agent Real Time

The direction in the Agent Real Time table is listed as Outbound.

Termination Call Detail

For custom reporting, the Termination Call Detail records contain a PeripheralCallType of 41 -Voice Callback. Calls which do not successfully connect to a customer have a call disposition of **10 - Disconnect/Drop no answer**. This includes agent request calls to busy numbers.



CHAPTER 4

Business Hours

- [Business Hours Overview, on page 45](#)
- [Business Hours Use Cases, on page 46](#)
- [Set the Principal AW for Business Hours, on page 46](#)
- [Business Hours Set Up Workflow, on page 47](#)

Business Hours Overview

The Business Hours feature lets you create schedules for regular working hours and extra working hours, and to close the contact center for holidays or emergencies. It provides the mechanism for routing these contacts to specific support teams based on the configured work hour schedules, holidays, emergency closures, or extra working hours. You can create Business Hour schedules for various scenarios for various contact center teams. This feature helps you create and apply several Business Hour schedules to the same team. On the other hand, you could apply the same Business Hour schedule to several support teams.

When a customer contacts the contact center, the response by the contact center is based on the status of the support team. This status is evaluated using the Business Hour configured for the team.

Use this feature to:

- Configure default working hours (regular hours) for contact center teams for each day of the week. This option is not applicable to 24x7 support teams.
- Configure the special hours for the contact center team or teams for any special days such as Sale days or holidays.
- Force Close the contact center for any emergency such as a natural calamity.
- Force Open the contact center on a holiday or a non-working day to cater to specific business requirements such as Sale days.
- Create and deploy customer notifications that are based on Business Hour status.

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.

Contact Center Enterprise Reference Design Support for Business Hours

Unified CCE supports Business Hours for these reference designs:

- 2000 Agents

- 4000 Agents
- 12000 Agents
- 24000 Agents

Business Hours Use Cases

Use the Business Hours feature to manage the incoming customer calls or digital channel contacts to your teams, by routing these contacts based on the Business Hours you configure.

Use the Business Hour status in an IF node in scripts to control the call and digital channel contacts, such as email and chat, and notify the customers accordingly.

You can have Business Hours scripts for the following treatments:

- When the business is open, route calls and digital contacts to the applicable skill groups and precision queues.
- When the business is closed, play the message for the closed status with the appropriate Status Reason and terminate the call. Route the digital contacts to the appropriate queues.
- When the business is not open 24x7, route the calls to skill groups and precision queues for after-hours support or play the after-hours message.
- When the business is open 24x7, at a predefined time before the end of each shift, route the calls and digital contacts to the appropriate queues for the next shift.
- When the business is closed for an emergency on a working day, notify the customers contacting your contact center appropriately about the emergency closing.

Based on reason code and status, the customers will hear appropriate prompts on the call.

Set the Principal AW for Business Hours

You must specify and set the Principal AW before configuring the Business Hours.

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.

-
- Step 1** In Unified CCE Administration, go to **Infrastructure > Inventory**.
 - Step 2** Click the AW that you want to set as **Principal AW**.
The Edit CCE AW window opens.
 - Step 3** Select the **Principal AW** check box.
 - Step 4** Enter the Unified CCE Diagnostic Framework Service domain, username, and password.
 - Step 5** Click **Save**.
 - Step 6** Restart Tomcat service on **Principal AW** machine.
-

Business Hours Set Up Workflow

This section provides information necessary to set up the Business Hours feature.

Table 4: Business Hours Set Up Workflow

Tasks	Documentation
Scripting for Business Hours	<i>Business Hours Variables</i> and <i>Dynamic Formula for Business Hours</i> in 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
Business Hours Configuration	Administration Guide for Cisco Unified Contact Center Enterprise at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-maintenance-guides-list.html

Scripting for Business Hours

To enable scripting for Business Hours, use the following variables:

- **Business Hour Status**—The real time status based on the configured Business Hours.
- **Reason Code**— The reason code associated with the current status.

These variables must be used in the CCE script IF node to route the customer contacts.

Business Hours Configuration

Business hours can be configured by defining the following:

- **Default Open/Close (as per Business Calendar)**: The status of the regular hours.
- **Force Open**: Force the status of Business Hours to Open with a reason code.
- **Force Closed**: Force the status of Business Hours to Closed with a reason code.
- **24x7** setting: Set the schedules for 24x7 working. Status is Always Open.
- **Special Hours & Holiday**: Configure a holiday or special day. On a holiday, you can close the Business Hours for the whole day or open it for specific hours. On a special day, you can configure extra working hours (in cases where 24x7 working is not set), the evaluation stops when the Special Hours & Holiday step is evaluated and the status is derived from this step. Further Business Hours setting for that day will not be evaluated.
- **Custom**: Configure the regular working hours for a weekday and, if necessary, specify the working hours for each day in a week.

The following variables control this feature:

- **Time Zone**: The line of Business or team's operational time zone.
- **Reason Code**: Reason code for special days and Force Open/Close status.

Apply the appropriate reason codes when you configure a Business Hour with **Force Open**, **Force Close**, and **Special Hours & Holidays**. When these Business Hour schedules are in effect, the associated reason code is available in the scripting environment and the real time reports. **Reason Code** configuration is not available for regular weekdays. In such cases, the system reports the default open and default close reason codes.

Configure Yearly Schedules

You can configure and maintain a Business hours calendar for the whole year.

- Configure the regular working hours for weekdays.
- Configure **Special Hours & Holidays** schedules for whole year by doing the following:
 - Add the **Special Hours & Holidays** details for all the special hours and holidays for the whole year into the CSV template file.
 - On the **Import Special Hours & Holidays** page, click **Choose File** and browse to the special hours and holidays file.
Click **Import** to upload the file.
After you import the configuration file, the configurations are loaded on the Business Hours page. Validate the configurations.
 - Click **Save**.



Note When you update the configured Business Hours, remove any elapsed schedules and then update the new schedules for any new special hours or holidays in a Business Hour configuration.

Daylight Saving Time

The Business Hours feature uses **Time Zone** to determine the status based on the Business Hours configured. **Time Zone** is set based on the local time. When the daylight saving time (DST) settings are applicable to any **Time Zone**, the status is automatically adjusted for DST.

When time zones are added or updated, the DST information changes. Apply all the Operating System (OS) updates related to time zones and DST, to both sides A and B of the deployment.

Business Hours Status Evaluation

The status is evaluated using the following order of the configured Business Hour settings:

1. Open/Close as per Business Calendar
2. Force Open or Close
3. Special Hours and Holiday schedule
4. 24x7 setting
5. Regular hour schedules

The evaluation terminates at the step at which the status is determined.

For example, if **Special Hours & Holidays** is configured, the evaluation stops when the **Special Hours & Holiday** step is evaluated and the status is derived from this step.

If any configuration is changed, the status is re-evaluated and updated to reflect the change.



CHAPTER 5

Call Transcription

- [Introduction, on page 51](#)
- [Prerequisites, on page 51](#)
- [Contact Center AI Services Task Flow, on page 52](#)
- [Enable or Disable Contact Center AI Services for Agents, on page 53](#)

Introduction

Unified CCE leverages Artificial Intelligence (AI) and Natural Language Understanding (NLU) to provide services that assist agents. These services are available for the agents in the Cisco Finesse desktop gadgets.

In the **Transcript** gadget, you can view in real-time, the voice conversation that was dynamically converted to text.

Prerequisites

The prerequisites for configuring Call Transcription are:

- Ensure Agent Answers is configured on a supported CUBE platform. For more details on supported CUBE platforms and configuration, see the WebSocket-Based Media Forking for Cloud Speech Services chapter in the *Cisco Unified Border Element Configuration Guide - Cisco IOS XE 17.6 Onwards* at <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/websocket-forking-for-cube.html>.
- The following components must be on release 12.6(2): CCE components (Router, Logger, AW, and PG), Cisco Finesse, Cisco Unified CVP, and Cloud Connect.



Note Ensure that the Unified CCE AW, Unified CCE OAMP, Cloud Connect, CUBE, and Agent Desktop components have access to Webex services to use the Call Transcription.

Contact Center AI Services Task Flow

Follow this procedure to enable the Contact Center AI (CCAI) Services that equips your Contact Center for Call Transcription Services.

-
- Step 1** Create a CCAI configuration in Cisco Webex Control Hub at <https://admin.webex.com>. A CCAI configuration leverages CCAI Connectors to invoke the CCAI services.
For details, see the [Create a Contact Center AI Configuration](#) article.
- Step 2** Ensure that the Cloud Connect publisher and subscriber are installed.
For more information, see the *Install Cloud Connect* section in *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html>.
- Step 3** Configure Cloud Connect in the CVP Operations Console (OAMP). For details see the section *Configure CVP Devices for Cloud Connect* in the *Administration 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>.
- Step 4** Register Cloud Connect in the Unified CCE Administration console to establish a secure and trusted communication channel between the Cisco Contact Center on-premises deployment and cloud services.
For details, see the *Cloud Connect Integration* section in the *Administration Guide for Cisco Unified Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-maintenance-guides-list.html>.
- Step 5** Import the Cloud Connect certificate to the CVP Server.
For details, see the section *Import Cloud Connect Certificate to Unified CVP Keystore* in the *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>.
- Step 6** In the Unified CCE Administration console, do the following with the CCAI configuration (created in step 1):
- To view and sync the Contact Center AI configuration which is associated with all call types as a global configuration, see [Associate Contact Center AI Configuration with All Call Types, on page 4](#).
 - To view, update, or delete the Contact Center AI configuration associated with a specific call type, see [Associate Contact Center AI Configuration with a Call Type, on page 5](#).
- Step 7** By default, the locale is set to English. To use languages other than English, in ICM Script Editor, set the **user.microapp.locale** variable to the language specified for your conversation profile. For example, set the value of the variable to "es-ES" for Spanish.
- Step 8** Provision Cloud Connect on Cisco Finesse.
For more information, see the *Cloud Connect Server Settings* topic in the *Cisco Finesse Administration Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html>.
- Step 9** To add the Call Transcript gadget to the Cisco Finesse desktop layout:
- Enable the Call Transcript gadget in Cisco Finesse Administration.
For details, see the *Manage Desktop Layout* section in the [Cisco Finesse Administration Guide](#).
 - Enable the Call Transcription service in Unified CCE Administration for an agent or multiple agents together.

For details, see [Enable or Disable Contact Center AI Services for Agents, on page 53](#).

Once enabled, the Call Transcript gadget appears on the Home tab. For details on how to use the gadget, see the [Contact Center AI Gadgets User Guide for Cisco Contact Center Enterprise](#).

Note Gadget auto-hide/un-hide and notifications capability is available only if the gadget is configured as a multi-tab gadget in Cisco Finesse. For more details, see [Configure Multi-Tab Gadget Layout](#) section in the [Cisco Finesse Administration Guide](#).

- Step 10** Perform the following steps to configure WebSocket-based forking in CUBE.
- Create a SIP profile and associate it at the dial-peer level in CUBE. For details, see [Create a SIP Profile at the Dial-Peer Level in CUBE, on page 8](#).
 - Import the WebSocket Connector certificate to CUBE. For details, see [Import or Verify WebSocket Connector Certificate to CUBE, on page 8](#).
 - Configure WebSocket-based forking in CUBE. For details, see the [WebSocket-Based Media Forking for Cloud Speech Services](#) chapter in the [Cisco Unified Border Element Configuration Guide - Cisco IOS XE 17.6 Onwards](#).
CUBE uses a WebSocket connection to fork the media streams of the agent and the caller towards the Webex CCAI Orchestrator service. For more details, see the Contact Center AI Services Considerations section in the [Solution Design Guide for Cisco Unified Contact Center Enterprise](#).

Enable or Disable Contact Center AI Services for Agents

Contact Center AI Services can be configured for each agent. Administrators and supervisors can enable or disable the services for an agent or multiple agents together.

Enable or Disable Contact Center AI Services for an Agent

This procedure explains how to enable or disable Contact Center AI Services for an agent.

-
- Step 1** In **Unified CCE Administration**, choose **Users > Agents**.
- Step 2** Click on the agent row whose services are to be modified.
- Step 3** Click the **Contact Center AI** tab.
Displays a list of services enabled or disabled for the agent.
- Step 4** To enable or disable the required Contact Center AI Services, check or uncheck the check boxes corresponding to the services.
- Step 5** Click **Save**.
-

Enable or Disable Contact Center AI Services for Multiple Agents

Administrators and supervisors can enable or disable Contact Center AI Services for multiple agents.

All agents must belong to the same site and the same department, or all agents must be global agents. The **Edit** button is disabled if:

- Agents from different sites, departments, or peripheral sets are selected.
- A mix of global and departmental agents are selected.

-
- Step 1** In **Unified CCE Administration**, choose **Users > Agents**.
- Step 2** Check the check box corresponding to each agent whose services you want to edit.
- Step 3** Click **Edit > Contact Center AI**.
The Edit Services dialog displays a list of services that are the service that is enabled or disabled.
- If the service is enabled for all the agents selected for editing, the check box is checked.
 - If the service is disabled for all the agents selected for editing, the check box is unchecked.
 - If the service is enabled for some agents and disabled for the others, the check box has a dash (—).
- Step 4** To enable or disable the Contact Center AI Services, check or uncheck the check boxes corresponding to the services.
- Step 5** Click **Save**, and then click **Yes** to confirm the changes.
-

Enable or Disable AnswersContact Center AI Services for Agents using Bulk Job

-
- Step 1** Navigate to **Unified CCE Administration > Overview > Bulk Import**.
- Step 2** Click **Templates**.
The **Download Templates** popup window opens.
- Step 3** Click the **Download** icon for the Contact Center AI template you want to use.
- Step 4** Click **OK** to close the **Download Templates** popup window.
- Step 5** Open the .csv template in Microsoft Excel.
- Step 6** Populate the file as described in the [Bulk Contact Center AI Services Content File, on page 7](#).
- Step 7** Save the populated file to the local machine.
- Step 8** Navigate to **Unified CCE Administration > Overview > Bulk Import**.
- Step 9** Click **New**.
- Step 10** In the optional **Description** field, enter up to 255 characters to describe the bulk job.
- Step 11** In the **Content file** field, choose the file to upload, and then click **Save**.
-

Bulk Contact Center AI Services Content File

The content file for Contact Center AI bulk job contains the fields given in the following table. Enter the values appropriately in the given fields to enable or disable Contact Center AI Services for the agents.



Note Bulk job is available for administrators only when Cloud Connect is added in the inventory and registered on the Control Hub.

Field	Required?	Description
agentId	Agent ID or Username	Existing agentId for which you want to enable or disable the Contact Center AI Services. You must provide either an agentId or the userName. If both are provided, agentId takes precedence over the userName. If the agentId value is left blank, the userName will reference an existing agent.
userName	Username or Agent ID	Username of the agent for which you want to enable or disable the Contact Center AI Services. If no agent is found with the given username, the Contact Center AI Services association fails.
agentServices	Yes (to enable Contact Center AI Services)	The type of Contact Center AI Services to be associated with the agent. Supported values are AgentAnswers and Transcript. To associate more than one services, separate the values using semicolon (;). If the value is updated, any existing enabled service gets overwritten. If the value is left empty, no service gets associated with the agent.



CHAPTER 6

Digital Channels Integration Using Webex Connect

- [Overview, on page 57](#)
- [Prerequisites, on page 57](#)
- [Redaction of sensitive data, on page 58](#)
- [Workflow for enabling and managing digital channel interactions, on page 59](#)
- [Generate public key certificate using Cisco IdS , on page 63](#)
- [Regenerate public key certificate using Cisco IdS, on page 63](#)
- [Reverse proxy configuration for digital channel interaction, on page 64](#)
- [ECC Variables for Digital Routing Tasks, on page 68](#)
- [Manage digital channels, on page 70](#)
- [Disposition codes for digital channel interaction, on page 79](#)
- [Agent Request or Web Callback using Webex Connect, on page 84](#)
- [Reporting, on page 88](#)

Overview

Today's customers want to connect with businesses through any communication channel of their choice. Webex Connect allows the Contact Center business and its customers to interact using digital channels such as email, chat, and SMS.

The Contact Center Enterprise (CCE) solution integrates with Webex Connect to create a seamless omnichannel experience for your customers. This integration helps your customers to interact across voice and digital channels of communication.

Webex Connect offers a rich self-service and bot integration to empower your customers to get answers to some common questions. It provides a unified solution for integrated routing, Agent Desktop, and reporting service. Webex Connect provides a simplified framework that helps partners and customers interact through digital channels.

Prerequisites

The following are the prerequisites for provisioning digital channels for Contact Center Enterprise:

- The following components must be on release 12.6(2) or higher: CCE components (Router, Logger, AW, and PG), Cisco Finesse, Cisco IdS, and Cloud Connect.
- Place an order for Digital service for your customer using Cisco Commerce Workspace (CCW). For more information, see the Cisco Collaboration Flex Contact Center Ordering Guide available at <https://www.cisco.com/c/en/us/partners/tools/collaboration-ordering-guides.html>.
- If you want your customers to reach you through SMS and if you are provisioning a US phone number for SMS communication, you must first procure a 10 Digit Long Code (10DLC), which is the mandated standard for Application-to-Person (A2P) text messaging. Work with your Account Manager to verify your business and set up your SMS Business account number. After you obtain the number, use it to configure the SMS contact handling. For instructions, see [SMS](#).
- Make sure that you enable the Single Sign-On (SSO) mode for agents who are required to handle digital channel tasks. To enable agents for SSO one at a time, use the configuration tools. To enable multiple agents at once for SSO, use the SSO migration tool. For instructions, see the *Migrate Agents and Supervisors to Single Sign-On Accounts* section in the [Cisco Unified Contact Center Enterprise Features Guide](#).
- Tokens created with Cisco IdS are used to authenticate CCE agents with Webex Engage. This necessitates synchronization of the time fields in the tokens between Cisco IdS and Webex Engage cloud services. As a result, the Cisco IdS NTP server configuration must be synchronized, either directly or indirectly, with a public NTP server that supports leap smearing in order for the premise and cloud NTP configurations to be in sync. Furthermore, when used with digital channels, the lifetime of a Cisco IdS token cannot be set to less than 2 hours.

Redaction of sensitive data

This feature redacts or masks all the sensitive data that you send over Webex Connect to ensure PCI compliance. The PCI service scans all your requests for sensitive data, masks the data, and sends it over to the Agent Desktop. The PCI service also scans the agent responses and sends the redacted data, including attachments that do not contain sensitive data, to the end customers.

The following are the supported file types on which the PCI service applies redaction:

Table 5: Supported File Types

Category	File Extension
Document	html, mhtml, mht, odt, pdf, pdfxml, rtf, shtml, xps, xml, xhtml, txt
E-mail	eml, msg
Microsoft	ods, doc, dohtml, docm, docx, docxml, dot, dohtml, dotx, dotm, pot, pohtml, ppthtml, pptmhtml, pptxml, potm, potx, pps, ppam, ppsm, ppsx, pptx, pptm, ppt, pub, pubhtml, pubmhtml, xls, xlshtml, xlhtml, xlt, xlsx, xltm, xlam, xlsb



Note Any file types that are not listed in the Supported File Types table are automatically dropped in the transmission. If there are any images in the attachments that are sent in the supported file types, the attachments are automatically dropped. For example, if your PDF file includes images, the file is automatically dropped in the transmission, even though PDF is a supported file type.

Workflow for enabling and managing digital channel interactions

As a partner, complete the following tasks to onboard your customer for Hybrid Services and provision the digital channel capabilities:



Note In some rare cases, the customer administrators can also perform the following tasks to provision the digital channel capabilities for their organization.

Table 6: Initial configurations to enable digital channel capabilities

Step #	Task	Reference
Onboard hybrid services for customers using Control Hub		
Note If your customer is already using a Hybrid Service such as CCAI, skip steps 1 and 2 in this section and directly start with provisioning the digital channel capabilities (step 3).		
1	Place an order for Digital service for your customer using Cisco Commerce Workspace (CCW), and your Contact Center subscription starts. Set up hybrid services for your customer.	See the Set up hybrid services for your organization .
2	(Optional) Create a user with Full Admin role to authorize task requests that are sent from Webex Connect to Contact Center Enterprise (CCE) through Cloud Connect.	<ul style="list-style-type: none"> • Add users manually in Control Hub • Assign organization account roles in Control Hub
3	Provision digital channels for your customer on Control Hub.	See the Provision Webex Connect digital services for your organization .
Integrate CCE and Webex Connect		
Part 1—Cloud Connect Configurations		
4	Install and add the Cloud Connect publisher and subscriber nodes to the inventory for your customer.	See the Install Cloud Connect section in the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide .

Step #	Task	Reference
5	Register Cloud Connect in the Unified CCE Administration portal.	See the <i>Cloud Connect Integration</i> section in the Administration Guide for Cisco Unified Contact Center Enterprise .
6	Configure the Media Routing Peripheral Interface Manager (MR PIM) for the Digital Routing service.	See the <i>Configure Peripheral Gateway Setup</i> section in the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide
7	Establish secure connections between Cloud Connect and Media Routing Peripheral Gateway (MR PG), and set up the Nginx reverse proxy server certificate for the digital channels interaction.	See the <i>Certificate Management for Digital Channels Integration</i> section in the Security Guide for Cisco Unified ICM/Contact Center Enterprise .
Part 2—Reverse Proxy Configurations		
8	Set up and configure reverse proxy server for the digital channel interaction.	See Workflow to configure reverse proxy using automated installer, on page 65 .
Part 3—CCE Configurations		
9	<p>Create a unique media routing domain (MRD) for each media channel and map it to your media channel if you want granular channel-specific reporting and agent state control. Use the Media Routing Domain List tool to create the MRDs.</p> <p>For Emails and asynchronous social chat channels like SMS, consider a longer Start Timeout and Max Duration for the Media Routing Domain.</p> <p>You can also map existing MRDs to the Digital Routing media channels. This will avoid having to create new skill groups, precision queues, and scripting logic changes to target the new media channels.</p>	<ul style="list-style-type: none"> • For instructions about how to create a new MRD, see the online help that is integrated with the Media Routing Domain List tool. • For instructions about how to map the existing MRDs to the Digital Routing media channels, see Set up media channels.

Step #	Task	Reference
10	<p>Associate the MRDs that you have created for the digital channel integration using Webex Connect to the system-defined application paths.</p> <p>For every agent peripheral gateway, there is a system-defined application path that gets created with a suffix "UQ.Desktop". There is also an associated system-defined application called UQ.Desktop that automatically gets created in the system and identifies the Cisco Finesse server as a client to the Agent PG, to control Agent states in MRDs created for digital channels. The first number in the application path identifies the Logical Controller ID of the PG. An example of the system-defined application path is 5000.UQ.Desktop.</p> <p>Note If you create the MRDs through the Unified CCE Administration portal, the MRDs get automatically associated to the system-defined application paths. If you have created the MRDs using the Media Routing Domain List tool under Configuration Manager, you must explicitly associate the MRD with the application path.</p>	See the online help that is integrated with the Application Path List tool
11	Create mandatory ECC variables in the Unified CCE Administration portal (Overview > Call Settings > Route Settings > Expanded Call Variables). The ECC variables are required to identify the incoming tasks as Digital Routing tasks and the tasks to carry the Webex Engage conversation ID.	<ul style="list-style-type: none"> • For instructions about how to create ECC variables, see the <i>Add and Maintain Expanded Call Variables</i> section in the online help that is integrated with the tool. • For the list of mandatory ECC variables, see the ECC Variables for Digital Routing Tasks, on page 68.
12	Configure digital channel capabilities for your customer in the Unified CCE Administration portal.	See Manage digital channels .
13	Create routing scripts for digital channel interaction.	See the <i>Example Scripts for Digital Channel Interactions Using Webex Connect</i> section in the Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise .

Step #	Task	Reference
14	(Optional) You can configure an Agent Request or Web Callback feature to allow your customers to place a web callback request to the contact center.	See Agent Request or Web Callback using Webex Connect , on page 84.
Part 4—Cisco Finesse Configurations		
Note Ensure that you complete all the prerequisites listed in the <i>Prerequisites to configure the Manage Digital Channels gadget</i> section in the Cisco Finesse Administration Guide before you proceed with Finesse configurations to set up the Manage Digital Channels gadget.		
15	Provision Cloud Connect on Cisco Finesse.	See the <i>Cloud Connect Server Settings</i> section in the Cisco Finesse Administration Guide .
16	Add the Manage Digital Channels gadget to the Cisco Finesse desktop layout.	See the <i>Add Manage Digital Channels Gadget</i> section in the Cisco Finesse Administration Guide .
Part 5—Webex Connect Configurations		
17	Configure node authorizations in Webex Connect to inject new tasks, retrieve a task's details, and close tasks directly on CCE.	See CCE Integration Nodes and Node Authorizations .
18	Configure channel assets for the required media channels such as SMS, Live Chat, and email.	See the following sections: <ul style="list-style-type: none"> • SMS • Live Chat • Email
19	Create flows using the Webex Connect Flow Builder feature for the various digital channels interactions such as SMS, Email, and Live Chat.	See Flow Configurations .
Part 6—Webex Engage Configurations		
20	Set up the customer chat widget.	See Administration and Setup Guide for Webex Engage with Cisco Contact Center Enterprise .
21	Verify that the agents who are enabled for digital channel interaction are synchronized to Webex Engage.	
Work with Manage Digital Channels gadget		
22	After you complete your initial configurations to enable digital channels interactions, the agents and supervisors can start interacting with customers using the Manage Digital Channels gadget.	See the Cisco Contact Center Enterprise Manage Digital Channels Gadget User Guide .

Generate public key certificate using Cisco IdS

The Manage Digital Channel gadget authenticates with Webex Engage in the Single Sign-On (SSO) mode, through tokens generated using public key cryptography. Use a secret private key to sign the tokens after which you can verify the tokens using a freely distributed public key certificate. Cisco Identity Service (IdS) generates the public and private keys that you can use to sign and verify the token. Cisco IdS exposes the CLI or REST interfaces to fetch the public key certificate for verifying the token. A public certificate authority (CA) must sign this public key certificate. You must then upload the CA signed public key certificate in Control Hub to authenticate and enable communication between Webex Engage and the Manage Digital Channel gadget.



Note You cannot use a self-signed certificate to provision digital channels in Webex Control Hub.

To generate the public key certificate:

-
- Step 1** Use SSH to log in to the Cisco IdS server's command line interface using the administrator credentials.
 - Step 2** Run the following CLI command to generate the Certificate Signing Request (CSR) that can be used to obtain a CA signed certificate:
show ids token csr—Displays the CSR corresponding to the public key that is used to validate the tokens.
 - Step 3** Copy the entire CSR including the header and footer (-----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----) from the Cisco IdS console and upload the same to the CA provided interface for generating the signed certificate.
 - Step 4** Save the contents of the CA provided certificate generated using the CSR in step 3, into a file with extension .pem or .der.

You must upload the certificate in Control Hub when you provision the Digital Channels for an Organization. For instructions, see [Provision Webex Connect digital services for your organization](#).

Note You need not upload the CA-signed certificate in the Cisco IdS server.

Regenerate public key certificate using Cisco IdS

To regenerate a public-private key pair:

Before you begin

You need to regenerate the public key certificate when the certificate is compromised, or when the CA-signed certificate or the Cisco IdS certificate expire. Regenerating the certificates for token signing requires all agents to logout and relogin to the Cisco Finesse desktop. Therefore, ensure that you plan for downtime to your Contact Center before you regenerate the public-private key pair that Cisco IdS uses to authenticate agents.

Step 1 Sign in to **Cisco Identity Service Management** using the following URL: `https://<hostname of Cisco IdS server>:8553/cmplatform`.

Step 2 From the left navigation pane, choose **Settings > Security > Keys and Certificates**.

Step 3 In the **Encryption/Signature Key** area, click **Regenerate**.

After you regenerate the new key pair, you must reboot Cisco IdS so that the agents can relogin to their applications. Ensure that a certificate authority signs the regenerated public-private key pair. You must reupload the CA signed certificate to the Control Hub for your agents to resume their tasks in the Manage Digital Channel gadget. For instructions, see [Provision Webex Connect digital services for your organization](#).

Reverse proxy configuration for digital channel interaction

A reverse proxy server is an intermediary server that you must deploy in the Demilitarized Zone (DMZ) in your network. The reverse proxy server forwards task requests and user configuration notifications from Webex Connect and Webex Engage to the Digital Routing and DataConn services respectively, that are running on the Cloud Connect platform. The task requests such as transfer and close that originate from Cisco Finesse are directly invoked on the Digital Routing service. The reverse proxy configuration enables automatic failover to the stand-by Cloud Connect in case of failures.

Reverse proxy deployment model

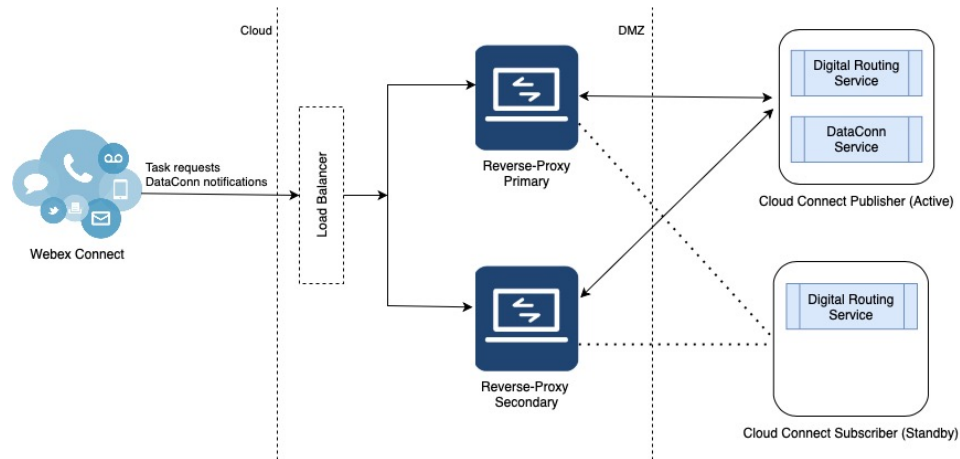
CCE supports the following two deployment models for reverse proxy:

- A pair of reverse proxy servers with physical load balancer.
- A pair of reverse proxy servers with DNS-based load balancer.



Note When using this deployment model with VPN-less Finesse, be sure to set up separate FQDNs for the reverse proxy servers so that Finesse desktop can access the specific reverse proxy IP addresses.

The following diagram depicts the task flow and the reverse proxy deployment model.



The following describes task requests and Dataconn flow:

- The Cloud Connect receives task requests from Webex Connect through either a single reverse proxy or a pair of reverse proxy servers deployed in the DMZ network, that is front-ended with a Load Balancer.
- The tasks are sent through reverse proxy only to the active side of Cloud Connect in both the deployment scenarios. That is, when a pair of reverse proxy servers are deployed, both the primary and the secondary reverse proxy servers are connected only to the active side of Cloud Connect.
- The active side of the Digital Routing service can either be on the publisher node or on the subscriber node of Cloud Connect. The following is the behaviour of the Digital Routing service and the DataConn service during failover:
 - The Digital Routing service supports automatic failover and all the task requests are routed through the Digital Routing service on the new active node.
 - The DataConn service runs only on the publisher node and does not failover to the subscriber node. As a result, when there are new users created in CCE, the user configurations are not synchronized in Webex Engage until the DataConn service on the publisher node is up and running.



Note The DataConn service is active only on the Cloud Connect publisher node.

Workflow to configure reverse proxy using automated installer

Complete the following tasks to configure reverse proxy using the automated installer for digital channel interaction:



Note For customers who've opted to set Country of Operation as Canada in Control Hub, you must install the reverse proxy shipped as part of [12.6\(2\) ES1](#). This is required to ensure that the traffic originating from the tenants hosted in that data center pass through to Cloud Connect. For a list of mapping between Country of Operation and Data Center, refer to <https://help.webex.com/en-us/article/n0p6xa1/Data-Locality-in-Webex-Contact-Center>.

-
- Step 1** Install and start the reverse proxy. For instructions, see [Reverse Proxy Automated Installer, on page 301](#).
- Note**
- Authentication is not supported at the edge of reverse proxy for all the requests and protocols that are related to digital channel interactions.
 - Configuration of mapping file is not required for digital channel interactions.
 - Configuration of Finesse is mandatory even if you want to install only Cloud Connect in your setup.
- Step 2** Configure the digital channel client hosts.
- a) Add the list of trusted digital channel client IP addresses and the corresponding hostnames to the reverse proxy Cloud Connect environment configuration file (cloudconnect.env). Use the variable, **NGX_CLOUDCONNECT_CLIENT_IPS** to add the IP addresses of Webex Connect and Webex Engage to the cloudconnect.env file.
- Note**
- The reverse proxy considers any requests as valid only if it receives requests from the configured hostnames or IP addresses. For more information about the environment configuration files, see [Configure deployment environment configurations, on page 315](#).
 - All the currently available IP addresses of Webex Connect and Webex Engage are already added in the 'cloudconnect.env' file. Depending on your deployed datacenter, remove any IP addresses that you do not need.
- b) Add load balancer or proxy IP addresses. For more information, see [Load balancer, WAF, and proxy support for reverse-proxy deployments, on page 249](#).
- Step 3** Configure the Mutual Transport Layer Security (mTLS) authentication between reverse proxy and Cloud Connect.
- a) Add the list of trusted reverse proxy IP addresses and the corresponding hostnames on the publisher and subscriber nodes of Cloud Connect. For details, see [Add Proxy IP, on page 66](#).
- b) Configure SSL certificate verification to establish communication between the reverse proxy host and the Digital Routing service. For details, see [Configure reverse proxy host verification, on page 67](#).
-

Add Proxy IP

You must add the list of trusted reverse proxy IP addresses and the corresponding hostnames on the publisher and subscriber nodes of Cloud Connect. The Cloud Connect nodes consider any requests as valid only if they receive the requests from the configured hostnames or IP addresses. Ensure that the allowed hosts contain only the internal and external FQDN and IP address of the reverse proxy.



Note Do not add the hostname or IP address of the load balancer.

The following is an example of the CLI to add the hosts and IP addresses:

```
admin:utils system reverse-proxy allowed-hosts add 10.78.95.178
Source 10.78.95.178 successfully added
admin:utils system reverse-proxy allowed-hosts add proxy.xyz.com
Source proxy.xyz.com successfully added
```

```
Restart Cisco Web Proxy Service for the changes to take effect: utils service restart Cisco
Web Proxy Service
```

If the added hostname is not resolvable from a component, the following error is displayed:

```
admin:utils system reverse-proxy allowed-hosts add xyz.com
```

```
Either IPv4 address or hostname is invalid or is not resolvable. Now validating IPv6 address
for source xyz.com
```

```
Operation failed, please enter valid source(s). Source xyz.com is invalid
```

After adding proxy hosts as trusted hosts through CLI on individual nodes, you must upload proxy server certificates to the Tomcat trust store of the respective components. This is required for proxy authentication to work. Otherwise, the traffic from proxy will be rejected by the components. For information about generating proxy certificates and uploading to the Tomcat trust store, see the *Set up Nginx reverse proxy certificate* and *Generate and Copy CA Certificates of VOS Components* sections in the [Security Guide for Cisco Unified ICM/Contact Center Enterprise](#).

The following is an example of the CLI to view the list of allowed hosts and IP addresses:

```
admin:utils system reverse-proxy allowed-hosts list
```

```
Source proxy.xyz.com successfully added list
```

The following source(s) are configured:

1. 10.78.95.178
2. proxy.xyz.com
3. proxy125.xyz.com

The following is an example of the CLI to delete an entry from the list of allowed hosts and IP addresses. This command lists all the configured proxy hosts and IP addresses, and gets user input to delete specific or all proxy hosts and IP addresses.

```
admin:utils system reverse-proxy allowed-hosts delete
Select the reverse-proxy source IP to delete:
```

- 1) 10.78.95.178
- 2) proxy.xyz.com
- 3) proxy125.xyz.com
- 4) all
- 5) quit

```
Please select an option (1 - 5 or "q" ): 1
```

```
Delete operation successful
```

Configure reverse proxy host verification

Reverse proxies are deployed in DMZ and are therefore security sensitive. So, the communication between the proxy and the upstream server that it is proxying, is recommended to be secured to a higher degree. This is achieved by having both the TLS certificates and the copy that is uploaded to the relevant servers be mutually verified. Run the following CLI commands on the publisher and subscriber nodes of Cloud Connect to configure SSL certificate verification for establishing communication between the reverse proxy host and the digital routing service:

utils system reverse-proxy client-auth

This command has the following parameters:

- enable
- disable
- status

By default, the host authentication is enabled.

The following is an example of the CLI to view the status of the host authentication:

```
admin:utils system reverse-proxy client-auth status
```

```
SSL certificate verification for connections established from reverse proxy hosts is disabled
```

The following is an example of the CLI to enable the host authentication:

```
admin:utils system reverse-proxy client-auth enable
```

```
SSL certificate verification enabled for connections established from reverse proxy hosts
```

Restart Cisco Web Proxy Service for the changes to take effect:

```
utils service restart Cisco Web Proxy Service
```

The following is an example of the CLI to disable the host authentication:

```
admin:utils system reverse-proxy client-auth disable
```

```
SSL certificate verification disabled for connections established from reverse proxy hosts
```

Restart Cisco Web Proxy Service for the changes to take effect:

```
utils service restart Cisco Web Proxy Service
```

Custom reverse proxy configuration

If you choose to not use the reverse proxy installer that Cisco has provided and want to deploy a custom reverse proxy, see [Guidelines for Custom Reverse Proxy Deployment, on page 375](#).

ECC Variables for Digital Routing Tasks

This section provides the list of ECC Variables that you must configure for the Digital Channel interaction. All ECC variables are of type scalar and they are case-sensitive.

Table 7: ECC Variables

Variable	Table Size	Length	Mandatory / Optional
user_DR_Primary	Used to hold the FQDN of either the publisher node or the subscriber node of Cloud Connect. The FQDN denotes the Digital Routing service node that injected the task into CCE.	1 character + the length of the Cloud Connect FQDN.	Mandatory

Variable	Table Size	Length	Mandatory / Optional
user_DR_Backup	Used to hold the FQDN of either the publisher node or the subscriber node of Cloud Connect. The FQDN denotes the peer node of the Digital Routing service, which can be used as a backup, in case the Primary node is unavailable.	1 character + the length of the Cloud Connect FQDN.	Mandatory
user_DR_MediaResourceID	Used to hold the Conversation ID of Webex Engage, which the Webex Connect injects. The Cisco Finesse uses this conversation ID to load the media in the Manage Digital Channels gadget.	16 characters	Mandatory
user_DR_CustomerName	Used to display the customer name in the pop-over notification that an agent views when a task is received in the Manage Digital Channels gadget.	Up to a maximum of 210 characters.	Optional

Variable	Table Size	Length	Mandatory / Optional
user_DR_MediaChannelName	<p>Used to populate the media channel name for the task, if you configure and add this ECC variable in the Unified Contact Center Enterprise Management portal. See the <i>Define ECC variables</i> section in the Cisco Unified Contact Center Enterprise Features Guide.</p> <p>This is typically required if you have mapped more than one Digital Routing media channel to the same MRD but still want unique task icons to appear on the agent desktop. For example, in CCE, the system-defined media channels, chat and SMS are both mapped to the same MRD. If there is a 1:1 mapping between the media channel and MRD, the system automatically identifies the icon to be displayed on the desktop based on the media channel with which the task was associated.</p>	8 character	Optional

- ¹ If there are lengthy FQDNs, the Digital Routing service compresses the FQDN such that it is below 100 characters, and thereby allow ECC variable some space out of the 2000 bytes limit per call / task to be saved by not having to send the long name. In such cases, the variable can be defined as 100 characters long in CCE. The Digital Routing service automatically fills in the first character to indicate whether the following data is compressed or uncompressed. A prefix of 1 denotes compressed data, while a prefix of 0 denotes uncompressed data.

Manage digital channels



Note To access this feature, ensure that you add Cloud Connect to the inventory in the Unified CCE Administration portal and register it.

As an administrator, perform the following configurations in the Unified CCE Administration portal to manage digital channel capabilities for your customers to reach business:

- Set up media channels such as chat, email, social, voice callback, . See [Set up media channels, on page 71](#).
- Synchronize agents in AW database to Webex Engage database. See [Configure User Sync, on page 74](#).
- Define Expanded Call Context (ECC) variables to assist agents with relevant information. See [Define ECC variables](#).
- Integrate Cloud Connect with Webex Connect using the Open Authorization v2.0 (OAuth v2.0) standard. See [Integrate Cloud Connect with Webex Connect](#) .
- Customize the connection parameters between Cloud Connect and MR PG. See [Manage connection between Cloud Connect and MR PG, on page 78](#).

Set up media channels

Contact Center Enterprise (CCE) supports media channels, such as Live Chat, Email, and SMS, with enhanced capabilities. These media channels are mapped to media type and Media Routing Domains (MRDs) for providing granular channel-specific reporting and agent state control. Based on this configuration, Cloud Connect associates the received task request to the appropriate MRD.

MRDs are used to map agents' skill group with the media channels, based on which the agents are assigned a task. You can map multiple media channels to the same MRD. For example, you can map SMS and Chat channels to the same MRD. For more information on MRDs, see the *Media Routing Domains* section in the [Configuration Guide for Cisco Unified ICM Enterprise](#).

Media type is a broad category of media channels and it is different from the media class or MRD in CCE. The Digital Routing service has internal sub-limits and different maximum queue time parameters that it applies for tasks of a certain Media Type as defined by the Queue Settings. The media types are **Chat**, **Email**, **Telephony** (Voice Callback), **Social**, , and .

Webex Connect offers support for the pre-provisioned system defined media channels. You can add a custom media channel if one of the many media channels that Webex Connect supports in the future has to be allowed in the CCE system. If not, you can skip adding a Media Channel.



Note System-defined media channels cannot be deleted.

Queue Settings for media channels is used to configure the maximum queue limit and maximum queue time for each media type, individually. For more information on configuring queue settings for media channels, see [Configure queue settings](#).

To set up media channels:

-
- Step 1** In the Unified CCE Administration portal, navigate to **Overview > Digital Channels > Digital Channel Settings > Media Channel**. The list of existing media channels is displayed in a grid. This is the default page.
- Step 2** Click **New**. On the **New Media Channel** page, do the following:
- a) In the **Name** field, type the name of the media channel.
 - b) From the **Media Type** drop-down list, select the required media type.

c) In the **Media Routing Domain** field, search and select the MRD that you want to map to the media channel.

Step 3 Click **Save**. The channel is added to the list on the **Digital Channel Settings** page.

When you have created a media channel, you can modify only the **Media Routing Domain** field. If you want to modify any other fields, you must delete the media channel and create afresh. To delete a media channel, hover over the media channel and click the **X** icon.

Configure queue settings

The Digital Routing service maintains a queue for all the incoming tasks. The service accommodates up to a maximum of 100,000 tasks in the queue at any given point in time. Out of these 100,000 tasks, you can configure the maximum number of tasks that can be queued for each media type in the Digital Routing service. The following are the default values in percentage for each media channel:

Media type	Queue setting in %	Description
Email	50%	50,000 tasks can be queued for Email.
Social	40%	40,000 tasks can be queued for SMS.
Voice callback	5%	5,000 tasks can be queued for Voice callbacks.
Chat	5%	5,000 tasks can be queued for live chat.

You can also define the maximum duration for which a task remains in the queue for each media type.

The following are the scenarios in which the Digital Routing service rejects the tasks and sends them back to Webex Connect:

- The number of tasks exceeds the maximum value that is configured for the media channel. For example, consider that the Digital Routing service queue has 50,000 email tasks, which is the maximum queue setting defined for the Email media channel. If Webex Connect further injects email tasks, the Digital Routing service rejects the incoming tasks and sends them back to Webex Connect with an error code of 20286 (MEDIA_TYPE_QUEUE_LIMIT_EXCEEDED). For example, a flow developer can decide to provide appropriate messaging to the end customer and invoke other backend systems to denote queue capacity issues.
- A task exceeds the maximum duration that is defined for the media channel. The Create Task node is successful. There is a Closed webhook event triggered when the task gets auto-closed after exceeding the maximum time in queue, with a specific disposition code set to CD_MAX_DIALOG_LIFETIME_EXCEEDED.

The flow debug logs show the error code returned by the Create Task node API call. For more information about the Create Task node, see [Create Task](#).

To configure the queue settings for the media channels:

-
- Step 1** In the Unified CCE Administration portal, navigate to **Overview > Digital Channels> Digital Channel Settings > Media Channel**.
- Step 2** Click **Queue Settings**.
- Step 3** Enter the required values in percentage for each media channel.
- Note** Make sure that the sum of the percentage values configured for all the media channels is 100.
- Step 4** Define the duration in days, hours, and minutes for each media channel. This is the maximum duration for which a task that belongs to the specific media channel remains in the queue after which it gets timed out. The default durations are 3 days for Email and Social media channels, and 2 hours for Voice callbacks and Chat media channels.
- Step 5** Click **Save**.
-

Synchronize CCE agents to Webex Engage

For CCE agents to be able to take up the digital channel tasks that are initiated from Webex Connect, the agent configuration details must be synchronized between the AW server and Webex Engage. The DataConn service that is running on the Cloud Connect platform is responsible for synchronizing agent configurations. The default periodic interval for synchronization is 30 minutes. Only the agent records created or updated during the synchronization period will be synchronized with Webex Engage.

The Finesse Desktop SSO login depends on the agent information that is synchronized between AW server and Webex Engage. The agent identity that is used to authenticate the login request, is possible only after this synchronization is complete.

Important considerations for agent synchronization

Consider the following when you synchronize agents between CCE and Webex Engage for the digital channel integration:

- After synchronizing the agents details between CCE and Webex Engage, if you delete an agent in CCE, the agent status in Webex Engage changes to Inactive. However, the agent record is not deleted in Webex Engage.
- The synchronization of agents details is possible only on the publisher node of Cloud Connect. Also, any update to the agent configuration takes effect only when the publisher node is up and running.
- Ensure that you create agents and update the agent configurations in CCE only. Do not create or update agent configurations in Webex Engage.
- Ensure that you always have the agent details synchronized between CCE and Webex Engage for the agents to be able to login to the Manage Digital Channels gadget.
- When you create a new agent in CCE, you must not associate the agent with an existing person record that is already associated with another agent. If you do not select any person record in the **Select Person** drop-down list in the **ICM Configuration Manager > Tools > Explorer Tools > Agent Explorer** tool, a new person record is automatically created for the agent. Also, you must not associate one person record with multiple agents.
- You must not modify the email address of the agent after the agent record and person record are created. If you need to update the email address, contact Cisco Support.

Enable agents for digital channels

To enable agents for digital channel interaction:

-
- Step 1** In the **Configuration Manager**, navigate to **Explorer > Agent Explorer**.
 - Step 2** Click on **Retrieve** button, and select the agent for whom you want to enable the digital channel interaction.
 - Step 3** Check the **Support Digital Channel** check box to enable the agent for digital channel interaction.
 - Step 4** Click **Save**.

Note You can perform the above task from the **List Tools>Person List** screen as well. For more information about List Tools, see the List Tools Online Help. Click the help button in List Tools to access the Online Help.

Configure SQL user account for digital channels

To configure SQL user account for digital channels:

-
- Step 1** Launch Microsoft SQL Server Management Studio using System Administrator login credentials on the Administration and Data Server.
 - Step 2** Navigate to **Security > Logins**, right-click **Logins** and select **New Logins**.
 - Step 3** On the General screen:
 - a) Enter the Login Name.
 - b) Select **SQL Server authentication**.
 - c) Enter and confirm the password.
 - d) Uncheck **Enforce password policy**.
 - Step 4** In the **Server Roles** page, check the **Public** check box.
 - Step 5** On the **User Mapping** page, do the following:
 - a) Check the **Real-time database** check box.
 - b) In the **Database role membership for** area, check the **db_datareader** check box.
 - Step 6** Click **OK**.
-

What to do next

Ensure that you configure SQL User Account on both the primary and secondary AW databases.

Configure User Sync

To synchronize the CCE agents who are configured for digital channel interactions with Webex Connect:

-
- Step 1** In the Unified CCE Administration portal, navigate to **Overview > Digital Channels> Digital Channel Settings > User Sync**.

Note The DataConn service is active only on the publisher node of Cloud Connect. Ensure that the publisher node is accessible for you to view the **User Sync** page.

Step 2 In the **Network Entry Point** field, enter the hostname or FQDN of the load balancer or the reverse proxy server based on your deployment. It is through this network entry point that the Webex Engage sends the response request to the DataConn service for agent synchronization.

For more information about network entry point, see the *Synchronize CCE agents to Webex Engage* section in the [Solution Design Guide for Cisco Unified Contact Center Enterprise](#).

Step 3 In the **AW Database Details** area, complete the following fields to configure the DataConn service for the Primary and the Secondary Server:

- a) In the **AW Datasource Host** field, enter the IP address or the host name of the AW server that has the agent configurations.
- b) In the **Port** field, enter the SQL port number of the AW database server.
- c) In the **Database Name** field, enter the name of the AW database server.
- d) In the **Database User ID** and **Password** fields, enter the user ID and password of the SQL user account that you created for digital channels. For more information see the *Configure SQL user account for digital channels* section in the [Cisco Unified Contact Center Enterprise Features Guide](#).

Step 4 Click **Test Connection** to make sure that the DataConn service can read the data from the AW Primary server.

Step 5 Switch on the **Enable Failover** toggle button to enable the failover to the Secondary AW server.

Step 6 To synchronize agents, choose one of the following options:

- a. Enable the **Enable Sync** toggle button to automatically synchronize agents in an interval of 30 minutes.
- b. Click **Sync Now** to manually synchronize the agents. This option is available only when the **Current Sync Status** field appears as **Scheduled**.

Note If you recreate your AW Database to fix any errors, ensure that you disable User Sync before starting with the recreation process. Enable the User Sync only after the AW Database is created and synchronized with the central controller database.

Step 7 In the **Last sync** field, view the date, time and status of the previous synchronization.

Step 8 In the **Agents Sync Details** field, view the number of agents that are synchronized successfully. The number of agents appears as a clickable link. Click the link to view the list of agent records that have failed to synchronize and the list of agent records that are pending for synchronization. You can choose to refresh the agent records at any given point in time.

Step 9 In the **Current Sync Status** field, you can view one of the following statuses:

- a. **No sync is in progress or scheduled**—This status appears when the **Enable Sync** toggle button is off.
- b. **Scheduled**—This status appears when the **Enable Sync** toggle button is on.
- c. **In Progress**—This status appears when the scheduled sync or manual sync is in progress.
- d. **Manual Sync Failed**—This status appears when the manual sync has failed.
- e. **Unknown**—When sync status is not available.

Step 10 Click **Save**.

Configure network entry point for agent synchronization using CLI

You must configure the network entry point for the DataConn service that is running on the Cloud Connect platform. It is through this network entry point that the Webex Engage sends the return request in response to the user configuration API request that the DataConn service sent to Webex Engage. For more information, see the *Synchronize CCE agents to Webex Engage* section in the [Solution Design Guide for Cisco Unified Contact Center Enterprise](#).

To configure the host for the network entry point, run the following command on the Cloud Connect console:

```
set cloudconnect dataconn settings
```

The following is the example of the CLI configuration:

```
admin:set cloudconnect dataconn settings
Fetching existing configuration...
Enter the Config details to be saved:
Network Entry Point Host: proxyhost.domain.com
The config details updated successfully.
```

To display the host that is configured for the network entry point, run the following command on the Cloud Connect console:

```
show cloudconnect dataconn settings
```

Field mapping between Webex Engage and CCE

Following table lists the payloads and attributes mapping between Webex Engage and the Contact Center Enterprise (CCE):

Webex Engage fields	CCE fields	Remarks
firstName	Person.FirstName	User's first name will contain only alphanumerics. All special characters from the given name will be removed. If this field is empty, the first name will be the username, which is obtained from the user's email without domain name.
lastName	Person.LastName	User's last name will contain only alphanumerics. All special characters from the family name will be removed. If this field is empty, the last name will be the first character of the username, which is obtained from the user's email without domain name.
aliasId	Person.LoginName	Agent's login name. Single Sign-On (SSO) authentication matches the Person.LoginName from AW database against the UPN or SamAccountName data from Cisco IdP and is used as the user_id in the SSO token. The Person.LoginName information is uploaded as aliasID in Webex Engage database for the purposes of token verification.
emailId	Person.Email	
loginId	Agent.SkillTargetID	Webex Engage uses this mapping to route the agent to the correct interaction.

Webex Engage fields	CCE fields	Remarks
concurrency	Not mapped	The Concurrency value is optional and is set to "99" by default on Webex Engage.
roleType	Fixed to customer_care	This is the fixed user role that is assigned to an agent.
status	Agent.Deleted	If a deleted flag is set in the CCE, the value is inactive.
loginUsingEmail	false	By default, every user on Webex Engage is created with the "loginUsingEmail" value as false.
role	team_agent	This is the fixed role that is assigned to team_agent.

Define ECC variables

The Expanded Call Context (ECC) variables are data that are embedded within the call and are visible to the agent on the Agent Desktop. ECC variables are passed back and forth in ECC payloads. ECC variables assist the agent with relevant information without the customer having to repeat the same information.

To define the ECC variables:

-
- Step 1** In the Unified CCE Administration portal, navigate to **Overview > Digital Channels > Digital Channel Settings > ECC Variable**.
 - Step 2** On the **ECC Variable** page, click the plus icon (+). The **Add ECC Variable** page appears with existing variables **Name** and **Enabled** details. It excludes the built-in variables.
 - Step 3** Select the required variable. The **ECC Variable** page displays the newly added ECC variable.
 - Step 4** Click **Save**.
-

Integrate Cloud Connect with Webex Connect

You can integrate Cloud Connect with Webex Connect using the Open Authorization v2.0 (OAuth v2.0) standard. You must configure Webex Connect client ID and client secret in the Digital Routing service for the service to gain access to Webex Connect using the access token. This set of client credentials uniquely identifies the Cloud Connect and its permissions to access Webex Connect.



Note The Cloud Connect Management service is active only on the publisher node of Cloud Connect.

To configure client credentials for OAuth v2.0 access token:

-
- Step 1** In the Unified CCE Administration portal, navigate to **Overview > Digital Channels > Digital Channel Settings > Integration**.
 - Step 2** On the **OAuth2 Authentication Details** page, perform the following steps.

- a) In the **Name** field, enter a name for the Cloud Connect integration. This field is editable.
- b) In the **Description** field, enter a description of what the client application does.
- c) In the **Client Id** and **Client Secret** fields, enter the client id and secret key that you can retrieve from the Webex Connect portal (navigate to **Assets > Integrations > CCE pre-built integrations > Actions > Manage**).
- d) In the field, enter the password that is provided to you at the time of registration. This is the secret key that was used for generating the token.
- e) Enter the access token URL that corresponds to the location of your Webex Connect tenant in the **Token Request URL** field.

For the list of access token URLs for various geographic regions, see the [Event Authorization](#) topic in the [Webex Connect Platform](#) documentation.

To find in which region your Webex Connect tenant is hosted, see the Tenant Domain column in the [Know Your API Endpoints](#) section in the [Webex Connect Platform](#) documentation.

- f) From the **Method** drop-down list, select the **POST** method for Webex Connect integration.
- g) From the **Content Type** drop-down list, select a media content type. This determines the response format. The available options are **application/json**, **application/xml**, and **application/x-www-form-urlencoded**. For Webex Connect integration, select **application/x-www-form-urlencoded**.
- h) In the **Access Token JSON path**, enter the path in the JSON response to fetch the value of the access token. For the Webex Connect integration, enter `access_token`.
- i) (Optional) In the **Header List** section, click + icon to add a header name and value and click **Add**. The header name and value are used to pass any additional information that Webex Connect may require for Cloud Connect integration.

Step 3 Click **Save** to save the OAuth2 authentication details.

Step 4 Go to the **Webhook** tab to register the Webhook URL in the Digital Routing service. To fetch the Webhook URL:

- a) In the Webex Connect portal, navigate to **Assets > Integrations**.
- b) In the CCE pre-built integrations row, from the **Actions** column, select **Manage**. The **Manage Integration - Prebuilt Integration** page appears.
- c) In the **Inbound Events** section, copy the Webhook URL.

Step 5 Paste the URL in the **Webhook URL** field in the Unified CCE Administration portal (**Overview > Digital Channels > Digital Channel Settings > Integration > Webhook**).

Manage connection between Cloud Connect and MR PG

To customize the connection parameters between Cloud Connect and Media Routing Peripheral Gateway (MR PG):

Step 1 In the Unified CCE Administration portal, navigate to **Overview > Digital Channels > Digital Channel Settings > Advanced Settings**.

Step 2 The **Port** is a display-only field and the default value is **38001**. It is through this port that Cloud Connect and MR PG communicates with each other.

Step 3 The **Secured** toggle switch is turned on by default. It is to establish a secured connection between Cloud Connect and MR PG. You can turn-off this toggle switch to disable the secure connection.

Step 4 Click **Save**.

Disposition codes for digital channel interaction

The Webhook notification that the Digital Routing service invokes for a closed task contains a disposition code that denotes the reason for the task closure. Using the disposition code in the Close Task, a flow designer can perform different actions as needed in the Webex Connect flow. For example, if a task fails after it has been queued, an error message can be displayed to customers with the option to contact the business through other support channels or schedule a callback, as opposed to a message indicating that the task has been closed due to a system error.

The following are the list of disposition codes that are available for digital channel interaction:

Table 8: Disposition Codes

Task Disposition	Disposition code value	Description
Normal End	CD_NORMAL_END_TASK	The task ended normally.
Transfer	CD_TASK_TRANSFER	This indicates the disposition when an agent initiates a task transfer using the Finesse desktop. The transfer operation triggers a Webhook notification to Webex Connect which would trigger another NEW task with the same TaskID using the Transferred workflow.
Transfer	CD_TASK_TRANSFERRED_ON_AGENT_LOGOUT	This occurs when Finesse server detects an Agent logout, or when the Agent closes the desktop while still having digital channel tasks that aren't completed or Closed yet. The Finesse server initiates a transfer of the task to the same script selector that routed the original task to the Agent.

Task Disposition	Disposition code value	Description
Transfer	CD_RING_NO_ANSWER	This indicates that the task timed out while waiting to be accepted by an Agent. Finesse invokes the TaskAction API with the Operation Code "Routed-Transfer" to redirect the task to another agent.
Transfer	CD_TASK_TRANSFER_TIMEOUT	The Digital Routing service sends a TRANSFERRED Webhook notification and waits for a maximum of 15 seconds for Webex Connect to complete its side of the processing, and for a create task request to be resubmitted from Webex Connect with the same TaskID. If Webex Connect fails to reinject the task into the Digital Routing service, then the Digital Routing service marks the task as Closed with this disposition code.
Task Lifetime Exceeded	CD_MAX_DIALOG_LIFETIME_EXCEEDED	The task ended because it exceeded the maximum task duration defined for the Media Routing Domain (MRD).
Customer Abandoned	CD_TASK_CUSTOMER_ABANDON	The disposition code is sent from Webex Connect when the task was abandoned by the customer before an agent was assigned to the task.

Task Disposition	Disposition code value	Description
Customer Abandoned	CD_TASK_ABANDONED_WHILE_OFFERED	The customer cancelled the task before the agent began working on the task. In this task disposition, the agent has viewed the offered task, but the dialog was deleted before the agent accepted the task.
Other	UNKNOWN	The reason for the task termination is unknown.
Other	CD_TASK_INVALID_MEDIA_RESOURCE_ID	The task gets closed by Finesse when the media can't be loaded in the Webex Engage widget. This depends on a mandatory ECC variable that is used by CCE to relay the Webex Engage ConversationID to Finesse desktop. This is to ensure that the media can be loaded in the widget, once the Agent selects the task.
Other	CD_TASK_ENDED_DURING_APP_INIT	This indicates that the task was in progress when the connection between the CTI server and Finesse went down, and the task ended before the connection was reinitialized. When the connection was reinitialized, the Agent PG ended the task.

Task Disposition	Disposition code value	Description
Failed Task Submission	CD_TASK_FAILED_SENDING_MR_REQUEST	This indicates that the task could not be sent to the MR PG owing to an error. The task is automatically marked as Closed with this disposition code.
Failed Task Submission	CD_FAILED_CREATING_NEW_TASK_EXECUTOR	Internal error in the Digital Routing service while processing a new task request. Such tasks get automatically closed with this disposition code.
Failure	CD_FAILED_INVALID_NEW_TASK_MESSAGE	The task failed as the new task message was invalid.
Failure	CD_FAILED_MEDIA_ROUTING_DISABLED	The task failed as the ICM media routing was disabled.
Failure	CD_FAILED_NO_SCRIPT	The task failed as there was no script to run.
Failure	CD_FAILED_INVALID_MRD_ID	The task failed as a result of invalid Media Routing Domain ID.
Failure	CD_FAILED_ICM_TIMEOUT	The task failed as a result of ICM timeout.
Failure	CD_FAILED_INVALID_SCRIPT_SELECTOR	The task failed as a result of invalid dialed number or script selector.
Failure	CD_FAILED_NO_TARGET	The task failed because there was no agent available to be assigned for the task.

Task Disposition	Disposition code value	Description
Failure	CD_FAILED_ROUTER_RELEASED_TASK	This disposition code is as a result of a Release Node being used in the CCE routing script to terminate the task purposely.
Failure	CD_FAILED_UNKNOWN_ROUTING_PROBLEM	The task failed as a result of unknown routing problem.
Failure	CD_FAILED_DUPLICATE_NEW_TASK_REQUEST	The task failed as it was a duplicate new task request.
Failure	CD_FAILED_UNSUPPORTED_SERVICE_REQUESTED	The task failed as the service requested was unsupported.
Failure	CD_FAILED_AGENT_NOT_MEMBER_OF_QUEUE	The task failed as agent not a member of the specified skill group of the precision queue.
Failure	CD_FAILED_INVALID_QUEUE_TYPE_OR_ID	The task failed as the specified Queue Type or ID. was invalid.
Failure	CD_FAILED_INVALID_DIALOG_ID	The task failed as the dialog ID was invalid.
Failure	CD_FAILED_INVALID_AGENT_ID	The task failed as a result of invalid agent ID.
Failure	CD_FAILED_AGENT_OVER_TASK_LIMIT	The task failed as the agent exceeded the task limit.
Failure	CD_FAILED_UNSUPPORTED_AGENT_PERIPHERAL_GATEWAY	The task failed as it was unsupported by the agent peripheral gateway for the service request.
Failure	CD_FAILED_INVALID_AGENT_STATE	The task failed as the agent state was invalid.

Task Disposition	Disposition code value	Description
Failure	CD_FAILED_INVALID_QUEUE_FOR_MRD	The task failed as a result of invalid queue for Media Routing Domain.
Failure	CD_FAILED_NO_PICK_PULL_NODE	The task failed as no pick pull node available.
Failure	CD_FAILED_AGENT_NOT_READY	The task failed as a result of agent not ready.
Failure	CD_FAILED_UNKNOWN	The session failed for unknown reason.
Failure	CD_FAILED_SESSION_ABANDON	The session failed as it was abandoned.
Failure	CD_FAILED_COMM_FAILURE_ROUTER_AND_PG	The communication failed as a result of router and PG failure.

Agent Request or Web Callback using Webex Connect

The Agent Request or Web Callback feature allows a customer to initiate a request on the web that results in a call from an agent. Use the Webex Connect platform to allow your customers to place a Web Callback request to the contact center. The customer needs to fill out a form with the preferred phone number to receive a callback as soon as an agent is available. Use this feature to switch between media channels when the wait time is more on a channel. For example, if the Live Chat media channel is experiencing an extended wait time, you can offer your customers an option to receive a voice callback from the contact center instead of the customer waiting in the Live Chat channel. The Webex Connect platform provides you the ability to route the web callback requests towards Contact Center Enterprise along with call variables and ECC variables that can carry customer-specific task context.

When CCE receives an agent request or a web callback request, it performs the following tasks:

- Processes the callback request.
- Routes the callback request to an agent and places a call from the agent's phone to the customer.
- Notifies the Webex Connect platform through a Closed Webhook notification that the agent has been selected.

The callback request is automatically closed from the Digital Routing service.

Agent Request Scenarios

1. From the web, the customer requests to speak to an agent.
2. The customer receives feedback that the request is accepted.

3. The customer receives feedback that the call is queued and the estimated wait time.
4. The customer receives feedback that a call is on its way.
5. The agent's phone places an outbound call.
6. The agent is presented with call context.

If	Then
The customer is available	The customer receives and answers the call, and speaks to the agent.
The customer is busy when the callback occurs	The agent receives a busy tone.
The customer does not answer when the callback occurs	The agent hears ringing.
The customer cancels the callback before an agent is selected	There is no impact on the agent.

Configure Web Callback

To configure a Web Callback request:

Table 9: Web Callback Configurations

Step #	Configure	Where	Configuration Details	Reference
1	Network VRU	Configuration Manager > Network VRU Explorer tool	Create a Type 2 Network VRU to queue voice callback tasks if an agent is not available to handle them.	For instructions about how to create a Network VRU, see the online help that is integrated with the Network VRU Explorer tool.
2	Network VRU script	Configuration Manager > Network VRU Script List tool	Add a Network VRU script that references the Network VRU that you created in step 1. Use the script for estimated wait time.	For instructions about how to create a Network VRU script, see the online help that is integrated with the Network VRU Script List tool.

Step #	Configure	Where	Configuration Details	Reference
3	Call Type	Configuration Manager > Call Type List tool	Create a call type to handle calls from an agent request voice callback.	For instructions about how to create a Call Type, see the online help that is integrated with the Call Type List tool.
4	Dialed Number / Script Selector	Configuration Manager > Dialed Number/Script Selector List tool	<ol style="list-style-type: none"> 1. Create a Script Selector corresponding to the Media Routing peripheral routing client that is used to integrate with Cloud Connect's Digital Routing service. Note The Webex Connect platform uses this script selector to request agents for voice callback. The script selector configured here must be the same as the one entered in the Webex Connect Platform. 2. On the Attributes tab, from the Media Routing Domain drop-down list, select Cisco_Voice 3. On the Dialed Number Mapping tab, map the script selector to the Call Type that you created in step 3. 	For instructions about how to create a Script Selector, see the online help that is integrated with the Dialed Number/Script Selector List tool.

Step #	Configure	Where	Configuration Details	Reference
5	Routing script	Script Editor	Create a routing script and schedule it for the Call Type that you created in step 3.	See the following sections in the Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise : <ul style="list-style-type: none"> • For instructions, see the <i>Create Routing Script</i> and <i>Schedule Routing Script</i> sections. • For a script example, see the <i>Example Digital Channel Interactions Using Webex Connect</i>.
6	ECC Variables	Configuration Manager > Expanded Call Variable List tool	Add one or more ECC variables for the callback request. Note Arrays are not supported with the Web Callback feature. The CCE solutions support the Latin 1 character set only for Expanded Call Context variables and Call variables.	For instructions about how to create a ECC Variable, see the online help that is integrated with the Expanded Call Variable List tool.
7	A representative flow using CCE Create Task node	Webex Connect > CCE Create Task	In the Media Type and Media Channel fields, select Web Callback .	For more information, see Create Task .

In the Unified CCE Administration portal, navigate to **Overview > Digital Channels > Digital Channel Settings > Media Channel**. You will see that the "Voice" media channel that has the **Media Type** field set as **Telephony** is associated with the "Cisco_Voice" MRD. For more information, see [Set up media channels](#), on page 71.

In the **Queue Settings** page, ensure that you have the right number of Web Callback requests (which by default is 5000 tasks) that you want to retain in the Digital Routing queue. For more information, see [Configure queue settings, on page 72](#).

Agent Targeting Rule for Web Callback

In addition to the above configurations, ensure that the Agent Targeting rule for the Agent Peripheral also applies to the MR PG routing client, which is required for the Digital Routing service, without which voice calls cannot be routed.

Reporting

Webex Connect reporting

You can view reports related to digital channel information from within the Webex Connect tenant. For more information, see [Reports](#).

View and download the following reports from Webex Connect:

- Count of inbound messages at a channel level
- Count of outbound messages to customers at a channel level
- Flow of tasks counts
- Other standard dashboard reports

Digital Routing reporting

The Cisco Unified Intelligence Center reports include data for voice calls and Digital Routing tasks.

For more information about multichannel reporting data, see the [Cisco Unified Contact Center Enterprise Reporting User Guide](#).

The Digital Routing media channels are mapped to MRDs and the Unified Intelligence Center reports can be filtered based on these mapped MRDs. Use the following All Fields and Live Data report templates to view the summary reports for each digital channel:

- Agent Real Time
- Agent Skill Group Real Time
- Peripheral Skill Group Real Time All Fields
- Precision Queue Real Time All Fields
- Agent Precision Queue Historical All Fields
- Agent Skill Group Historical All Fields
- Peripheral Skill Group Historical All Fields
- Precision Queue Abandon Answer Distribution Historical

- Precision Queue Interval All Fields
- Skill Group Abandon-Answer Distribution Historical
- Precision Queue - Live Data
- Skill Group - Live Data

Digital Routing task-level reporting

The task-level reporting is not available in Cloud Connect. Tasks in the Digital Routing service remain in the service memory only for 15 minutes after the tasks are closed. There is no persistence of closed tasks in the Digital Routing service. This 15-minute interval is a system setting and you cannot modify it.

The individual tasks that are escalated to CCE can be queried using the `Route_Call_Detail` (RCD) and `Termination_Call_Detail` (TCD). For more information see the *All Tables* chapter in the [Database Schema Handbook for Cisco Unified ICM/Contact Center Enterprise](#).



CHAPTER 7

Call Transcript

- [Feature Overview, on page 91](#)
- [Capabilities, on page 91](#)
- [Getting Started, on page 91](#)

Feature Overview

Call Transcript is an Enterprise Voice Assistant that provides advanced speech recognition and transcription to the Contact Center solution. When Call Transcript is integrated with the Contact Center solution, agents can view the live transcript of the call on their desktop. This transcript enables the agent to wrap-up the call quickly and ensures that the wrap-up notes are accurate and readily available for future reference.

This also enhances agent experience, reduces agent workload, and reduces the cost of Contact Center operations. The reduced wrap-up time increases agent productivity and makes tangible impact to the business.

Capabilities

The following benefits are derived when Call Transcript is integrated with the Contact Center solution:

- Availability of the call transcript with the agent on the desktop.
- Faster turn-around time to wrap-up the call by the agent.
- Agents can quickly prepare notes and summary for quick reference.
- Option to configure Hot words for easy reference.
- Search option on the transcript and notes to easily find relevant information.
- Quicker issue resolution.

Getting Started

This section explains the prerequisites, configuration task flow, and the documentation resources for Call Transcript. The call flow and design considerations for the Call Transcript feature are described in the *Unified*

CCE Solutions Design Guide at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html>.

Prerequisites

CUBE or Ingress gateway is required for sending media and SIP signals to the public IP of the Call Transcript service. For supported IOS versions for Call Transcript, 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>.

Configuration Task Flow

Table 10: Call Transcript Configuration Task Flow

Step	Component	Configuration	Link
Step 1	Call Transcript Service	Create a tenant for the customer.	Refer section <i>Create Manu</i>
Step 2	CUCM	Configure SIP trunk from CUCM to CVP (CVP is the recording server).	Refer section <i>Configure the</i>
		Enable agent phones for NBR media forking (gateway-preferred forking).	Refer section <i>Gateway Set</i>
Step 3	CUBE	Configure CUBE to route the calls coming from CVP to the Call Transcript Service.	Refer section <i>Configure C</i>
Step 4	Cloud Connect	Onboard the tenant created in Step 1 into the current deployment.	Refer section <i>Set CloudCon</i>
Step 5	Unified CVP	Integrate Cloud Connect from Cisco CVP NOAMP.	Refer section <i>Operations C</i>
		Import Cloud Connect certificate to CVP keystore.	Refer section <i>Operations C</i>
Step 6	Unified CCE	Configure ICM / CCE.	Refer section <i>Configuratio</i>
Step 7	Cisco Finesse	Configure Cloud Connect.	Refer section <i>Configure C</i>
		Configure Highlights.	Refer section <i>Highlight Cu</i>
		Configure Gadgets.	Refer section <i>Add Call Tra</i>

Documentation Resources

The following table lists the reference documents for Call Transcript:

Table 11:

Information	Resource
Design Considerations and Call Flow	<i>Unified CCE Solutions Design Guide</i> , https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html
Pre-Install Setup	<i>Unified CCE Solutions Features Guide</i> , Prerequisites, on page 92
Cloud Connect Configurations	<i>Unified CCE Configuration Guide</i> , https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html
CVP Integrations	<i>Unified CVP Administration Guide</i> , https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html
Desktop Application	<i>Cisco Finesse User Guide</i> , https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/tsd-products-support-series-home.html



CHAPTER 8

Contact Sharing

- [Contact Sharing Overview, on page 95](#)
- [Failover for Contact Sharing, on page 97](#)
- [Contact Director Installation and Setup, on page 97](#)
- [Set Up Contact Sharing, on page 102](#)
- [Scripting for Contact Sharing, on page 106](#)

Contact Sharing Overview

The Contact Sharing feature uses a Contact Director to distribute incoming contacts to up to 3 Unified CCE instances. The 3 instances can support a total of 24,000 active agents.

Contact Sharing uses extrapolation to distribute calls and increase the overall agent and call handling capacity. Contact Sharing enables customers with multiple Unified Contact Center Enterprise (Unified CCE) systems to distribute calls across those systems. The Contact Director (sometimes called an IVR ICM) acts as an initial entry point for the call. If the call needs agent attention, Contact Sharing decides where to route the call based on Live Data real-time state information from the Unified CCE target systems. You can configure Contact Sharing to base routing decisions on factors such as the number of calls in queue, agent availability, average handle time, and custom calculations.

Use Unified CCE Administration to create and maintain the Contact Sharing groups and rules. A group is a collection of skill groups and precision queues across target systems. Each group has a rule that defines the logic for selecting the best skill group or precision queue in that group for a routing request. Each group has an `Accept Queue If` condition to include or exclude the individual skill groups and precision queues from the group for the routing decision. You can then route the call to the Unified CCE target system whose precision queue or skill group is the best match for the group's rule. The target system's routing scripts determine the final method for handling the request.



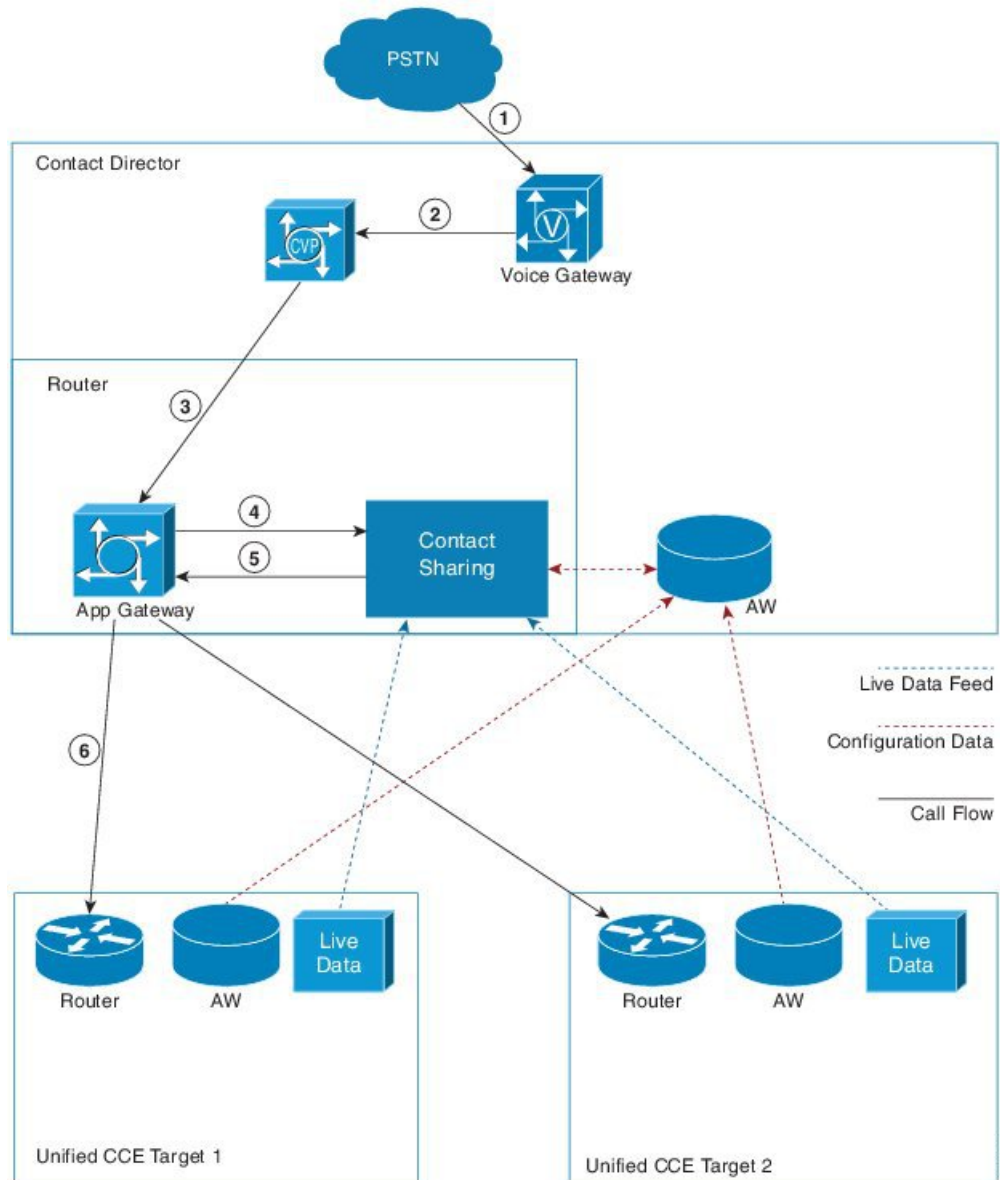
Note Contact Sharing gadgets are enabled only for the Contact Director deployment type.

For Contact Director configuration limits, see the chapter on configuration limits in the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html>.

Contact Sharing Call Flow

The basic Contact Sharing call flow runs as shown in this diagram:

Figure 6: Contact Sharing Call Flow



1. A call comes into the Voice Gateway on the Contact Director.
2. The Voice Gateway passes the call to CVP for VRU processing.
3. When the caller opts to speak to an agent, CVP passes the call data to the Router through the VRU PG.
4. The Router runs a script that assigns the call to a particular Contact Sharing Group. The Router sends the call data to the Application Gateway to pass to that Contact Sharing node.

5. The Contact Sharing node uses the Group Rule to determine which skill group or precision queue in its Queue should get the call. The node passes the selected target instance and its extrapolated guess of the best skill group or precision queue back to the Application Gateway.
6. The Application Gateway passes the information to the Router which routes the call to the selected target instance.

Failover for Contact Sharing

Like all the main components in Unified CCE, Contact Sharing nodes run in redundant pairs. The redundant pair operates in hot-standby mode. Side B's data is kept in sync with Side A to ensure minimum failover time.

When the Side A process fails over, Side B takes over routing. Because the nodes operate in hot-standby mode, Side B does not reread Queues from the database. Side B requests a snapshot from Live Data. Until the snapshot arrives, Side B continues routing based on the last available Live Data modified by the current extrapolated data.

During failover, some route requests may receive an error. Error handling sends those requests to the default route. When Side A comes back online, it does not take over immediately. Side A remains in a ready state until Side B fails over.

The Contact Sharing process monitors the AW to see whether it has the latest configuration changes. If the AW configuration database does not have those changes or is not accessible, the Contact Sharing process switches to the alternate AW configuration data source.

When core components fail over on a target instance, reporting data can occasionally zero out. In that case, the Contact Sharing routing sends calls to the instance with reported resources. If Live Data does not zero out reporting data, then Contact Sharing continues to route on stale data until the snapshot information begins to arrive. If the active Contact Sharing side loses both Live Data connections, that side goes inactive and fails over to other side.

Contact Director Installation and Setup

Contact Sharing runs on a Contact Director that you connect with up to three target Unified CCE deployments. You configure the Contact Director to monitor the Live Data feed from the targets. The task flow for installing a Contact Director is as follows:

Task	See
Ensure that virtual machines are ready for installation.	<i>Cisco Unified Contact Center Enterprise Installation and Upgrade Guide</i>
Install Unified Communications Manager.	<i>Installation Guide for Cisco Unified Communications Manager and IM and Presence Service</i>
Install Unified CCE components (Router, Logger, Administration & Data Servers, peripherals).	<i>Cisco Unified Contact Center Enterprise Installation and Upgrade Guide</i>
Optionally, install Cisco Unified Intelligence Center.	<i>Installation and Upgrade Guide for Cisco Unified Intelligence Center</i>

Task	See
Install Unified CVP.	<i>Installation and Upgrade Guide for Cisco Unified Customer Voice Portal</i>

Install Unified CCE

This section expands the installation process outlined in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html>.

After setting up the VMs for the Contact Director, you install the Unified CCE components. The install and configuration of a Contact Director varies slightly from a Unified CCE deployment. The following table lists the applicable parts of the Unified CCE install procedures with any necessary changes for the Contact Director:

Task	Steps	Contact Director Notes
Install Unified CCE Component Software (running the ICM-CCEInstaller)	—	—
Set up Organizational Units	Add a Domain	—
	Add Organizational Units	—
	Add Users to Security Groups	—
Set Up Unified CCE Central Controller Components	Add Unified CCE Instance	—
	Create Logger Database	Select NAM .
	Create HDS Database	—
	Add Logger Component to Instance	Choose Hosted > Network Application Manager (NAM) for the Logger Type .
	Add Router Component to Instance	Set the following values for a Contact Director: <ul style="list-style-type: none"> • Check Enable Remote Network Routing. • Set the NAM ID. • Check Contact Sharing when you create the Router.
Add Administration & Data Server Component to Instance	For a Contact Director, choose Hosted > Network Administration & Data Server for Network Application Manager (NAM) for the Deployment Type .	

Task	Steps	Contact Director Notes
Set up Peripheral Gateways	Configure Peripheral Gateways	—
	Add Peripherals to Peripheral Gateways	—
	Set Up Peripheral Gateways	—
After completing the standard installation, perform these Contact Director-specific setup procedures.		
Application Gateway Access Between Systems	Create Unified ICM Application Gateway	—
	Create an INCRP on Each Target Instance	—
	Set Application Gateway Default Values	—

Application Gateway Access Between Systems

The Contact Director uses a type of Unified ICM Application Gateway to access a target instance. After adding the components to the target instance, set up a Unified ICM Application Gateway in the Configuration Manager on the Administration & Data Server.

After setting up the Unified ICM Application Gateway, you can reference it with a Unified ICM Remote ICM node in a routing script on the Contact Director.

Create Unified ICM Application Gateway

This procedure creates a Unified ICM Application Gateway on the Contact Director. You also need an application gateway on each target Unified CCE system.

Step 1 Open the **Configuration Manager** on an Administration & Data Server that your Contact Director uses.

Step 2 Select **Tools > List Tools > Application Gateway List**.
The **Application Gateway List** window appears.

Step 3 Click **Retrieve**.

Step 4 Click **Add**.
The **Attributes** tab appears.

Step 5 Specify the following values on the **Attributes** tab:

Field	Description
Name	A name for the Unified ICM Application Gateway
Type	Select Remote ICM .
Preferred Side	Indicates the preferred side of the Application Gateway to use when both are available. If only one side is available, that side is always used. This option applies only for

Field	Description
	Custom Gateways. For Remote ICM systems, a suffix on the connection address indicates the preference.
Encryption	Indicates whether requests to the Application Gateway are encrypted. Select None .
Fault Tolerance	Specify the fault-tolerance strategy that the Application Gateway uses.
Connection	Select Duplex .
Description	Any additional information about the Unified ICM Application Gateway.

Step 6 Save your changes to create the Unified ICM Application Gateway.

Note Copy down the Unified ICM Application Gateway ID value. You use the ID when you set up the INCRP NIC on the target instance.

Step 7 Select either of the **Connection** tabs to set the connection information.

Step 8 Click **Enter Address**.

The **Enter Contact Director Address** dialog appears.

Step 9 Specify the following information:

Field	Description
IP Address/Name	Enter the Public (high priority) IP address of the target instance. Alternatively, You can use the SAN with assistance from your Cisco certified partner or TAC. Use the <i>same address</i> that you specified for the INCRP NIC on the target instance. You can use the hostname in place of the address.
Instance Number	Enter the number of the customer ICM on the target instance (0 — 24).
Side	<p>Indicate which side of the Contact Director prefers this connection:</p> <ul style="list-style-type: none"> • Side A—Contact Director Side A prefers to use this connection. • Side B—Contact Director Side B prefers to use this connection. • None—Neither side of the Contact Director prefers to use this connection. • Both Side A and B—Both sides of the Contact Director prefer to use this connection. <p>Note Use this setting to avoid unnecessary WAN traffic. For example, if you collocate Contact Director Side A with target instance Side A, this correct choice avoids WAN traffic to the other side.</p>

Note The **Enter Contact Director Address** dialog displays different fields depending on the type of Application Gateway chosen.

Step 10 Repeat this process for the other side of the redundant pair.

Step 11 Save your work and exit the dialog.

Create an INCRP on Each Target Instance

The Contact Director communicates with the target instance by an INCRP NIC. Perform this procedure on each target instance.

Step 1 From the Configuration Manager menu on the target instance, select **Tools > Explorer Tools > NIC Explorer**. The **NIC Explorer** window appears.

Step 2 In the **Select Filter Data** box, click **Retrieve**.

Step 3 Select a NIC or click the **Add NIC** button to create a new NIC.

Step 4 Specify the following values on the **Logical Interface Controller** tab:

Field	Description
Name	An enterprise name that serves as the NIC name.
Client Type	Select INCRP .

Step 5 Click the **Add Physical Interface Controller** button. The Physical Interface Controller dialog displays.

Step 6 Specify an **Enterprise Name** and click **OK**.

Step 7 In the NIC tree window, click the routing client for your newly created NIC.

Step 8 Specify the following values on the **Routing Client** tab:

Option	Description
Name	An enterprise name that serves as the Routing Client name.
Configuration Parameters	/customerID <RCID> where <RCID> is the Routing Client ID of the matching routing client on the Contact Director.
Network Routing Client	The same value as the Name field.

Step 9 Click **Save**.

The newly defined NIC is saved in the database. A **Physical Controller ID** is assigned, and the **To Be Inserted** icon is removed from the tree window.

Set Application Gateway Default Values

If you see performance issues, the Cisco Technical Assistance Center might advise you to change some of the application gateway's default values. Use the following procedure to change these values.

Step 1 In the **Configuration Manager**, select **Enterprise > System Information > System Information**. The **System Information** dialog appears.

Step 2 In the **Application Gateway** section, select **Remote ICM**.

Step 3 Use the other tabs to set the default values for the Unified ICM Application Gateway connections. Take account of the Contact Director NIC settings for timeout, late, and so on as you set the Unified ICM Application Gateway timeout settings for a target Unified CCE system.

Step 4 Click **OK** and close the dialog.

Install Cisco Unified Intelligence Center (Optional)

To run the Contact Sharing reports at the Contact Director site, you can install Cisco Unified Intelligence Center there. For installation procedures, see the *Installation and Upgrade Guide for Cisco Unified Intelligence Center* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html>.

Install Unified CVP

The Contact Director uses Unified CVP for VRU processing of the incoming calls. For installation procedures, see the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html>.



Note The Unified CCE Reference Designs specify that you use Unified CVP. In a non-Reference Design deployment, you can alternately use Unified IP IVR or a third-party VRU.

Set Up Contact Sharing

After installing the Contact Director and connecting the Contact Director to the target Unified CCE instances, you set up the contact sharing feature as follows:

Task	See this Topic
Set up the contact sharing node on the Contact Director.	Set Up a Contact Sharing Node
Set up the machine inventory for the contact sharing node.	Set up Contact Sharing Machine Inventory
Add contact sharing rules.	Add and Maintain Rules
Add contact sharing groups.	Add and Maintain Groups



Note Your solution can only have one contact sharing node.

Set Up a Contact Sharing Node

You set up a contact sharing node, as opposed to the target instances, with the same procedure for setting up an application gateway.

Step 1 In the Configuration Manager, select **Tools > List Tools > Application Gateway List**. The **Application Gateway List** window appears.

Step 2 To enable **Add**, click **Retrieve**.

Step 3 Click **Add**. The **Attributes** tab appears.

Step 4 Fill out the **Attributes** tab as follows:

Option	Description
Name	Name of your contact sharing node
Type	Contact Share

Note The remaining fields are preset and cannot be modified.

Step 5 On the **Connection Side A** tab, set the **Address** field to the router's IP address. The default port is 5070.

Step 6 On the **Connection Side B** tab, set the **Address** field to the router's IP address. The default port is 5070.

Step 7 Click **Save** to create the contact sharing node.

Set up Contact Sharing Machine Inventory

You set up the machine inventory for contact sharing through the `icm/bin/csMachineInventory.csv` file. Changes to the machine inventory do not take effect until the router restarts.

Step 1 Open your machine inventory file for contact sharing, by default `csMachineInventory.csv`.

Step 2 Follow the instructions for editing the `csMachineInventory.csv` file. The instructions are contained within the file.

Step 3 Run the following command:

csMachineInventory.bat *[options] username password inputfile*

options: /list, /help, /config

`/list` - This option lists the contact sharing machine inventory.

`/help` - This option displays the usage of the tool.

`/config` - This option configures the contact sharing machine inventory based on the input file.

username

Username for the REST API request

password

Password for the REST API request.

inputfile

Machine inventory file, including the path, for contact sharing, by default `csMachineInventory.csv`

What to do next

If the router has already started, restart the router after setting up the machine inventory.

Add and Maintain Rules



Note Contact Sharing comes with a default rule that cannot be deleted or modified. The name of this rule is **DefaultRule**.

Step 1 Navigate to **CCE Web Administration > Feature > Contact Share Rules**.

Step 2 Click **New** to open the **New Rule** window, or click an existing rule to open the **Edit Rule** window.

Step 3 Complete the following fields:

Field	Required	Description
Name	Yes	Enter a name using up to 32 alphanumeric characters, periods (.), and underscores (_). The name must start with an alphanumeric character.
Expression	Yes	Enter a formula that the Contact Share server uses to select the skill group or precision queue from a Contact Sharing group for a routing request.
Description	No	Enter up to 255 characters to describe the rule.

Step 4 Click **Save** to return to the List window.

Step 5 To delete a rule, do one of the following:

- To delete a single rule, hover over the row for that rule and click the **trash can** icon at the end of the row.
- To delete up to 50 rules, check the check box for each rule that you want to delete. To select all rules in a list, check the **Select All** check box in the list header. Click **Delete**.

Deleting a rule is permanent.

Add a New Rule by Copying an Existing Rule

You can also create a new rule by copying an existing rule. The **Description** and **Expression** fields are copied to the new rule.

Step 1 Navigate to **Unified CCE Administration > Feature > Contact Share Rules**.

Step 2 Either:

- Click the rule you want to copy, and then click the **Copy** button in the **Edit Rule** window.
- Hover over the row for that rule, and click the **copy** icon that appears at the end of the row.

The **New Rule** window opens.

- Step 3** Enter a **Name** for the rule, using up to 32 alphanumeric characters, periods (.), and underscores (_). The name must start with an alphanumeric character.
- Step 4** Review **Description** and **Expression** fields that were copied from the original rule, and make any necessary changes.
- Step 5** Click **Save**.

Add and Maintain Groups

Before you begin

Ensure that the Live Data connection is active before you configure Groups.

- Step 1** Navigate to **CCE Web Administration > Feature > Contact Share Groups**.
- Step 2** Click **New** to open the **New Group** window, or click an existing group to open the **Edit Group** window.
- Step 3** Complete the following fields:

Field	Required	Description
Name	Yes	Enter a name using up to 32 alphanumeric characters, periods (.), and underscores (_). The name must start with an alphanumeric character.
Description	No	Enter up to 255 characters to describe the group.
Rule	Yes	Select a rule that defines the logic for selecting a skill group or precision queue in this group for a routing request: <ol style="list-style-type: none"> a. Click the magnifying glass icon to display the Select Rule window. b. Click the row to select a rule.
Accept Queue If	No	Enter a logical expression to determine if the individual skill groups and precision queues in the group can be included in the routing decision.

- Step 4** Complete the Queues tab:
- This tab shows the list of queues for this group.
- a) Click **Add** to open **Add Queues**.
 - b) Click the queues you want to add to this group. The queues you chose appear on the **List of Queues**.
 - c) Close **Add Queues**.
 - d) Click **Save** on this tab to return to the List window.

Note The maximum number of queues is 100.

- Step 5** To delete a group, do one of the following:
- To delete a single group, hover over the row for that group and click the **trash can** icon at the end of the row.

- To select all groups in a list, check the **Select All** check box in the list header. Click **Delete**.

Deleting a group is permanent.

Scripting for Contact Sharing

Expression Formula for Contact Sharing

About Contact Sharing Expression Formula

You can enter expressions for the following fields:

Field	Description
Accept Queue If for a group	A logical expression to determine whether to include the individual skill groups or precision queues in the Contact Sharing group in the routing decision. The field is a freeform editor with a maximum length of 512 characters. Any result except zero evaluates as TRUE. There is an implicit Accept Queue If of <code>Queue.*.LoggedOn > 0</code> . You cannot override this implicit check.
Expression for a rule	A formula that the Contact Share server uses to calculate the value to be considered against other queues in a Contact Sharing group. The expression always selects the queue with the minimum value. The field is a freeform editor with a maximum length of 512 characters.

Contact Sharing Expression Format

To evaluate all the skill groups and precision queues in a Contact Sharing group, use this syntax:

```
Queue.*.<FieldName>
```

Where *FieldName* is the name of the field that the expression evaluates, for example, *Ready*.

To evaluate a specific skill group or precision queue, use this syntax:

```
<ObjectType>.<InstanceName>/<TargetQueueName>.<FieldName>
```

- *ObjectType* must be *SkillGroup* or *PrecisionQueue*.
- *InstanceName* is the application gateway name.
- *TargetQueueName* is the enterprise name of the skill group or precision queue in the target system.
- *FieldName* is the name of the field that the expression evaluates.

Contact Sharing Expression Examples

The following examples demonstrate some basic Contact Sharing expressions.

Expression for a Group

A Contact Sharing group can take an Accept Queue If expression. The expression determines whether to include specific skill groups and precision queues in the group in the routing decision.

```
Queue.*.Avail > 5
```

This expression accepts all queues with more than five agents that are available.

Expression for a Skill Group

```
SkillGroup.<InstanceName>/<TargetQueueName>.Avail > 5
```

This expression accepts the named skill group if it has more than five agents available.

Expression for a Precision Queue

```
PrecisionQueue.<InstanceName>/<TargetQueueName>.Avail > 5
```

This expression accepts the named precision queue if it has more than five agents available.

Expression for a Rule

A rule must take an expression. The expression selects a skill group or precision queue from a Contact Sharing group.

```
-1 * (Queue.*.Avail)
```

This expression selects the queue with the most available agents.

Expression for MED Only

This expression calculates the Minimum Expected Delay (MED) to determine which target system receives the call for routing.

```
(Queue.*.QueuedNow+1) * (Queue.*.AvgHandledCallsTimeToInterval>0?  
Queue.*.AvgHandledCallsTimeToInterval: 120) / (Queue.*.Ready>0?Queue.*.Ready:1)
```

The Default Rule

Contact Sharing comes with a default rule. You cannot modify or delete the default rule. The default rule combines a MED calculation with an Agent Occupancy calculation to determine which target system receives the call for routing.

If there are calls in queue,

```
Queue.*.QueuedNow > 0?
```

Then use the MED calculation:

```
((Queue.*.QueuedNow+1) * (Queue.*.AvgHandledCallsTimeToInterval>0?  
Queue.*.AvgHandledCallsTimeToInterval: 120) / (Queue.*.Ready>0?Queue.*.Ready:1)):
```

Otherwise, use the Agent Occupancy calculation:

```
((Queue.*.LoggedOnTimeToInterval - Queue.*.NotReadyTimeToInterval)==0  
|| (Queue.*.AvailTimeToInterval <= 10 * Queue.*.XAvail) )?  
0: -1 * (Queue.*.AvailTimeToInterval - 10 * Queue.*.XAvail) /  
(Queue.*.LoggedOnTimeToInterval - Queue.*.NotReadyTimeToInterval)
```

This expression chooses a queue on the target instance with the least occupied agents or the least queued calls.



Note The default rule is only an example. Customize the rule to match your needs or write your own rules.

Contact Sharing Expression Reference

Supported Operations

The following table lists the supported operations:

Type of Operation	Operator	Description
Conditional	&&	Conditional-AND
		Conditional-OR
	? :	Ternary (shorthand for if-then-else statement) ex. A ? B : C If A, then B, otherwise C.
Relational	==	Equal to
	!=	Not equal to
	>	Greater than
	>=	Greater than or equal to
	<	Less than
	<=	Less than or equal to
Bitwise and Bit Shift	~	Unary bitwise complement
	<<	Signed left shift
	>>	Signed right shift
	&	Bitwise AND, for strings, also used for string concatenation
	^	Bitwise exclusive OR
		Bitwise inclusive OR
Arithmetic	+	Addition
	-	Subtraction
	*	Multiplication
	/	Division
	%	Percentage

Type of Operation	Operator	Description
Prefix	+	Unary plus operator; indicates positive value
	-	Unary minus operator; negates an expression
	!	Logical complement operator; inverts the value of a boolean
Wildcard	*	Wildcard support similar to the expression used in router. For example, in <code>SkillGroup.*.Ready</code> , the actual target replaces the asterisk when applying the expression.

Supported Objects and Fields

The following table lists the fields available from the Live Data feed or calculated by Contact Sharing for use in Contact Sharing expressions:

Field Name	Description
ApplicationAvailable	The number of agents belonging to this Queue who are currently ApplicationAvailable for the MRD to which the Queue belongs. An agent is Application available if the agent is Not Routable and Available for the MRD.
Avail	The extrapolated number of agents in the READY state for this Queue. The extrapolation is as follows: (The number of agents that Live Data reports in READY state) - XAvail If the extrapolation results in a negative number, Contact Sharing sets this field to zero.
AvailTimeToInterval	Total seconds agents in the Queue have been in the READY state during the current interval.
AvgHandledCallsTimeToInterval	Average handle time in seconds for calls counted as handled by the Queue during the interval.
BusyOther	Number of agents currently in the BusyOther state for this Queue.
CallsHandledToInterval	Calls that by been answered and have completed wrap-up by the Queue during the interval.
Hold	The number of agents that have all active calls on hold.
ICMAvailable	The number of agents belonging to this Queue who are currently ICMAvailable for the MRD to which the Queue belongs. An agent is ICM available if the agent is Routable and Available for the MRD.
LoggedOn	Number of agents that are currently logged on to the Queue.
LoggedOnTimeToInterval	Total time, in seconds, agents were logged on to the Queue during the current interval.

Field Name	Description
NotReady	Number of agents in the Not Ready state for the Queue.
NotReadyTimeToInterval	Total seconds agents in the Queue have been in the Not Ready state during the interval.
QueuedNow	The extrapolated number of calls currently queued to this Queue. The extrapolation is as follows: (The number of calls that Live Data reports queued to the Queue) + XQueuedNow
Ready	The number of agents who are Routable for the MRD associated with this Queue, and whose state for this Queue is not currently NOT_READY or WORK_NOT_READY.
ReservedAgents	The number of agents for the Queue currently in the Reserved state.
TalkingAutoOut	The number of agents in the Queue currently talking on AutoOut (predictive) calls.
TalkingIn	The number of agents in the Queue currently talking on inbound calls.
TalkingOther	The number of agents in the Queue currently talking on internal calls, rather than inbound or outbound calls. Examples of other calls include agent-to-agent transfers and supervisor calls.
TalkingOut	The number of agents in the Queue currently talking on outbound calls.
TalkingPreview	The number of agents in the Queue currently talking on outbound Preview calls.
TalkingReserve	The number of agents in the Queue currently talking on agent reservation calls.
WorkNotReady	The number of agents in the Queue in the Work Not Ready state.
WorkReady	The number of agents in the Queue in the Work Ready state.
XAvail	The number of Contact Sharing requests assigned to the available agent count for this Queue during the extrapolation period. The extrapolation period defaults to 10 seconds. Contact Sharing request increments this field when QueuedNow = 0 and Avail > 0.

Field Name	Description
XQueuedNow	<p>The number of Contact Sharing requests assigned to the queued call count for this Queue during the extrapolation period. The extrapolation period defaults to 10 seconds.</p> <p>Contact Sharing request increments this field when one of the following conditions apply:</p> <ul style="list-style-type: none"> • QueuedNow = 0 and Avail = 0 • QueuedNow > 0 and Avail = 0 • QueuedNow > 0 and Avail > 0

The following table lists the Call Variables that are available for use in Contact Sharing expressions:

Call Variable Name	Description
CallerEnteredDigits	Digits caller entered in response to prompts.
CallingLineID	Billing phone number of the caller. (Commonly referred to as CLID).
CustomerProvidedDigits	Digits to be passed to the call recipient.
DialedNumberString	Phone number dialed by the caller.
PeripheralVariable1 through 10	Value passed to and from the peripheral.
RouterCallDay	An encoded value that indicates the date on which the software processes the call.
RouterCallKey	A value that is unique among all calls the software has processed since midnight. RouterCallDay and RouterCallKey combine to form a unique call identifier.
RoutingClient	Name of the routing client making the route request.

Routing and Scripting for Contact Sharing

Contact Sharing uses two non-persistent call variables, `Call.ContactShareStatus` and `Call.ContactShareTarget`.

A successful route request returns `Call.ContactShareStatus` populated with the application gateway selected to receive the call. Use the call variable to route the call to the target Unified CCE instance.

`Call.ContactShareTarget` is populated only when the Gateway node takes a success path. The variable contains the target queue type and the target queue id. The target queue id is the Skill Group ID or Precision Queue ID on the target instance. The format is "Target Type, Target Queue ID". For example, "SG,5000 or PQ,5005". You can pass this data to the target instance in a call or ECC variable. Then, you have the Contact Sharing result available to use in scripting on the target instance.

Error Handling for Contact Sharing

If a Contact Share route request fails, the router populates `Call.ContactShareStatus` with the following error codes. The call flow takes the failure branch out of the Gateway node. The error codes appear in the RCD table.

Status Variable	Description
CS_NOT_CONNECTED (2)	No connection to the contact share process.
CS_TIMED_OUT (3)	Request to the contact share process failed.
CS_CONFIG_ERROR (4)	Contact share process encountered a configuration related error.
CS_EXECUTION_ERROR (5)	Contact share process encountered an expression execution related error.
CS_APPGTW_ERROR (8)	Unable to lookup the application gateway with the code that the contact share process returned.
CS_UNKNOWN_ERROR (9)	Contact sharing encountered an unknown error.

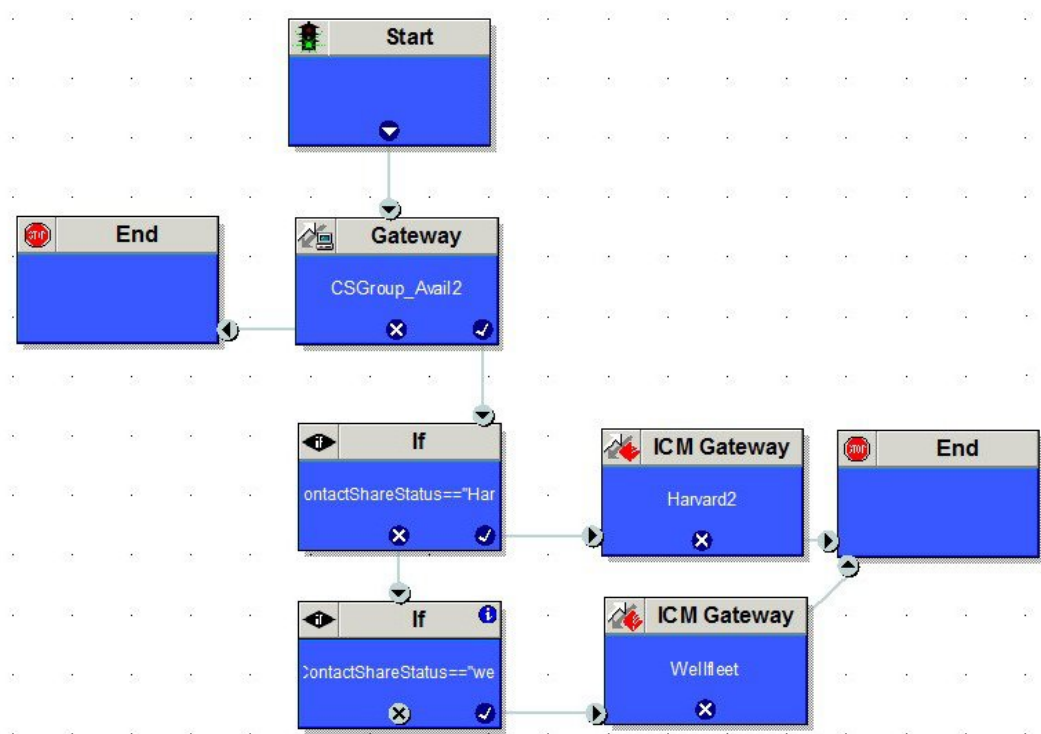
The following error messages can also appear:

Status Variable	Description
ERROR_CONTACT_SHARE_GROUP_NOT_FOUND (1)	The Contact Share Group with the listed ID was not found.
ERROR_CONTACT_SHARE_RULE_NOT_FOUND (2)	The Contact Share Rule with the listed ID was not found.
ERROR_CONTACT_SHARE_RULE_EXPRESSION_INVALID (3)	The Contact Share Rule has an invalid rule expression.
ERROR_CONTACT_SHARE_GROUP_CONSIDERIF_EXPRESSION_INVALID (4)	The Contact Share Rule has an invalid AcceptQueueIf expression.
ERROR_CONTACT_SHARE_GROUP_NO_QUEUE_CONFIGURED (5)	There are no queues configured for the Contact Share Group.
ERROR_CONTACT_SHARE_ROUTING_EXCEPTION (6)	The route request failed for an unspecified reason.
ERROR_CONTACT_SHARE_ROUTING_NO_ELIGIBLE_TARGET (7)	No eligible queue was found for the route request.
ERROR_CONTACT_SHARE_ROUTING_TARGET_CONGESTED (8)	No eligible queue was found for the route request because of congestion control.

Other Scripting Considerations

A simple Contact Sharing script looks like the following:

Figure 7: Sample Contact Sharing Script



Consider the following points when you create Contact Sharing scripts:

- Always double check the logic in the routing to the Contact Sharing node.



Tip If you see all calls routing to one target system, check the IP Addresses in the machine inventory table and your script. The relationship between the Application Gateway ID and the IP Addresses might be wrong.

- Use Call Tracer to test your call flows.
- Never put two Contact Sharing nodes in the same path of your script.
- To search for a particular Contact Sharing node, use the string selection type to search for the Contact Sharing Group name.
- Contact Sharing returns the current Application Gateway name, not the ID. If you change the Application Gateway name for one of your target systems, change your scripts to match the new name.

Script with Extrapolation in Mind

Contact Sharing's extrapolation assumes that the target systems route calls within the same Contact Sharing Group that the Contact Director used. If the target system's router does not follow this assumption, Contact Sharing's extrapolated data gets out of sync.

For Contact Sharing, have the target system route by one of the following methods:

- Route to the skill group or precision queue specified in `Call.ContactShareTarget`. You can pass the value from the Contact Director to the target system in a call or ECC variable.
- Route only among the same skill groups and precision queues that are part of the Contact Sharing Group that the Contact Director used.



CHAPTER 9

Mobile Agent

- [Mobile Agent, on page 115](#)

Mobile Agent

Deployments that need connectivity from the agent desktop over the internet without using a VPN is supported using the [Reverse Proxy Automated Installer, on page 301](#).

Capabilities

Cisco Unified Mobile Agent Description

Mobile Agent enables an agent to use any PSTN phone and in case you want to use the VPN connection (for agent desktop communications) see [VPN-less Access to Finesse Desktop, on page 247](#)

Unified Mobile Agent supports call center agents using phones that your contact center enterprise solution does not directly control. You can deploy a Mobile Agent as follows:

- Outside the contact center, by using an analog phone or a mobile phone in the home.
- On an IP phone connection that is not CTI-controlled by Unified CCE or by an associated Unified Communications Manager.
- On any voice endpoint of any ACD (including endpoints on other Unified Communication Managers) that the contact center Unified Communication Manager can reach by a SIP trunk.

A Mobile Agent can use different phone numbers at different times; the agent enters the phone number at login time. An agent can access the Mobile Agent functionality using any phone number that is included in the Unified Communications Manager dial plan.

With Cisco Unified Mobile Agent, contact centers can:

- Add or enable temporary staff during seasonal high call volume who can be brought on line with reduced startup costs
- Provide agents with the flexibility to work from home with similar quality, function, performance, convenience, and security as are available in the corporate headquarters contact center
- Allow agents to use the device they are most comfortable with, which improves agent productivity, helps to retain agents, and reduces training costs

- Hire skilled employees where they live and integrate remote workers into geographically dispersed teams with access to equivalent corporate applications

The sections that follow highlight some of the benefits of Unified Mobile Agent, and describe its features.

Unified Mobile Agent Extends Unified CCE Capabilities

Before Mobile Agent, Unified CCE used a JTAPI interface to Unified CM to connect customer calls arriving on a voice gateway to an agent's IP phone. Mobile Agent enables the Unified CCE architecture to connect customer calls to an agent phone that Unified CCE does not directly control.

Mobile Agent uses a pair of CTI ports that function as proxies for the Mobile Agent phone and the caller phone. Every logged-in Mobile Agent requires two CTI ports (local and remote). The two CTI ports take the place of the Cisco IP Phone monitored and controlled by Unified CM JTAPI. The agent at login uses the local CTI port DN. When this agent is selected, the router transfers the caller to that CTI port. The remote CTI port calls the agent either at login for a nailed (permanent) connection or upon being selected for a call-by-call connection.

Cisco Unified Contact Center functionality remains intact whether an agent is mobile or local:

- Mobile Agents have the same capabilities and functionality that local agents have.
- Mobile Agents do not need any specialized equipment; they can receive calls on an analog or mobile phone.
- Unified Mobile Agent supports Cisco Finesse.
- Mobile Agent activity is recorded in the same contact center reports as local agent activity.
- Mobile Agent CTI and application data uses the same security mechanisms as local agent data.

Unified Mobile Agent Provides Agent Sign-In Flexibility

Agents can be either local agents or Mobile Agents, depending on how they sign in at various times.

Regardless of whether agents sign in as local or Mobile Agents, their skill groups do not change. Because agents are chosen by existing selection rules and not by how they are connected, the same routing applies regardless of how the agents log in. If you want to control routing depending on whether agents are local or mobile, assign the agents to different skill groups and design your scripts accordingly.

Connection Modes

Cisco Unified Mobile Agent allows system administrators to configure agents to use either call by call dialing or a nailed connection, or the administrator can configure agents to choose a connection mode at login time.

Mobile Agents are defined as agents using phones not directly controlled by Unified CC, irrespective of their physical location. (The term local agent refers to an agent who uses a phone that is under control of Unified CC, irrespective of physical location.)

You can configure Mobile Agents using either of two delivery modes:

- 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 Connection—In this mode, the agent is called at login time and the line stays connected through multiple customer calls.



Note The administrator can select the *Agent chooses* option, which allows an agent to select a call delivery mode at login.

Call by Call

In a *call by call* delivery mode, the Mobile Agent's phone is dialed for each incoming call. When the call ends, the Mobile Agent's phone disconnects before it is made ready for the next call.

The *call by call* call flow works as follows:

1. At login, the agent specifies an assigned extension for a CTI port.
2. A customer call arrives in the system and, through Unified ICM configuration and scripting, is queued for a skill group or an agent. (This is no different than existing processing for local agents.)
3. The system assigns an agent to the call. If the agent's Desk Setting is Unified Mobile Agent-enabled and configured for either call by call or Agent chooses mode, the router uses the extension of the agent's CTI port as a label.
4. The incoming call rings at the agent's CTI port. The JTAPI Gateway and PIM notice this but do not answer the call.
5. A call to the agent is initiated on another CTI port chosen from a preconfigured pool. If this call fails, Redirect on No Answer processing is initiated.



Note In call by call mode, the Answer Wait Time is 3 to 15 seconds longer than in a local agent inbound call scenario. Specify a Redirect on No Answer setting large enough to accommodate the extra processing time.

6. When the agent takes the remote phone off-hook to answer the call, the system directs the customer call to the agent's call media address and the agent's call to the customer's call media address.
7. When the call ends, both connections are terminated and the agent is ready to accept another call.



Note To configure Mobile Agent in call by call delivery mode, you must set the wrap-up timer to at least one second using the Agent Desktop Settings List tool in the Configuration Manager.

In call by call delivery mode, callers often perceive a longer ring time compared to nailed connection delivery mode. This is because callers hear the ringtone during the call flow; ringing stops only after the agent answers. From the Unified CCE reporting perspective, a Mobile Agent in call by call delivery mode has a longer Answer Wait Time for the same reason.

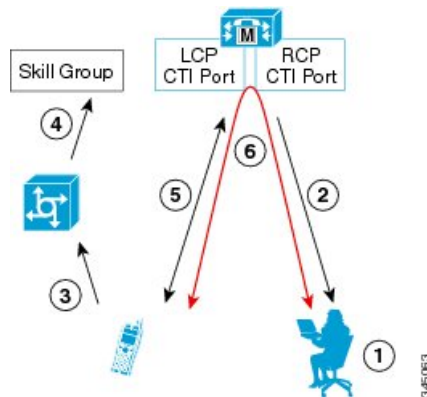
Related Topics

[Configure Agent Desk Settings with Configuration Manager](#), on page 134

Nailed Connections

In *nailed connection* delivery mode, the agent is called once, at login, and the phone line remains connected through multiple customer calls. See the following figure.

Figure 8: Nailed Connection Call Flow



The nailed connection call flow works as follows:

1. At login, the agent specifies an assigned extension for a CTI port from a pool.
2. A call to the agent is initiated on another CTI port chosen from a preconfigured pool. The agent answers the call. (The agent must answer this setup call to complete the connection and finalize the login procedure.)
3. A customer's call arrives in the system and, through Packaged CCE configuration and scripting, is queued for a skill group or an agent. (This is no different than existing processing for local agents.)
4. The system assigns an agent to the call. If the agent's Desk Setting is Unified Mobile Agent-enabled and configured for either nailed connection or Agent chooses mode, the router uses the extension of the agent's CTI port as a label.
5. The incoming call rings at the agent's CTI port. The JTAPI Gateway and PIM notice this but does not answer the call.
6. The agent desktop indicates a call is ringing and the agent clicks **Answer**.
7. When the agent indicates that they will answer the phone, the system directs the customer call to the agent's call media address and the agent call to the customer's call media address.
8. When the call ends, the customer connection is terminated and the agent state is set to Ready.

Connect Tone

The *Connect Tone* feature in the nailed connection mode enables the system to play a tone to the Mobile Agent through the agent's headset to let the agent know when a new call is connected. In the nailed connection mode, you can configure an audible connect tone in addition to a call arrival notice (on the desktop only).

Connect Tone is particularly useful when Auto Answer is enabled or the agent is an Outbound agent. Here are its features:

- An audible tone (two beeps) is sent to the Mobile Agent headset when the call to the nailed connection Mobile Agent is connected. It is a DTMF tone played by Unified CM and cannot be modified.
- The Connect Tone plays only when the nailed connection Mobile Agent receives a call, as in the following examples:
 - The agent receives a consultation call.
 - The agent receives an outbound call.

- The Connect Tone does not play when the nailed connection Mobile Agent initiates a call, as in the following examples:
 - The agent makes a call.
 - The agent makes the consultation call.
 - Outbound direct preview call is made.
 - Supervisor barge-in call is made.

Related Topics

[Enable Mobile Agent Connect Tone](#), on page 139

Agent Greeting and Whisper Announcement

The Agent Greeting and Whisper Announcement features are available to Unified Mobile Agents. The following sections explain more about how these features apply to Unified Mobile Agents.

Agent Greeting

You can use the Agent Greeting feature to record a message that plays automatically to callers when they connect to you. Your greeting message can welcome the caller, identify you, and include other useful information.

Limitations

The following limitations apply to the Agent Greeting feature for Mobile Agents.

- If a Mobile Agent ends the call when an Agent Greeting plays, the customer still hears the complete Agent Greeting before the call ends. This applies for both call by call and nailed-up calls.



Note In the Agent Greeting Call Type Report, this call does not appear as a failed agent greeting call.

- A supervisor cannot barge in when an Agent Greeting is playing.
- If a Peripheral Gateway (PG), JTAPI Gateway (JGW), or PIM failover occurs when an Agent Greeting plays for a Mobile Agent, the call fails.
- If a Mobile Agent ends the call when an Agent Greeting plays, the customer still hears the complete Agent Greeting before the call ends.



Note In the Agent Greeting Call Type Report, this call does not appear as a failed agent greeting call.

- If a Peripheral Gateway (PG), JTAPI Gateway (JGW), or PIM failover occurs when an Agent Greeting plays for a Mobile Agent, the call fails. This applies for both call-by-call and nailed-up calls.



Note You can use Agent Greeting for Mobile Agents only with parent/child deployments that are approved by Cisco Assessment-to-Quality (A2Q) with Design Mentoring Services (DMS).

For more information about Agent Greeting, see [Capabilities, on page 11](#).

Whisper Announcement

With Whisper Announcement, agents can hear a brief prerecorded message just before they connect with each caller. The announcement plays only to the agent; the caller hears ringing (based on existing ringtone patterns) while the announcement plays. The announcement can contain information about the caller, such as language preference or customer status. This information helps the agent prepare for the call.

Configuration Requirement

For the Whisper Announcement feature for Unified Mobile Agents, you require a Media Termination Point (MTP) resource on an incoming SIP device.

Feature Requirements

Hardware and Software Requirements

Hardware and software requirements for the Unified Mobile Agent are identical to those of Unified CCE. For more information on feature requirements, consult these documents:

- *Solution Design Guide for Cisco Unified Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html>
- *Virtualization for Unified Contact Center Enterprise* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html
- *Contact Center Enterprise Compatibility Matrix* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html>

Phone Requirements

A Unified Mobile Agent can use an analog, digital, or IP phone to handle calls.

Conference Requirements

To use Agent Greeting for Mobile Agents, you must configure external conference-bridge (hardware) resources. To estimate the number of required resources, you can use the following formula:

Number of conference bridge resources = Mobile Agent call rate × Average greeting time (in seconds)

For information about configuring external conference-bridge resources, see the `dspfarm profile 1 for conference` configuration section in the sample configuration gateway, listed in [Media Termination Points Configuration, on page 135](#).

CTI Port Requirements

You need two CTI ports (local and remote) for every logged-in Mobile Agent.

Unified Mobile Agent uses Unified CM CTI Port as a proxy for the agent's phone. When this proxy is set up, whenever a Mobile Agent is selected to handle a customer call, the following happens:

- The call is directed to the CTI port extension.
- Unified CCE, using the JTAPI Gateway, intercepts the call arriving on the CTI Port and directs Unified CM to connect the call to the Mobile Agent.

Unified Mobile Agent requires that maximum number of calls is set to 2 and busy trigger is set to 1.

For Unified Mobile Agent to work properly, you must configure two CTI ports:

- One port to serve as the agent's virtual extension.
- The other port to initiate calls to the agent.

You must assign these CTI ports to the Unified ICM application. The ports are recognized by Unified ICM when receiving the Unified CM configuration.

For these CTI ports in IPv6 enabled deployments, you have to set **IP Addressing Mode** to **IPv4 Only**. You do this by creating a **Common Device Configuration** and referencing it to these CTI ports.

Supported Unified CCE Features

The following features are supported:

- Unified CCE supports temporary uninstallation while preserving Mobile Agent data.
For more information about temporary uninstallation, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.
- Mobile Agents can participate in outbound campaigns, but they must use a nailed-up connection for all outbound dialing modes.
- Unified Mobile Agent supports Redirect on No Answer (RONA). If the Mobile Agent fails to answer, the agent is made Not Ready, and the call is redirected to a RANA DN route point.
- Unified Mobile Agent supports G.711A-law, G.711u-law, and G.729 codecs.
- There is no direct interaction between Unified Mobile Agent and multichannel applications. Email and Chat are IP applications that continue to operate, assuming the Mobile Agent has a desktop with enough bandwidth on the broadband connection to support them.
- Unified Mobile Agent supports Cisco Unified Customer Voice Portal (Unified CVP) and Cisco Unified IP-IVR (Unified IP IVR).

Related Topics

[Silent Monitoring](#), on page 123

Fault Tolerance Support

Fault tolerance for the Unified Mobile Agent follows the behavior of Unified CCE:

- The JTAPI Gateway, Unified CCE PIM, and CTI components record key events related to Unified Mobile Agent as part of the logging process.
- As with standard Unified CCE calls, if a Peripheral Gateway (PG) component such as the JTAPI Gateway fails, the phone call is not lost, but subsequent call control (transfer, conference, or hold) might not be

possible after a failover. The Mobile Agent is notified of a failure (on the desktop), but they must log in again after a Unified CM or Unified ICM failure occurs.

- Where CTI data is delivered for screen pops, CTI data is preserved.

Unified Mobile Agent can experience many of the same failure cases as Unified CCE:

- Side A/B failure
- VRU failure
- Unified CM failure
- CTI server failure

There are also some failure cases that are unique to Unified Mobile Agent:

- A situation where a Mobile Agent is using a cellular phone and the connection is dropped due to non-availability of a signal, is deemed as external failure. The agent must call back and log-in again.
- If a Mobile Agent's phone line disconnects while using nailed connection mode, the agent must log in again to receive new calls.

Important Considerations

Before you proceed, consider the following Unified Mobile Agent limitations and considerations:

Failover

- During a failover, if an agent in call by call mode answers an alerting call, the call can drop. This occurs because the media cannot be bridged when there is no active PG.
- During a prolonged Peripheral Gateway (PG) failover, if an agent takes call control action for a Unified Mobile Agent-to-Unified Mobile Agent call, the call can drop. This occurs because the activating PG may not have information for all agents and calls at that point.
- Unified Communications Manager failover causes a Mobile Agent call to be lost.
- If a call by call Mobile Agent initiates a call (including a supervisor call) and does not answer the remote leg of the call before PG failover, the call fails. The agent must disconnect the remote agent call leg and reinitiate the call.

Performance

- Mobile Agent call processing uses more server resources and therefore reduces the maximum number of supported agents on both Unified CM and the Unified ICM Agent PG.

For more information about sizing Mobile Agents, see the *Solution Design Guide for Cisco Unified Contact Center Enterprise*.

- Because Unified Mobile Agent adds processing steps to Unified CCE default functionality, Mobile Agents may experience some delay in screen popup windows.
- From a caller's perspective, the call by call delivery mode has a longer ring time compared with the nailed connection delivery mode. This is because Unified CCE does not start to dial the Mobile Agent's phone number until *after* the call information is routed to the agent desktop. In addition, the customer call media stream is not connected to the agent until after the agent answers the phone.

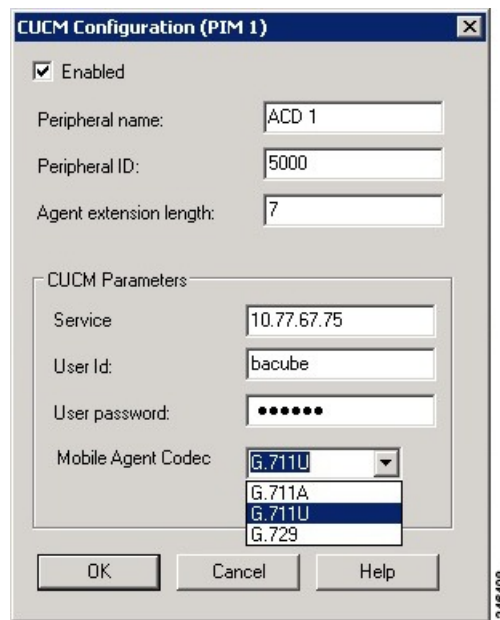
The caller hears a repeated ringtone while Unified CCE makes these connections.

Codec

The codec settings on the Peripheral Gateway and Voice Gateway must match. Perform the following procedure:

1. Launch the Peripheral Gateway Setup.
2. In the Peripheral Gateway Component Properties, select the UCM PIM and click **Edit**.
3. In the CallManager Parameters section, select the appropriate codec from the Mobile Agent Codec drop down list.

Figure 9: Mobile Agent Codec Selection



Silent Monitoring

Unified Mobile Agent provides the following silent monitoring support:

- Unified Mobile Agent requires that caller and agent voice gateways be on separate devices if silent monitoring is to be used.
- Unified Mobile Agent does not support desktop monitoring.
- Whenever silent monitoring is used on Unified Mobile Agent, caller and agent voice gateways must be on separate devices. Similarly, if MTP is enabled when silent monitoring is used, MTP resources for caller and agent must also be on separate devices.

Mobile Agent Scalability

Mobile Agent scalability may be contingent on specific Unified CM versions. For more information, see the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html>.

Unsupported Features

The following is a list of unsupported features for Mobile Agent:

- Web Callback
- Blended Collaboration
- Unified CM-based Silent Monitoring
- Agent Request

Unified Mobile Agent Call Flows

This section provides sample Unified Mobile Agent call flows for:

- Inbound calls
- Local consultation calls
- Remote consultation calls
- Remote conference calls

In all Unified Mobile Agent call flows, the JTAPI Gateway maintains the signaling association between the inbound and outbound calls and, if necessary, performs further operations on the call. JTAPI Gateway, however, does not terminate media; it uses CTI to deliver the customer call from the inbound gateway port to the outbound gateway port.

This means that a Mobile Agent *must* use an agent desktop application to log in, change agent state, log out, send dual-tone multifrequency (DTMF) digits, and perform call control.

About Figures in This Section

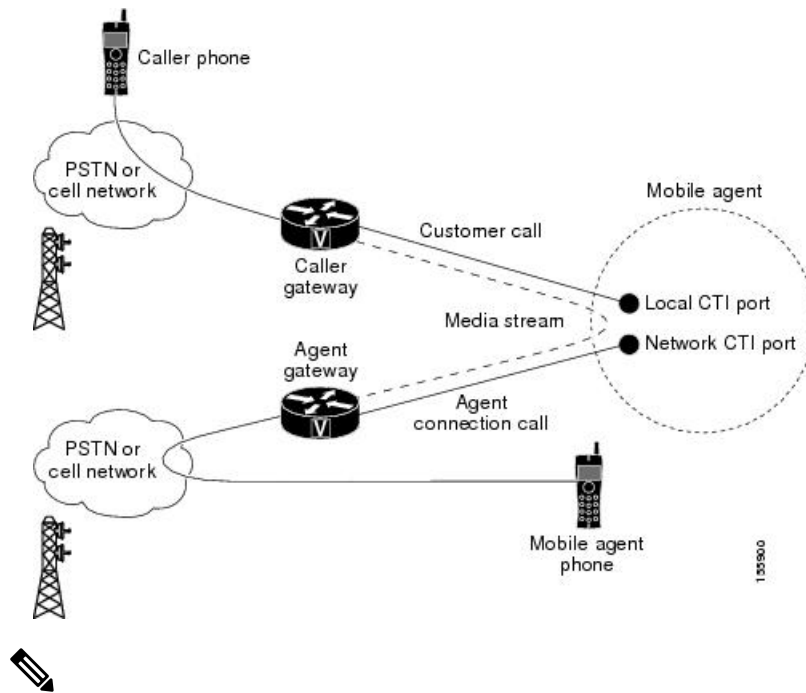
The figures in this section:

- Show a caller and a Mobile Agent in a cellular network. However, the same concepts apply whether the Mobile Agent is using an enterprise desk phone, an IP Phone spanning another Unified CM cluster, standard analog phone, or a third-party ACD phone.
- Focus solely on call media flow; a Mobile Agent must use a CTI Desktop with broadband access to perform agent state and call control.
- Show only a sampling of the call flows possible with Unified Mobile Agent.

Inbound Call Flow

The following figure shows an inbound call flow.

Figure 10: Mobile Agent Inbound Call Flow



Note Caller and Agent voice gateways can coreside on one device, except in deployments where Silent Monitoring is required.

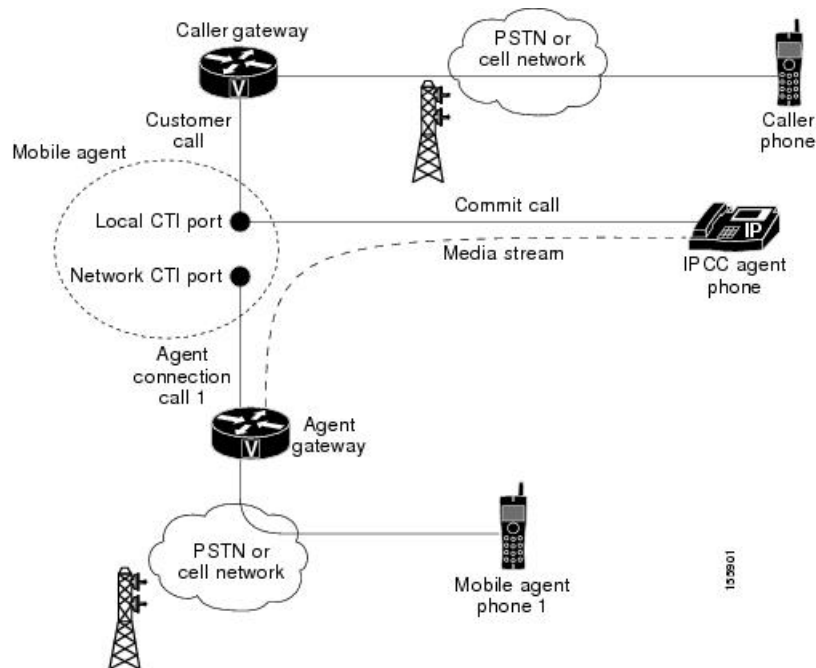
The following describes an inbound call flow:

1. The Mobile Agent becomes available to answer calls by:
 - Logging in to the corporate domain using VPN over the ADSL/Cable connection
 - Launching the agent desktop interface and logging in with their remote phone information
 - Entering the Ready mode
2. A customer call arrives at the Unified CC.
3. The JTAPI Gateway creates a Mobile Agent class to manage local and network CTI ports for a Mobile Agent.
4. The Router passes the call to the *local* CTI Port of a Mobile Agent.
5. The JTAPI Gateway places a call on a *network* CTI port to the agent's cell phone.
6. The JTAPI Gateway uses local and network CTI ports of the Mobile Agent to stream the media for the call from the inbound (caller) gateway port to the outbound (agent) gateway port.

Local Consult Calls

The following figure shows a consult call flow between a Mobile Agent and a local agent.

Figure 11: Mobile Agent Consult Call Flow



Note Caller and Agent voice gateways can coreside on one device, except in deployments where Silent Monitoring is required.

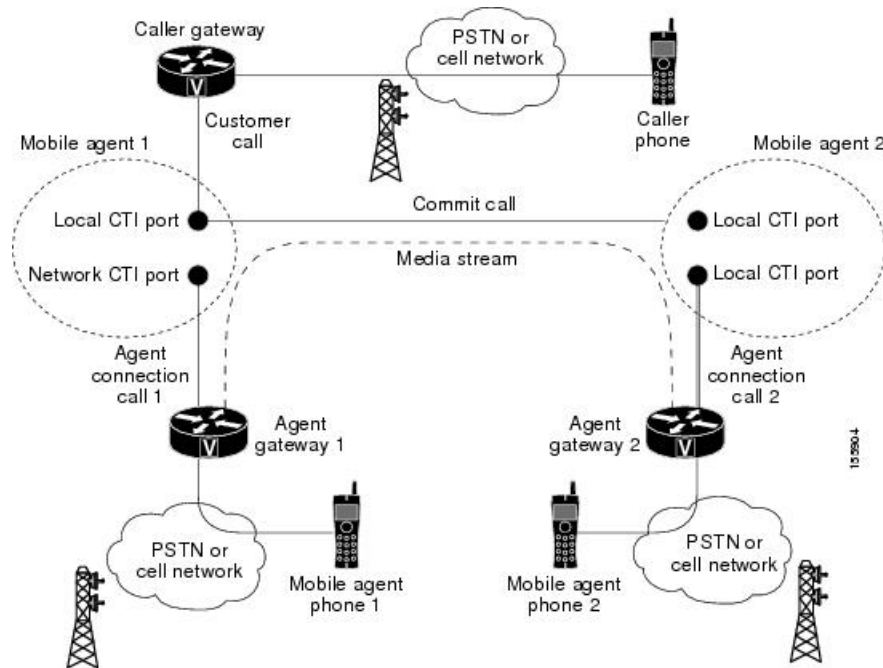
The following describes a local consult call flow:

1. The Mobile Agent becomes available to answer calls by:
 - Logging in to the corporate domain using VPN over the ADSL/Cable connection
 - Launching the agent desktop interface and logging in with their remote phone information
 - Entering the Ready mode
2. A customer call arrives at the Unified CC.
3. The JTAPI Gateway creates a Mobile Agent class to manage local and network CTI ports for a Mobile Agent.
4. The Router passes the call to the *local* CTI Port of a Mobile Agent.
5. The JTAPI Gateway places Agent Connection Call 1 on a *network* CTI port to the agent's cell phone.
6. The Mobile Agent places the customer call on hold and consults a local Unified CCE agent.
7. The JTAPI Gateway uses local and network CTI ports of the Mobile Agent to stream the media for the call from the IP hard phone to the outbound gateway port.

Remote Consult Calls

The following figure shows a remote consult call flow between two Mobile Agents.

Figure 12: Mobile Agent Remote Consult Call Flow



Note Caller and Agent voice gateways can coreside on one device, except in deployments where Silent Monitoring is required.

The following describes a remote consult call flow:

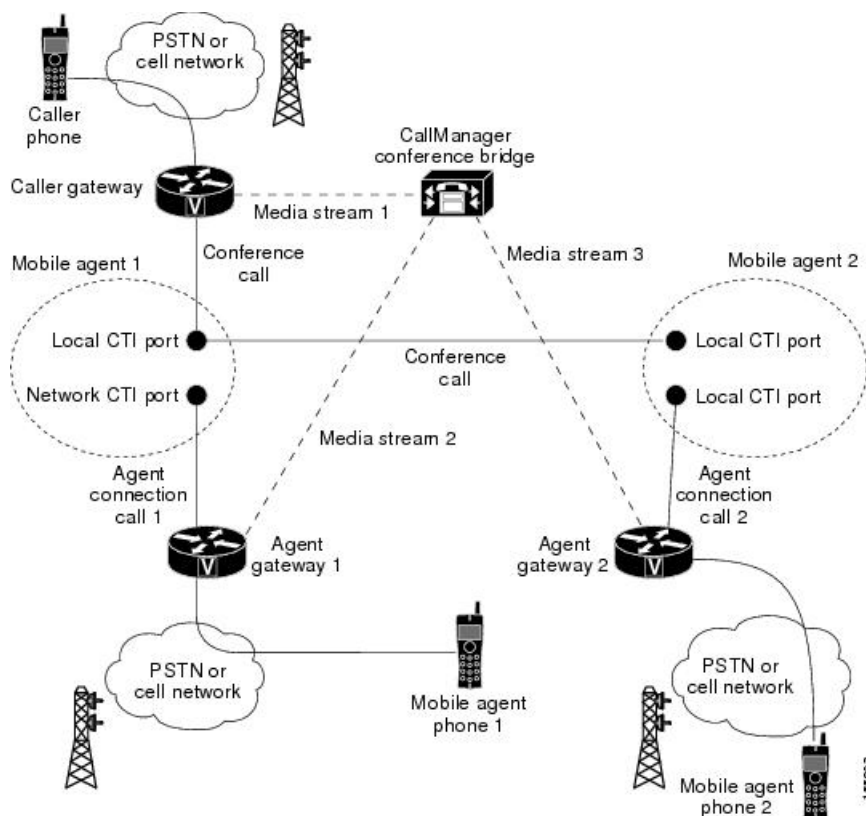
1. The Mobile Agent becomes available to answer calls by:
 - Logging in to the corporate domain using VPN over the ADSL/Cable connection
 - Launching the agent desktop interface and logging in with their remote phone information
 - Entering the Ready mode
2. A customer call arrives at the Unified CC.
3. The JTAPI Gateway creates a Mobile Agent class to manage local and network CTI ports for a Mobile Agent.
4. The Router passes the call to the *local* CTI Port of a Mobile Agent.
5. The JTAPI Gateway places Agent Connection Call 1 on a *network* CTI port to the agent's cell phone.
6. Mobile Agent 1 puts the customer call on hold and consults Mobile Agent 2.

- The JTAPI Gateway uses the network CTI port of Mobile Agent 1 and the network CTI port of Mobile Agent 2 to stream the media for the call from the outbound gateway port on Agent Gateway 1 to the outbound gateway port on Agent Gateway 2.

Remote Conference Calls

The following figure shows a remote conference call flow between two Mobile Agents.

Figure 13: Mobile Agent Remote Conference Call Flow



Note Caller and Agent voice gateways can coreside on one device, except in deployments where Silent Monitoring is required.

The following describes a remote conference call flow:

- The Mobile Agent becomes available to answer calls by:
 - Logging in to the corporate domain using VPN over the ADSL/Cable connection
 - Launching the agent desktop interface and logging in with their remote phone information
 - Entering the Ready mode
- A customer call arrives at the Unified CC.

- Launching the agent desktop interface and logging in with their remote phone information
 - Entering the Ready mode
2. The JTAPI Gateway creates a Mobile Agent class to manage local and network CTI ports for a Mobile Agent.
 3. Outbound Option dials the customer number and, after reaching a live customer, the Dialer redirects the customer call to the *local* CTI Port of an Outbound Option Mobile Agent.
 4. The JTAPI Gateway places a call on a *network* CTI port to the agent's cell phone.
 5. The JTAPI Gateway uses local and network CTI ports of the Mobile Agent to stream the media for the call from the inbound gateway port to the outbound gateway port.

Unified Mobile Agent Reporting

Unified Mobile Agent-specific call data is contained in the following Cisco Unified Intelligence Center reports: Agent Team Historical, Agent Real Time, and Agent Skill Group Historical. These “All Field” reports contain information in multiple fields that show what kind of call the agent is on (nonmobile, call by call, nailed connection) and the Unified Mobile Agent phone number.

Notes about Mobile Agents and reporting:

- The Mobile Agent must be logged in through the agent desktop for call data to be recorded in Unified CC reports.
- Service level for Mobile Agent calls might be different than local agent calls, because it takes longer to connect the call to the agent.

For example, a call by call Mobile Agent might have a longer Answer Wait Time Average than a local agent. This is because Unified CCE does not start to dial the Mobile Agent phone number until *after* the call information is routed to the agent desktop. In addition, the customer call media stream is not connected to the agent until after the agent answers the phone.

For more information about Unified Mobile Agent fields in the database schema, see *Database Schema Handbook for Cisco Unified Contact Center Enterprise*.

Initial Setup

Summary of Unified Mobile Agent System Configuration Tasks

The following table describes system configuration tasks for Unified Mobile Agent.

Table 12: Unified Mobile Agent System Configuration Tasks

Task	See
Configure Unified CM CTI Port pools	Unified CM CTI Port Configuration and Mapping for Unified Mobile Agent, on page 131
Configure Unified CM Call Duration Timer	Maximum Call Duration Timer Configuration, on page 134

Task	See
Configure Agent Desk Settings	Agent Desk Setting Configuration for Unified Mobile Agent, on page 134
Configure Devices	Device Configuration for Unified Mobile Agent, on page 135
Configure Media Termination Points	Media Termination Points Configuration, on page 135

Unified CM CTI Port Configuration and Mapping for Unified Mobile Agent

This section describes the CTI Port Pool configuration tasks *specific* to Mobile Agent Option configuration. It does not discuss installation or configuration of Unified CCE.



Note For more information about installing and configuring Unified CM with Unified CCE, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.

Unified Mobile Agent must have two CTI ports configured on Unified CM:

- A *local* CTI port, which Unified Mobile Agent uses as the agent's virtual extension.
- A *remote* CTI port, which Unified Mobile Agent uses to initiate a call to the Mobile Agent's phone.

Naming Conventions for Local and Network Ports

- The local port *must* begin with the string LCP.
- The remote port *must* begin with the string RCP.
- The remaining characters in the device names for the LCP and RCP pair *must match*. For example an LCP port named LCP0000 has a corresponding RCP port named RCP0000.
- For example, you can use the following naming convention:
 - For a local CTI Port pool name, configure a name in the format LCP:xxx:Fyyy, where LCP identifies a local CTI Port Pool, xxx is the peripheral ID for the Unified CM PIM, and yyy is the number of local CTI Port.
Example: LCP5000F0000 represents CTI Port: 0 in a local CTI Port pool for the Unified CM PIM with the peripheral ID 5000.
 - For a network CTI Port pool name, use the same format, except substitute RCP as the first three characters.



Note While you do not require a naming convention, the substrings identifying the Unified CM PIM peripheral ID and the CTI Port *must* match for each local/network pair.

CTI Port configuration consists of the following steps:

1. Add the CTI port as you would for an IP Phone.
2. Use the naming convention described above to map the local and network CTI ports.



Note Each local CTI port must have a corresponding network CTI port.

3. Add a directory number for the local CTI port (that is, the agent's virtual extension).
4. Map the local and network CTI ports with the PG user.

Music on Hold Design

If you want callers to hear music when a Mobile Agent places the caller on hold, you must assign Music on Hold (MoH) resources to the ingress voice gateway or trunk that is connected to the *caller* (as you do with traditional agents). In this case, the user or network audio source is specified on the local CTI port configuration. Similarly, if a Mobile Agent must hear music when the system puts the agent on hold, you must assign MoH resources to the ingress voice gateway or trunk that is connected to the *Mobile Agent*. In this case, the user or network audio source is specified on the remote CTI port configuration.

Do not assign MoH resources to local ports and remote CTI ports, because it might affect the system performance.

If a remote Mobile Agent calls over a nailed connection and if there is no active call to the agent, the agent is put on hold. Enable MoH to the Mobile Agent phone for nailed connection calls. If MoH resources are an issue, consider multicast MoH services.

If a remote Mobile Agent calls over a nailed connection, and if MoH is disabled, the hold tone plays to the agent phone during the hold time. This depends on the call processing agent that controls the Mobile Agent remote phone. For Unified CM, the hold tone is enabled by default (it is similar to the Mobile Agent connect tone). Because the hold tone is similar to the connect tone, it is difficult for the agent to identify if a call arrived from listening to the Mobile Agent connect tone. The hold tone prevents the agent from hearing the connect tone.

Therefore, disable the hold tone by changing the setting of the Tone on Hold Timer service parameter to 0. For more information about setting this parameter, see the Unified CM product documentation available at: <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html>.

Configure Unified CM CTI Port Pools for Unified Mobile Agent

Perform the following steps to configure CTI Ports.

-
- Step 1** In Unified CM Administration, select **Device > Phone**.
 - Step 2** Click **Add a New Phone**.
 - Step 3** From Phone Type, select **CTI Port**.
 - Step 4** Click **Next**.
 - Step 5** In Device Name, enter a unique name for the local CTI Port pool name; click **OK** when finished.

Using the naming convention format LCPxxxxyyy:

- LCP identifies the CTI Port as a local device.

- *xxxx* is the peripheral ID for the Unified CM PIM.
- *yyyy* is the local CTI Port.

The name LCP5000F0000 would represent CTI Port: 0 in a local CTI Port pool for the Unified CM PIM with the peripheral ID 5000.

The name LCP0000 represents the local port.

- Step 6** In Description, enter text that identifies the local CTI port.
- Step 7** Use the **Device Pool** drop-down list to choose the device pool to which you want to assign the network CTI port pool. Do not select Default. (The device pool defines sets of common characteristics for devices.)
- Step 8** Click **Save**.
- Step 9** Highlight a record and select **Add a New DN**.
- Step 10** Add a unique directory number for the CTI port you just created.
- Step 11** In Maximum Number of Calls, enter **2**.
- Step 12** In Busy Trigger, enter **1**.
- Step 13** When finished, click **Save**, and click **Close**.
- Step 14** Repeat the preceding steps to configure the network CTI port pool.

In Device Name, using the naming convention format RCP*xxxxyyyy*, where:

- RCP identifies the CTI port as the Remote CTI port where the call between the agent's remote device and the Unified CM Port is nailed up at agent login time.
- *xxxx* is the peripheral ID for the Unified CM PIM.
- *yyyy* is the network CTI port.

The name RCP5000F0000 represents CTI Port: 0 in a network CTI Port pool for the Unified CM PIM with the peripheral ID 5000.

- Step 15** In Description, enter text that identifies the network CTI port pool.
- Step 16** Use the **Device Pool** drop-down list to choose the device pool to which you want to assign the network CTI port. Do not select Default. pool. (The device pool defines sets of common characteristics for devices.)
- Step 17** Click **Save**.
- Step 18** Highlight a record and select **Add a New DN**.
- Step 19** Add a unique directory number for the CTI port you just created.
- The extension length can be different from the extension length of the LCP Port if your dial plan requires it.
- Step 20** When finished, click **Save**, and click **Close**.

Map Local and Remote CTI Ports with Peripheral Gateway User

After you define the CTI Port pool, you must associate the CTI Ports with PG users.

-
- Step 1** In Unified CM Administration, select **Application User**.
- Step 2** Select a username and associate ports with it.

Step 3 When finished, click **Save**, and then click **Close**.

Note If CTI ports for Unified Mobile Agent are disassociated at the Unified CM while a Mobile Agent is on an active call, the call can drop.

Maximum Call Duration Timer Configuration

By default, Mobile Agents in nailed connection mode log out after 12 hours. This happens because a Unified CM Service Parameter—the Maximum Call Duration Timer—determines the amount of time an agent phone can remain in the Connected state after login.

If you anticipate that nailed connection agents in your Unified Mobile Agent deployment will be logged on *longer than* 12 hours, use the following instructions to either:

- Increase the Maximum Call Duration Timer setting.
- Disable the timer entirely.

Configure Maximum Call Duration Timer



Note This procedure applies only to Unified Mobile Agent deployments where agents logged in to nailed connection mode are to remain connected *longer than* 12 hours. Also, if your Mobile Agent deployment uses intercluster trunks, you must perform the following steps on both local and network Unified CM clusters.

Step 1 In Unified CM Administration, choose **System > Service Parameters**.

Step 2 In the Server drop-down list, choose a server.

Step 3 In the Service drop-down list, choose a server .

The **Service Parameters Configuration** window appears.

Step 4 In the Cluster-wide Parameters section, specify a **Maximum Call Duration Timer** setting.

The default is 720 minutes (12 hours); the maximum setting allowed is 35791 minutes.

Note To disable the timer, enter **0**.

Step 5 Click **Save**.

Agent Desk Setting Configuration for Unified Mobile Agent

This section describes Agent Desk Settings that you must modify to accommodate Unified Mobile Agent features.

Configure Agent Desk Settings with Configuration Manager

This section describes Agent Desk Settings configuration settings you should specify in Unified ICM Configuration Manager to accommodate Unified Mobile Agent features.

The following instructions describe how to configure *one* Agent Desk Setting. Repeat this process for each different Agent Desk Setting in your deployment.

-
- Step 1** From the Unified ICM Configuration Manager, choose **Configure ICM > Enterprise > Agent Desk Settings List**.
The Unified ICM Agent Desk Settings List dialog box opens.
- Step 2** Click **Retrieve**.
- Step 3** Click **Add**.
- Step 4** Fill in the following Attributes tab information, making sure to include settings for the following fields and check boxes:
- **Ring no answer time.** The system allows a call to ring at the agent's station before redirecting the call. This can be from 1 to 120 seconds.
Note If you use call by call mode, the answer wait time will be longer than in a local agent inbound call scenario, so specify a value in this field to accommodate the extra processing time.
 - **Logout non-activity time.** The number of seconds of agent inactivity while in the not ready state before the system logs out the agent. A blank entry disables the timer.
 - **Cisco Unified Mobile Agent** (check box). Enables the Mobile Agent feature so that the agent can log in remotely and take calls from any phone.
 - **Mobile Agent mode.** Select how call connections are made to the Mobile Agent's phone:
 - **Agent chooses.** Agent selects call by call or nailed connection at login.
 - **Call by call.** Agent's phone is dialed for each incoming call. When a call ends, the connection is terminated before the agent is made ready for next call.
 - **Nailed connection.** Agent is called once, at login. The line stays connected through multiple customer calls.
- Step 5** Click **Save**.



Note For more information about configuring Agent Desk Settings in Unified CCE, see *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.

Device Configuration for Unified Mobile Agent

Use the Agent Targeting Rules (ATR) mechanism described in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* to configure a device as you would for a phone, but using the LCP Port in place of the agent's phone extension.

Media Termination Points Configuration

If you use SIP trunks, you must configure Media Termination Points (MTPs). You must also configure MTPs if you use TDM trunks to create an interface with service providers.

Additionally, MTPs are required for Mobile Agent call flows that involve a Cisco Unified Customer Voice Portal (CVP) solution. Because in DTMF signaling mode the Mobile Agent uses out-of-band signaling,

whereas Unified CVP supports in-band signaling, the conversion from out-of-band to in-band signaling requires an MTP resource.

MTPs may be allocated as required in deployments that use a mix of IPv4 and IPv6 connections. MTP resources are allocated provided that the Media Resource Group List is configured on the IPV4 endpoint.

MTPs are available in the following forms, but not all are supported in Mobile Agent environments:

- Software-based MTPs in Cisco IOS gateways—use these MTPs for Mobile Agent as they provide codec flexibility and improved scalability compared with other MTP options. The following is a sample configuration on a gateway.

```
sccp local GigabitEthernet0/0
sccp ccm 10.10.10.31 identifier 1 priority 1 version 7.0
sccp ccm 10.10.10.131 identifier 2 priority 2 version 7.0
sccp
!
sccp ccm group 1
  associate ccm 1 priority 1
  associate ccm 2 priority 2
  associate profile 3 register gw84xcode
  associate profile 1 register gw84conf
  associate profile 2 register gw84mtp
!
dspfarm profile 3 transcode
  codec g729abr8
  codec g729ar8
  codec g711alaw
  codec g711ulaw
  codec g729r8
  codec g729br8
  maximum sessions 52
  associate application SCCP
!
dspfarm profile 1 conference
  codec g729br8
  codec g729r8
  codec g729abr8
  codec g729ar8
  codec g711alaw
  codec g711ulaw
  maximum sessions 24
  associate application SCCP
!
dspfarm profile 2 mtp
  codec g711ulaw
  maximum sessions software 500
  associate application SCCP
```

- Hardware-based MTPs in Cisco IOS gateways—These MTPs are supported. If you choose these, consider the extra cost, codec restrictions, and scalability constraints.
- Software-based MTPs using the Cisco IP Voice Media Streaming Application—These MTPs are not supported with Mobile Agents.



Note Because Unified CM-based software MTPs are used implicitly, you must add a special configuration to avoid using thcce-in10360-01-pcceucceipv6support-1101em. Create a new Media Resource Group (MRG) as a place holder, and place the software MTPs in that MRG. For instructions, refer to the Unified CM help documentation.



Note Ensure the `sccp ccm` configuration matches the Cisco Unified CM Group order used in the Device Pool assigned to the Media Termination Point in **CUCM > Media Resource**.

Configure Media Termination Points in Unified CM

Add MTP Resources to Unified CM

Perform these steps to add media termination points (MTPs) to Unified CM.

-
- Step 1** In Unified CM Administration click **Media Resources > Media Termination Point**.
 - Step 2** Click **Add New**.
 - Step 3** Choose **Cisco IOS Enhanced Software Media Termination Point** from the **Media Termination Point Type** drop-down list.
 - Step 4** Enter an MTP name. This name must match the device name you chose in IOS. In the example in the previous section, the MTP was called `gw84mtp`, as from the config line: `associate profile 2 gw84mtp`.
 - Step 5** Choose the appropriate device pool.
 - Step 6** Click **Save** and then click **Apply config**.
 - Step 7** Navigate back to **Media Termination Point** and ensure the newly added MTP is listed as being registered with *<Unified CM subscriber IP address>* in the Status column.
 - Step 8** Repeat steps 1 through 7 for each `sccp ccm` group you configured on each of your gateways.
-

Configure Media Termination Point Resources in Unified CM

This section explains how to create media resource groups and media resource group lists.

-
- Step 1** Navigate to **Media Resources > Media Resource Group** in Unified CM Administration.
 - Step 2** Click **Add New**.
 - Step 3** Specify a name and description.
 - Step 4** From the Available Media Resources that you just created, move the those devices from the Available to the Selected list by clicking the down arrow. Ensure that you do *not* include Unified CM Software resources. For example, type anything that starts with `ANN_`, `MTP_`, or `MOH_`.
 - Step 5** Navigate to **Media Resources > Media Resource Group List**.
 - Step 6** Click **Add New**.
 - Step 7** Move the Media Resource Group you just created from the Available Media Resource Groups to the Selected Media Resource Groups.
 - Step 8** Click **Save**.
-

Associate Media Resource Group List with Device Pools

-
- Step 1** Navigate to **System > Device Pool** and click on the device pool that contains the CTI ports for Mobile Agent. If there are multiple pools, perform the next step for each device pool that applies.
- Step 2** In the Media Resource Group List drop-down list, select the Media Resource Group List that you just created, click **Save** and then click **Apply config**.
-

Quarantine Unified CM Software-Based Resources

Unified CM-based software MTPs are used by default. However, Cisco contact center deployments do not support these resources because they may cause performance problems in call processing. You must quarantine them with a special configuration. Perform the following steps:

-
- Step 1** Create a new Media Resource Group (MRG) as a place holder.
- Step 2** Place the software MTPs in that MRG.
- For further instructions, refer to the Unified CM help documentation.
-

Insert MTPs

If you use SIP trunks, you must configure MTPs. This also applies if you use TDM trunks to interact with service providers. Mobile Agent cannot use an MTP with codec pass through. When you configure the MTP, you must select No pass through. KPML is not supported with Mobile Agent.

-
- Step 1** Log in to Unified CM Administration and select **Device > Trunk**.
- Step 2** Select the trunk on which you want to configure MTPs.
- Step 3** Depending on the scenario listed below, perform the corresponding step listed in the Description column. Note that if you configure Trunk Groups to dynamically insert MTPs, only the calls that require MTPs use them.
- If you want to always insert MTPs for inbound and outbound calls through a given trunk: In the Trunk Configuration settings, select the **Media Termination Point Required** check box.
 - If you want to dynamically insert MTPs when Unified ICM detects media or signaling incompatibility between the caller and called endpoints: In the Trunk Group Configuration settings, in DTMF Signaling Method, select **RFC2833**.
-

Enable Call Progress Tones for Agent-Initiated Calls

When **MTP Required** is not enabled, extra configuration is required to enable an agent to hear call progress tones for agent initiated calls. If instead you have dynamic MTP allocation by forcing mismatched DTMF settings, then configure the Unified Communications Manager to enable Early Offer.

For information on configuring the Unified Communications Manager, see the Unified Communications Manager product documentation at <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html>. The Cisco Annunciator does not

generate ringback and other call progress tones, as it does for regular phones and softphones. Instead, Mobile Agent relies on the called party generating these tones (and the early offer setting triggers sending these tones to the agent).

Note This selection does not affect MTP sizing for IP Phones and other endpoints that support RFC2833 signaling, as is the case for many Cisco phones. For more information about supported phones, see the Contact Center Enterprise Compatibility Matrix at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html>.

Verify MTP Resource Utilization

Since Unified CM comes preconfigured with Software MTP resources, these resources may sometimes be used to provide MTP for Mobile Agent calls without proper configuration. Because we don't support the use of Unified CM based software MTPs, we explicitly quarantined them in the above section, Disabling Unified CM Based Software MTPs. To ensure that the new IOS-based MTPs are the ones being used for Mobile Agents, perform the following steps to verify that correct MTPs are used.

-
- Step 1** Install the Unified CM Realtime monitoring tool. This tool can be downloaded under **Application > Plugins** within Unified CM Administration.
 - Step 2** Place a call to a logged-in Mobile Agent.
 - Step 3** Open the Unified CM Realtime monitoring tool and navigate to **System > Performance > Open Performance Monitoring**.
 - Step 4** Expand the node(s) that are associated with your IOS-based MTP resources and choose **Cisco MTP Device**.
 - Step 5** Double-click **Resources Active** and choose all of the available resources to monitor. This includes both IOS and Unified CM-based resources. Ensure that the only resources that are active during the Mobile Agent phone call are the IOS-based resources. Also, ensure that all UCM-based MTP resources are *not* active.
 - Step 6** Repeat the previous step for each node that has MTP resources associated with it.
-

Enabled Connect Tone Feature

In a nailed connection, the system can play a tone to the Unified Mobile Agent through the agent headset to let the agent know when a new call is connected. In the default Installation, the Mobile Agent Connect Tone feature is disabled.

Enable Mobile Agent Connect Tone

If you require Unified Mobile Agent Connect Tone, you must make the following change in the Windows Registry for the key PlayMAConnectTone under the JTAPI GW PG registry entries.

Perform the following procedure to allow a Mobile Agent in the nailed connection mode to hear a tone when a new call is connected.

Before you begin

MTP resources must be associated with the CUCM trunk that connects to the Agent Gateway.

-
- Step 1** On the PG machine, open the Registry Editor (regedit.exe).

- Step 2** Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM*<InstanceName>*\PG1A\PG\CurrentVersion\JGWS\jgw1\JGWData\Config\PlayMACConnectTone. The Edit DWORD Value dialog box appears.
- Step 3** In the Value data: field, enter **1** to enable Mobile Agent Connect Tone and click **OK**.
- Step 4** Exit the Registry Editor to save the change, and cycle the PG service.
-

Administration and Usage

Cisco Finesse

Finesse provides a browser-based desktop for agents and supervisors. Mobile agents can perform the same call control functions as Unified CCE agents. Mobile supervisors can perform all call control functions except for silent monitoring.

Sign in to Cisco Finesse Desktop

- Step 1** Enter the hostname of the Finesse server in the fully qualified domain name (FQDN) format: `https://<FQDN of Finesse server>`, where FQDN is the fully qualified domain name of the Finesse server.
- In an IPv6-enabled environment, you must include the port number in the URL (`https://FQDN of Finesse server:8082/desktop`).
- Step 2** In the ID field, enter your agent ID.
- Step 3** In the Password field, enter your password.
- Step 4** In the Extension field, enter your extension.
- For a mobile agent, the extension represents the virtual extension for the agent, also known as the local CTI port (LCP).
- Step 5** Check the **Sign in as a Mobile Agent** check box.
- The Mode and Dial Number fields appear.
- Step 6** From the Mode drop-down list, choose the mode you want to use.
- In **Call by Call** mode, your phone is dialed for each incoming call and disconnected when the call ends.
- In **Nailed Connection** mode, your phone is called when you sign in and the line stays connected through multiple customer calls.
- Step 7** In the Dial Number field, enter the number for the phone you are using.

Option	Description
ID	The agent ID.
Password	Your supervisor assigns this password.
Extension	The agent's extension.
Sign in as Unified Mobile Agent	Select to sign in as a Unified Mobile Agent.
Mode	Call by Call or Nailed Connection
Dial Number	The number of the phone being used.

Step 8 Click **Sign In**.

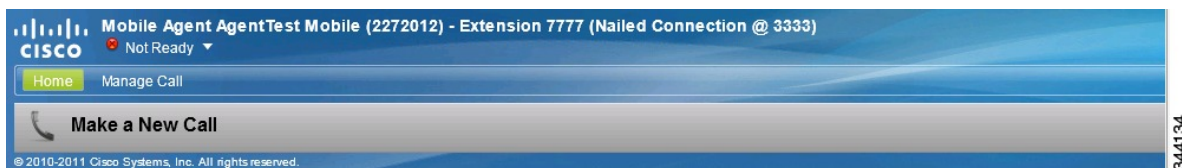
Note In Nailed Connection mode, the desktop must receive and answer a setup call before sign-in is complete.

In Call by Call mode, the dial number provided is not verified. To ensure that the number is correct, verify the number in the header on the Agent Desktop after sign-in is complete.

Verify Sign-In to Cisco Finesse

Check to be sure the Finesse Agent Desktop displays the following in the header:

- *Mobile Agent* before your agent name
- The mode used (Call by Call or Nailed Connection)
- The dial number you provided



Enable Ready State

You must be in Ready state to process incoming calls.

Choose **Ready** from the drop-down list below the agent name.

Note If you are in call-by-call mode, you must answer and end each incoming call on your physical phone. After you answer a call, you must perform all other call control functions (such as Conference, Transfer, Hold, Retrieve) using the desktop.

With call-by-call connection, an agent cannot end one leg of a transfer without terminating it at the other end. The transfer must either be fully completed or both legs completely dropped.

If you are in Nailed Connection mode, after you answer the initial setup call, you must perform all other call control functions using the desktop.

Make a Call

Step 1 From the drop-down list below the agent name, choose **Not Ready**.

Note You must be in Not Ready state to make a call.

Step 2 Click **Make a New Call**.

Step 3 Enter the number you want to call on the keypad, and then click **Call**.

If you are in Call by Call mode, the CTI server sends a setup call to your phone. A message appears on the keypad that states the following:

A call will be initiated to your phone which must be answered before an outbound call to your destination can be made.

After the setup call is answered, the system establishes the outbound call to the destination specified.

Serviceability

On a Mobile Agent call flow, CUCM may return a 404 error due to the absence of a agent greeting, leading to call failure. To fix this issue, do the following:

1. Create a new Run External Script node. Map the backup media of the script to the agent greeting recording (media file).

2. Add the Run External Script node between the failure path of the AgentGreeting Run External Script node and the End node.
3. Connect the Run External Script node's success path to the existing Release Call node and failure path to the existing End node.



Note This fix may add a short delay of one to two seconds to the call flow.
For information about [Agent Greeting Play Script](#), on page 30.



CHAPTER 10

Post Call Survey

- [Post Call Survey, on page 145](#)
- [Configure Post Call Survey in CVP, on page 146](#)
- [Configure Unified CCE, on page 146](#)

Post Call Survey

A Post Call Survey takes place after the call. Typically, you use the survey to determine whether a customer was satisfied with the call experience. You configure a call flow that sends the call to a DNIS for the Post Call Survey after the agent disconnects from the caller.

Your VRU asks callers whether they want to participate in a Post Call Survey. If they choose to do so, they are automatically transferred to the Post Call Survey after the call flow completes.

Post Call Survey Use Case

The caller is typically asked if they want to participate in a survey after the call. Your solution can determine based on dialed numbers to invoke the post call survey at the end of a call. When the customer completes the conversation with an agent, the customer is automatically redirected to a survey. When the agent ends the call, it initiates the Post Call Survey.

A customer can use the keypad on a touch tone phone and voice with ASR/TTS to respond to questions asked during the survey. For the solution, the post call survey call is just like another regular call. The Post Call Survey retrieves the call context information from the original customer call.

Post Call Survey Design Impacts

Observe the following conditions when designing a Post Call Survey:

- A Post Call Survey initiates when the last agent ends the call. The call routing script launches a survey script.
- The mapping of a dialed number pattern to a Post Call Survey number enables the Post Call Survey feature for the call.
- The value of the expanded call variable `user.microapp.isPostCallSurvey` controls whether the call transfers to the Post Call Survey number.

- If **user.microapp.isPostCallSurvey** is set to **y** (the implied default), the call transfers to the mapped post call survey number.
- If **user.microapp.isPostCallSurvey** is set to **n**, the call ends.
- To route all calls in the dialed number pattern to the survey, your script does not have to set the **user.microapp.isPostCallSurvey** variable. The variable is set to **y** by default.
- You cannot have a REFER call flow with Post Call Survey. REFER call flows remove Unified CVP from the call. But, Post Call Survey needs Unified CVP because the agent has already disconnected.
- For Unified CCE reporting purposes, the Post Call Survey call inherits the call context for the initial call. When a survey starts, the call context of the customer call that was transferred to the agent replicates into the call context of the Post Call Survey call.
- The expanded call variable **isPostCallSurvey** will be cached only when the UCCE router generates a label for CVP.

Configure Post Call Survey in CVP

Complete the following procedure to configure Post Call Survey in Unified CVP.

Step 1 Log in to the Unified CVP Operations Console and choose **System > Dialed Number Pattern**.

Step 2 Enter the following configuration settings to associate incoming dialed numbers with survey numbers:

- **Dialed Number Pattern** - Enter the appropriate dialed number.

The incoming Dialed Number for calls being directed to a Post Call Survey Dialed. This is the Dialed Number you want to redirect to the survey.

- **Enable Post Call Survey for Incoming Calls** - Select to enable post call survey for incoming calls.
- **Survey Dialed Number Pattern** - Enter the dialed number of the Post Call Survey. This is the dialed number to which the calls should be transferred to after the normal call flow completes.
- Click **Save** to save the Dialed Number Pattern.

Step 3 Click **Deploy** to deploy the configuration to all Unified CVP Call Server devices.

Configure Unified CCE

Configure ECC Variable

You need not configure Unified CCE to use Post Call Survey, however, you can turn the feature off (and then on again) within an ICM script by using the ECC variable **user.microapp.isPostCallSurvey** and a value of **n** or **y** (value is case insensitive) to disable and re-enable the feature.

Configure the ECC variable to a value of **n** or **y** before the label node or before the Queue to Skillgroup node. This sends the correct value to Unified CVP before the agent transfer. This ECC variable is not needed to

initiate a Post Call Survey call, but you can use it to control the feature when the Post Call Survey is configured using the Operations Console.

When the DN is mapped in the Operations Console for Post Call Survey, the call automatically transfers to the configured Post Call Survey DN.

Complete the following procedure to enable or disable the Post Call Survey:

-
- Step 1** On the Unified CCE Administration Workstation, using configuration manager, select the **Expanded Call Variable List tool**.
 - Step 2** Create a new ECC Variable with **Name: user.microapp.isPostCallSurvey**.
 - Step 3** Set **Maximum Length** to 1.
 - Step 4** Select the **Enabled** check box then click **Save**.
-



CHAPTER 11

Precision Queue

- [Capabilities, on page 149](#)
- [Initial Setup, on page 155](#)

Capabilities

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)]

Administrators can see and manage attributes. Supervisors can configure attributes for their supervised agents on the Attributes tab of the Agents tool.

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.

Attributes

Attributes identify a call routing requirement, such as language, location, or agent expertise. You can create two types of attributes: Boolean or Proficiency.

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.

You must take system limits into account when you assign attributes to agents, and satisfy both of the following conditions:

- A) an agent can have a maximum of 50 attributes

and

- B) an agent can belong to a maximum total of 50 combined precision queues and skill groups

Failure to meet both of these conditions will result in an unsuccessful configuration operation.

For example, if a particular attribute is used in many precision queues, and that attribute is assigned to an agent, that agent belongs to all of those precision queues. It is therefore possible to exceed condition B by assigning just a few attributes to an agent, if those attributes are used in many precision queues.

It is therefore prudent to plan carefully and to keep system limits in mind when creating attributes and adding them to precision queues.

Navigate to **Unified CCE Administration > Organization > Skills > Attributes** 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.

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 to 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).

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.

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.

Dynamic Limits for Skill Groups and Precision Queues Per Agent

The number of skill groups and precision queues per agent significantly affects the following subcomponents of Unified CCE:

- Cisco Finesse servers
- Agent PGs
- Router
- Logger



Note We use *queue* as a common term for skill groups and precision queues.

To maintain the performance of your solution, periodically remove unused queues.

The Reference Designs set a standard limit for the average queues per agent on each PG. On a particular PG, some agents can have more queues than other agents. As long as the average across all the agents on the PG is within the limit, you can still have the maximum active agents on that PG.

For example, assume that you have three groups of agents on a PG in a 4000 Agent Reference Design:

- Group A has 500 agents with five queues each.
- Group B has 1000 agents with 15 queues each.
- Group C has 500 agents with 25 queues each.

These three groups average to 15 queues per agent, so you can have them all on a single PG under the standard limits.

You can also exceed that standard limit if you reduce the number of agents on each PG and on the whole system.



Note See the configuration tables in the configuration limits chapter for the standard limits.

The Cisco Finesse server doesn't display statistics for unused queues. So, the active queues affect the performance of the Cisco Finesse server more than the total configured queues.

The Cisco Finesse desktop updates queue (skill group) statistics at 10-second intervals. The Cisco Finesse Desktop also supports a fixed number of queue statistics fields. You can't change these fields.

This table shows the approximate reduction in the number of agents your solution can support with more queues per agent:

Table 13: Dynamic Agents and Queues Limits

Average Queues per Agent	Maximum Agents per PG	Maximum Agents for 2000 Agent Reference Design	Maximum Agents for 4000 Agent Reference Design ²	Maximum Agents for 12000 Agent Reference Design	Maximum Agents for 24000 Agent Reference Design
10	2000	2000	4000	12000	24000
15	2000	2000	4000	12000	16000
20	1500	1500	3000	9000	12000
30	1000	1000	2000	6000	8000
40	750	750	1500	4500	6000
50	600	600	1200	3600	4800

² You can't have more than 4000 Agents on a Rogger deployment.

Unified CCE supports a maximum of 50 unique skill groups across all agents on a supervisor's team, including the supervisor's own skill groups. If this number is exceeded, all skill groups that are monitored by the supervisor still appear on the supervisor desktop. However, exceeding this number can cause performance issues and isn't supported.



Note Each precision queue that you configure creates a skill group for each Agent PG and counts toward the supported number of skill groups per PG. The skill groups are created in the same Media Routing Domain as the precision queue.

Initial Setup

When you configure precision queues associated with a large number of agents, the system avoids potential overload conditions by updating the agent associations as system resources allow. Updates may take a few minutes. If you submit multiple configuration updates, the system has a threshold of five concurrent configuration updates, and will reject any updates that exceed the threshold.

Add Attributes

- Step 1** Navigate to **Unified CCE Administration > Organization > Skills > Attributes**.
- 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> .

Field	Required	Description
Description	no	Enter a maximum of 255 characters to describe the attribute.
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 Click **Save**.

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 department is available only when departments are configured.

Assign Attributes to Agents

Step 1 With the selected agent displayed, click the **Attributes** tab.

Step 2 Complete the **Attributes** tab:

This tab shows the attributes associated with this agent and their current values.

Click **Add** to open a popup list of all attributes, showing the name and current default value for each.

- Click the attributes you want to add for this agent.
- Set the attribute value as appropriate for this agent.

Add Precision Queue

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
Description	no	Enter up to 255 characters to describe the precision queue.
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> .
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.

Name	Required	Description
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>
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.</p> <p>The field defaults to the system default.</p> <p>To select a different bucket interval:</p>

- 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**.

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.

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.

-
- 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 159](#) 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.

Configure a Static Precision Queue

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

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.



CHAPTER 12

Single Sign-On

- [Single Sign-On](#), on page 163
- [Single Sign-On Configuration Flow](#), on page 166
- [Configure an Identity Provider \(IdP\)](#), on page 166
- [Set the Principal AW for Single Sign On](#), on page 174
- [Set Up the System Inventory for Single Sign-On](#), on page 174
- [Configure the Cisco Identity Service](#), on page 175
- [Register Components and Set Single Sign-On Mode](#), on page 178
- [Hostname or IP Address Change](#), on page 179
- [Single Sign-On and the Agent Tool](#), on page 179
- [Migration Considerations Before Enabling Single Sign-On](#), on page 179
- [Migrate Agents and Supervisors to Single Sign-On Accounts](#), on page 181
- [Allowed Operations by Node Type](#), on page 182
- [Configure SAML Certificate Secure Hash Algorithm from SHA-1 to SHA-256](#), on page 183
- [Access Public Key Signing Certificate](#), on page 183
- [Single Sign-On Log Out](#), on page 184

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.



Note Before enabling SSO in Unified CCE, ensure to sign in to the Cisco Unified Intelligence Center OAMP interface and perform the Unified CCE User Integration operation (Cluster Configuration > UCCE User Integration) once manually to import the Supervisors with the required roles.

SSO is an optional feature whose implementation requires you to enable the HTTPS protocol across the enterprise solution.

You can implement single sign-on in one of these modes:

- **SSO** - Enable *all* agents and supervisors in the deployment for SSO.
- **Hybrid** - Enable agents and supervisors *selectively* in the deployment for SSO. Hybrid mode allows you to phase in the migration of agents from a non-SSO deployment to an SSO deployment and enable SSO for local PGs. Hybrid mode is useful if you have third-party applications that don't support SSO, and some agents and supervisors must be SSO-disabled to sign in to those applications.
- **Non-SSO** - Continue to use existing Active Directory-based and local authentication, without SSO.

SSO uses Security Assertion Markup Language (SAML) to exchange authentication and authorization details between an identity provider (IdP) and an identity service (IdS). The IdP authenticates based on user credentials, and the IdS provides authorization between the IdP and applications. The IdP issues SAML assertions, which are packages of security information transferred from the IdP to the service provider for user authentication. Each assertion is an XML document that contains trusted statements about a subject including, for example, username and privileges. SAML assertions are digitally signed to ensure their authenticity.

The IdS generates an authentication request (also known as a SAML request) and directs it to the IdP. SAML does not specify the method of authentication at the IdP. It may use a username and password or other form of authentication, including multi-factor authentication. A directory service such as LDAP or AD that allows you to sign in with a username and a password is a typical source of authentication tokens at an IdP.

Cisco IdS has now shifted to asymmetric key encryption for signing the tokens generated for authentication. This allows any client with the matching public key to easily and conveniently authorize any other client that has a token that is signed using the matching private key. You can access the public key using the Cisco IdS CLIs that are described in [Access Public Key Signing Certificate, on page 183](#). The public key can be freely distributed without any security concerns. All solution components monitor the public encryption key exposed by Cisco IdS using the REST APIs for their token authentication purposes. For more information about the SSO SDK, see [Cisco Finesse REST API with SSO Guide](#).



Note Due to the change in Cisco IdS token mechanism starting 12.6.2, agents must log out and log in to Finesse Desktop after Cisco IdS is upgraded to 12.6(2). To avoid this requirement, install 12.6(2) ES02. For more information, see the [Cisco Unified Contact Center Enterprise Installation and Upgrade Guide](#) or [Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide](#).

Prerequisites

The Identity Provider must support Security Assertion Markup Language (SAML) 2.0. See the *Compatibility Matrix* for your solution at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html><https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html> for details.

Contact Center Enterprise Reference Design Support for Single Sign-On

Unified CCE supports single sign-on for these reference designs:

- 2000 Agents
- 4000 Agents

- 12000 Agents
- 24000 Agents
- Contact Director (Maximum of 24000 agents, Each target system must include a dedicated Cisco IdS deployment.)

Co-residency of Cisco Identity Service by Reference Design

Reference Design	Unified CCE
2000 Agent	Cisco IdS is co-resident with Unified Intelligence Center and Live Data on a single VM.
4000 Agent	Standalone Cisco IdS VM
12000 Agent	Standalone Cisco IdS VM
24000 Agent	Standalone Cisco IdS VM

Single Sign-On Support and Limitations

Note the following points that are related to SSO support:

- To support SSO, enable the HTTPS protocol across the enterprise solution.
- SSO supports agents and supervisors only. SSO support is not available for administrators in this release.
- In the 12,000 Agent Reference Design, a maximum of 12,000 agents use SSO at one time.
- SSO supports multiple domains with federated trusts.
- SSO supports only contact center enterprise peripherals.
- SSO support is available for Agents and Supervisors that are registered to remote or main site PG in global deployments.

Note the following limitations that are related to SSO support:

- SSO support is not available for third-party Automatic Call Distributors (ACDs).
- The SSO feature does not support Cisco Finesse IP Phone Agent (FIPPA).
- The SSO feature does not support Cisco Finesse Desktop Chat.
- In Hybrid mode,
 - When an agent in SSO mode tries to log in to CUIC, and if the agent does not exist in CUIC, the agent cannot log in to CUIC.
 - When a Supervisor in SSO mode tries to log in to CUIC, and if the Supervisor user does not exist in CUIC, the Supervisor cannot log in to CUIC. For the Supervisor to log in to CUIC, perform Unified CCE User Integration. For more information on Unified CCE User Integration, see *Administration Console User Guide for Cisco Unified Intelligence Center* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html>.

Single Sign-On Configuration Flow



Note To ensure that token validations based on token lifetimes are correctly applied, it is mandatory that you synchronize the time in Cisco IdS, IdP, and all IdS clients, including VPN-Less reverse proxy hosts, to the same NTP source (preferred) or to the same NTP stratum.



Note It is recommended that the Administrator configures SSO from the IdS publisher node.

1. Install the appropriate release of the CCE solution. For more information, see Cisco Unified Contact Center Enterprise Installation and Upgrade Guide at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html>
2. Install the Cisco Identity Service (Cisco IdS). For more information, see Cisco Unified Contact Center Enterprise Installation and Upgrade Guide at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html>
3. Configure an Identity Provider (IdP).
4. Configure System Inventory.
5. Configure the Cisco IdS.
6. Register and test SSO-compatible components with the Cisco IdS.
7. Choose the SSO mode.
8. Enable multiple users at once for SSO by using the SSO migration tool, or enable users one at time by using the configuration tools.

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 167

Sequence	Task
2	Set Authentication Type. See Authentication Types , on page 167.
4	Enable Signed SAML Assertions , on page 171
5	Optionally Customize the AD FS Sign-In Page in Windows Server to Allow User ID , on page 172

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>.
- For AD FS in Windows Server, see *AD FS Technical Reference* at <https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services>.



Note SSO for Unified CCE supports IdPs other than MS, and AD FS. For the list of supported IdPs see the Compatibility matrix <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html>



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.

Authentication Types

Cisco Identity Service supports form-based authentication and Kerberos windows 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.

Integrate Cisco IdS with AD FS

Follow these steps to integrate the Cisco IdS with AD FS.

SUMMARY STEPS

1. In the Server Manager, open **AD FS Management**.
2. For form-based authentication, set the **Authentication Methods** for **Intranet** to **Forms Authentication**.
3. Download LAN SP metadata and reverse-proxy cluster SP metadata from the Cisco IdS publisher.
4. Download the IdP metadata file, `federationmetadata.xml`, from the following location:
5. Do one of the following to upload the IdP metadata file, you downloaded at step 4, to the Cisco Ids server:
6. Follow these steps to create a Relying Party Trust.
7. Do the following to set the properties for the Relying Party Trust created at Step 5. Right-click on the Relying Party Trust and click **Properties**. In the **Properties** window:
8. In the list of Relying Party Trusts, right-click on your Relying Party Trust, and select the option to edit the Rules/Claim Issuance Policy from the menu.
9. In the **Edit Claim Rules/Edit Claim Issuance Policy** window that opens, click **Add Rule** and then click **OK**.
10. In the **Add Transform Claim Rule Wizard** that opens, follow these steps to create the first claim:
11. Repeat steps 8 and 9 to open the **Add Transform Claim Rule** wizard. In the **Add Transform Claim Rule** wizard, follow these steps to create the second claim:
12. Click **OK**.

DETAILED STEPS

Step 1 In the Server Manager, open **AD FS Management**.

Step 2 For form-based authentication, set the **Authentication Methods** for **Intranet** to **Forms Authentication**.

Step 3 Download LAN SP metadata and reverse-proxy cluster SP metadata from the Cisco IdS publisher.

- Open the **Identity Service Management** console at `https://<CiscoIdS server address>:8553/idsadmin`

From the menu on the left, select **Settings**. In the **IdS Trust** tab, download the XML file.

- In Unified CCE Administration, go to **Infrastructure Settings > Device Configuration > Identity Service > Identity Service Settings**.

In the **IdS Trust** tab, download the XML file.

Note Ensure your browser's security settings allow downloads from the Cisco IdS site.

Step 4 Download the IdP metadata file, `federationmetadata.xml`, from the following location:

`https://<ADFS Server FQDN>/federationmetadata/2007-06/federationmetadata.xml`

Step 5 Do one of the following to upload the IdP metadata file, you downloaded at step 4, to the Cisco Ids server:

- In the **Identity Service Management** console, select **Settings > IdS Trust**.

Click **Next** and then click **Upload Idp Metadata**.

- In the **Unified CCE Administration** console, navigate to **Infrastructure Settings > Device Configuration > Identity Service > Identity Service Settings > Ids Trust**.

Click **Next** and then click **Upload Idp Metadata**.

Note Cisco IdS supports SAML self-signed certificates for authorization and authentication.

Step 6 Follow these steps to create a Relying Party Trust.

- a) In the Server Manager, open **AD FS Management**.
- b) Select the **Add Relying Party Trust** option from the AD FS menu.
- c) In the **Add Relying Party Trust** wizard, click **Select Data Source**.
- d) Select the **Import data about the relying party from a file** option and then click **Browse** to open the SAML SP metadata XML file you downloaded at Step 3 and click **Next**.
- e) In the **Display name** field, enter a unique name for the relying party and click **Next**.
- f) *This step is applicable only for Windows Server 2012 R2.* In the **Configure Multi-factor Authentication Now** step, select **I do not want to configure multi-factor authentication settings for the relying party at this time**.
- g) Select the option that permits all users and click **Next**.
- h) Skip the option to edit the Rule/Claim Issuance Policy for now (you edit the policy from Step 8 onwards) and click **Close** to complete adding the relying party trust.

Step 7 Do the following to set the properties for the Relying Party Trust created at Step 5. Right-click on the Relying Party Trust and click **Properties**. In the **Properties** window:

- Configure the following under the **Identifiers** tab:

Field	Description
Display name	The unique name of the identifier.
Relying party identifier	FQDN of the publisher node of Cisco Identity Server from which you downloaded the Cisco IdS metadata file at step 3.
	FQDN of the subscriber node of Cisco Identity Server.

- Under the **Advanced** tab, choose **SHA-256** from the **Secure hash algorithm** field.

Step 8 In the list of Relying Party Trusts, right-click on your Relying Party Trust, and select the option to edit the Rules/Claim Issuance Policy from the menu.

Step 9 In the **Edit Claim Rules/Edit Claim Issuance Policy** window that opens, click **Add Rule** and then click **OK**.

Step 10 In the **Add Transform Claim Rule Wizard** that opens, follow these steps to create the first claim:

- a) In the **Choose Rule Type** step, select **Send LDAP Attributes as Claims** from the **Claim rule template** drop-down list and click **Next**.
- b) In the **Configure Claim Rule** step, configure the following:

Field	Description
Claim Rule Name	Enter "NameID"
Attribute Store	Select Active Directory .

Field	Description
Mapping of LDAP Attributes to Outgoing Claims	<p>If the identifier is a Security Account Name (SAM), do the following:</p> <ul style="list-style-type: none"> • Select SAM-Account-Name as one of the LDAP attributes and set the Outgoing Claim Type to "uid." • Select User-Principal-Name as one of the LDAP attributes and set the Outgoing Claim Type to "user_principal". <p>If the identifier is a User Principal Name (UPN), do the following:</p> <ul style="list-style-type: none"> • Select User-Principal-Name as one of the LDAP attributes and set the Outgoing Claim Type to "uid." • Select User-Principal-Name again as the LDAP attribute and set the Outgoing Claim Type to "user_principal." <p>The "uid" identifies the authenticated user in the claim sent to the applications.</p> <p>The "user_principal" identifies the authentication realm of the user in the assertion sent to Cisco Identity Service.</p>

- c) Click **Finish**.

Step 11

Repeat steps 8 and 9 to open the **Add Transform Claim Rule** wizard. In the **Add Transform Claim Rule** wizard, follow these steps to create the second claim:

- a) In the **Choose Rule Type** step, select **Send Claims Using a Custom Rule** from the **Claim rule template** drop-down list and click **Next**.
- b) In the **Configure Claim Rule** step, configure the following:

1. In the **Claim rule name** field, enter the FQDN of the Cisco Identity Server publisher's primary node.
2. Add the following to the **Custom Rule** field:

```
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>");
```

- c) 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 12 Click **OK**.

Enable Signed SAML Assertions

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

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 Click **Next** as you have already downloaded the required metadata.

Step 7 Click **Next** as you have already established trust relationship between IdP and IdS.

The configured IdP Entity ID is listed.

Note If reverse-proxy is configured for IdP, the IdP proxy url is listed at the bottom of the page.

Step 8 Click **Test SSO Setup** to test the required entity where the **SSO Status** displays **Needs Validation**. **SSO Status** can be **Successful**, **Unsuccessful**, or **Needs Validation**.

Note If **Unsuccessful**, ensure that the claim you created on the AD FS is enabled or the rule has the correct names for IdS and AD FS.

Administrator client machine requires connectivity to reverse-proxy nodes for validating SSO connection with reverse-proxy.

Multi-Domain Configuration for Federated ADFS

In Multi-Domain Federation in ADFS, an ADFS in one domain provides federated SAML authentication for users in other configured domains. In such cases, additional configuration is required:

- Primary ADFS Configuration that refers to the ADFS to be used in IdS.

- Federated ADFS Configuration that refers to the ADFS, whose users can log in via IdS, thus is the primary ADFS.

Federated ADFS Configuration

In each federated ADFS, create the relying party trust for primary ADFS and the claim rules configured.

Primary ADFS Configuration

Before you begin

In the Claim Provider Trust, ensure that the **Pass through or Filter an Incoming Claim** rules are configured with pass through all claim values as the option

-
- Step 1** Name ID
- Step 2** Choose Name ID from Incoming Claim Type drop box
- Step 3** Choose **Transient** as the option for Incoming NameID format
- Step 4** uid: This is a custom claim. Enter the value uid in the **Incoming Claim Type** drop box.
- Step 5** user_principal: This is a custom claim. Type the value user_principal in the **Incoming Claim Type** drop box.
- In the relying party trust for IdS, add **Pass though or Filter an Incoming Claim** rules with pass through all claim values as the option.
- Step 6** NameIDFromSubdomain
- Step 7** Choose Name ID from Incoming Claim Type drop box
- Step 8** Choose Transient as the option for Incoming NameID format
- Step 9** uid: This is a custom claim. Type the value uid in the Incoming Claim Type drop box
- Step 10** user_principal: This is a custom claim. Type the value user_principal in the Incoming Claim Type drop box
-

Kerberos Authentication (Integrated Windows Authentication)

Before you begin

The CCE solution supports Kerberos authentication.

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.

-
- 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
```
-

Set the Principal AW for Single Sign On



Note This procedure is applicable only for Packaged CCE 4K or 12K agent reference design.

During deployment, the first SideA AW machine in the CSV file is the Principal AW.

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.

After deployment, you can change the Principal AW by selecting a different AW on the Inventory page. Set the AW on which you make most of your configuration changes as the Principal AW.

Step 1 In Unified CCE Administration, choose **Inventory** to open the **Inventory** page.

Step 2 Set the Principal AW:

a) Click the AW that you want to be the Principal AW.

Note You can only specify one Principal AW for each Unified CCE system.

The Edit CCE AW window opens.

b) Check the **PrincipalAW** check box.

c) Enter the Unified CCE Diagnostic Framework Service domain, username, and password.

d) Click **Save**.

Set Up the System Inventory for Single Sign-On

Step 1 As there's no automatic association of IDS in UCCE, UCCE deployment is manual from CCE Administration for each VM. Navigate to **CCE Administration > Overview > Inventory**.

Step 2 Click the pencil icon for the External HDS for 2000 Agents deployment.

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**.

Note If you're working with a Cisco IdS cluster, perform these steps on the Cisco IdS primary publisher node.

For CCE 4000, 12000, and 24000 Agents deployment, ensure that the Principal AW is configured and functional before using the Single Sign-On tool in UCCE Administration.

Also, add the SSO-capable machines to the Inventory, and select the default Cisco IdS for each of the SSO-capable machines.

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**

- 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.

If you are working with a Cisco IdS cluster, perform these steps on the Cisco IdS primary publisher node.

Step 1 In the Unified CCE Administration, choose **Overview > Infrastructure Settings > Device Configuration**.

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 Click **Save**.

Step 7 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. Regenerating the certificates for token signing requires all agents to logout and relogin to the Cisco Finesse desktop. Therefore ensure that you plan for downtime to your Contact Center before you regenerate the public-private key pair that Cisco IdS uses to authenticate agents. After you regenerate the new key pair, you must reboot Cisco IdS so that the agents can relogin to their applications. Ensure that you CA sign the regenerated public-private key pair, if required and then reupload it to the clients that are dependent on the public-private key pair. For example, if you are using the digital channels service, you must reupload the private-public key pair on to Control Hub for your agents to resume with the Manage Digital Channel gadget. For instructions, see *Provision Webex Connect digital services for your organization*.
- 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 8 Click **Save**.**Step 9** 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 10 To add a client on the **Identity Service Clients** tab:

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

Step 11 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 12 Click **Identity Service Settings**.**Step 13** Click **Troubleshooting** to perform some optional troubleshooting.**Step 14** From the **Log Level** drop-down list, set the local log level by choosing **Error**, **Warning**, **Info** (the default), **Debug**, or **Trace**.**Step 15** To receive errors in Syslog format, enter the name of the Remote Syslog Server in the **Host** (Optional) field.**Step 16** Click **Save**.

You can now:

- Register components with the Cisco IdS.
- Enable (or disable) SSO for the entire deployment.



Note If SSO is enabled in the deployment, then import all the IdS server nodes certificate into Cisco Finesse, CUIC, and LiveData component trust store.

Install Certification Authority (CA) Certificate

To eliminate browser security warnings each time you sign in, obtain an application and root certificate signed by a CA. To obtain the application and a root certificate, use the Certificate Management utility from Cisco Unified Operating System Administration.

To open Cisco Unified Operating System Administration in your browser, enter: `https://fqdn of IdS server:8443/cmplatform`.

Sign in using the username and password for the Application User account created during IdS installation.

If you want to install CA signed certificates for IdS instead of out of the box self-signed certificates, you need to install the certificates on both the Cisco IdS nodes.

-
- Step 1** Log in to Cisco Unified Operating System Administration.
 - Step 2** Navigate to **Security > Certificate Management** and then click **Find** to list all the certificates. The **Certificate List** page is displayed.
 - Step 3** Click **Generate CSR**. The **Generate Certificate Signing Request** window is displayed.
 - Step 4** Select **tomcat** from the **Certificate Purpose** list. By default, **tomcat** is selected.
 - Step 5** Ensure that the default values are retained in the **Distribution**, **Common Name**, **Parent Domain**, **Key Type**, **Key Length**, and **Hash Algorithm** fields.
 - Step 6** Click **Generate** to generate the CSR.
 - Step 7** Click **Close**. The **Certificate List** page is displayed.
 - Step 8** Click **Download CSR**. The **Download Certificate Signing Request** window is displayed.
 - Step 9** Select **tomcat** from the **Certificate Purpose** list and click **Download CSR**.
 - Step 10** Use the downloaded CSR and share it with the certificate authority to obtain the public certificate.
 - Step 11** Log in to Cisco Unified Operating System Administration again and navigate to **Security > Certificate Management**, and then click **Find** to list all the certificates. The **Certificate List** page is displayed.
 - Step 12** Click **Upload Certificate/Certificate chain**. The **Upload Certificate/Certificate chain** window is displayed.
 - Step 13** Select **tomcat** from the **Certificate Purpose** list.
 - Step 14** Click the **Choose File** button and navigate to select the certificate chain that includes the certificated obtained from the certiciate authority and then click **Open**.
 - Step 15** Click **Upload** to upload the certificate.
 - Step 16** Click **Close**. The **Certificate List** page is displayed.
 - Step 17** After successfully uploading the certificate, navigate to **Security > Certificate Management**.
 - Step 18** Click **Find** to open the list of certificates. The **Certificate List** page is displayed. Verify that the uploaded certificates are listed.
 - Step 19** Restart the nodes using the CLI command `utils system restart`.
-

**Note**

- To avoid the certificate exception warning, you must access the servers using the Fully Qualified Domain Name (FQDN). Ensure that the Distribution field in the CSR is the FQDN of the server
- Ensure that the Certificate Authority (CA) certificate is RSA-signed.

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.

Step 1 In the Unified CCE Administration, navigate to **Features > Single Sign-On**.

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.

Hostname or IP Address Change

If you change the Hostname or IP Address of the Cisco IdS server, then perform the following:

- Re-generate the SAML certificate.
- Re-establish trust relationship between IdP and IdS.
- If the components are registered earlier, then
 - Re-register all the SSO components.
 - Perform the SSO Test to check if all the SSO components are registered. Verify that the test is successful for each component.

Single Sign-On and the Agent Tool

When the global SSO-enabled setting is Hybrid, you can use the Unified CCE Administration Agent Tool to enable agents individually for single sign-on.

In the tool, check the **Single Sign-On** check box to require a selected agent to sign in with SSO authentication. For supervisors and for agents with single sign-on (SSO) enabled, the username is the user's Active Directory or SSO account username.



Note The check box is disabled when the global SSO mode is set to SSO or non-SSO.

To update agent records in bulk, use the Bulk Jobs Agent content file.

Migration Considerations Before Enabling Single Sign-On

Administrator User and Single Sign-On in Unified Intelligence Center

During installation, Cisco Unified Intelligence Center creates an administrator user. This user is not enabled for SSO, as the user is known only to Unified Intelligence Center.

When you enable SSO, this administrator user is no longer able to log in to the Unified Intelligence Center and perform administrative tasks. These tasks include configuring datasources and setting permissions for other users, for example. To avoid this situation, perform the following steps before enabling SSO.

1. Create a new SSO user who has the same roles and permissions as those of the administrator user.
2. Log in to the CLI.
3. Run the following command:

```
utils cuic user make-admin username
```

in which the user name is the complete name of the new user, including the authenticator prefix as shown on the Unified Intelligence Center User List page.

The command, when performed, provides all the roles to the new user and copies all permissions from the administrator user to this new user.


Note

- The administrator's group memberships are not copied to the new user by this CLI command and must be manually updated. The new user, now a Security Administrator, can set up the group memberships.
- For any entity (for example, reports or report definitions), if this new user's permissions provide higher privileges than the administrator, the privileges are left intact. The privileges are not overwritten by this CLI command.

Browser Settings and Single Sign-On

If you have enabled single sign-on and are using Chrome, Edge Chromium (Microsoft Edge), or Firefox, verify that the browser options are set as shown in the following table. These settings specify that you do not want a new session of the browser to reopen tabs from a previous session.

Browser	Browser options to verify when using SSO
Chrome	<ol style="list-style-type: none"> 1. Open Chrome. 2. Click the Customize and control Google Chrome icon. 3. Click Settings. 4. In the On startup section of the Settings page, verify that the Open the New Tab page option is selected.
Edge Chromium (Microsoft Edge)	<ol style="list-style-type: none"> 1. Open Microsoft Edge. 2. Click the Settings and more (Alt+F) (...) icon. 3. Click Settings. 4. On the Settings page, click On startup, and verify that the Open a new tab radio button is selected.
Firefox	<ol style="list-style-type: none"> 1. Open Firefox. 2. Click the Open menu icon. 3. Click Options. 4. In the Startup section of the General page, verify that either the home page or a blank page is chosen in the When Firefox starts drop-down list.

Migrate Agents and Supervisors to Single Sign-On Accounts

If you are enabling SSO in an existing deployment, you can set the SSO state to hybrid to support a mix of SSO and non-SSO users. In hybrid mode, you can enable agents and supervisors selectively for SSO making it possible for you to transition your system to SSO in phases.

Use the procedures in this section to migrate groups of agents and supervisors to SSO accounts using the SSO Migration content file in the Unified CCE Administration Bulk Jobs tool. You use the Administration Bulk Jobs tool to download a content file containing records for agents and supervisors who have not migrated to SSO accounts. You modify the content file locally to specify SSO usernames for the existing agents and supervisors. Using the Administration Bulk Jobs tool again, you upload the content file to update the agents and supervisors usernames; the users are also automatically enabled for SSO.

If you do not want to migrate a user, delete the row for that user.



Important While the Finesse agent is logged in, changing the login name prevents the agent from answering or placing calls. In this situation, the agent can still change between *ready* and *not_ready* state. This affects all active agents, independent of whether SSO is enabled or disabled. Should you need to modify a login name, do so only after the corresponding agent is logged out. Note too that SSO migration (moving a non-SSO agent to be SSO-enabled, by either hybrid mode or global SSO mode) should not be done when the agent is logged in.

Step 1 In Unified CCE Administration, navigate to **Manage > Bulk Jobs**.

Step 2 Download the SSO Migration bulk job content file.

a) Click **Templates**.

The **Download Templates** popup window opens.

b) Click the **Download** icon for the SSO Migration template.

c) Click **OK** to close the **Download Templates** popup window.

Step 3 Enter the SSO usernames in the SSO Migration content file.

a) Open the template in Microsoft Excel. Update the **newUserName** field for the agents and supervisors whom you want to migrate to SSO accounts.

The content file for the SSO migration bulk job contains these fields:

Field	Required?	Description
userName	Yes	The user's non-SSO username.
firstName	No	The user's first name.
lastName	No	The user's last name.
newUserName	No	The user's new SSO username. Enter up to 255 ASCII characters. If you want to enable a user for SSO, but keep the current username, leave newUserName blank, or copy the value of userName into newUserName .

b) Save the populated file locally.

Step 4 Create a bulk job to update the usernames in the database.

- a) Click **New** to open the **New Bulk Job** window.
- b) Enter an optional **Description** for the job.
- c) In the **Content File** field, browse to the SSO Migration content file you completed.

The content file is validated before the bulk job is created.

d) Click **Save**.

The new bulk job appears in the list of bulk jobs. Optionally, click the bulk job to review the details and status for the bulk job. You can also download the log file for a bulk job.

What to do next

After all of the agents and supervisors in your deployment are migrated to SSO accounts, you can enable SSO globally in your deployment.

Allowed Operations by Node Type

The Cisco IdS cluster contains a publisher and a subscriber node. A publisher node can perform any configuration and access token operations. The operations that a subscriber node can perform depends on whether the publisher is connected to the cluster.

This table lists which operations each type of node can perform.

Table 14: Single Sign-On Allowed Operations

Operation	Allowed on Publisher	Allowed on Subscriber
Upload IdP metadata	Always	Never
Download SAML SP metadata	Always	Never
Regenerate SAML Certificate	Always	Never
Regenerate Token Encryption/Signing Key	Always	Never
Update AuthCode/Token Expiry	Always	Only when publisher is connected
Download Token Public Key	Always	Always
Add/Update/Delete Cisco IdS client configuration	Always	Only when publisher is connected
View Cisco IdS client configuration	Always	Always
View Cisco IdS status	Always	Always
Set Troubleshooting Log Level	Always	Always

Operation	Allowed on Publisher	Allowed on Subscriber
Set Remote Syslog server	Always	Always

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.

After the expiry of SHA-1, the administrator must configure SHA-256..

Perform this procedure after the upgrade has completed successfully.

-
- 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>
```
- 

## Access Public Key Signing Certificate

Login to the Cisco IdS admin console, and then run the following commands to access the public key signing certificate:

- **show ids token csr**—Displays the CSR corresponding to the public key that is used to validate the tokens.
- **show ids token certificate**—Displays the X.509 token certificate.
- **show ids token public\_key**—Displays the base64 encoded public key that is used for VPN-less SSO authentication.

# 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.

---



## CHAPTER 13

# Task Routing

---

- [Task Routing, on page 185](#)
- [Control SocialMiner Application Access, on page 194](#)
- [Task Routing API Request Flows, on page 196](#)
- [Failover and Failure Recovery, on page 203](#)
- [Task Routing Setup, on page 206](#)
- [Sample Code for Task Routing, on page 213](#)
- [Task Routing Reporting, on page 215](#)

## Task Routing

Task Routing describes the system's ability to route requests from different media channels to any agents in a contact center.

You can configure agents to handle a combination of voice calls, emails, chats, and so on. For example, you can configure an agent as a member of skill groups or precision queues in three different Media Routing Domains (MRD) if the agent handles voice, e-mail, and chat. You can design routing scripts to send requests to these agents based on business rules, regardless of the media. Agents signed into multiple MRDs may switch media on a task-by-task basis.

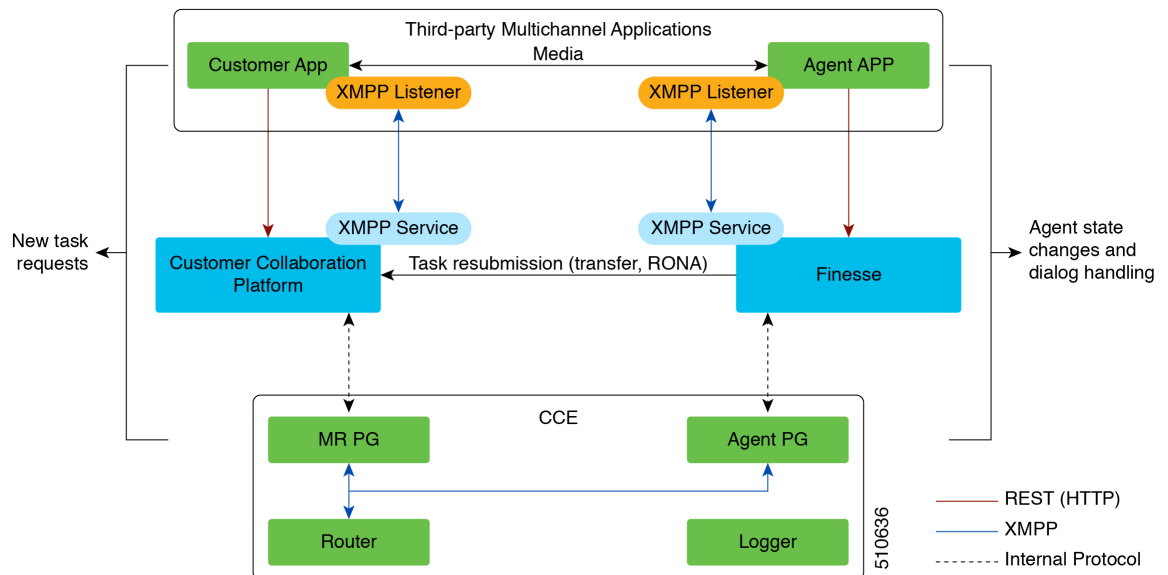
Enterprise Chat and Email provides universal queue out of the box. Third-party multichannel applications can use the universal queue by integrating with CCE through the Task Routing APIs.

Task Routing APIs provide a standard way to request, queue, route, and handle third-party multichannel tasks in CCE.

Contact Center customers or partners can develop applications using Customer Collaboration Platform and Finesse APIs in order to use Task Routing. The Customer Collaboration Platform Task API enables applications to submit nonvoice task requests to CCE. The Finesse APIs enable agents to sign into different types of media and handle the tasks. Agents sign into and manage their state in each media independently.

Cisco partners can use the sample code available on Cisco DevNet as a guide for building these applications (<https://developer.cisco.com/site/task-routing/>).

Figure 15: Task Routing for Third-party Multichannel Applications Solution Components



### Customer Collaboration Platform and Task Routing

Third-party multichannel applications use Customer Collaboration Platform's Task API to submit nonvoice tasks to CCE.

The API works in conjunction with Customer Collaboration Platform task feeds, campaigns, and notifications to pass task requests to the contact center for routing.

The Task API supports the use of Call variables and ECC variables for task requests. Use these variables to send customer-specific information with the request, including attributes of the media such as the chat room URL or the email handle.



**Note** CCE solutions support only the Latin 1 character set for Expanded Call Context variables and Call variables when used with Finesse and Customer Collaboration Platform. Arrays are not supported.

### CCE and Task Routing

CCE provides the following functionality as part of Task Routing:

- Processes the task request.
- Provides estimated wait time for the task request.
- Notifies Customer Collaboration Platform when an agent has been selected.
- Routes the task request to an agent, using either skill group or precision queue based routing.
- Reports on contact center activity across media.

### Finesse and Task Routing

Finesse provides Task Routing functionality via the Media API and Dialog API.

With the Media API, agents using third-party multichannel applications can:

- Sign into different MRDs.
- Change state in different MRDs.

With the Dialog API, agents using third-party multichannel applications can handle tasks from different MRDs.

## Task Routing Deployment Requirements

Task Routing for third-party multichannel applications deployment requirements:

- Finesse and Customer Collaboration Platform are required. Install and configure Finesse and Customer Collaboration Platform before configuring the system for Task Routing.

See the [Finesse documentation](#) and [Customer Collaboration Platform documentation](#).

By default, access to the Customer Collaboration Platform administration user interface is restricted. Administrator can provide access by unblocking the IP addresses of the clients. For more details, see the *Control Customer Collaboration Platform Application Access* topic in the [Cisco Customer Collaboration Platform Installation and Upgrade Guide](#) guide.

- You can install only one Customer Collaboration Platform machine in the deployment.
- Customer Collaboration Platform must be geographically colocated with one side of the Media Routing Peripheral Gateway (MR PG).
- Install Customer Collaboration Platform in a location from which CCE, Finesse, and the third-party multichannel Customer Collaboration Platform Task Routing application can access it over the network.

If you install Customer Collaboration Platform in the DMZ, open a port for CCE and Finesse to connect to it. The default port for CCE to connect to Customer Collaboration Platform is port 38001. Finesse connects to Customer Collaboration Platform over HTTPS, port 443.

Install the third-party multichannel application locally with Customer Collaboration Platform, or open a port on the Customer Collaboration Platform server for the application to connect to it.

## Supported Functionality for Third-Party Multichannel Tasks

Blind transfer is supported for third-party multichannel tasks submitted through the Task Routing APIs.

We do not support the following functionality for these types of tasks:

- Agent-initiated tasks.
- Direct transfer.
- Consult and conference.

## Plan Task Routing Media Routing Domains

Media Routing Domains (MRDs) organize how requests for each communication medium, such as voice and email, are routed to agents. You configure an MRD for each media channel in your deployment.

Finesse agents can sign in to any of the multichannel MRDs you create for Task Routing.

Important factors to consider when planning your MRDs include the following:

- Whether the MRD is interactive.
- The maximum number of concurrent tasks that an agent can handle in an MRD.
- Whether the MRDs are interruptible.
- For interruptible MRDs, whether Finesse accepts or ignores interrupt events.

To configure the settings and parameters described in the following sections, see the following documents:

- [Cisco Customer Collaboration Platform Developer Guide](#).
- [Cisco Finesse Web Services Developer and JavaScript Guide](#)
- [Unified CCE Administration and Configuration Manager Tools, on page 211](#)

### Interactive and Non-interactive MRDs

Interactive tasks are tasks in which an agent and customer communicate in real time with each other, such as chats and SMS messages. The customer usually engages with the agent through an application, like a chat window, and leaves this application open while waiting to be connected to an agent. Non-interactive tasks are asynchronous, such as email. The customer submits the request and then may close the application, checking later for a response from an agent.

| API Parameter or Setting                                                                                                                                                                                                              | API/Tool                                            | Possible Values                                                                                                                                      |                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                       |                                                     | Interactive Task/MRD                                                                                                                                 | Non-interactive Task/MRD                                                                                                                                            |
| <p><b>requeueOnRecovery</b></p> <p>Whether Customer Collaboration Platform re-queues or discards the task when Customer Collaboration Platform recovers from a failure.</p> <p>Set this parameter when submitting a task request.</p> | Customer Collaboration Platform Task Submission API | <b>False</b> - customers are waiting at an interface for an agent and can be notified if there is a problem. You don't need to resubmit these tasks. | <b>True</b> - customers are not waiting at an interface for an agent, and there is no way to alert them that there was a problem. You need to resubmit these tasks. |
| <p><b>dialogLogoutAction</b></p> <p>Whether active tasks are closed or transferred when an agent signs out or loses presence.</p> <p>Set this parameter when an agent signs in to a Media Routing Domain.</p>                         | Finesse Media Sign In API                           | <b>Close</b> - customers are engaged with an agent, and can be notified that the task has ended.                                                     | <b>Transfer</b> - customers are not engaged with an agent, and there is no way to alert them that the task has ended.                                               |



| API Parameter or Setting                                                                                                                                                                                                                                          | API/Tool                                                       | Possible Values                                                                                                                    |                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                   |                                                                | Interactive Task/MRD                                                                                                               | Non-interactive Task/MRD                                                                                                                                     |
| <p><b>Start Timeout</b></p> <p>The amount of time that the system waits for an agent to accept an offered task. When this time is reached, the system makes the agent not routable and re-queues the task.</p> <p>Set this parameter when configuring an MRD.</p> | Media Routing Domains tool in Unified CCE Administration       | <b>Shorter duration</b> - customer is waiting at an interface for the agent                                                        | <b>Longer duration</b> - customer is not waiting at an interface for an agent                                                                                |
| <p><b>Monitoring status of submitted tasks</b></p> <p>You can monitor status of submitted and queued tasks using either the Customer Collaboration Platform Task API to poll for status or Customer Collaboration Platform XMPP BOSH eventing.</p>                | Customer Collaboration Platform Task API or XMPP BOSH eventing | Use Customer Collaboration Platform Task API status polling for MRDs when you want to monitor the status of a single contact/task. | Use Customer Collaboration Platform XMPP BOSH eventing to receive updates on all contacts/tasks in the campaign supporting Universal Queue over one channel. |

### Maximum Concurrent Tasks Per Agent

Specify the maximum number of concurrent tasks for an agent in an MRD when an agent signs into the Finesse application, using the **maxDialogLimit** parameter in the **Finesse Media - Sign In API**.

See the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html> for the maximum number of tasks supported within an MRD and across MRDs for a single agent.

For agents handling interactive tasks, consider how many concurrent tasks an agent can handle reasonably. How many simultaneous chat sessions, for example, can an agent handle and provide good customer care? If you are using precision queue routing, keep in mind that CCE assigns tasks to agents who match attributes for step one, **up to their task limit**, until all of those agents are busy. CCE then assigns tasks to agents who match attributes for step two, up to their task limit, and so on.

### Interruptible and Non-Interruptible MRDs

When you create an MRD in the Unified CCE Administration Media Routing Domains tool, you select whether the MRD is interruptible.

- **Interruptible:** Agents handling tasks in the MRD can be interrupted by tasks from other MRDs. Non-interactive MRDs, such as an email MRD, are typically interruptible.
- **Non-interruptible:** Agents handling tasks in the MRD cannot be interrupted by tasks from other MRDs. The agents can be assigned tasks in the same MRD, up to their maximum task limits. For example, an

agent can handle up to three non-interruptible chat tasks; if the agent is currently handling two chat tasks, CCE can assign the agent another chat, but cannot interrupt the agent with a voice call. Interactive MRDs, such as a chat MRD, are typically non-interruptible. Voice is non-interruptible.

When an agent is working on a non-interruptible task, CCE does not assign a task in any other MRD to the agent. Any application handling the non-voice MRDs must follow the same rule. In certain cases, it is possible that a task from another media routing domain gets assigned to an agent who is working on a non-interruptible task in an MRD.

For example, if an agent is working on a non-interruptible chat MRD and makes an outbound call (internal or external) using the desktop or phone, CCE cannot prevent the agent from making that call. Instead, the system handles this situation differently. CCE marks the agent temp not routable across all media domains until the agent has completed all non-interruptible tasks the agent is currently working on. Because of this designation, the agent is not assigned any new tasks from any MRDs until finishing all current tasks. Even if the agent tries to go ready or routable, the agent's temp not routable status is cleared only after all tasks are complete.




---

**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.

---

### Accept and Ignore Interrupts

Specify whether an MRD accepts or ignores interrupt events when an agent signs into the Finesse application, using the **interruptAction** parameter in the **Finesse Media - Sign In API**. This setting controls the agent's state in an interrupted MRD and ability to work on interrupted tasks. The setting applies only when a task from a non-interruptible MRD interrupts the agent.

- **Accept:** When an agent is interrupted by a task from a non-interruptible MRD while working on a task in an interruptible MRD, Finesse accepts the interrupt event.

The agent, CCE task, and Finesse dialog state in the interrupted MRD change to INTERRUPTED.

The agent cannot perform dialog actions while a task is interrupted.



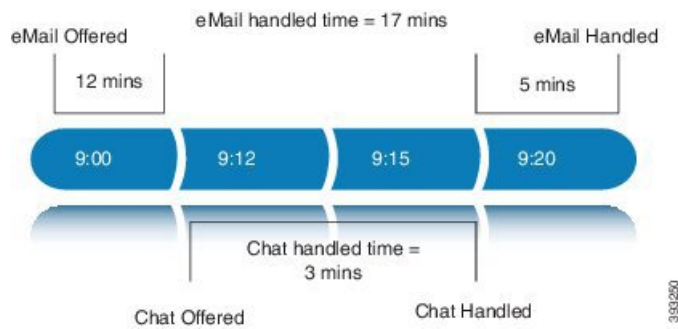

---

**Important** The application is responsible for disabling all dialog-related activities in the interface when an agent's state changes to INTERRUPTED.

---

The agent's time on task stops while the agent is interrupted.

Example: An agent has an email task for 20 minutes, and is interrupted for 3 of those minutes with a chat task. The handled time for the email task is 17 minutes, and the handled time for the chat task is 3 minutes.

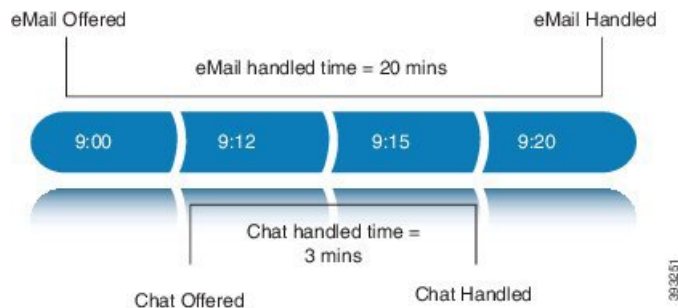


- **Ignore:** When an agent is interrupted by another task while working on a task in an interruptible MRD, Finesse ignores the interrupt event.

The new task does not affect any of the agent's other assigned tasks. The agent, CCE task, and Finesse dialog state in the interrupted MRDs do not change.

The agent can perform dialog actions on original task and the interrupting task at the same time. The agent's time on the original task does not stop while the agent is handling the interrupting task.

Example: An agent has an email task for 20 minutes, and is interrupted for 3 of those minutes with a chat task. The handled time for the email task is 20 minutes, and the handled time for the chat task is 3 minutes. This means that during a 20-minute interval, the agent handled tasks for 23 minutes.



If an agent is working on a task in an interruptible MRD and is routed a task in another interruptible MRD, CCE does not send an interrupt event. Therefore, interruptAction setting does not apply.

## Plan Dialed Numbers

Dialed numbers, also called script selectors, are the strings or numbers submitted with Task Routing task requests through Customer Collaboration Platform. Each dialed number is associated with a call type, and determines which routing script CCE uses to route the request to an agent.

Dialed numbers are media-specific; you associate each one with a Media Routing Domain.

For Task Routing, plan which dialed numbers the custom Customer Collaboration Platform application will use when submitting new task requests. Consider whether you will use the same dialed numbers for transfer and tasks that are queued on RONA, or if you need more dialed numbers.



**Important** You must associate each Task Routing dialed number with a call type. The default call type is not supported for Task Routing.

## 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.

---

## Agent State and Agent Mode

An agent's state and routable mode in an MRD work together to determine whether CCE routes tasks to the agent in that MRD.

### Agent Routable Mode

The agent's routable mode controls whether CCE can assign the agent tasks in that MRD. If the agent is routable, CCE can assign tasks to the agent. If the agent is not routable, CCE cannot assign tasks to the agent.

The agent changes to routable/not routable through Finesse Media - Change Agent to Routable/Not Routable API calls.

### Agent State

The agent's state in an MRD indicates the agent's current status and whether the agent is available to handle a task:

- Ready: The agent is available to handle a task.
- Reserved/Active/Paused/Work Ready/Interrupted: The agent is available to handle a task if the agent has not reached their maximum task limit in the MRD.
- Not Ready: The agent is not available to handle a task.

The agent changes to Ready and Not Ready through calls to the Finesse Media - Change Agent State API. The agent's state while working on a task depends on the actions the agent performs on the Finesse dialog related to the task, through calls to the Finesse Dialog - Take Action on Participant API.

### **How Mode and State Work Together to Determine if an Agent Receives Tasks**

CCE will route an agent a task in the MRD if ALL of the following are true:

- The agent's mode is routable, and
- The agent is in any state other than NOT\_READY, and
- The agent has not reached the maximum task limit in the MRD, and
- The agent is not working on a task in a different and non-interruptible MRD.

CCE will NOT route an agent a task in the MRD if ANY of the following are true:

- The agent's mode is not routable, or
- The agent is NOT\_READY, or
- The agent has reached the maximum task limit in the MRD, or
- The agent is working on a task in a different and non-interruptible MRD.

### **Why Change the Agent's Mode to Not Routable?**

By changing the agent's mode to not routable, you stop sending tasks to the agent without changing the agent's state to Not Ready. You may want to make an agent not routable if the agent is close to ending the shift, and needs to complete in progress tasks before signing out.

If an agent changes to Not Ready state while still working on tasks, CCE reports show those tasks as ended; time spent working on the tasks after going Not Ready is not counted. By making the agent not routable instead of Not Ready, the agent's time on task continues to be counted.

In RONA situations, in which agents do not accept tasks within the Start Timeout threshold for the MRD, Finesse automatically makes agents not routable. Finesse resubmits the tasks through for routing through Customer Collaboration Platform. The application must make the agent routable in order for the agent to receive tasks again.

## **Customer Collaboration Platform and Finesse Task States**

In most cases, Customer Collaboration Platform social contact states do not map directly to Finesse dialog states. For Customer Collaboration Platform, social contacts are created when the customer submits a task request. For Finesse, the dialog with which the agent engages with the customer is created when the task is routed to the agent.

This table shows the relationships between Customer Collaboration Platform social contact task states and Finesse dialog states.

| Customer Collaboration Platform Social Contact Task State                                                                                                                                                                            | Finesse Dialog State                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Unread:</b> The task request has not been submitted to the contact center.                                                                                                                                                        | None                                                                                                              |
| <b>Queued:</b> The task request is successfully submitted to the contact center as a result of creating a new task or resubmitting a task due to agent transfer, automatic transfer on agent logout, or automatic transfer for RONA. | None                                                                                                              |
| <b>Reserved:</b> The task is assigned to an agent. This state includes all work on a task.                                                                                                                                           | <b>Offered:</b> The dialog is being offered to the agent.                                                         |
|                                                                                                                                                                                                                                      | <b>Accepted:</b> The agent accepted the dialog but has not started working on it.                                 |
|                                                                                                                                                                                                                                      | <b>Active:</b> The agent is working on the dialog.                                                                |
|                                                                                                                                                                                                                                      | <b>Paused:</b> The agent paused the dialog.                                                                       |
|                                                                                                                                                                                                                                      | <b>Wrapping Up:</b> The agent is performing wrap up activity on the dialog.                                       |
| <b>Interrupted:</b> The agent is interrupted with a task from a non-interruptible Media Routing Domain. The agent cannot work on this task until the interrupting task is complete.                                                  |                                                                                                                   |
| <b>Handled:</b> Customer Collaboration Platform receives a handled notification from Finesse indicating that the task ended.                                                                                                         | <b>Closed:</b> The agent ended the task. Finesse sends a handled notification to Customer Collaboration Platform. |

## Control SocialMiner Application Access

By default, access to SocialMiner administration user interface is restricted. Administrator can provide access by allowing clients IP addresses and revoke by removing the client's IP from the allowed list. For any modification to the allowed list to take effect, Cisco Tomcat must be restarted.



**Note** IP address range and subnet masks are not supported.

### utils whitelist admin\_ui list

This command displays all the allowed IP addresses. This list is used to authorize the source of the incoming requests.

**Syntax****utils whitelist admin\_ui list****Example**

```
admin: utils whitelist admin_ui list
Admin UI whitelist is:
10.232.20.31
10.232.20.32
10.232.20.33
10.232.20.34
```

## utils whitelist admin\_ui add

This command adds the provided IP address to the allowed list of addresses.

**Syntax****utils whitelist admin\_ui add****Example**

```
admin:utils whitelist admin_ui add 10.232.20.33
Successfully added IP: 10.232.20.33 to the whitelist
Restart Cisco Tomcat for the changes to take effect
```

## utils whitelist admin\_ui delete

This command deletes the provided IP address from the allowed list.

**Syntax****utils whitelist admin\_ui delete****Example**

```
admin:utils whitelist admin_ui delete 10.232.20.34
Successfully deleted IP: 10.232.20.34 from the whitelist
Restart Cisco Tomcat for the changes to take effect
```

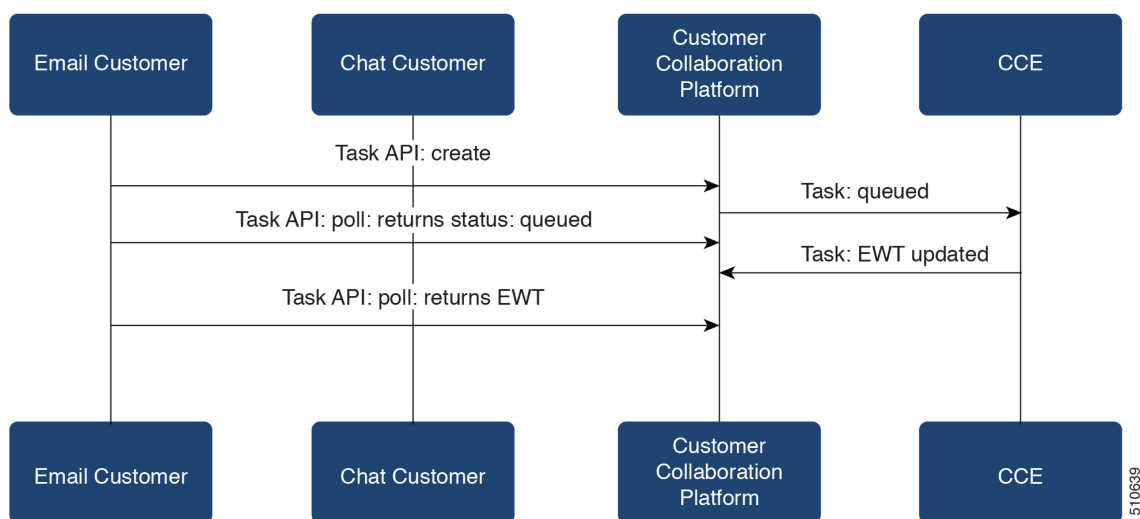
# Task Routing API Request Flows

## Task Routing API Basic Task Flow

This topic provides the Customer Collaboration Platform and Finesse API calls and events when an active email task is interrupted by a chat request.

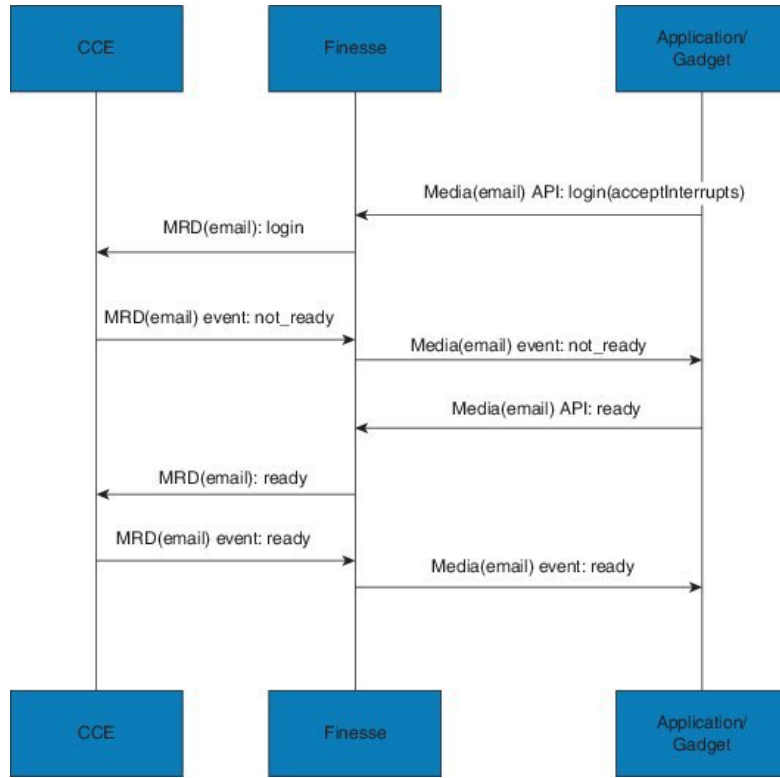
In this scenario, the email MRD is interruptible. When the agent signs into the email MRD, the application uses the Finesse Media API to accept interrupts. The chat MRD is non-interruptible.

1. The email application submits a new email task request to CCE, and polls for status and Estimated Wait Time (EWT).

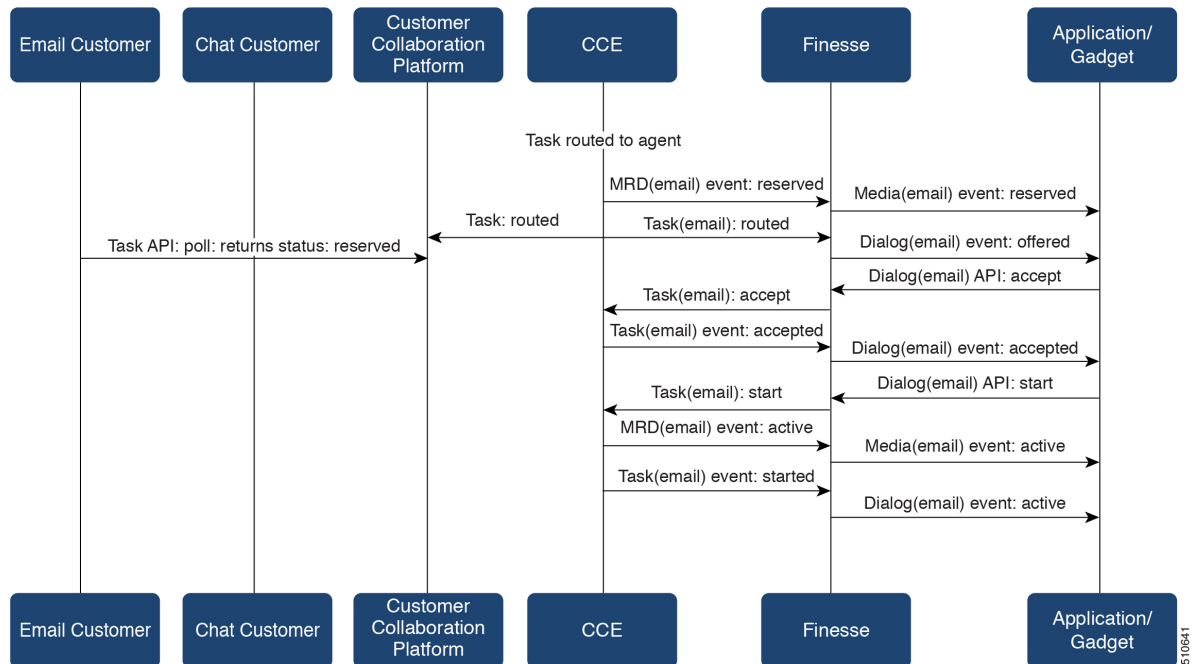


2. An agent signs in to the email MRD and changes state to Ready.

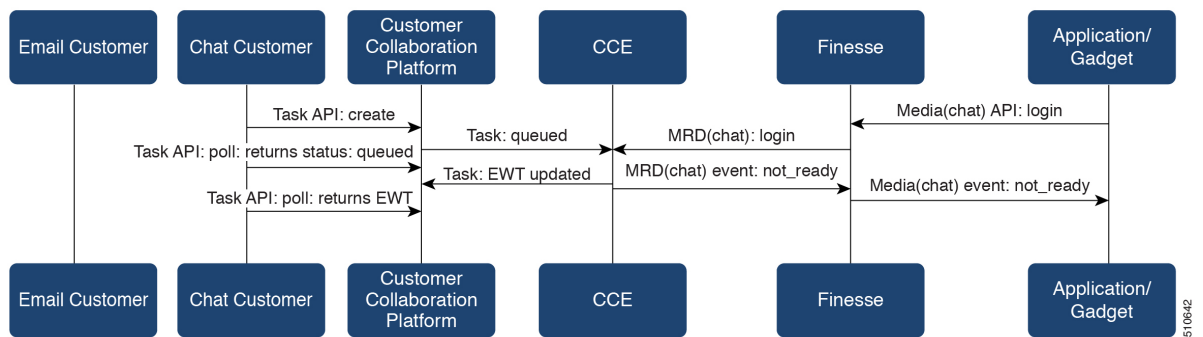




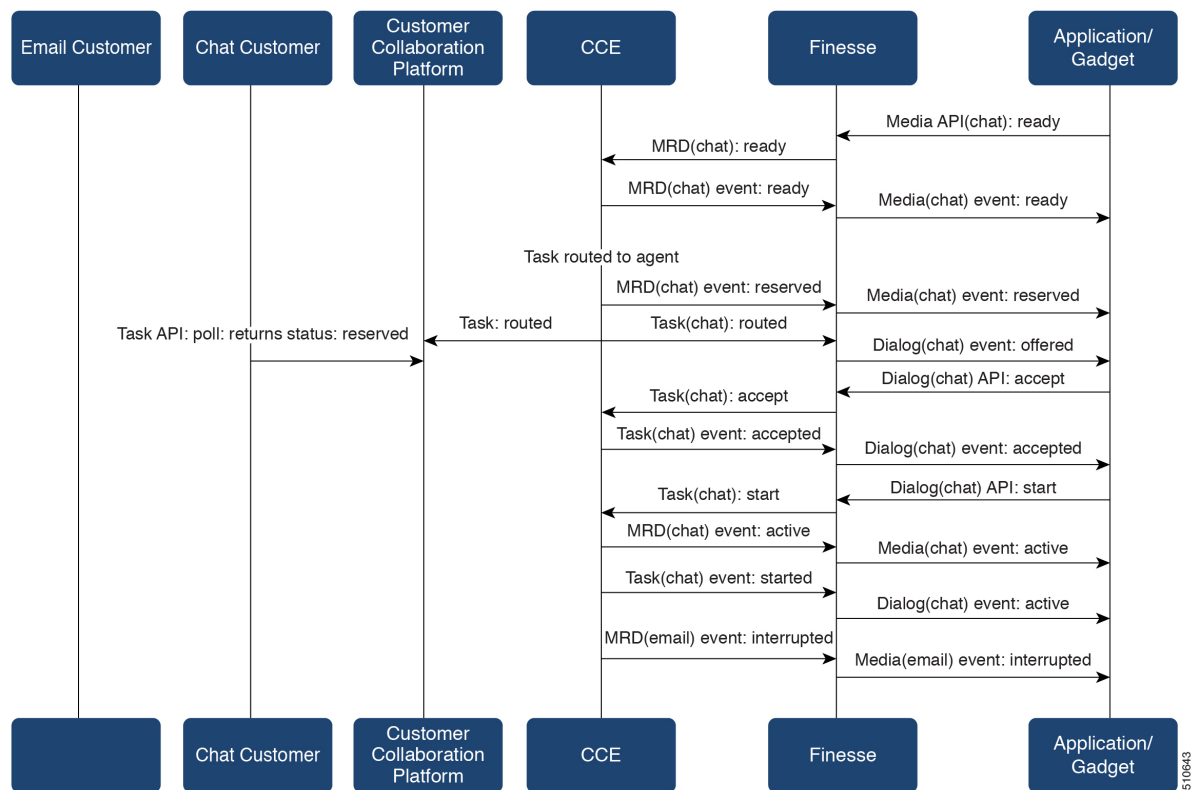
3. CCE assigns the agent the email task. The Call and ECC variables used to create the task are included in the dialog's media properties, and contain information such as the handle to the email. The variables can be used to reply to the email. The agent starts work on the email dialog in Finesse.



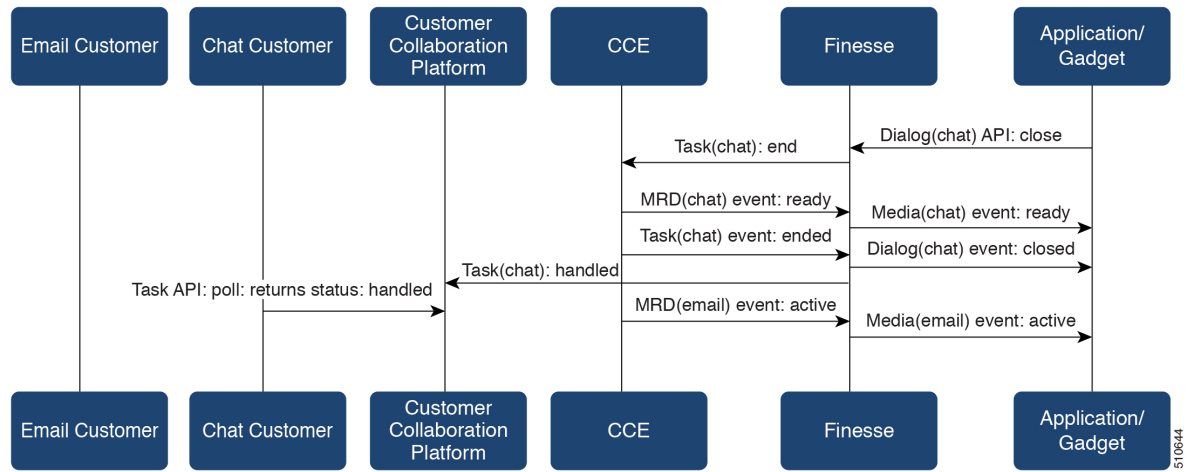
4. The chat application submits a new chat request, and polls for status and EWT. The same agent logs into the chat MRD.



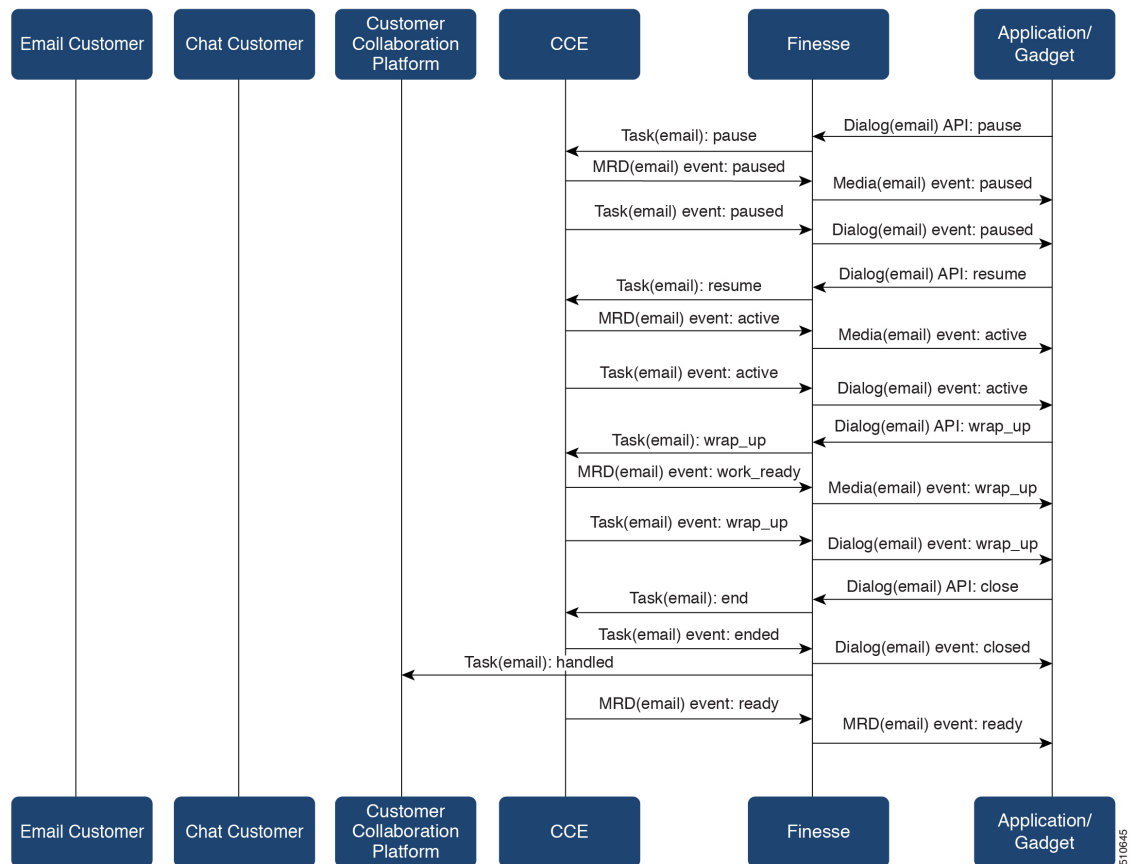
5. The agent changes state to Ready in the chat MRD. CCE assigns the chat task to the agent. The Call and ECC variables used to create the task are included in the dialog's media properties, and contain information such as the chat room URL. The variables can be used to join the chat room with the customer. The agent starts the chat dialog in Finesse. The Email dialog is interrupted.



6. The agent completes work on the chat dialog and closes the dialog. Finesse sends a handled event to Customer Collaboration Platform for the chat task. The application is responsible for closing the chat room. The agent is not handling other non-interruptible dialogs, and the email dialog becomes active.

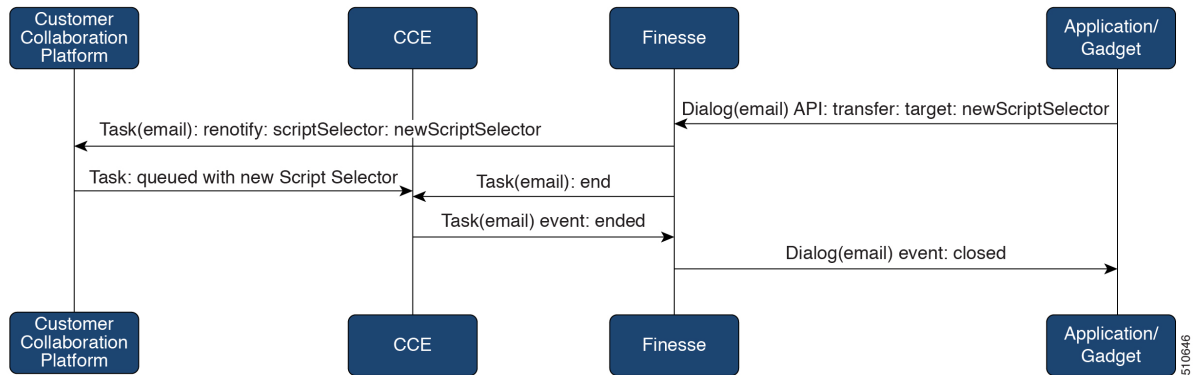


7. The agent continues working on the email dialog, including pausing, resuming, and wrapping up the dialog. The agent closes the dialog. Finesse sends a handle event to Customer Collaboration Platform for the email task. The application is responsible for sending the email reply to the customer.



## Task Routing API Agent Transfer Flow

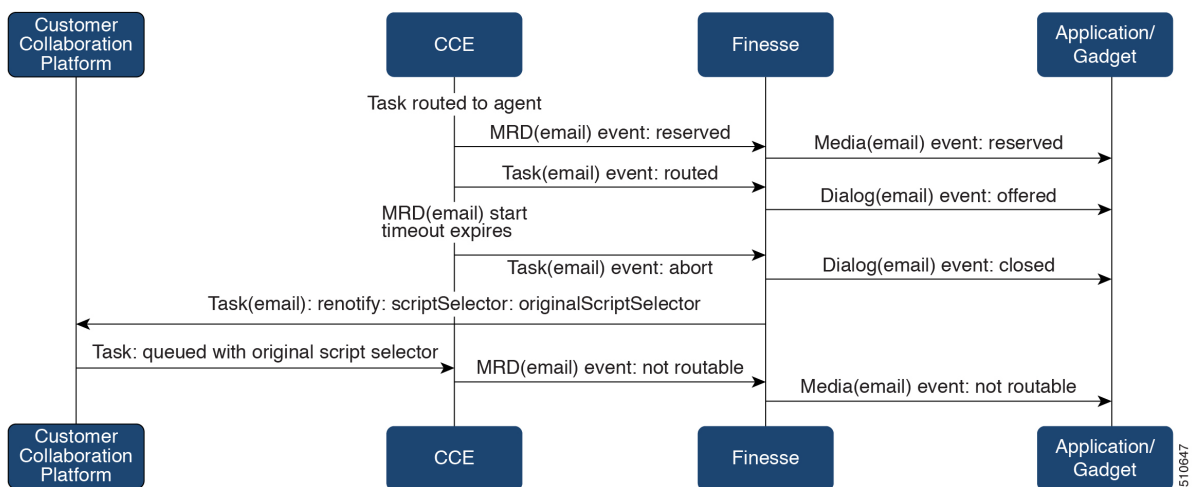
This illustration provides the Customer Collaboration Platform and Finesse API calls and events when an agent transfers a task.



1. The agent transfers the dialog from the Finesse application, selecting the script selector to which to transfer the task.
2. Finesse resubmits the task to Customer Collaboration Platform, and the task is queued to the script selector as a new task.
3. Finesse puts the original dialog in the CLOSED state, with the disposition code CD\_TASK\_TRANSFERRED. Finesse does not send a handled notification to Customer Collaboration Platform.

## Task Routing API RONA Flow

This illustration provides the Customer Collaboration Platform and Finesse API calls and events in a RONA scenario, in which an agent does not accept an offered task within the Start Timeout threshold for the MRD.



1. The task is routed to an agent, and the dialog is offered to the agent.

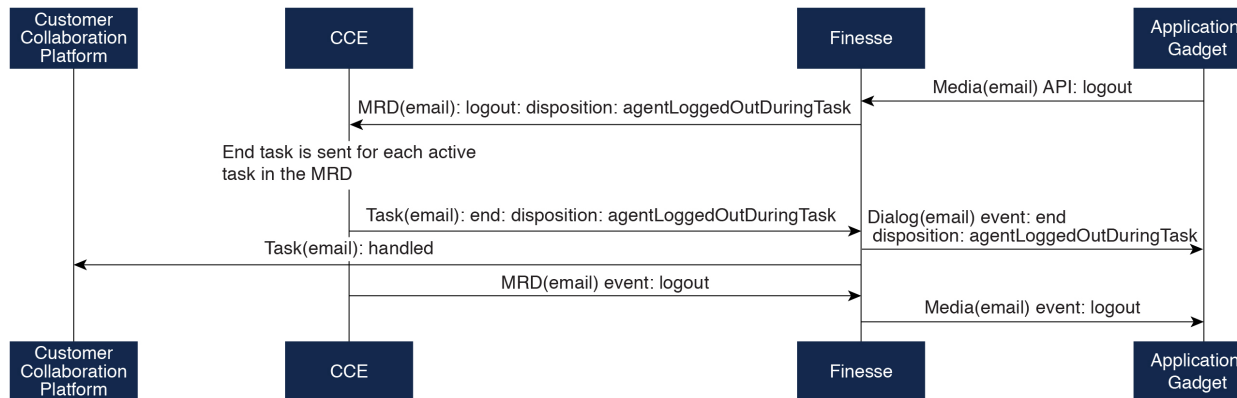
2. The Media Routing Domain's Start Timeout threshold expires.
3. CCE instructs Finesse to end the dialog. Finesse puts the dialog in the CLOSED state, with the disposition code CD\_RING\_NO\_ANSWER. Finesse does not send a handled notification to Customer Collaboration Platform.
4. The Finesse server on which the agent was last signed in resubmits the task to Customer Collaboration Platform with the original script selector. The task is queued to the script selector as a new task.
5. CCE instructs Finesse to make the agent not routable in that Media Routing Domain, so that the agent is not routed more tasks.

## Task Routing API Agent Sign Out with Tasks Flows

The Finesse Media - Sign Out API allows agents to sign out with assigned tasks. The dialogLogoutAction parameter set by the Media - Sign In API determines whether those tasks are closed or transferred when the agent signs out.

### Close Tasks on Sign Out

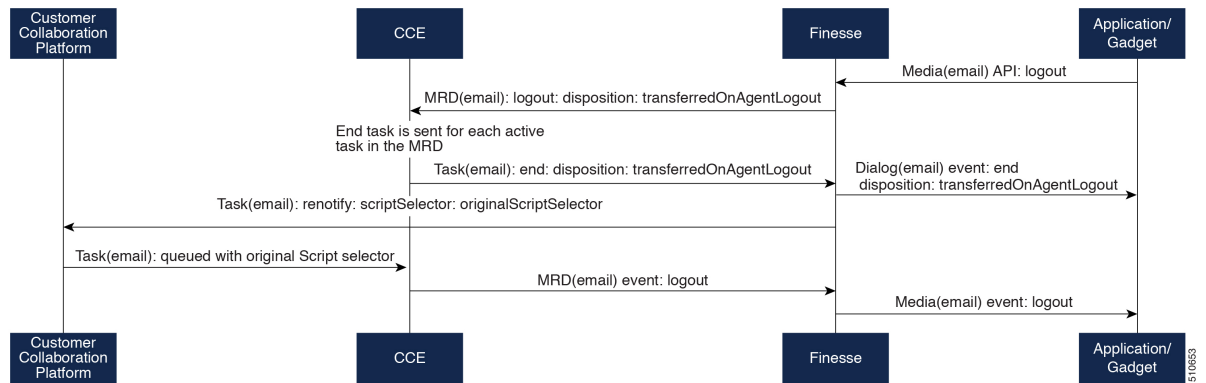
This illustration provides the Customer Collaboration Platform and Finesse API calls and events when agents are set to have assigned tasks closed on sign out.



1. The agent requests to sign out of the MRD with an active task.
2. CCE instructs Finesse to end the task. Finesse puts the dialog in CLOSED state, with the disposition code CD\_AGENT\_LOGGED\_OUT\_DURING\_DIALOG.
3. The agent is signed out of the MRD.

### Transfer Tasks on Sign Out

This illustration provides the Customer Collaboration Platform and Finesse API calls and events when agents are set to have assigned tasks transferred on sign out.



1. The agent requests to sign out of the MRD with an active task.
2. CCE instructs Finesse to end the dialog. Finesse puts the dialog in the CLOSED state, with the disposition code `CD_TASK_TRANSFERRED_ON_AGENT_LOGOUT`. Finesse does not send a handled notification to Customer Collaboration Platform.
3. The Finesse server on which the agent was signed in resubmits the task to Customer Collaboration Platform with the original script selector. The task is queued to the script selector as a new task.
4. The agent is signed out of the MRD.

# Failover and Failure Recovery

| Component                       | Failover/Failure Scenario                                                                                                                                                                                                   | New Task Request Impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Queued, Offered, and Active Task Impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Customer Collaboration Platform | <p>MR connection fails. For example, there is a networking problem, the PG loses connection, or Customer Collaboration Platform loses connection.</p> <p>Finesse loses connection with Customer Collaboration Platform.</p> | <p><b>New task requests from Customer Collaboration Platform application:</b> New task requests fail, and the failures are delivered back to the application. Details of these failures are described in the next column.</p> <p><b>Automatic transfer request from Finesse</b> (for transfer on sign out or RONA): Results in a lost transfer request.</p> <p><b>Agent transfer request:</b> The request fails, and Finesse sends an error back to the application. Finesse retains the task.</p> | <p><b>Queued tasks:</b> When tasks are submitted, they can be set to requeue on recovery. Typically, non-interactive tasks, such as email, are set to requeue on recovery because there is not a way to alert the customer that there was a problem while in queue. Interactive tasks, such as chat, are set not to requeue on recovery because the customer is waiting at an interface for an agent, and there is a way to alert the customer that there is a problem.</p> <p>If tasks are set to requeue on recovery, the task is resubmitted when the MR connection is reestablished. The status and statusReason of the contact does not change.</p> <p>If tasks are set NOT to requeue on recovery, the task's contact's status is marked discarded. The task's contact's statusReason is marked as follows:</p> <p><b>Customer Collaboration Platform failure:</b></p> <p>NOTIFICATION_CCE_<br/>CUSTOMERCOLLABORATIONPLATFORM_SYSTEM_FAILURE</p> <p><b>MR connection failure:</b></p> <p>NOTIFICATION_CCE_CONNECTION_LOST</p> <p><b>Offered and active tasks:</b> No impact.</p> |
| Customer Collaboration Platform | <p>Customer Collaboration Platform overruns the new task queue limit.</p> <p>For the limit, see the <a href="#">Cisco Customer Collaboration Platform Developer Guide</a>.</p>                                              | <p><b>New task requests from Customer Collaboration Platform application:</b> New task requests are discarded with the statusReason NOTIFICATION_RATE_LIMITED.</p> <p><b>Automatic or agent transfer requests:</b> No impact</p>                                                                                                                                                                                                                                                                   | <p><b>Queued, offered, and active tasks:</b> No impact.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Component | Failover/Failure Scenario                            | New Task Request Impact                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Queued, Offered, and Active Task Impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Finesse   | Finesse loses connection with Agent PG or CTI Server | <p><b>New task request from Customer Collaboration Platform application:</b> No impact</p> <p><b>Automatic transfer requests from Finesse</b> (for transfer on logout or RONA): Automatic transfers are initiated on the Finesse server on which the agent was signed in. Any outage on that Finesse server can result in lost transfer requests.</p> <p><b>Agent transfer request:</b> The request fails because Finesse is out of service, and Finesse retains the task.</p> | <p>Agents signed into media on the failed Finesse server are put into <code>WORK_NOT_READY</code> state and made not routable. Tasks on that server are preserved in their current state, and time continues to accrue towards the maximum task lifetime. The agent fails over to the secondary Finesse server, and must sign in to the media again. The agent is put into the previous state. If the agent doesn't have tasks, the agent is put in <code>NOT_READY</code> state.</p> <p><b>Queued tasks:</b> No impact.</p> <p><b>Offered tasks:</b> These tasks RONA because the agent cannot accept them.</p> <p><b>Active tasks:</b> These tasks fail over to the other Finesse server and are recovered on that server.</p> <p><b>Note</b> Any active tasks that were in <code>INTERRUPTED</code> state at the time of the lost connection change are recovered. However, these tasks change to the <code>UNKNOWN</code> state when the task is no longer <code>INTERRUPTED</code>. The agent can only close tasks when they are in the <code>UNKNOWN</code> state.</p> |



| Component           | Failover/Failure Scenario                                        | New Task Request Impact                                                                                                                                  | Queued, Offered, and Active Task Impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Finesse             | Agent logs out, or presence is lost while agent has active tasks | <p><b>New task request from Customer Collaboration Platform application:</b> No impact</p> <p><b>Automatic or agent transfer requests:</b> No impact</p> | <p><b>Queued tasks:</b> No impact.</p> <p><b>Offered tasks:</b> These tasks fail over to the other Finesse server and are recovered on that server. If a task's Start Timeout threshold is exceeded during failover, the task RONAs.</p> <p><b>Active tasks:</b> If an agent logs out with active tasks, or agent presence is lost with active tasks, the tasks are either closed or transferred to the original script selector depending on how the agent was configured when signing into the MRD.</p> <p>If the tasks are transferred, the disposition code is<br/>CD_TASK_TRANSFERRED_AGENT_LOGOUT.</p> <p>If the tasks are closed, the disposition code is<br/>CD_AGENT_LOGGED_OUT_DURING_DIALOG.</p> |
| Finesse application | Finesse application fails                                        | <p><b>New task request from Customer Collaboration Platform application:</b> No impact</p> <p><b>Automatic or agent transfer requests:</b> No impact</p> | <p><b>Queued tasks:</b> No impact.</p> <p><b>Offered tasks:</b> These tasks may RONA depending on how the application is structured. A Task Routing application may prevent an agent from accepting a dialog when the application is down because the agent cannot handle the dialog while the application is down. In this case, the dialog RONAs.</p> <p><b>Active tasks:</b> Varies by application. Applications are responsible for managing the tasks while the application is down. Finesse retains the tasks, and the tasks are recovered once the application is restored.</p>                                                                                                                      |

| Component         | Failover/Failure Scenario       | New Task Request Impact                                                                                                                                                                                                                                                                                       | Queued, Offered, and Active Task Impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CTI Server or OPC | One CTI Server or one OPC fails | <p><b>New task request from Customer Collaboration Platform application:</b> No impact</p> <p><b>Automatic transfer requests from Finesse</b> (for transfer on logout or RONA): Results in lost transfer requests.</p> <p><b>Agent transfer request:</b> The request fails, and Finesse retains the task.</p> | <p><b>Queued tasks:</b> No impact.</p> <p><b>Offered tasks:</b> These tasks fail over to the other Finesse server and are recovered on that server. If a task's Start Timeout threshold is exceeded during failover, the task RONAs.</p> <p><b>Active tasks:</b> These tasks fail over to the other Finesse server and are recovered on that server.</p> <p><b>Note</b> Any active tasks that were in INTERRUPTED state at the time of the lost connection change are also recovered. However, these tasks change to the UNKNOWN state when the task is no longer INTERRUPTED. The agent only can only close tasks when they are in the UNKNOWN state.</p> |
| OPC               | Both OPCs fail                  | <p><b>New task request from Customer Collaboration Platform application:</b> No impact</p> <p><b>Automatic or agent transfer requests:</b> Results in lost transfers.</p>                                                                                                                                     | <p><b>Queued tasks:</b> No impact</p> <p><b>Offered and active tasks:</b> These tasks are lost</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Task Routing Setup

### Initial Setup

| Step              | Task                                                                                                                                                                                  | Notes |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| <b>Set up CCE</b> |                                                                                                                                                                                       |       |
| 1                 | Configure Finesse with the AW, so that Finesse can access Customer Collaboration Platform connection information.<br>See <a href="#">Configure Finesse with the AW, on page 208</a> . |       |
| 2                 | Configure a Network VRU and Network VRU scripts.<br>See <a href="#">Configure Network VRU and Network VRU Scripts, on page 209</a> .                                                  |       |

| Step                                                                   | Task                                                                                                                                                                                                                                                                                                                                                                                                       | Notes                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3                                                                      | Configure the MR PG and PIM<br>See <a href="#">Configure the Media Routing PG and PIM, on page 209.</a>                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                |
| 4                                                                      | Set up the MR PG and PIM for Customer Collaboration Platform.<br>See <a href="#">Set up the Media Routing PG and PIM, on page 210.</a>                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                |
| 5                                                                      | Add Customer Collaboration Platform as an External Machine in the System Inventory.<br>See <a href="#">Add Customer Collaboration Platform as an External Machine, on page 210.</a>                                                                                                                                                                                                                        | The system configures the following settings automatically in Customer Collaboration Platform Administration: <ul style="list-style-type: none"> <li>• Enables and configures the <b>CCE Multichannel Routing settings</b>.</li> <li>• Configures the Task feed and the associated campaign and Connection to CCE notification needed for the Task Routing feature.</li> </ul> |
| 6                                                                      | Configure the following in Unified CCE Administration or Configuration Manager: <ul style="list-style-type: none"> <li>• Media Routing Domains</li> <li>• Call types</li> <li>• Dialed numbers</li> <li>• Skill groups or precision queues</li> <li>• ECC variables</li> <li>• Agent desk settings</li> </ul> See <a href="#">Unified CCE Administration and Configuration Manager Tools, on page 211.</a> |                                                                                                                                                                                                                                                                                                                                                                                |
| 7                                                                      | Increase the TCDTimeout registry key value, if you are using precision queues and will be submitting potentially long tasks, like email.<br>See <a href="#">Increase TCDTimeout Value, on page 213.</a>                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                |
| 9                                                                      | Create routing scripts<br>See <a href="#">Create Routing Scripts for Task Routing, on page 213.</a>                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Create Customer Collaboration Platform and Finesse Applications</b> |                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                |

| Step                  | Task                                                                                                                                                                                                                                                                                                                                               | Notes |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| 10                    | Create the Customer Collaboration Platform multichannel application to begin task requests.<br>See <a href="#">Sample Customer Collaboration Platform HTML Task Application</a> , on page 214.                                                                                                                                                     |       |
| 11                    | Create the Finesse applications to manage nonvoice agent and dialog states.<br>See <a href="#">Sample Finesse Code for Task Routing</a> , on page 214.                                                                                                                                                                                             |       |
| <b>Set up Finesse</b> |                                                                                                                                                                                                                                                                                                                                                    |       |
| 12                    | Upload the Finesse desktop gadgets to the desktop layout (optional).<br>See the <i>Cisco Finesse Administration Guide</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html</a> . |       |

## Configure Finesse with the AW

Finesse connects to Customer Collaboration Platform to transfer Task Routing tasks and resubmit tasks for RONA. The Finesse AWDB user requires special database permissions to access Customer Collaboration Platform connection information. Map the user to the Side A, AWDB, and primary databases. In these databases, give the user the db\_datareader and public roles.

### Before you begin

Configure the Contact Center Administration and Data Server Connection Settings on Finesse. You need the Finesse AWDB username to complete this procedure.

See the *Cisco Finesse Administration Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html>.

- 
- Step 1** Determine whether the Finesse AWDB user is a domain user or a SQL user. If the user is a domain user, proceed to the last step in the procedure (step 7). Otherwise, complete all of the steps.
- Step 2** Launch Microsoft SQL Server Management Studio on the Unified CCE Administration Client workstation.
- Step 3** Connect to the Side A Logger using the default credentials.
- Step 4** Navigate to **Security > Logins**. Right-click the Finesse AWDB username. The Login Properties screen opens.
- Step 5** Select the **User Mapping** page, and perform the following:
- Verify that the databases associated with Side A and AWdb are checked.
  - Check the primary database.
  - Select the Side A database. In the **Database role membership for** section, check the **db\_datareader** and **public** roles.

Repeat this step for the AWdb and primary databases.

d) Click **OK**.

**Step 6** Repeat these steps on the Side B Logger.

**Step 7** Run the following SQL queries as the SQL administrative user "sa" or as a user with sysadmin privileges.

For <user>, enter the Finesse AWDB username. If the Finesse AWDB user is a domain user, rather than a SQL user, use the <domain\user> format.

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

---

## Configure Network VRU and Network VRU Scripts

The Network VRU is used to queue nonvoice tasks if an agent is not available to handle them. The Network VRU Script is used to return estimated wait time to customers. For more information on writing routing scripts that return estimated wait time, 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>.

When you configure the Network VRU Script, you specify whether it is interruptible. The **Interruptible** setting for the Network VRU Script controls whether the script can be interrupted (for example if an agent becomes available). This setting is not related to the Media Routing Domain **Interruptible** setting, which controls whether an agent working on a task in that MRD can be interrupted by a task from a non-interruptible MRD.

---

**Step 1** In Configuration Manager, use the **Network VRU Explorer** tool to configure and save a type 2 VRU.

**Step 2** Use the **Network VRU Script List** tool to add a Network VRU Script that references this Network VRU.

You can accept the default values.

---

## Configure the Media Routing PG and PIM

---

**Step 1** In Configuration Manager, open the PG Explorer tool to configure a media routing PG.

**Step 2** Create a media routing PIM and routing client for Customer Collaboration Platform.

Write down the Logical Controller ID and the Peripheral ID. You will use them when you set up the PG.

**Step 3** On the Peripheral tab in the PG Explorer tool, check the **Enable post routing** check box.

**Step 4** On the Routing Client tab in the PG Explorer tool, select the **Multichannel** option from the **Routing Type** drop-down list box.

**Note** The **Default call type** setting is not supported for tasks submitted through the Task Routing APIs.

**Step 5** On the Advanced tab in the PG Explorer tool, select the type 2 Network VRU that you created.

---

## Set up the Media Routing PG and PIM



**Caution** Before performing the step to enable the secured connection between the components, ensure that the security certificate management process is completed.

Set up the Media Routing PG and PIM

- 
- Step 1** From Cisco Unified CCE Tools, select **Peripheral Gateway Setup**.
- Step 2** On the Components Setup screen, in the Instance Components panel, select the PG Instance component. If the PG does not exist, click **Add**. If it exists, click **Edit**.
- Step 3** In the Peripheral Gateways Properties screen, click **Media Routing**. Click **Next**.
- Step 4** Click **Yes** at the prompt to stop the service.
- Step 5** From the Peripheral Gateway Component Properties screen, click **Add**, select the next PIM, and configure with the Client Type of Media Routing as follows.
- Check **Enabled**.
  - In the **Peripheral Name** field, enter **MR**.
  - In the **Peripheral ID** field, enter the Peripheral ID that you recorded when you configured the Media Routing PG and PIM.
  - For **Application Hostname (1)**, enter the hostname or IP address of Customer Collaboration Platform.
  - By default, Customer Collaboration Platform accepts the MR connection on **Application Connection Port 38001**. The Application Connection Port setting on Customer Collaboration Platform must match the setting on the MR PG. If you change the port on one side of the connection, you must change it on the other side.
  - Leave the **Application Hostname (2)**, field blank.
  - Keep all other values.
  - Check the **Enable Secured Connection** option.
- This establishes a secured connection between MR PIM and Application Server.
- Ensure that you provide the correct information in the Application Hostname (1) and Application Connection Port (1) fields.
- Click **OK**.
- Step 6** On the Peripheral Gateway Component Properties screen, enter the Logical Controller ID that you recorded when you configured the Media Routing PG and PIM.
- Step 7** Accept defaults and click **Next** until the Setup Complete screen opens.
- Step 8** At the Setup Complete screen, check **Yes** to start the service. Click **Finish**.
- Step 9** Click **Exit Setup**.
- Step 10** Repeat this procedure for Side B.
- 

## Add Customer Collaboration Platform as an External Machine

When you add Customer Collaboration Platform as an External Machine in the Unified CCE Administration System Inventory, the system automatically performs the following Customer Collaboration Platform configuration:

- Enables and completes the **CCE Configuration for Multichannel Routing** settings in Customer Collaboration Platform Administration.

These settings include the hostnames of the MR PGs and the Application Connection Port you specified when setting up the MR PG and PIM.

- Configures the Task feed and the associated campaign and Connection to CCE notification needed for the Task Routing feature, with the following names:
  - **Task feed:** Cisco\_Default\_Task\_Feed
  - **Campaign:** Cisco\_Default\_Task\_Campaign
  - **Notification:** Cisco\_Default\_Task\_Notification
  - **Tag:** cisco\_task\_tag



---

**Note** If the Task feed has been configured to use a different tag, the Connection to CCE notification is configured to use that tag.

---

- 
- Step 1** Navigate to **Unified CCE Administration > Infrastructure > Inventory**.
- Step 2** Click Add.
- Step 3** Select Customer Collaboration Platform from the drop-down list.
- Step 4** Enter the fully qualified domain name (FQDN), hostname or IP address in the **Hostname** field.
- Note** The system attempts to convert the value you enter to FQDN.
- Step 5** Enter the Customer Collaboration Platform Administration username and password.
- Step 6** Select the **Side A** and **Side B** Media Routing PGs.
- Step 7** Enter the Application Port you specified when setting up the MR PG and PIM. The default value is 38001.
- Step 8** Click **Save**.
- 

## Unified CCE Administration and Configuration Manager Tools

This topic explains the Unified CCE Administration and Configuration Manager tools you need to configure Task Routing.

### Before you begin

For details on the procedures for these steps, refer to the Unified CCE Administration online help and the Configuration Manager online help.

---

- Step 1** Sign in to Unified CCE Administration.
- Step 2** From the **Manage** menu, configure the following:

| Item to Configure     | Details                                                                                                                                                                                                                                                                                                                |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Media Routing Domains | Create an MRD for each type of task that the third-party multichannel application submits to CCE (email, chat, and so on).                                                                                                                                                                                             |
| Precision Queues      | Configure either skill groups or precision queues.<br>If you configure precision queues: <ul style="list-style-type: none"> <li>• For <b>Media Routing Domain</b>, select one of the Task Routing MRDs you created.</li> <li>• Associate agents with attributes that are part of the precision queue steps.</li> </ul> |

**Step 3** Launch Configuration Manager.

**Step 4** Configure the following:

| Item to Configure      | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Call Types             | Create call types for Task Routing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Dialed Numbers         | Create dialed numbers for Task Routing. Add the numbers or strings that the custom application will use when submitting task requests. <ul style="list-style-type: none"> <li>• On the <b>Attributes</b> tab, select a Task Routing MRD from the <b>Media routing domain</b> drop-down list box.</li> <li>• On the <b>Dialed Number Mapping</b> tab, map the script selector to a call type you created for Task Routing.</li> </ul> <p><b>Important</b> Each dialed number must be associated with a call type. Default call type is not supported for tasks submitted with Task Routing APIs.</p> |
| Skill Groups           | Configure either skill groups or precision queues.<br>If you configure skill groups: <ul style="list-style-type: none"> <li>• For <b>Media Routing Domain</b>, select one of the Task Routing MRDs you created.</li> <li>• Assign agents to the skill group.</li> </ul>                                                                                                                                                                                                                                                                                                                             |
| Expanded Call Variable | You can use an existing Expanded Call Variable, or you can create an Expanded Call Variable for Task Routing, depending on the needs of your third-party multichannel application. <p><b>Note</b> Arrays are not supported with the Task Routing feature.</p> <p>CCE solutions support the Latin 1 character set only for Expanded Call Context variables and Call variables when used with Finesse and Customer Collaboration Platform.</p>                                                                                                                                                        |



| Item to Configure   | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Agent Desk Settings | <p>If agents will use a Task Routing gadget in the Finesse desktop, leave the <b>Logout inactivity time</b> setting for those agents blank, or remove the existing value.</p> <p>Otherwise, if the agent exceeds the <b>Logout inactivity time</b> in the voice MRD, the agent is logged out of the Cisco Finesse desktop, even if the agent is actively working on tasks from nonvoice MRDs. The agent needs log into the desktop again to continue working on the nonvoice tasks.</p> |

## Increase TCDTimeout Value

Complete this procedure only if you are using precision queues and routing tasks with potentially long durations, like emails.

Several precision queue fields in the Termination\_Call\_Detail record are not completed until the end of a task. These precision queue fields are blank for tasks whose durations exceed the TCDTimeout registry key value. The default value of the TCDTimeout registry key is 9,000 seconds (2.5 hours).

If you are configuring a system to handle email or other long tasks, you can increase the TCDTimeout registry key value to a maximum of 86,400 seconds (24 hours).

Change the registry key on either the Side A or B Router.

Modify the following registry key: HKEY\_LOCAL\_MACHINE\SOFTWARE\Cisco Systems, Inc.\Icm\

## Create Routing Scripts for Task Routing

For complete multichannel scripting information, 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>.



### Important

Ensure that the routing scripts include skill groups or precision queues from the appropriate Media Routing Domains to handle all of the types of tasks that can be routed with the scripts. For example, if a script is used to route email tasks, be sure that the script includes skill groups or precision queues from an email MRD.

## Sample Code for Task Routing

Cisco Systems has made sample Task Routing application code for Customer Collaboration Platform and Finesse available to use as baselines in building your own applications.

## Sample Customer Collaboration Platform HTML Task Application

The sample Customer Collaboration Platform HTML Task application:

- Submits task requests to CCE.
- Retrieves and displays the estimated wait time, if it has been configured in CCE.




---

**Note** You cannot copy and paste this code to achieve a working application. It is only a guideline.

---

The sample application uses the Task API. For more information about how to use the Task API, see the [Cisco Customer Collaboration Platform Developer Guide](#).

- 
- Step 1** Download the sample HTML Task application from DevNet: <https://developer.cisco.com/site/task-routing/>.  
**Step 2** Read the sample application's **readme.txt** file to complete the prerequisites and use the sample application.
- 

## Sample Finesse Code for Task Routing

The Finesse sample Task Management Gadget application lets agents perform the following actions in individual nonvoice Media Routing Domains:

- Sign in and out.
- Change state.
- Handle tasks.

The sample gadget also signals the Customer Context gadget to display a customer record.




---

**Note** You cannot copy and paste this code to achieve a working application. It is only a guideline.

---

For more information about how to use the APIs available for Task Routing, see the *Cisco Finesse Web Services Developer Guide* at <https://developer.cisco.com/site/finesse/>.

- 
- Step 1** Download the sample Task Management Gadget application (TaskManagementGadget-x.x.zip) from DevNet: <https://developer.cisco.com/site/task-routing/>.

- Step 2** Read the sample application's **readme.txt** file to complete the prerequisites and use the sample application.

For more information about uploading third-party gadgets to the Finesse server, see the "Third Party Gadgets" chapter in the *Cisco Finesse Web Services Developer Guide* at <https://developer.cisco.com/site/finesse/>.

For more information about adding third-party gadgets to the Finesse desktop, see the "Manage Third-Party Gadgets" chapter in the *Cisco Finesse Administration Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/tsd-products-support-series-home.html>.

---

## Task Routing Reporting

Cisco Unified Intelligence Center CCE reports include data for voice calls and nonvoice Task Routing tasks.

You can filter these All Fields and Live Data report templates by Media Routing Domain:

- Agent Real Time
- Agent Skill Group Real Time
- Enterprise Skill Group Real Time
- Peripheral Skill Group Real Time All Fields
- Precision Queue Real Time All Fields
- Agent Precision Queue Historical All Fields
- Agent Skill Group Historical All Fields
- Peripheral Skill Group Historical All Fields
- Precision Queue Abandon Answer Distribution Historical
- Precision Queue Interval All Fields
- Skill Group Abandon-Answer Distribution Historical
- Precision Queue - Live Data
- Skill Group - Live Data

See the *Reporting Concepts 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> for information about multichannel reporting data.





## CHAPTER 14

# Unified Communications Manager Extension Mobility

- [Capabilities, on page 217](#)
- [Configuration, on page 218](#)

## Capabilities

Extension Mobility is a Unified Communications Manager feature that you can use in Unified CCE. The feature enables users to temporarily configure a phone as their own by logging in to that phone. Once a user logs in, the phone adopts the individual user device profile information, including line numbers, speed dials, services links, and other user-specific properties of a phone.

Cisco Extension Mobility (EM) works on phones that are located within the same Cisco Unified Communications Manager cluster. Cisco Extension Mobility Cross Cluster (EMCC) works on phones that are located in different Cisco Unified Communications Manager clusters.

The main documentation on this feature is in the Unified Communications Manager documentation. For more information, see the following sources:

| Information Type                      | Sources                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Design considerations                 | <i>Cisco Collaboration System Solution Reference Network Designs</i> at <a href="https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html">https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html</a> |
| Feature description and configuration | <i>Feature Configuration Guide for Cisco Unified Communications Manager</i> at <a href="https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a>              |
| Extension Mobility API                | <a href="https://developer.cisco.com/site/extension-mobility/">https://developer.cisco.com/site/extension-mobility/</a>                                                                                                                                                                                                                                                                               |

## Configuration

You configure EM and EMCC in the Cisco Unified Communications Manager. Take into account the following interactions between Unified CCE and Unified Communications Manager for successful implementation of EM and EMCC within a Unified CCE solution:

- For Unified CCE configurations with multiline agent phone line control on the PG, configure all directory numbers for the user profile in Cisco Unified Communications Manager as follows:

| Setting                 | Value |
|-------------------------|-------|
| Maximum Number of Calls | 2     |
| Busy Trigger            | 1     |

- For Unified CCE configurations with single-line agent phone line control on the PG, configure the secondary lines (but not the primary ACD line) for the directory number of the user profile in Cisco Unified Communications Manager as follows:

| Setting                 | Value |
|-------------------------|-------|
| Maximum Number of Calls | 4     |
| Busy Trigger            | 2     |

- You cannot use phones with an **IP Addressing Mode** of **IPv6 Only** for Cisco Extension Mobility. If you want to use Cisco Extension Mobility with the phone, you must configure the phone with an **IP Addressing Mode** of **IPv4 Only** or **IPv4 and IPv6**.
- Agents can log in to multiple devices, depending on the **Intra-cluster Multiple Login Behavior** service parameter. You can set this parameter for EM implementations. EMCC implementations require that you set this parameter for multiple logins.

If an agent fails to log out of a device, another agent who attempts to access that device gets a "shared line" error. Follow these Unified Communications Manager configuration guidelines to avoid shared line errors:

- For EM implementations with hard phones, set the **Intra-cluster Multiple Login Behavior** Extension Mobility service parameter to "Auto Logout".
- For EM implementations with a mix of hard and IP phones and for all EMCC implementations, limit the time that an agent can remain logged in to a device. Set the **Intra-cluster Maximum LoginTime** service parameter to the typical time that an agent remains logged in to a device during a shift.

For more information on Extension Mobility with Unified CCE, see *UCCE Integration with CM Configuration Example* at <https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-enterprise/117777-config-ucce-00.html>.



## CHAPTER 15

# Virtual Agent–Voice

- [Feature Overview, on page 219](#)
- [Onboarding Experience, on page 220](#)
- [VAV via Cloud-Based Connector, on page 220](#)
- [VAV via Premise-Based Connector, on page 226](#)
- [Documentation Resources, on page 237](#)
- [Regional Media Data Center Region Mapping, on page 238](#)

## Feature Overview

Virtual Agent–Voice (VAV) feature, which was referred to as Customer Virtual Assistant (CVA) in 12.5(1) release, enables the IVR platform to integrate with cloud-based speech services. This feature supports human-like interactions that enable customers to resolve issues quickly and more efficiently within the IVR, thereby reducing the calls directed toward agents.



---

**Note** The Dialogflow ES GCP project trial version should not be used in a production environment.

---

VAV-based IVR enables a new mechanism to leverage cloud-based-AI-enabled speech services. VAV provides the following speech services:

- **Text-to-Speech:** Integration with cloud-based TTS services in your application for Speech Synthesis operations. VAV currently supports [Google Text to Speech](#) service.
- **Speech-to-Text:** Integration with cloud-based ASR services in your application for Speech Recognition operations. VAV currently supports [Google Speech to Text](#) service.
- **Speech-to-Intent:** VAV provides capability of identifying the intent of customer utterances by processing the text that is received from Speech-to-Text operations. VAV offers this service by using cloud-based Natural Language Understanding (NLU) services. VAV currently supports [Google Dialogflow](#) service.

For accessing VAV functionality, Cisco Virtualized Voice Browser (VVB) uses one of the following connectors to leverage AI services:

**Cloud-based connector:** VVB uses a cloud-based connector to connect to the Cisco CCAI service. This service is enabled through the *VirtualAgentVoice* element of Cisco Unified Call Studio. VAV currently supports Google's Dialogflow CX service via cloud-based connector.

**Premise-based connector:** VVB uses an original connector to connect to the Google Dialogflow service. This service is enabled through the *Dialogflow* or *DialogflowCX* elements of Cisco Unified Call Studio. VAV currently supports Google's Dialogflow ES and CX services via premise-based connector.

## Onboarding Experience

From 12.6(1) release, the VAV feature provides different onboarding experience for OEM users (who use Cisco's contract, billing, and support for Google's speech services) via Webex Control Hub. For details, see the [Create a Contact Center AI configuration](#) article. Non-OEM users use NOAMP in the Unified CCE solution and CCE Administration Portal in the Packaged CCE solution for onboarding.

The following table lists the onboarding channel and Google APIs used for OEM and non-OEM customers:

| Release           | Services Billing                               | Onboarding        | Google APIs         |
|-------------------|------------------------------------------------|-------------------|---------------------|
| 12.6(1) and above | Cisco-billed (OEM) and Vendor-billed (non-OEM) | Webex Control Hub | AnalyzeContent (V2) |
| 12.6(1) and above | Vendor-billed (non-OEM)                        | NOAMP/CCEAdmin    | DetectIntent (V2)   |

The following table lists the support for VAV Dialogflow CX and VAV Dialogflow ES via cloud-based or premise-based connectors for OEM and non-OEM customers:

|                                    | VAV Dialogflow CX (OEM) | VAV Dialogflow ES (OEM) | VAV Dialogflow CX (Non-OEM) | VAV Dialogflow ES (Non-OEM) |
|------------------------------------|-------------------------|-------------------------|-----------------------------|-----------------------------|
| <b>Via cloud-based connector</b>   | Yes (12.6(2) and above) | No                      | Yes (12.6(2) and above)     | No                          |
| <b>Via premise-based connector</b> | Yes (12.6(1) and above) | Yes (12.6(1) and above) | Yes (12.6(2) and above)     | Yes (12.6(1) and above)     |

## VAV via Cloud-Based Connector

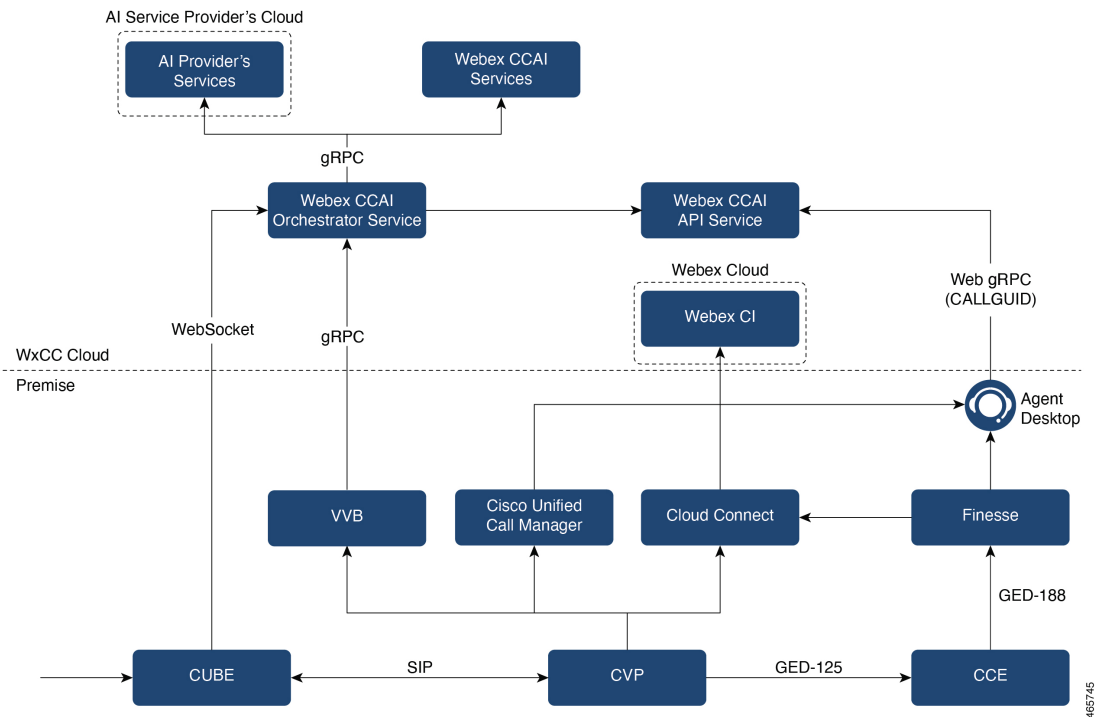
### Overview

Virtual Agent–Voice via cloud-based connector leverages Cisco's cloud-based Artificial Intelligence (AI) and Natural Language Understanding (NLU) services for designing virtual voice agents and creating complex IVR call flows.

The Webex Contact Center AI (Webex CCAI) services platform enables integration with speech-based services from different vendors. On the premise side, VVB interfaces with the Orchestrator service and connects to the CCAI service via cloud-based connector. This service is enabled through the *VirtualAgentVoice* element of Cisco Unified Call Studio.



Figure 16: Contact Center AI Services Architecture



**Note** Webex Contact Center Enterprise leverages Webex Contact Center AI (WCCA) Cloud Orchestration Platform (Universal Harnes) for AI services.

For details of the *VirtualAgentVoice* element, refer to the *Element Specifications for Cisco Unified CVP VXML Server and Call Studio* guide at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-programming-reference-guides-list.html>.

The partial response feature is supported via cloud-based connector. It notifies the caller that their request is being processed. By default, the partial prompt will stop playing when the final response is received from the webhook. For more information, see the [Configure Partial Response in Dialogflow CX](#) article.

## Important Considerations

Consider the following before configuring VAV via a cloud-based connector:

- Supported codec is u-law.
- This feature is available with Cisco-Billed and Vendor-Billed (Non-OEM) subscription services.
- Google performs the voice activity detection.
- If the call gets transferred to a real agent, then the transcript of the voice conversation between the customer and the virtual voice agent is displayed in the *Transcript* widget in the Agent Desktop (provided that the *Transcript* widget is configured on the Agent Desktop).

- Non barge-in prompt is supported only until the control gets transferred to the cloud.

## Prerequisites

To configure VAV via cloud-based connector, you should have completed the following:

- 
- The allowed list of your customer's network must include the following group of URLs:
    - [accounts.google.com/o/oauth2](https://accounts.google.com/o/oauth2)
    - \*.cisco.com
    - \*.ciscoservice.com
    - \*.ciscoccservice.com
    - \*.ciscospark.com
    - \*.cloud.google.com/dialogflow
    - \*.google.com
    - \*.googleapis.com
    - \*.gcr.io
    - \*.rtmsprod.net
    - \*.webex.com
    - \*.wbx2.com
  - The customer's CX Agent ID and GCP Project ID are created. For more information, refer to Google documentation at <https://dialogflow.cloud.google.com/cx/projects>.
  - Assessment to Quality (A2Q) process for Contact Center AI (CCAI) is completed and Cisco subscription Flex SKU for CX is procured.
    - Customer's GCP project ID is mapped with Cisco's GCP partner projects.
    - Control Hub credentials (For more information, see <https://www.webex.com/us/en/solutions/cross-platform/control-hub.html>) and Hybrid Org (For more information, see <https://www.webex.com/us/en/solutions/hybrid-work.html>) are generated.
  - Access the associated location settings for regions at Google at <https://cloud.google.com/dialogflow/cx/docs/concept/region>
  - Add non-proxy hosts using VVB CLI commands. For more information, refer to the *Command Line Interface > Set Commands* section in the *Operations Guide for Cisco Virtualized Voice Browser* at <https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/products-maintenance-guides-list.html>.

### CCE (on premise):

- Cisco VVB is upgraded to 12.6(2) using a generic COP.
- Cisco Unified CVP and Cisco VVB are configured:

- Date and time in CVP, VVB, and proxy are synchronized with a common NTP server.
- Access to DNS server is configured in CVP and VVB.

For more information on NTP and DNS server configurations in CVP, refer to the Microsoft Windows platform documentation.

For more information on NTP and DNS server configurations in VVB, refer to the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>.

- Port 443 and HTTP/2 are enabled in the proxy and firewall.
- Average bandwidth consumption per call is 106 kbps.
- The new Cisco Unified Call Studio application with the *VirtualAgentVoice* element is deployed. You can download and install the latest patch from <https://software.cisco.com/download/specialrelease/c359e375005563ceec2081c9151b482e>.

For details of the *VirtualAgentVoice* element, refer to the *Element Specifications for Cisco Unified CVP VXML Server and Call Studio* guide at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-programming-reference-guides-list.html>.

- Ensure that the Unified CCE OAMP, Cloud Connect, and VVB components have access to Webex services to use the Virtual Agent–Voice via cloud-based connector.

#### CCAI (in Cisco Webex Control Hub):

- Service provider-specific **Integration Connector** is configured. For more details, see the article <https://help.webex.com/en-us/article/9zvadb/Configure-Google-CCAI-connector-for-Webex-Contact-Center>.
- Design Google Dialogflow CX Agents. For more information, refer to Google documentation at <https://cloud.google.com/dialogflow/cx/docs/>.
- CX conversational profile ID is created using credentials provided by Cisco via email. For detailed steps, see the section *Create a Conversation Profile using Google Cloud SDK*.

**Note** En-US global customers can create the conversational profile ID through the UI at <https://agentassist.cloud.google.com/projects>. While creating the profile, enable the option **Enable virtual agent** under **Choose to use Dialogflow**. This profile ID can be used both for the Agent Answers and VAV features.

This conversation profile URL must be used to create the CCAI configuration.

- CCAI configuration is created at <https://admin.webex.com/>. For detailed steps, refer to the [Create a Contact Center AI configuration](#) article.

For further assistance, contact [Cisco Support](#).

---

#### What to do next

Configure Google Dialogflow CX Agent with Cisco Unified CCE solution.

## Configuration Task Flow

Task flow for configuring Google Dialogflow CX Agent with Cisco Unified CCE solution.

- 
- Step 1** Ensure that the Cloud Connect publisher and subscriber nodes are installed.
- For more information, see the *Install Cloud Connect* section in *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html>.
- Step 2** Register and add Cloud Connect in Control Hub. For more details, see <https://help.webex.com/en-us/article/n24wo0fb/Register-Cloud-Connect>.
- Step 3** Configure Cloud Connect with VVBs in the Operations Console (NOAMP for Cisco Unified CCE, and CCE Admin for Packaged CCE).
- For details, see the *Cisco Unified Customer Voice Portal > Operations Console (NOAMP) > Integration > Cloud Connect > Configure CVP or VVB Devices for Cloud Connect* section in the *Administration 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>.
- Note** After an VVB upgrade, Cloud Connect has to be reconfigured with VVB devices.
- Step 4** Import the Cloud Connect certificate to the CVP server.
- For details, see the *Unified CVP Security > Import Cloud Connect Certificate to Unified CVP Keystore* section in the *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>.
- Step 5** View the default CCAI configuration (created as part of CCAI prerequisites). If required, synchronize the configuration (using *Sync* option), in the CVP Operations Console (NOAMP for Cisco Unified CCE, and CCE Admin for Packaged CCE).
- For details, see the *Cisco Unified Customer Voice Portal > Operations Console (NOAMP) > Contact Center AI > Configuration for Cisco-Billed AI Services* section in the *Administration 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>.
- Step 6** Design Google Dialogflow CX application.
- For more information, refer to Google documentation at <https://dialogflow.cloud.google.com/cx/projects>.
- For further assistance, contact the Cisco TAC team.
- Step 7** To use the regionalised media support, see the [Regional Media Data Center Region Mapping, on page 238](#) section.
- 

## Hybrid IVR with VAV via Cloud-Based Connector

Dialogflow CX enables contact centers to use cloud-based AI features via Cisco Cloud. With Cisco's Hybrid IVR functionality, customers who have on-premises applications can leverage their traditional ASR/TTS/CRM integrations, along with cloud-based Dialogflow CX AI capabilities. They can select a few nodes or sections of their application to be processed in the cloud and few nodes to be processed on-premises. For example, in

an application, OTP (Open Time Password) generation can be performed on-premises, while other tasks can be processed in the cloud.

Hybrid IVR with Dialogflow CX provides the flexibility to switch from the cloud services to the on-premises application, to use the on-premises subroutine calls, and perform the required operations. After these operations are done, the flow can go back to the cloud services and resume from where it left.

The switching between the cloud services and the on-premises application is achieved by defining a custom payload with an event and associated parameters. This custom payload is passed to the on-premises application. When the flow resumes in the cloud, Dialogflow CX uses the event and parameters that are received from the on-premises application.

The *VirtualAgentVoice* element of Cisco Unified Call Studio is used to engage the Google Dialogflow CX services with Hybrid IVR functionality via Cisco Cloud.

To configure the Hybrid IVR functionality with Dialogflow CX, see [Configure Hybrid IVR, on page 225](#).


**Note**

- Hybrid IVR and IVR transcription functionalities are available *only* with Dialogflow CX from 12.6(2) and higher.
- The *VirtualAgentVoice* element supports both Cisco DTMF and Nuance adapters.

## Configure Hybrid IVR

Task flow to configure Hybrid IVR with Google Dialogflow CX agent via Cisco Cloud:

- Step 1** In the Google Dialogflow CX console, select the project and the agent.
- Step 2** In the Google Dialogflow CX agent screen, under the **Build** tab, select the required flow and the required page (**Start/End Flow/End Session**) in this flow, in which a fulfillment is needed from the on-premises application. The details of the selected page appears.
- Step 3** Under **Routes** section, define a route and conditions that satisfy the custom exit criteria, for triggering the transition.
- Step 4** In this route, under **Fulfillment** section, click **Add dialogue option** and select **Custom payload**.
- Note** Only **Custom payload** has to be defined here. Do not add any other dialogue options.
- Step 5** Add the custom payload of type *Execute\_Request* that defines the action and elements to be filled in the Unified Call Studio *VirtualAgentVoice* element.

The format for defining the custom payload is as follows:

```

{"Execute_Request":{
 "Event_Name": "<Name of the event>",
 "Data" : {
 "Params":{
 "<param1 name>": "<param1 value>",
 "<param2 name>": "<param2 value>"
 }
 }
}

```

**Note** Ensure that you map this event name with the same event name in Unified Call Studio *VirtualAgentVoice* element for decision mapping.

**Step 6** Select **Page** under the **Transition** section, to set the transition to the same page when the flow resumes.

**Step 7** For re-entry from the on-premises application to cloud, create an event handler. This event name is to be provided to the *VirtualAgentVoice* element during re-entry. For more information, refer to <https://cloud.google.com/dialogflow/cx/docs/reference/rest/v3/EventHandler>.

It's the responsibility of the Dialogflow CX developer to create this event handler. Otherwise, the application fails.

## VAV via Premise-Based Connector

Virtual Agent–Voice via premise-based connector leverages Google's cloud-based Artificial Intelligence (AI) and Natural Language Understanding (NLU) services for designing virtual voice agents and creating complex IVR call flows.

VAV currently supports two flavors of Google Dialogflow services via premise-based connector:

## VAV for Dialogflow CX

### Overview

Virtual Agent–Voice for Dialogflow CX leverages Google's Dialogflow CX service that allows designing virtual voice agents and creating and connecting complex IVR call flows.

Using Google Dialogflow CX, multiple agents can be created under the same Project ID. These agents can be accessed and managed for different lines of business with a single Google account. For more information, refer to the Google Dialogflow CX documentation at <https://cloud.google.com/dialogflow/cx/docs>.

VVB uses a premise-based connector to connect to the Google Dialogflow service. This service is enabled through the *DialogflowCX* element of Cisco Unified Call Studio.

For details of the *DialogflowCX* element, refer to the *Element Specifications for Cisco Unified CVP VXML Server and Call Studio, Release 12.6(1)* guide at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-programming-reference-guides-list.html>.



- Note**
- Only u-law codec is supported.
  - This feature is available with Cisco subscription services and Vendor-billed (Non-OEM).

### Prerequisites

For supported minimum versions, refer to the *Cisco Unified Customer Voice Portal > New Features > Virtual Agent–Voice for Dialogflow CX* section in the *Release Notes for Cisco Contact Center Enterprise Solutions Release 12.6(1)*.



**Note** Ensure that the Unified CCE OAMP and Cloud Connect components have access to Webex services and the VVB components have access to both Webex and Google services to use the Virtual Agent-Voice for Dialogflow CX via premise-based connector.

To configure Google Dialogflow CX, you should have completed the following procedures:

- The customer's CX Agent ID and GCP Project ID are created. For more information, refer to Google documentation at <https://dialogflow.cloud.google.com/cx/projects>.
- Assessment to Quality (A2Q) process for Contact Center AI (CCAI) is completed and Cisco subscription Flex SKU for CX is procured.
  - Customer's GCP project ID is mapped with Cisco's GCP partner projects.
  - Control Hub credentials and Hybrid Org are generated.

For assistance, you can contact the Cisco TAC team.

- CX conversational profile ID is created using credentials provided by Cisco via email. For details, see [Create a Conversation Profile using Google Cloud SDK, on page 229](#).

This conversation profile URL is to be used for creating the CCAI configuration.

- Cisco Unified CVP and Cisco VVB are configured:
  - Date and time in CVP, VVB, and proxy are synchronized with a common NTP server.
  - Access to DNS server is configured in CVP and VVB.

For more information on NTP and DNS server configurations in CVP, refer to the Microsoft Windows platform documentation.

For more information on NTP and DNS server configurations in VVB, refer to the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>.

- Port 443 and HTTP/2 are enabled in the proxy and firewall.
- The new Cisco Unified Call Studio application with the *DialogflowCX* element and *VirtualAgentVoice* element is deployed. You can download and install the latest patch from <https://software.cisco.com/download/specialrelease/c359e375005563ceec2081c9151b482e>.

For details of the *DialogflowCX* element and *VirtualAgentVoice* element, refer to the *Element Specifications for Cisco Unified CVP VXML Server and Call Studio, Release 12.6(1)* guide at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-programming-reference-guides-list.html>.

- The following table lists the required versions for Cisco Unified CVP, Cisco VVB, Cloud Connect, CCE components (Router, Logger, AW, and PG), and ICM.

| CVP             | VVB             | Cloud Connect   | CCE Components  | ICM             |
|-----------------|-----------------|-----------------|-----------------|-----------------|
| 12.6 and higher | 12.6 and higher | 12.6 and higher | 12.6 and higher | 12.6 and higher |

### What to do next

Configure Google Dialogflow CX Agent with Cisco Unified CCE solution.

## Configuration Task Flow

Task flow for configuring the Google Dialogflow CX Agent with Cisco Unified CCE solution.

- 
- Step 1** Ensure that the Cloud Connect publisher and subscriber nodes are installed.
- For more information, see the *Install Cloud Connect* section in *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html>.
- Step 2** Configure Cloud Connect with VVBs in the Operations Console (NOAMP for Cisco Unified CCE and CCE Admin for Packaged CCE).
- For details, see the *Cisco Unified Customer Voice Portal > Operations Console (NOAMP) > Integration > Cloud Connect > Configure CVP or VVB Devices for Cloud Connect* section in the *Administration 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>.
- Step 3** Import the Cloud Connect certificate to the CVP server.
- For details, see the *Unified CVP Security > Import Cloud Connect Certificate to Unified CVP Keystore* section in the *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>.
- Step 4** Create Contact Center AI (CCAI) configuration in Cisco Webex Control Hub at <https://admin.webex.com>. A CCAI configuration leverages CCAI Connectors to invoke the CCAI services.
- For detailed steps to set up Integration Connectors, see the <https://help.webex.com/en-us/article/9zvadf/Configure-Google-CCAI-connector-for-Webex-Contact-Center> article.
- For detailed steps to create CCAI configuration, see the *Create a Contact Center AI configuration* article. This default config can be used for accessing multiple AI services on multiple devices.
- Step 5** View the default CCAI configuration. If required, synchronize the configuration (using *Sync* option) in the CVP Operations Console (NOAMP for Cisco Unified CCE and CCE Admin for Packaged CCE).
- For details, see the *Cisco Unified Customer Voice Portal > Operations Console (NOAMP) > Contact Center AI > Configuration for Cisco-Billed AI Services* section in the *Administration 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>.
- Step 6** Design Google Dialogflow CX Agents. For more information, refer to Google documentation at <https://dialogflow.cloud.google.com/cx/projects>.
- Step 7** Configure a welcome event for all Google Dialogflow CX Agents. For details, see [Create a Welcome Event, on page 231](#).



- Note**
- You can configure custom events to override the default welcome event. Provide the element data *event\_name* in the Dialogflow CX element and ensure that you configure the same name in the CX Agent to start the flow. For instructions, see [Configure custom events in Dialogflow CX](#).
  - For further assistance, contact [Cisco Support](#).

---

## Create a Conversation Profile using Google Cloud SDK



---

**Note** The steps in the following procedure are for reference only. For more details, refer to Google Documentation.

---

- Step 1** Get the agent ID:
- Open <https://dialogflow.cloud.google.com/cx/projects>.
  - Select the appropriate project. The list of configured agents is displayed.
  - Note the agent ID to be configured. If no new agents are created, you can select a preconfigured agent.
- Step 2** Create a user via Google IAM (Identity and Access Management) and add the following roles: Dialogflow API admin, Service Account Token Creator, and Service Account user .
- For more information, see <https://cloud.google.com/iam/docs/creating-managing-service-accounts>.
- Step 3** Install and configure the Google SDK on your system.
- For more information, see <https://cloud.google.com/sdk/docs/quickstart>.
- Step 4** When you are asked to log in during the installation of Google SDK, log in using the ID of the agent for whom you want to create the conversation profile.
- Note** You can also log in using the same ID to the GCP CLI with the command `gcloud auth login` after installing the Google SDK.
- Step 5** Run the following command: `gcloud auth print-access-token --impersonate-service-account=Service Account ID`
- For more information, see <https://cloud.google.com/iam/docs/impersonating-service-accounts>.
- Step 6** Create the conversation profile using REST API for Dialogflow by using Postman:
- In the Postman workspace, select the method as **POST**.
  - In the URL field, add the address in the following format after replacing the *regionId* and *projectId* appropriately:  
`https://<regionId>-dialogflow.googleapis.com/v2beta1/projects/<projectId>/locations/<regionId>/conversationProfiles`
  - Under the **Headers** section, add the following key values for Authorization and Content-type:
    - Authorization: *Bearer <token generated with the Google command>*
    - Content-type: *application/json*
  - Under the **Body** section, select **raw**. From the last dropdown, select **JSON**.

- e) In the code space, enter the following code (after replacing the *regionId*, *projectId*, and *agentId* in the **agent** tag with actual values):

```
{
 "name": "TACCXTest",
 "automatedAgentConfig": {
 "agent": "projects/<projectId>/locations/<regionId>/agents/<agentId>"
 },
 "displayName": "TACCXTest",
 "humanAgentAssistantConfig": {
 "messageAnalysisConfig": {
 "enableEntityExtraction": true,
 "enableSentimentAnalysis": true
 }
 }
}
```

- f) Click **Send** to run the command.

Example response:

```
{
 "name": "projects/projectrtp2020/locations/us-central1/conversationProfiles/QlO36mwSUa3cJg",
 "displayName": "TACCXTest",
 "automatedAgentConfig": {
 "agent":
 "projects/projectrtp2020/locations/us-central1/agents/40d0-aa2a-1bf453d9bf5c/environments/draft"
 },
 "humanAgentAssistantConfig": {
 "notificationConfig": {},
 "messageAnalysisConfig": {
 "enableEntityExtraction": true,
 "enableSentimentAnalysis": true
 }
 },
 "languageCode": "en-US"
}
```

In the above example response, the following conversation profile is obtained:  
*projects/projectrtp2020/locations/us-central1/conversationProfiles/dQlO36mwSUa3cJg*.

You can use this profile while creating the Control Hub configuration.

For more information, see <https://cloud.google.com/sdk/gcloud/reference>.

## Step 7 Create the conversation profile using REST API for Dialogflow by using Postman:

- Add headers: Content-type Application/json.
- Authorization: Bearer - add the token generated with the Google command.
- Add the method as POST.
- In the URL section, add the address after replacing the *regionId* and the *projectId* appropriately. The address is in the following format:  
`https://<regionId>-dialogflow.googleapis.com/v2beta1/projects/<projectId>/locations/<regionId>/conversationProfiles`
- In the body section, choose RAW and JSON.
- In the **Agent** tag, use the appropriate *regionId*, *projectId*, and *agentId*.

```
{
 "name": "TACCXTest",
 "automatedAgentConfig": {
 "agent": "projects/<projectId>/locations/<regionId>/agents/<agentId>"
 },
 "displayName": "TACCXTest",
```

```
"humanAgentAssistantConfig": {
 "messageAnalysisConfig": {
 "enableEntityExtraction": true,
 "enableSentimentAnalysis": true
 }
}
```

Example response:

```
{
 "name": "projects/tacprojectrtp2020/locations/us-central1/conversationProfiles/dCv41C1uQ1O36mwSUa3cJg",
 "displayName": "TACCXTest",
 "automatedAgentConfig": {
 "agent":
 "projects/tacprojectrtp2020/locations/us-central1/agents/5cca975a-bbb3-40d0-aa2a-1bf453d9bf5c/environments/draft"
 },
 "humanAgentAssistantConfig": {
 "notificationConfig": {},
 "messageAnalysisConfig": {
 "enableEntityExtraction": true,
 "enableSentimentAnalysis": true
 }
 },
 "languageCode": "en-US"
}
```

This is the conversation profile that you obtain in the example.

*projects/tacprojectrtp2020/locations/us-central1/conversationProfiles/dCv41C1uQ1O36mwSUa3cJg*. You can use this profile while creating the Control Hub configuration.

For more information, see <https://cloud.google.com/sdk/gcloud/reference>.

- Step 8** In a new browser tab, open <https://agentassist.cloud.google.com/> and select the appropriate project. The list of profiles is displayed.
- Step 9** Click the copy icon next to the profile ID to be used. Copy the profile URL in the following format:  
*projects/<project\_ID>/locations/<location>/conversationProfiles/<profile ID>*.
- You can use this profile URL while creating the Control Hub configuration.

---

## Create a Welcome Event

Create a welcome event to be played to the caller when a call is initiated.

- 
- Step 1** Open <https://dialogflow.cloud.google.com/cx/projects>.
- Step 2** Select the project and agent for which the welcome event is to be configured.
- Step 3** In the Google Dialogflow CX Agent screen, click **Default Start Flow** in the left panel.
- Step 4** Click **Start > Event handlers**.
- Step 5** In the right panel, click **Add event handler**.
- Step 6** Check the **Use custom event** checkbox.
- Step 7** In the **Custom Event** textbox, type **welcome\_event**.
- Step 8** In the **Agent says** textbox, type the welcome message to be played.
- Step 9** Save the changes.

**Note** To override the default welcome event, provide the element data *event\_name* in the DialogflowCX element. The same name must be configured in the CX Agent to start the flow.

## VAV for Dialogflow ES



**Note** The Dialogflow ES GCP project trial version should not be used in a production environment.

### Dialogflow ES via VVB (OEM Users)

#### Overview

Virtual Agent–Voice (VAV) feature provides an enhanced onboarding experience to OEM customers via Webex Control Hub. All contract, billing, and support are managed through Cisco for OEM customers and they can use Cisco services coupled with Google’s cloud-based-AI-enabled speech services.

A single config ID generated via Control Hub can be leveraged across all CVP/VVB instances as compared to the earlier experience where each instance was required to be configured individually.

From 12.5(1) release, OEM users use NOAMP in Unified CCE solution, and Single Pane of Glass (SPOG) in Packaged CCE solution for VAV onboarding.

The following table lists the onboarding channel and Google APIs used for non-OEM customers:

| Release             | Services Billing   | Onboarding        | Google APIs         |
|---------------------|--------------------|-------------------|---------------------|
| 12.6(1) and 12.6(2) | Cisco-billed (OEM) | Webex Control Hub | AnalyzeContent (V2) |

#### Prerequisites



**Note** Ensure that the VVB components have access to Google and Webex services and Cloud Connect components have access to Webex services to use the Virtual Agent–Voice for Dialogflow ES via VVB (OEM users).

The prerequisites for configuring Virtual Agent–Voice for OEM users are:

- OEM users must provision Google Contact Center AI (CCAI) for Cisco Contact Center Enterprise. For details, see the [Create a Contact Center AI configuration](#) article.
- CVP/VVB configuration:
  - Enable access to cloud-based services from CVP and VVB directly or via proxy.

For details, see the *Cisco Unified Customer Voice Portal > Operations Console (NOAMP) > Integration > Cloud Connect > Configure CVP or VVB Devices for Cloud Connect* section in the *Administration 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>.

- Synchronize the date/time in CVP, VVB, and proxy with a common NTP server.
- Configure access to DNS server in CVP/VVB.

For more information on NTP and DNS server configurations in CVP, refer to the Microsoft Windows platform documentation.

For more information on NTP and DNS server configurations in VVB, refer to the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>.

- The following table lists the required versions for Cisco Unified CVP, Cisco VVB, Cloud Connect, CCE components (Router, Logger, AW, and PG), and ICM.

| CVP             | VVB             | Cloud Connect   | CCE Components                    | ICM                               |
|-----------------|-----------------|-----------------|-----------------------------------|-----------------------------------|
| 12.6 and higher | 12.6 and higher | 12.6 and higher | 12.5 and higher with A2Q approval | 12.5 and higher with A2Q approval |



**Note** If you are using 12.5 and higher, you are required to use Single Pane of Glass (SPOG) based onboarding for Packaged CCE solution for VAV onboarding and NOAMP based onboarding for Unified CCE solution for VAV onboarding.

## VAV Onboarding for OEM Users Task Flow

Follow this procedure to provision Google CCAI with Cisco Unified Contact Center Enterprise. A single configuration created via Control Hub can be used for accessing multiple AI services, such as VAV and Agent Answers on multiple devices.

- Step 1** Create a CCAI configuration in Cisco Webex Control Hub at <https://admin.webex.com>. A CCAI configuration leverages CCAI Connectors to invoke the CCAI services.
- For details, see the [Create a Contact Center AI configuration](#) article. This default config can be used for accessing multiple AI services on multiple devices.
- Note** While creating a CCAI configuration (explained in the article [Create a Contact Center AI configuration](#)):
- Skip the creation of conversation profile.
  - Select the **Apply as default for Virtual Agent** configuration, because it is mandatory for ASR and TTS.
- Step 2** Ensure that the Cloud Connect publisher and subscriber are installed.
- For more information, see the *Install Cloud Connect* section in *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html>.
- Step 3** Import the Cloud Connect certificate to the CVP server.

For details, see the *Unified CVP Security > Import Cloud Connect Certificate to Unified CVP Keystore* section in the *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>.

**Step 4** Configure Cloud Connect with CVP in the Operations Console (NOAMP).

**Step 5** Configure Cloud Connect with VVBs in the Operations Console (NOAMP).

For details, see the *Cisco Unified Customer Voice Portal > Operations Console (NOAMP) > Integration > Cloud Connect > Configure CVP or VVB Devices for Cloud Connect* section in the *Administration 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>.

**Step 6** View the default CCAI configuration (created in step 1). If required, synchronize the configuration (using *Sync* option) in the CVP Operations Console (NOAMP).

For details, see the *Cisco Unified Customer Voice Portal > Operations Console (NOAMP) > Contact Center AI > Configuration for Cisco-Billed AI Services* section in the *Administration 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>.



**Note** To change or override the default config (created in step 1), configure the `CCAI.configId` property of the `Dialogflow` element in Call Studio.

For details, see the *Dialogflow Element > Custom VoiceXML Properties* section in the *Element Specifications for Cisco Unified CVP VXML Server and Call Studio* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-programming-reference-guides-list.html>.

## Migration for OEM Users

OEM users migrating from 12.5(1) or 12.5(1a) to 12.6(1) must onboard via Webex Control Hub for better experience and enhanced security. They can continue to use the old method of key generation by retaining their old configurations until their onboarding via Webex Control Hub is complete.

## Important Considerations

VVB periodically refreshes the CCAI configurations. Whenever these configurations are changed in the Control Hub, it may take up to 10 minutes for the changes to reflect in VVB. For applying the changes instantly, you need to restart the VVB speech server service.

## Dialogflow ES via VVB (Non-OEM Users)

### Overview

From 12.5(1) release, non-OEM users use NOAMP in Unified CCE solution, and CCE Administration Portal in Packaged CCE solution for VAV onboarding.

The following table lists the onboarding channel and Google APIs used for non-OEM customers:

| Release             | Services Billing        | Onboarding     | Google APIs       |
|---------------------|-------------------------|----------------|-------------------|
| 12.6(1) and 12.6(2) | Vendor-billed (non-OEM) | NOAMP/CCEAdmin | DetectIntent (V2) |

## Prerequisites




---

**Note** Ensure that the VVB components have access to Google services to use the Virtual Agent–Voice for Dialogflow ES via VVB (non OEM users).

---

- Enable access to cloud-based services from CVP and VVB directly or via proxy. For details, see the *Cisco Unified Customer Voice Portal > Operations Console (NOAMP) > Integration > Cloud Connect > Configure CVP or VVB Devices for Cloud Connect* section in the *Administration 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>.
- Synchronize the date/time in CVP, VVB, and proxy with a common NTP server.
- Configure access to DNS server in CVP/VVB.

For more information on NTP and DNS server configurations in CVP, refer to the Microsoft Windows platform documentation.

For more information on NTP and DNS server configurations in VVB, refer to the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>.

- Access key for Google Text-to-Speech. For more information, see <https://cloud.google.com/text-to-speech/docs/quickstart-client-libraries>.
- Access key for Google Speech-to-Text. For more information, see <https://cloud.google.com/speech-to-text/docs/quickstart-client-libraries>.
- Configure Dialogflow Agent:
  1. Get the Dialogflow Agent Key. For more information, see <https://dialogflow.com/docs/reference/v2-auth-setup>.
  2. Migrate your Dialogflow Agent to Enterprise Essential (**Console Left Bar > Migrate from Standard to Enterprise Essential**).
  3. Enable the enhanced Speech Model in Dialogflow console (**Settings > Speech > Enable Enhanced Speech Model and Data Logging**).




---

**Note** If this option is enabled, speech recognition data is shared with Google. For more information see <https://cloud.google.com/speech-to-text/docs/enhanced-models>.

---

- Non-OEM users must enable speech services and generate JSON key. To know more about enabling speech services, see [Enable Speech Services \(For Non-OEM Users\)](#), on page 236. To know more about generating JSON key, see [Generate JSON Key \(for Non-OEM Users\)](#), on page 236.
- The following table lists the required versions for Cisco Unified CVP, Cisco VVB, Cloud Connect, CCE components (Router, Logger, AW, and PG), and ICM.

| CVP             | VVB             | Cloud Connect | CCE Components                    | ICM                               |
|-----------------|-----------------|---------------|-----------------------------------|-----------------------------------|
| 12.5 and higher | 12.5 and higher | NA            | 12.5 and higher with A2Q approval | 12.5 and higher with A2Q approval |



**Note** Trial version of Dialogflow ES GCP project should not be used in production environment.

## VAV Onboarding for Non-OEM Users Task Flow

**Step 1** Enable speech services for your account.

To know more about enabling speech services, see [Enable Speech Services \(For Non-OEM Users\)](#), on page 236.

**Step 2** Generate JSON key for your account.

To know more about generating JSON key, see [Generate JSON Key \(for Non-OEM Users\)](#), on page 236.

**Step 3** Configure VVB devices for speech services.

For details, see the *Cisco Unified Customer Voice Portal > Operations Console (NOAMP) > Contact Center AI > Configuration for Vendor-Billed AI Services* section in the *Administration 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>.

### Enable Speech Services (For Non-OEM Users)

To enable speech services, follow these steps:

1. Log in to your Dialogflow account at <https://dialogflow.cloud.google.com/>.
2. Scroll down on the homepage and click **Project ID** of your Dialogflow agent.  
This takes you to the Google Cloud Platform (GCP) homepage.
3. Select **APIs & Services** from the left pane (through the hamburger menu).
4. Select the API services (such as Cloud Text-to-Speech, Cloud Speech-to-Text, and Dialogflow) to be enabled.
5. Click **Enable** to enable the selected API for the given Project ID.

### Generate JSON Key (for Non-OEM Users)

To generate the JSON key, follow these steps:

1. In the GCP homepage, select **IAM & Admin** from the left pane (through the hamburger menu).
2. Select **Service accounts** which shows the list of your enabled services.
3. Select the service for which the JSON key is to be generated.
4. Click the ellipsis menu on the right and click **+Create Key**.



5. Select JSON as **Key type** and then click **Create**.

The key is downloaded.

For best results:

- Migrate your Dialogflow Agent to Enterprise Essential (**Console Left Bar > Migrate from Standard to Enterprise Essential**).
- Enable the enhanced Speech Model in Dialogflow console (**Settings > Speech > Enable Enhanced Speech Model and Data Logging**).

If this option is enabled, speech recognition data is shared with Google. For more information see <https://cloud.google.com/speech-to-text/docs/enhanced-models>.

## Documentation Resources

The following table lists the reference documents for VAV.

| Information                                                     | Resource                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sample VAV Application                                          | See <a href="https://github.com/CiscoDevNet/cvp-sample-code/tree/master/CustomVirtualAssistant">https://github.com/CiscoDevNet/cvp-sample-code/tree/master/CustomVirtualAssistant</a> .                                                                                                                                                                                                                                                                                                            |
| Design Considerations                                           | <i>Design Considerations for Integrated Features &gt; Virtual Agent–Voice Considerations</i> section in <i>Solution Design Guide</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html</a> .                                              |
| VAV configuration in Unified CCE Deployment                     | <i>Operations Console (NOAMP)</i> section in <i>CVP Administration Guide</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html</a> .                                                                                            |
| TTS Prompt Cache Management and proxy setting for Speech Server | <i>VVB Operations Guide</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/products-maintenance-guides-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/products-maintenance-guides-list.html</a> .                                                                                                                                                                                           |
| Proxy settings for VXML Server                                  | See the <i>VXML Server Configuration &gt; Proxy Settings in VXML Server for Virtual Agent–Voice</i> section in <i>CVP Configuration Guide</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html</a> .                           |
| Configuration of Call Studio elements for VAV                   | The following chapters in <i>CVP Element Specification Guide</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-programming-reference-guides-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-programming-reference-guides-list.html</a> : <ul style="list-style-type: none"> <li>• <i>Dialogflow Element</i></li> <li>• <i>DialogflowIntent Element</i></li> </ul> |

| Information                   | Resource                                                                                                                                                                                                                                                                     |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                               | <ul style="list-style-type: none"> <li>• <i>DialogflowParam Element</i></li> <li>• <i>Transcribe Element</i></li> </ul>                                                                                                                                                      |
| VAV Speech Configuration APIs | See <i>VAV Speech Configuration</i> section in <i>VVB Developer Guide</i> at <a href="https://developer.cisco.com/site/customer-voice-portal/documents/virtual-voice-browser/">https://developer.cisco.com/site/customer-voice-portal/documents/virtual-voice-browser/</a> . |

## Regional Media Data Center Region Mapping

Contact Center Enterprise (CCE) now extends support for regional media across all supported data centre locations. This feature allows both customer and agent media (including audio and SIP signalling) to remain local to a specific geographic region, irrespective of the location of the CCAI cloud services data center tenant or home location.

To utilize regional media from a country or location that differs from your customer's organization, it is necessary to configure the appropriate variables in the SIP profile. This configuration should be done within the Session Border Controller (SBC) for both Virtual Agent-Voice and Agent Answers.

To enable regional media, follow these steps:

**Step 1** Access the SBC console and modify the existing SIP profile configuration, which was used during the setup of both Virtual Agent-Voice and Agent Answers. For more information, see [Create a SIP Profile at the Dial-Peer Level in CUBE, on page 8](#).

**Step 2** Run the following command to add the `X-Cisco-Clusterid` variable. This variable is added using a custom SIP header in the outgoing `INVITE` request as shown below:

### Syntax:

```
request INVITE sip-header Call-Info add "X-Cisco-Clusterid : rtmsClusterId = <Regional Media Variable> ; wxccClusterId = <Cisco CCAI Services Variable>"
```

The `x-Cisco-Clusterid` variable requires the following key values:

- **rtmsClusterId:** The value of the variable used for Regional Media data center.
- **wxccClusterId:** The value of the variable used for CCAI cloud services data center.

### Example:

```
request INVITE sip-header Call-Info add "X-Cisco-Clusterid : rtmsClusterId = US1 ; wxccClusterId = US1"
```

The following tables list the variables associated with regional media data centers located in different countries. If your region is not listed below, ensure that you select the nearest data center location applicable to your region.

**Important** Ensure that you input the values of the variable exactly as they are specified in the tables below. These values are case sensitive. Any discrepancies in the values could potentially lead to data loss or system downtime. Therefore, it is crucial to verify these values before implementing them in a production environment.

Table 15: Data Center Location - APAC

| S. No | Country of Operation | Regional Media Data Center | Regional Media Variable | Cisco CCAI Services Variable | Default Regional Media Variable | Default Cisco CCAI Services Variable |
|-------|----------------------|----------------------------|-------------------------|------------------------------|---------------------------------|--------------------------------------|
| 1     | Australia            | Australia                  | AS1                     | ANZ1                         | AS1                             | ANZ1                                 |
| 2     | Indonesia            | Singapore                  | SN1                     | ANZ1                         | AS1                             | ANZ1                                 |
| 3     | Jordan               | United Kingdom             | UK1                     | EU1                          | UK1                             | EU1                                  |
| 4     | Malaysia             | Singapore                  | SN1                     | ANZ1                         | AS1                             | ANZ1                                 |
| 5     | New Zealand          | Australia                  | ANZ1                    | ANZ1                         | AS1                             | ANZ1                                 |
| 6     | Philippines          | Singapore                  | SN1                     | ANZ1                         | AS1                             | ANZ1                                 |
| 7     | Singapore            | Singapore                  | SN1                     | ANZ1                         | AS1                             | ANZ1                                 |
| 8     | South Korea          | Japan                      | JA1                     | JP1                          | AS1                             | ANZ1                                 |
| 9     | Thailand             | Singapore                  | SN1                     | ANZ1                         | AS1                             | ANZ1                                 |
| 10    | Vietnam              | Singapore                  | SN1                     | ANZ1                         | AS1                             | ANZ1                                 |
| 11    | Japan                | Japan                      | JA1                     | JP1                          | JA1                             | JP1                                  |

Table 16: Data Center Location - EMEA

| S. No | Country of Operation | Regional Media Data Center | Regional Media Variable | Cisco CCAI Services Variable | Default Regional Media Variable | Cisco CCAI Services Variable |
|-------|----------------------|----------------------------|-------------------------|------------------------------|---------------------------------|------------------------------|
| 1     | Austria              | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 2     | Belgium              | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 3     | Bulgaria             | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 4     | Croatia              | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 5     | Cyprus               | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 6     | Czech Republic       | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 7     | Denmark              | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 8     | Estonia              | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 9     | Finland              | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 10    | France               | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 11    | Georgia              | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |

| S. No | Country of Operation | Regional Media Data Center | Regional Media Variable | Cisco CCAI Services Variable | Default Regional Media Variable | Cisco CCAI Services Variable |
|-------|----------------------|----------------------------|-------------------------|------------------------------|---------------------------------|------------------------------|
| 12    | Germany              | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 13    | Greece               | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 14    | Hungary              | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 15    | Ireland              | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 16    | Italy                | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 17    | Latvia               | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 18    | Lithuania            | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 19    | Luxembourg           | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 20    | Malta                | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 21    | Netherlands          | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 22    | Norway               | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 23    | Poland               | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 24    | Portugal             | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 25    | Romania              | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 26    | Slovakia             | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 27    | Slovenia             | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 28    | Spain                | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 29    | Sweden               | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 30    | Switzerland          | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 31    | Ukraine              | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 32    | United Arab Emirates | Germany                    | GM1                     | EU2                          | GM1                             | EU2                          |
| 33    | Saudi Arabia         | United Kingdom             | UK1                     | EU1                          | UK1                             | EU1                          |
| 34    | South Africa         | United Kingdom             | UK1                     | EU1                          | UK1                             | EU1                          |
| 35    | South Sudan          | United Kingdom             | UK1                     | EU1                          | UK1                             | EU1                          |

| S. No | Country of Operation | Regional Media Data Center | Regional Media Variable | Cisco CCAI Services Variable | Default Regional Media Variable | Cisco CCAI Services Variable |
|-------|----------------------|----------------------------|-------------------------|------------------------------|---------------------------------|------------------------------|
| 36    | United Kingdom       | United Kingdom             | UK1                     | EU1                          | UK1                             | EU1                          |

Table 17: Data Center Location - AMER

| S. No | Country of Operation | Regional Media Data Center | Regional Media Variable | Cisco CCAI Services Variable | Default Regional Media Variable | Default Cisco CCAI Services Variable |
|-------|----------------------|----------------------------|-------------------------|------------------------------|---------------------------------|--------------------------------------|
| 1     | Argentina            | United States              | US1                     | US1                          | US1                             | US1                                  |
| 2     | Aruba                | United States              | US1                     | US1                          | US1                             | US1                                  |
| 3     | Bahamas              | United States              | US1                     | US1                          | US1                             | US1                                  |
| 4     | Belize               | United States              | US1                     | US1                          | US1                             | US1                                  |
| 5     | Bermuda              | United States              | US1                     | US1                          | US1                             | US1                                  |
| 6     | Brazil               | United States              | US1                     | US1                          | US1                             | US1                                  |
| 7     | Caymen Islands       | United States              | US1                     | US1                          | US1                             | US1                                  |
| 8     | Chile                | United States              | US1                     | US1                          | US1                             | US1                                  |
| 9     | Colombia             | United States              | US1                     | US1                          | US1                             | US1                                  |
| 10    | Costa Rica           | United States              | US1                     | US1                          | US1                             | US1                                  |
| 11    | Curacao              | United States              | US1                     | US1                          | US1                             | US1                                  |
| 12    | Dominican Republic   | United States              | US1                     | US1                          | US1                             | US1                                  |
| 13    | Ecuador              | United States              | US1                     | US1                          | US1                             | US1                                  |
| 14    | El Salvador          | United States              | US1                     | US1                          | US1                             | US1                                  |
| 15    | Guatemala            | United States              | US1                     | US1                          | US1                             | US1                                  |
| 16    | Honduras             | United States              | US1                     | US1                          | US1                             | US1                                  |
| 17    | India                | India                      | IN1                     | EU1                          | US1                             | US1                                  |
| 18    | Jamaica              | United States              | US1                     | US1                          | US1                             | US1                                  |
| 19    | Mexico               | United States              | US1                     | US1                          | US1                             | US1                                  |
| 20    | Nicaragua            | United States              | US1                     | US1                          | US1                             | US1                                  |
| 21    | Panama               | United States              | US1                     | US1                          | US1                             | US1                                  |

| S. No | Country of Operation | Regional Media Data Center | Regional Media Variable | Cisco CCAI Services Variable | Default Regional Media Variable | Default Cisco CCAI Services Variable |
|-------|----------------------|----------------------------|-------------------------|------------------------------|---------------------------------|--------------------------------------|
| 22    | Peru                 | United States              | US1                     | US1                          | US1                             | US1                                  |
| 23    | Puerto Rico          | United States              | US1                     | US1                          | US1                             | US1                                  |
| 24    | Trinidad and Tobago  | United States              | US1                     | US1                          | US1                             | US1                                  |
| 25    | United States        | United States              | US1                     | US1                          | US1                             | US1                                  |
| 26    | Canada               | Canada                     | CA1                     | CA1                          | CA1                             | CA1                                  |

**Step 3**

To ensure connection with the Cisco Finesse gadget, you must enable the `POD.ID` Extended Call Context (ECC) variable in **Unified CCE Configuration Manager > List Tools > Expanded Call Variables List**.

---



## CHAPTER 16

# Virtual Agent–Voice Call Transcription

- [VAV Transcript Overview, on page 243](#)
- [Prerequisites, on page 244](#)
- [Configuration Task Flow, on page 244](#)

## VAV Transcript Overview

Cisco Contact Center Enterprise leverages Artificial Intelligence (AI) and Natural Language Understanding (NLU) to provide transcription services that assist agents. These services are available for the agents in the Cisco Finesse desktop gadgets.

If a customer has interacted with a virtual agent at the beginning of the call and then the call gets routed to an agent, the **Transcript** gadget displays the transcript of the voice conversation between the customer and the virtual agent along with the live transcript. It helps in gathering context from the earlier interaction with the virtual agent and capturing high level summary points for wrapping up the call. In addition, the gadget displays the **Highlights** panel where you can view the following information:

- Intents and intent parameters (appear only if offered by the CCAI cloud provider). The intents and intent parameters are based on the customers' queries. For example, a customer's query is to book a flight ticket. The intent for this query is Flight Booking and the parameters for this intent are Source, Destination, and Date of departure depending on the customer's interaction with the virtual agent.
- A confidence score of high, medium, or low for each intent.
- A customer sentiment indicator – happy, neutral, or sad, for each intent (appears only if offered by the CCAI cloud provider).

You can also view the overall sentiment indicator of the customer for the entire call.

The **Transcript** gadget shows the transcript of the voice conversation along with their timestamp in the local time zone of the agent desktop.

On the gadget interface, you can do the following:

- Filter the transcripts based on Customer, Virtual Agent, and Agent.
- Search the transcripts using keywords.



- 
- Note**
- The Search box is disabled when the call is not active.
  - If redaction or advance security settings are not enabled, PII and PCI information is also reflected in the gadget.
- 

## Prerequisites

To configure VAV Call Transcription:



- 
- Note** Ensure that the Unified CCE AW, Unified CCE OAMP, VVB, Cloud Connect, and Agent Desktop components have access to Webex services to use VAV Call Transcription.
- 

### Procedure

|               | Command or Action                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Complete the prerequisites for configuring VAV via Cloud-based connector. For more details, see <a href="#">Prerequisites, on page 244</a> . | <p><b>Note</b> For this feature to work, you must deploy VAV via Cloud-based connector.</p> <p>The following components must be on release 12.6(1) or higher:</p> <ul style="list-style-type: none"> <li>• Cisco Unified CCE components (Router, Logger, AW, and PG)</li> <li>• Cisco Finesse</li> <li>• Cisco Unified CVP</li> <li>• Cloud Connect</li> </ul> <p>For further assistance, you can contact the Cisco TAC team. For more details, see <a href="https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html">https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html</a>.</p> |

## Configuration Task Flow

Follow this procedure to enable the Cisco Contact Center AI (CCAI) Services that equip your Cisco Contact Center for VAV Call Transcription service.

- 
- Step 1** Configure VAV via Cloud-based connector. See [VAV via Cloud-Based Connector, on page 220](#).
- Step 2** Add the **Transcript** gadget and the VAV Transcription service to the Cisco Finesse desktop layout:



- a. Enable the **Transcript** gadget in Cisco Finesse Administration.  
For details, see the *Manage Desktop Layout* section in the *Cisco Finesse Administration Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html>.
- b. Enable the VAV Transcript service in Unified CCE Administration for an agent or multiple agents together.  
For details, see [Enable or Disable Contact Center AI Services for Agents](#), on page 53.

Once enabled, the **Transcript** gadget appears on the **Home** tab. For details on how to use the gadget, see the Cisco Contact Center AI Gadgets guide at [https://ccaigadgets.produs1.ciscoccservice.com/doc/en\\_us/index.html](https://ccaigadgets.produs1.ciscoccservice.com/doc/en_us/index.html).

**Note** Gadget auto-hide/un-hide and notifications capability is available only if the gadget is configured as a multitab gadget in Cisco Finesse. For more details, see *Call Transcript Gadget* in the *Cisco Finesse Administration Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html>.

---





## CHAPTER 17

# VPN-less Access to Finesse Desktop

---

- [VPN-less access to Finesse desktop, on page 247](#)

## VPN-less access to Finesse desktop

To enable this feature, use the Cisco provided [Reverse Proxy Automated Installer](#) that provides an in-built reverse-proxy, which is based on the OpenResty® Nginx proxy. Alternatively, any custom reverse-proxy pair must be deployed in the DMZ and configured to enable this feature.

VPN-less access to the desktop supports all standard functionality on the desktop including Real-Time and Historical Reports. The SSO authentication is supported along with mechanisms to tunnel ADFS access through the same proxy.

Media access remains unchanged in reverse-proxy deployments. To connect to the media, agents and supervisors can use the Cisco Jabber over Mobile and Remote Access solution (MRA). Otherwise, use the Mobile Agent capability of Contact Center Enterprise with a PSTN or mobile endpoint.

After deploying a reverse-proxy, if you want to access the Cisco Finesse desktop without connection to the VPN, read this chapter. Also, refer to the Nginx rules provided as part of the Reverse-Proxy installer artifact to replicate the same in your custom reverse-proxy. Refer to [Reverse-Proxy selection and configurations](#) section to determine the capabilities required for a custom reverse-proxy.



---

**Note** For Nginx-based reverse-proxy rules, installation, configuration, and security hardening instructions, refer to the [Reverse-Proxy Installer, on page 303](#) section. Any reverse-proxy that meets the requirements as mentioned in the [Minimum and additional requirements](#) section can be used in place of Nginx.

---

For the list of issues, see the [Caveats](#) section.



---

**Attention** The term "upstream servers" is used in this section to refer to all the solution components such as Finesse, CUIC, Cisco IdS, and IM&P servers that are configured to be accessed through reverse-proxy.

---

## Prerequisites

To configure VPN-less access to the Finesse desktop:

- Finesse, IdS, and Cisco Unified Intelligence Center must be 12.6(1) ES02 or above.
- In coresident deployments, LiveData and Cisco Unified Intelligence Center should be 12.6 ES02 or above.
- LiveData and Unified CCE must be of the same version for a given deployment.
- Unified CCE and LiveData standalone must be 11.6(1) or above with the latest ES for the respective versions.
- DMZ with internet connectivity must be available to host the reverse-proxy.

## Supported Reverse-Proxy Deployment Models

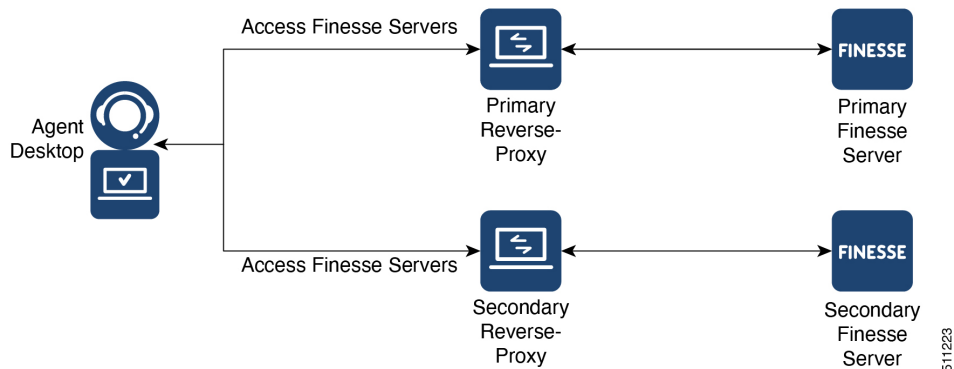
Reverse-Proxy deployment allows agents and supervisors to concurrently access the Finesse desktop from both LAN and via reverse-proxy. Cisco Contact Center supports the following two deployment models for VPN-less access to Finesse desktop using reverse-proxy:

- One Finesse cluster connects to one high availability (HA) pair of reverse-proxy.
- Multiple Finesse clusters connect to one HA pair of reverse-proxy.



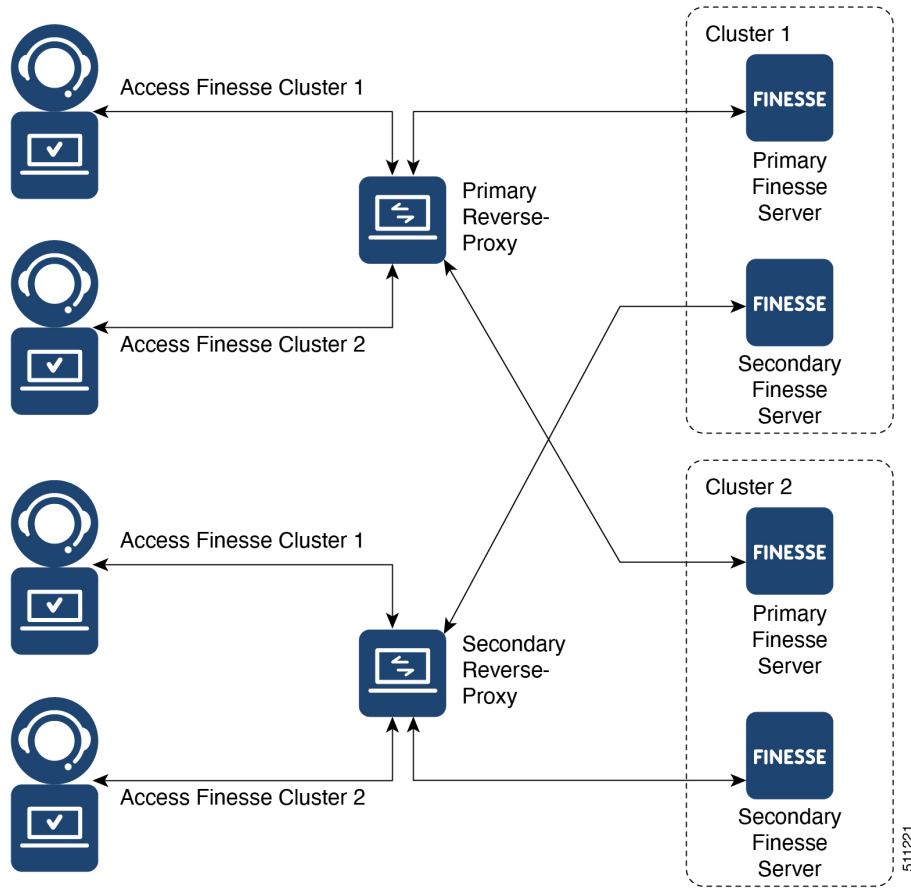
**Note** This is applicable to Finesse, IdS, Cisco Unified Intelligence Center, and Live Data clusters.

**Figure 17: Single Finesse Cluster per HA Reverse-Proxy**



511223

Figure 18: Multiple Finesse Clusters per HA Reverse-Proxy



## Load balancer, WAF, and proxy support for reverse-proxy deployments

The reverse-proxy configurations have security features that are dependent on the information about the actual client IP which is making the request. This information is required for enforcing security features such as enforcing rate limits, logging of client activity and blocking brute force attempts and for logging access to the system.

Deployments which directly terminate the internet Agent connections on the reverse-proxy don't need anything special to be done here, as the reverse-proxy receives the client IP due to the client connections terminating on the reverse-proxy.

However when other network devices are used to terminate the client connections, before forwarding them as fresh requests to the reverse-proxy itself, the client IPs are no longer visible to the reverse-proxy.



This happens when there are Load Balancers, Web Application Firewall (WAF), and so on, or when the client access itself is made from behind a forward proxy. CDN deployments also employ multiple reverse-proxies and fall into the same deployment category.

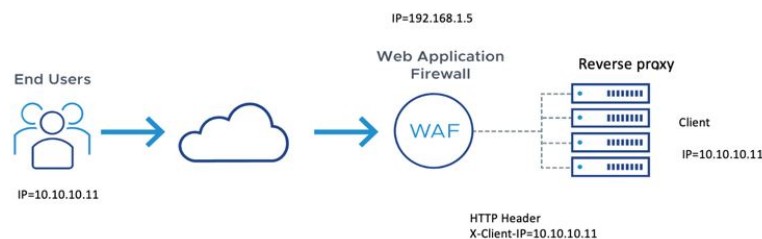
Such deployments **MUST** add certain configurations to enable the reverse-proxy to identify the actual client IP. The configurations that are required for such deployments are as follows:

1. The public IPs or the hostnames of these devices which forward the requests to the proxy in the reverse-proxy configurations, must be added in the `core.env` file using the variable `NGX_LOAD_BALANCER_IPS`.
2. The new requests originating from the intermediary devices, **MUST** populate the HTTP request header fields with the end-client IP to communicate the same to the reverse-proxy.

The name of this field isn't predetermined and can be configured in the `core.env` file, in the variable `NGX_LOAD_BALANCER_REAL_IP_HEADER`.



**Note** All CDN deployments provide a mechanism to extract the client IP as an HTTP header containing a single-client IP as part of the request payload. A custom header is often recommended to avoid conflict with the standard `X-FORWARDED-FOR` header. The VPN-less reverse-proxy deployments are also recommended to provide the client IP using a custom header for similar reasons.



3. For security purpose, the devices which are front-ending the reverse-proxy **MUST** replace `X-FORWARDED-FOR` and `X-REAL-IP` headers provided by the client with the actual client IP or drop them if the deployment doesn't need these headers.
4. If the deployment is using a custom HTTP header for communicating to the client IP, the particular field **MUST** be replaced with the client IP before forwarding them to the upstream reverse-proxy.
5. Verify the configuration by transmitting a high rate of requests to a Finesse API such as `SystemInfo/DesktopConfig` from an external client. Verify through the Load Balancer or WAF to ensure that the client is blocked while the Load Balancer or intermediate devices aren't blocked or rate limited. Ensure that the configurations are working as expected before going live.

Refer to the [Frequently Asked Questions, on page 329](#) section for instructions on how to send the requests to the proxy, and also on how to check whether a client is blocked or rate-limited.

6. Pretest the deployments with all WAF/IPS rules enabled to verify that the desktop API patterns are compatible with them before going live with the deployment. Certain WAF rules can be too restrictive and may need some modifications before they are deployed.



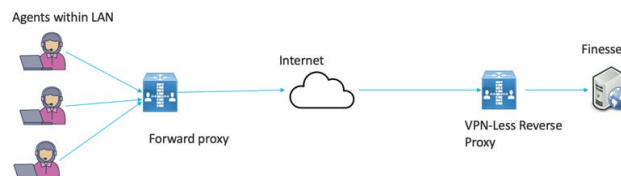
**Note** The reverse-proxy configurations provided have no protection against layer-3 attacks such as IP address spoofing or flooding. The proxy provides only rate-limiting, brute force attack detection, and restricting of requests to the allowed destinations. The operating system IP configurations are hardened to a certain level but there are no further protections that are available. It's assumed that the relevant operating system hardening and traffic protection devices are employed to secure the deployment of Cisco Contact Center.

For more details, refer to the *Security Guidelines for Reverse-Proxy Deployment* section in the [Security Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.6\(1\)](#) guide.

Load Balancers and other devices that don't have the HTTP header support can skip the second and third points that are mentioned above. However, this causes a suboptimal deployment which will be functional but loses some critical security features listed previously and isn't a recommended configuration for certain features such as client IP logging for debugging purposes and blocking users attempting to brute force guess passwords.

### Access VPN-Less proxy through Forward proxy and NAT

The VPN-less configuration assumes that the proxy is accessed by clients/agents from the internet, who have separate individual IPs which can be used for enforcing security features. However, not all deployments dedicatedly use agents from the internet with their own unique IP addresses. Most deployments have agents accessing the reverse-proxy deployments both from the internet and from LAN using the same reverse-proxy access URI.



So, if you have a deployment which uses agents behind a proxy or a NAT that looks like what is shown above, certain configuration changes have to be made to ensure that the end-user IPs are correctly communicated to the reverse-proxy. The steps to configure are as follows:

1. The Forward proxy (device A in the diagram above) has to be well known in advance.
2. The Forward proxy device has to transmit the agent IPs in a predefined header. For example, `X-Client-IP` as shown above.
3. If there are other intermediary devices such as a Load Balancer or WAF at the network where Finesse is deployed, before the requests reach the reverse-proxy, these devices must be able to allow the Forward proxy by its IP address and then transmit the HTTP header without any changes.



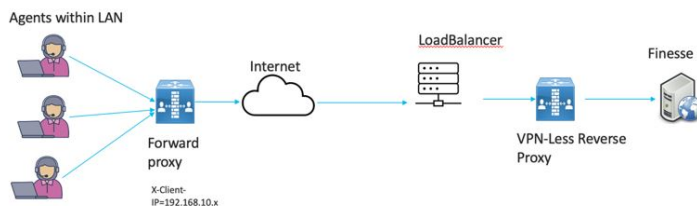
**Note** It's crucial that the Forward proxy IP address is identified and only requests from this IP should be allowed to contain the predefined header from step 3. All other requests unless they are an identified proxy IP should strip this header `X-Client-IP`.

4. In the `core.env` file, the variable `NGX_LOAD_BALANCER_REAL_IP_HEADER` should identify the header used to send the client IP. For example, `X-Client-IP`.
5. The public IPs or the hostnames of the forward proxy needs to be added in the installer `core.env` using the variable `NGX_LOAD_BALANCER_IPS`, if the deployment doesn't have any other intermediary such as WAFS before the request reaches the reverse-proxy



**Note** Deployments that don't have the HTTP header support can skip the steps 2–4. However, this causes a suboptimal deployment which is functional but loses certain security features listed above. These are dependent on client IP knowledge and these deployments are therefore not suggested.

Reverse-proxy deployment can't support multiple HTTP header names to transmit the client IP corresponding to different Forward proxies that the network is interacting with.



Deployments that need to support forward proxies AND intermediary devices.

Deployments such as these should transmit or detect the final client IP of the users who are connecting from behind the **Forward proxy A** and this would be an agreement between Load Balancer and the Forward Proxy.

The Load Balancer or the final intermediary devices that forward requests to the VPN-less reverse-proxy should transmit the required headers. It must be configured as described in the section above. The Forward proxy information isn't required to be added to the VPN-less configuration, if the intermediary device is able to identify the correct client IPs and transmit them to the reverse-proxy using the steps mentioned above.

However, if the actual client IP resolution isn't set up between the Forward proxy and the Load Balancer, the reverse-proxy considers the IP of the Forward proxy as the actual client IP.

In this case to avoid rate-limiting to block the Forward proxy, its IP must be configured in the `NGX_LOAD_BALANCER_IPS` variable so that the proxy isn't blocked or rate-limited. This would be a suboptimal deployment and such deployments aren't suggested due to security constraints.

## Authentication

For all requests and protocols that are accepted at the proxy, authentication is enforced before they are forwarded to the respective component servers (Finesse, LD, CUIC, and IM&P). The component servers also enforce authentication locally. Authentications made at the proxy use the Finesse login credentials, irrespective of the component server to which the requests are made.

Persistent connections such as WebSockets that rely on post connection application protocols (such as XMPP) for authentication, are authenticated at the proxy by verifying the peer IP address of the connection. The peer IP address must correspond to a system that has successfully authenticated an API request prior to establishing the socket connection.

Requests that do not require authentication, such as static files and images, are configured to be served by the reverse-proxy from its cache.



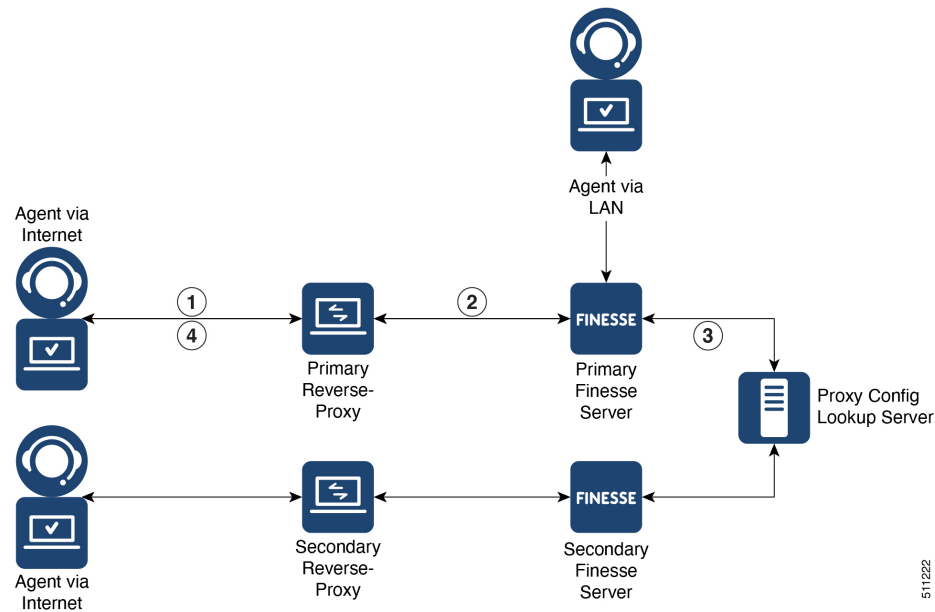
## Non-SSO

Non-SSO authentication doesn't require any extra component configurations and works along with the Nginx authentication scripts provided with the corresponding ES release. Authentication relies on the Finesse sign-in credentials. Access to all the end points are validated using the Finesse authentication services.

The list of valid users is cached at the proxy locally (updated every 15 minutes), which is used to validate the user in a request. User credentials are validated by forwarding the request to the configured Finesse URI and thereafter the credential hash is cached locally (every 15 minutes) to authenticate new requests locally. Any change in the username or password will take effect only after 15 minutes.

The following figure illustrates the sequence of non-SSO authentication, followed by a step-by-step description:

**Figure 19: Non-SSO authentication**



## SSO

SSO authentication requires the administrator to configure the Cisco IdS token encryption key at the Nginx server within the configuration file. Obtain the Cisco IdS token encryption key from the Cisco IdS server using the **show ids secret** CLI command. For the SSO authentication to work, configure the key as part of one of the mandatory replacements that the administrator must perform.

### Cisco Identity Service 12.6(2)

After the reverse-proxy backend onboarding is complete using the **utils system reverse-proxy allowed-hosts add** CLI, the new reverse-proxy installer components will be able to successfully get the public key automatically from the Cisco IdS server and use that for authenticating the JWT tokens.



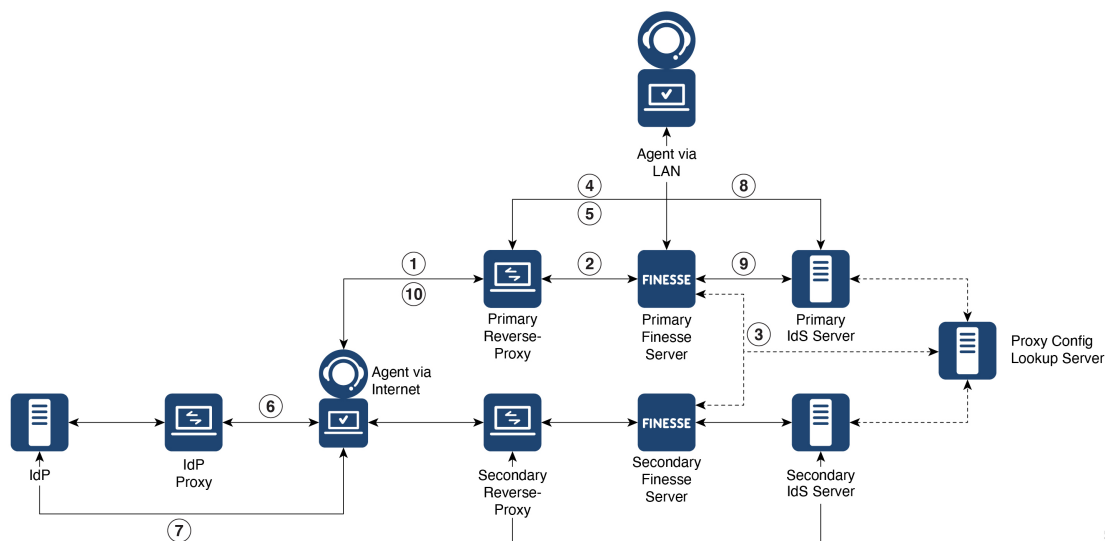
**Note** ADFS 3.0 can be configured to be accessed through the reverse-proxy with the [Introduction, on page 301](#). Other IdP proxy configuration (proxy configuration, internet visibility, and High Availability for IdP) must be done separately by referring to the relevant IdP documentation. However, VPN-less configuration allows you to configure a different IdP hostname corresponding to the IdP-proxy to access the Finesse desktop.

Cisco IdS SAML configuration has to be performed for the SSO authentication to work at the proxy. For more information on Cisco IdS SAML configuration, see the [Single Sign-On](#) chapter.

After SSO authentication is configured, a pair of valid tokens can be used to access any of the endpoints in the system. The proxy configuration validates the credentials by intercepting the token retrieval requests made to Cisco IdS or by decrypting valid tokens and thereafter caching them locally for further validations.

The following figure illustrates the sequence of SSO authentication, followed by a step-by-step description:

**Figure 20: SSO**



1. Agents and supervisors connect to one of the Finesse servers through the configured reverse-proxy.
2. Based on the hostname and reverse-proxy rules, the reverse-proxy forwards the request to the configured Finesse server.
3. The Finesse server checks the proxy configuration map to get the current Cisco IdS proxy hostname.
4. The browsers of agents and supervisors redirect to Cisco IdS through the reverse-proxy.
5. Cisco IdS redirects to the configured IdP URL.
6. The browsers of agents and supervisors redirect the SAML consumer endpoint request to the IdP proxy.
7. IdP sends the self-posting SAML assertion HTML from the browsers of agents and supervisors.
8. Cisco IdS verifies the SAML assertion and issues an authentication code to the Finesse servers.

9. Finesse validates the authentication code and gets a token from Cisco IdS. Finesse uses the token for authentication. The token has a time limit. For more information about SSO configuration and flow, see the [Single Sign-On](#) chapter.
10. Finesse serves the request to agents and supervisors through the reverse-proxy.



---

**Note** After sign-in, consecutive API requests are forwarded to the Finesse server. If the token is valid, the requests are authenticated using the token and is responded.

---

### Authenticate WebSocket connections

WebSocket connections don't have a standard authentication mechanism. Therefore, applications rely on post-connection application level protocol payloads for validating the established connection. However, this mechanism is used to establish unauthenticated connections at scale, mounting DoS or DDoS attacks on the servers.

To mitigate this possibility, the provided OpenResty® Nginx reverse-proxy configuration performs specific checks before allowing WebSocket connections. The WebSocket connections are accepted only from those IP addresses that have successfully made an authenticated REST request. The REST request must be authenticated before establishing the WebSocket connection.

Reverse-proxy deployments that use L7 intermediaries, such as Content Delivery Network (CDN), often redirect traffic through interim servers before the traffic reaches the reverse-proxy. In such deployments, ensure that the **X-Forwarded-For** headers are correctly relayed to identify the client IP address. The **X-Forwarded-For** headers are used to authenticate the WebSocket connection by matching it with the previously authenticated REST request.



---

**Note** The clients that attempt to create WebSocket connections before issuing any REST requests, an **Authorization Failed** error message is displayed.

---

### Host-Mapping file for network translation

Reverse-proxy deployment requires an invalid mapping file to configure the list of externally visible hostname/port combinations. It's also used to map to the actual server names and ports that are used by the Finesse, IdS, and CUIC servers. This mapping file which is configured on internal servers is the key configuration that allows the clients connected over the internet to be redirected to the required hosts and ports that are used on the internet.

The mapping file has to be deployed on a web server accessible to the component servers. Its URI must be configured using a dedicated web server available within the LAN. If such a server isn't available, the reverse-proxy can be used instead. This requires that the proxy is accessible from within the LAN. Using the reverse-proxy presents a risk of exposing the information to external systems which can make an unauthorized connection to the DMZ.



---

**Note** For details on how to configure a Proxy Map to be served by the reverse-proxy itself, see the [Reverse Proxy Automated Installer, on page 301](#) section.

---

For all the requests that come through the reverse-proxy, the Finesse, IdS, and CUIC servers check the host-mapping file, to translate the internal hostnames and ports that are used on the LAN. They are translated to the publicly resolvable hostnames and ports that have to be used on the internet. This mapping file referred to as the Proxy-config map file, is the key configuration that allows the clients connected over the reverse-proxy to be redirected to the required hosts and ports that are used on the internet.

Configure the proxy-config map file by using the CLI available on Finesse, Cisco IdS, and CUIC servers. For details on the mapping file format and the data configured, refer to the *Populate Network Translation Data* section. For details on the CLI used to configure the file, refer to the section.

Configure the proxy-config map file by using the CLI available on Finesse, Cisco IdS, and CUIC servers. For details on the mapping file format and the data configured, refer to the *Populate Network Translation Data* section. For details on the CLI used to configure the file, refer to the **utils system reverse-proxy config-uri** CLI in the [Configure Proxy Mapping by Using CLI](#) section.

## Port management

One of the main design aspects in deploying a reverse-proxy are the domain and the ports used to access the application. These aspects are interdependent and influence each other when designing the deployment.

The reverse-proxy must be able to determine to which upstream server an incoming request can be forwarded to where an incoming request should be forwarded to. This can be accomplished by changing either the port or the hostname used to access the application. Primarily, the combination of host and port must be unique for the proxy to differentiate and route traffic to the correct upstream component. It's a requirement for the proxy to even start correctly. The following are the options available to design the domain and port access:

- Use a common domain and differentiate application access using multiple ports.
- Use a common port and differentiate application access using multiple domains

After determining the domain and the port distribution, perform the following steps:

1. Change the proxy map configuration to match the required port and domain. See the [Configure Proxy Mapping by Using CLI, on page 267](#) section.
2. The respective upstream component environment configuration in the reverse-proxy installer must be configured with the required hostname and port. See the [Configure deployment environment configurations, on page 315](#) section.

### Using a common domain with multiple ports

The following example illustrates how multiple application servers can be configured using this access pattern:

- FinesseA = ReverseProxyDomain.com:8445
- FinesseB = ReverseProxyDomain.com:8446
- Finesse1A = ReverseProxyDomain.com:8447
- Finesse2B = ReverseProxyDomain.com:8448

The following are the benefits of using multiple ports:

- More granular packet level rate-limits applicable to each application can be applied at the ingress point to control rate-limits. Domain-level access means that the rate-limits can't be granular.
- A single-domain requires only a single SSL certificate to access the application. It could be a factor in reducing costs, unlike a multiple-domain application which requires a wildcard certificate.

The following are the disadvantages in using multiple ports:

- Certain network deployments like CDNs don't support custom ports.
- Security devices that automatically apply security rules might require custom configurations with non-standard ports.
- Multiple ports must be opened in the DMZ firewall (10–15 ports are required for a standard 2k deployment). This isn't recommended by the network security teams.
- There's an increased overhead regarding the port manageability.
- Deploying new instances of the application requires firewall/network changes.



---

**Note** Ports other than the ones mentioned in the ProxyMap must be blocked and shouldn't be available for access on the reverse proxy host. This must be blocked at the ingress point as the proxy doesn't currently have rules to block this access at network level.

The Cisco provided installer supports running multiple instances which cater to different sets of upstream servers, to aid in ease of maintenance. Multiple instances of the installer don't allow to use the same ports across different instances of the proxy. Only one process can bind to the same TCP port.

Consider the above two points when deciding the port management strategy against proxy installer configuration.

---

### Using a common port and with multiple domains

The following example illustrates how multiple application servers can be configured using this access pattern.:

- FinesseA = FinesseA-ReverseProxyDomain.com:443
- FinesseB = FinesseB-ReverseProxyDomain.com:443
- Finesse1A = Finesse1A-ReverseProxyDomain.com:443
- Finesse2B = Finesse2B-ReverseProxyDomain.com:443

The single port configuration reverses the pros and cons listed above with the multiple port configuration.



---

**Note** Supporting a single port of access requires Unified Intelligence Center and LiveData components to be on 12.6(2) versions.

---

### DNS Configuration for Finesse, IdS, and CUIC servers

Each Finesse, IdS, CUIC, IM&P, and third-party component servers corresponding to a host that needs internet access must be addressable from the internet. This calls for a hostname and associated port which is resolvable from the internet to be mapped to the public port and matching IP of the reverse-proxy. It's required so that the traffic is directed to the respective component servers.

DNS registration of the publicly resolvable hostnames and the corresponding IP addresses is mandatory before the requests reach the reverse-proxy.

### SSL Certificates

For the hostnames that are configured, corresponding to each unique hostname that is used by the internet client, the respective certificates must be acquired and configured on the reverse-proxy. Even though self-signed certificates are supported, they are risky because the users access directly from the internet. The clients can be more secure by using CA-signed certificates. The best practice is to get CA certificates for proxy servers and third-party-gadget servers.

## Reverse-Proxy selection and configurations

This section provides information about the recommendations for hardware, performance, scale, and gadget compatibility for reverse-proxy.

If you choose to not use the reverse-proxy installer that Cisco has provided and want to deploy a custom reverse proxy, see the [Guidelines for Custom Reverse Proxy Deployment, on page 375](#) section.

### Performance and Hardware Recommendations

Unified CCE deployments can be supported by Open Source Nginx 1.20 running on a CentOS 8.0 (4.18.0-305 64 bit) distribution, with the configurations and settings (mentioned in the [Installing Nginx](#) site) on a dual core 4 CPU (8 logical CPU) Intel Xeon CPU E5-2690 v2 (3.00GHz, 25MB cache) at an average of 10% CPU usage and peak of 15% CPU usage during logins.




---

**Note** The load has been tested on 2K deployments.

---

It is expected that the same configuration can support three Finesse clusters with the required CUIC LD reports, and access to IdS.

A minimum of 8 GB memory is recommended for the proxy server when all other nonessential services and graphical subsystems are disabled.




---

**Note** It is recommended that deployments gradually onboard new solution components to the proxy until 50-55% of the proxy CPU is free. With this it can cope with unexpected spikes in traffic from the internet.

---

Additional memory must be configured based on the in-memory cache configuration added to Nginx.

The data analysis of top equivalent performance capture, made with the nmon tool, is available from the Installer download page [https://software.cisco.com/download/home/283613135/type/284259728/release/12.6\(2\)](https://software.cisco.com/download/home/283613135/type/284259728/release/12.6(2)). The data represents the state of the proxy for desktop and supervisor operations, on a sample 2000 and 4000 UCCE deployment using SSO logins and CUIC LD reports as configured in the default layout for all agents for a period of eight hours. It can be used to derive the compute, disk, and network requirements for an installation using Nginx on comparable hardware.

---

### Determine Scale and Hardware for Proxy

Contact Center administrators should analyze the hardware required for the reverse-proxy, based on the number of agents and supervisors who may access the Finesse desktop without connecting to VPN. You can use the reference request rates provided for Finesse, IdS, and CUIC.

The type of proxy selected guides the hardware to be used, depending on whether the proxy is shipped as an installable software or is a hardware-based application.

Sizing configurations are pre-tested for OpenResty® Nginx proxy. Custom proxy deployments should consult their product documentation or run basic scaling tests to determine the rates that can be supported by the respective proxy and scale their hardware accordingly.

## Determine Gadget Compatibility

Determining the gadget compatibility is an important activity for planning a VPN-less Finesse deployment.

After deploying the reverse-proxy, all Cisco-provided gadgets (Cisco Finesse and Cisco Unified Intelligence Center) work seamlessly with their respective servers of Release 12.6(1) or later. The Webex Experience Management and CCAI gadgets also work seamlessly with VPN-less Finesse deployments.

In some scenarios, depending on the gadget design, custom third-party gadgets require workarounds to enable them to work with the reverse-proxy deployment. Refer to the following sections to determine if any of your gadgets require workarounds.



---

**Note**

- Gadgets that are loaded from servers other than Finesse server should use **exclude-url** feature in the gadget XML specification to load the Finesse resources such as Finesse.js. For more information, refer to the **Use Gadget URI Exclude Feature to Refer to Finesse Resources** section.
- If you use two different URLs, one internal and one external, in Enterprise Chat and Email (ECE), you must update the Finesse desktop layout to use only the external URL. If you use an internal-only ECE (for integrations that support only ECE email routing), you must change the ECE web server to ensure that the ECE services are accessible externally.

---

### Gadget Types and VPN-less Compatibility

Finesse gadgets are classified into the following types based on how they are designed operationally:

- Gadgets that are self-contained within the desktop. These gadgets do not have to make any additional network requests, or are restricted to invoking Finesse APIs and APIs on the internet.
- Gadgets that provide their functionality by communicating with an accompanying server that is deployed in the DMZ and is reachable directly from the internet and LAN.



---

**Note**

To enable the same desktop layout to be used by both LAN-based and internet-based clients, the server installed in a DMZ should also be reachable from servers such as Finesse in LAN, and from clients that are running within the LAN.

- 
- Gadgets that need to communicate with an accompanying server deployed in LAN, but uses desktop-provided **makeRequest** API to communicate to the server. The **makeRequest** API routes all the requests through the Finesse server and does not directly reach the server that is deployed in the LAN.




---

**Note** These requests succeed in a reverse-proxy deployment only if the requests are made using the hostname and port. The hostname and the port must be reachable from LAN because the requests are run by Finesse server which runs on LAN.

---

- Gadgets that have to communicate directly with any one of the following types of accompanying server:
  - Server deployed within the LAN and is not reachable directly from the internet.
  - Server that communicates with an additional port apart from the HTTP port used to load the gadget.

The last two types of gadgets have to be modified to be used in a reverse-proxy deployment. The steps required to enable these gadgets to be accessed from internet clients are as follows:

- Enable VPN-less access for custom gadgets
- Send hostname and port information to gadgets
- Use gadget's **URI Exclude** feature to refer to Finesse resources

### Enable VPN-less Access for Custom Gadgets

Gadgets that communicate directly with accompanying servers that are deployed in LAN must handle the following aspects to work correctly in a reverse-proxy deployment:

- Use the right hostname and port for communicating with its accompanying server.

A gadget can find the correct hostname and port corresponding to the server from which the gadget was loaded, by using the `gadgets.util.getUrlParameters().up_urlPrefs` API provided by the Finesse Javascript API.

To find additional ports or hostnames that are required, data can be passed in as gadget preference such that the additional host and port information can be sent to the gadget. For more information, refer to the **Send Hostname and Port Information to Gadgets** section.

- Ensure that the communications are forwarded correctly by the reverse-proxy.

After the gadget starts communicating with the correct host and port information, the hostname and port number have to be forwarded to the server deployed in the LAN. This can be done by opening the appropriate ports in the DMZ firewall. Also, ensure that the appropriate ports and rules are added to the reverse-proxy rules to forward the traffic to the correct server in the LAN.

- **Best Practice:** If requests to external servers are made using Finesse authentication headers, a common validation is enabled to authenticate the requests at the proxy. Gadgets that do not use Finesse authentication should plan to implement their own custom authentication schemes to ensure that the requests are validated at the proxy before sending to the Finesse server.

### Send Hostname and Port Information to Gadgets

Gadgets that send host and port information corresponding to a server deployed within the LAN can use the **UserPreferences** feature supported by Finesse gadgets. This feature allows a configurable, named information to be passed to the gadget. The information can be referenced within the gadget XML or programmatically by using a Javascript.



For more information on how to use **UserPreferences** method, refer to <https://developer.cisco.com/docs/finesse/#!/gadget-preferences>.

The **UserPreferences** that are created for this purpose should start with the keyword *externalServerHostAndPort* in its name. This enables Finesse to substitute the host and port that are provided with the corresponding entry from the **proxyMap** file. For example:

```
<UserPref name="externalServerHostAndPort_chat" display_name="Chat_externalServerHostAndPort"
default_value="SMHostName:7443" datatype ="hidden"/>
```



**Note** The `default_value` parameter is not case sensitive.

When accessed from the LAN, the **UserPreferences** continues to have the default value that is configured in the XML. However, when accessed through the reverse-proxy, the **UserPreferences** receives the value from the **proxyMap** file. For example:

```
SMHostName:7443=external-proxy-host:4043
```

When accessed through the reverse-proxy, the gadget receives the port **4043** and host name as **external-proxy-host**.

#### Use Gadget URI Exclude Feature to Refer to Finesse Resources

Add the following content within the `ModulePrefs` tag of the gadget XML to ensure that the resources that are loaded from Finesse server are excluded from concatenation. This step is mandatory for gadgets that load their XML from custom servers.

```
<Optional feature="content-rewrite">
<!-- these files will be directly served by Finesse, not through shindig -->
<Param name="exclude-url">finesse.min.js</Param></Optional>
```

## Finesse URL

Agents and supervisors should bookmark two different pairs of URLs (publisher and subscriber) for accessing the Finesse desktop through both the Contact Center network and the reverse-proxy.

## VPN-less Finesse configurations

To configure VPN-less access to Finesse desktop, the Contact Center administrators and the network administrators must work in tandem.



**Note** Don't allow access to the reverse-proxy in your external firewall until all security configurations are in place. To test your changes, use a host that isn't publicly accessible.

The configuration steps are as follows:

1. Populate Network Translation Data
2. Host the Mapping File
3. Add Proxy IP by Using CLI

4. Configure Reverse-Proxy Host Verification
5. Configure Proxy Mapping by Using CLI
6. Configure CORS and Frame-Ancestors
7. Configure SSO

## Populate Network Translation Data

The Proxy-config map file is similar to a plain property file in which the values are separated by the equal sign. Left Hand Side (LHS) contains the host and port of Finesse, IdS, and Cisco Unified Intelligence Center. Right Hand Side (RHS) contains the values of the host and port that are exposed through reverse-proxy to access the Finesse desktop.

Network administrator and Finesse administrator must create a Proxy-config map file that has the mapping for all the default ports of the Cisco components. The external traffic from the Internet will be redirected to the default ports. For example, 8445 port of Finesse, 8553 port of IdS, and 8444 port of Cisco Unified Intelligence Center.

The Proxy-config map file must be hosted on a web server that is accessible by the Finesse, IdS, and Cisco Unified Intelligence Center servers. The following list is an example of systems and hosts that are required for a two-node Finesse cluster with two Cisco Unified Intelligence Center nodes using SSO mode:

- Publisher = finesse1.internal.com
- Subscriber = finesse2.internal.com
- IdS Publisher = idspub.internal.com
- IdS Subscriber = idssub.internal.com
- IdP = idp.internal.com (optional)
- CUIC Publisher = cuicpub.internal.com
- CUIC Subscriber = cuicsub.internal.com
- Proxy Node1 = proxy1.xyz.com
- Proxy Node2 = proxy2.xyz.com

If the selected proxy supports port-based forwarding, the following is an example of a mapping file that contains the entries that are required for a two-node Finesse cluster with two Cisco Unified Intelligence Center nodes using non-SSO mode.

```
finesse1.internal.com:8445=finesse1.xyz.com:443
finesse2.internal.com:8445=finesse2.xyz.com:443
idspub.internal.com:8553=idspub.xyz.com:443
idssub.internal.com:8553=idssub.xyz.com:443
idp.internal.com:443=idp.xyz.com:443
cuicpub.internal.com:8444=cuicpub.xyz:8444
cuicsub.internal.com:8444=cuicsub.xyz:8444
```

**Note**

- The IdP entry `idp.internal.com:443=idp.xyz.com:443` is optional. You must add this entry when the IdP hostname configured with IdS is different for reverse-proxy and LAN.
- The LHS entries of the hostname in the proxy-map file are not case sensitive. The RHS entries are case sensitive and must match exactly with the hostnames that are configured.
- If the proxy map file entries do not contain colon (:), it is assumed that only the hostname is entered. If you have not provided any port value, the port number 443 is considered as the default port.

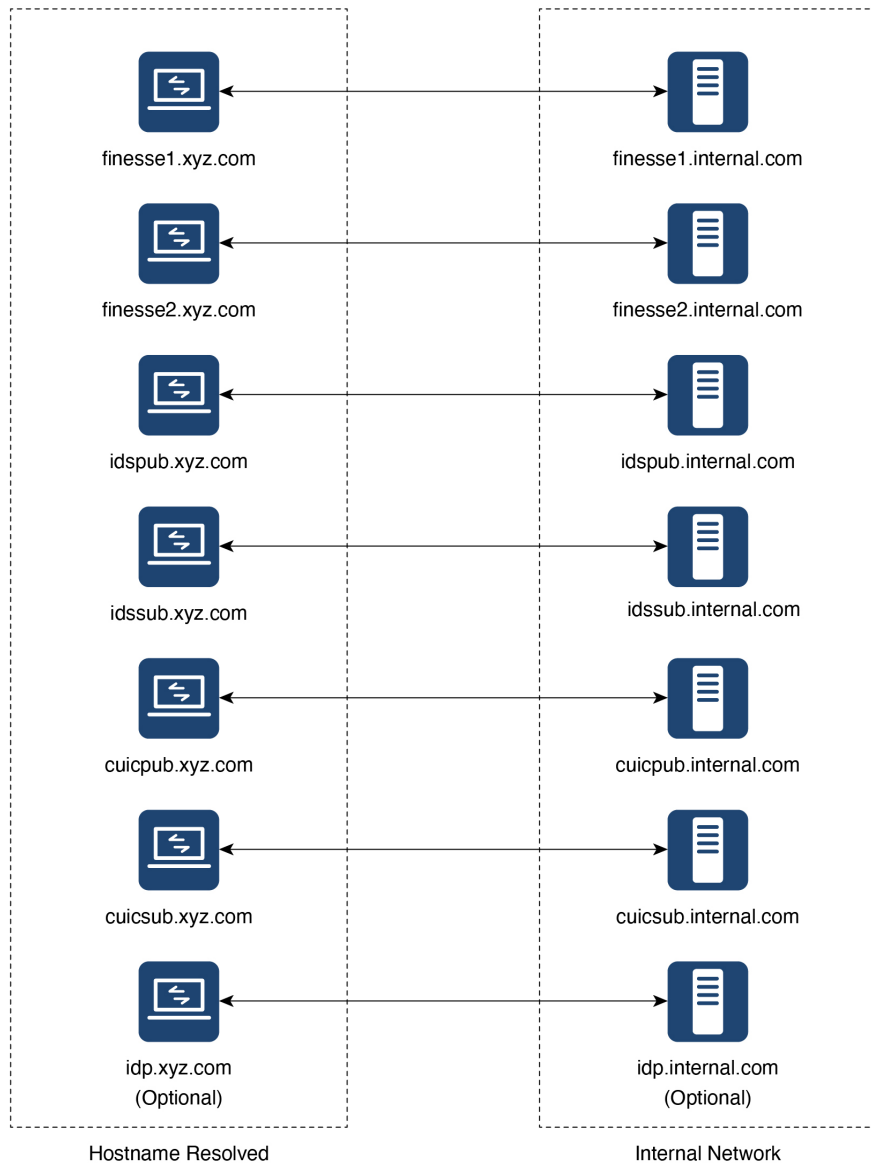
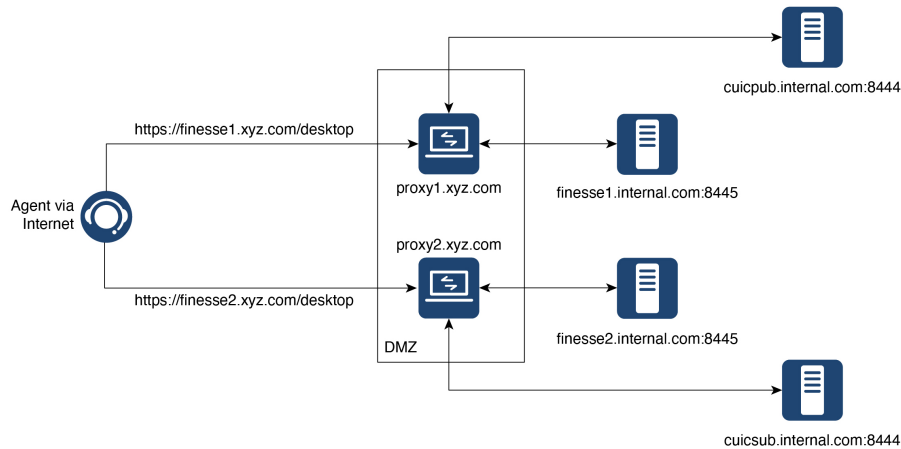
**Figure 21: Hostname Mapping Example**

Figure 22: Network Architecture Example



## Host the Mapping File

The mapping file that is created in the *Populate Network Translation Data* section, is used by the solution components (Finesse, IdS, and CUIC servers) servers to modify their responses, to enable clients to access the solution via the reverse-proxy. This requires the file to be hosted on any web server accessible by the component servers. The reverse-proxy server, Finesse server, or any web server configured by the administrator can be used for this purpose.

To access the mapping file, the host server's SSL certificate must be uploaded (using the *cmplatform admin* application) to the individual nodes of the services. After uploading the file, verify if the URL is accessible from Finesse, IdS, and CUIC servers. For example, *https://proxyserver.xyz.com:10000/proxymap.txt*. HTTP-based URLs are allowed for hosting the mapping file through HTTPS, which is the recommended access scheme.

The following is an example of the CLI to view the content of the proxy map file.

```
admin:utils system reverse-proxy show-proxy-config-map

finesseXX.autobot.cvp:8445=astproxy.cisco.com:8445
finesseXYZ.autobot.cvp:8445=astproxy125.cisco.com:8445
cuic-YY.autobot.cvp:8444=astproxy.cisco.com:8444
cuic-YY.autobot.cvp:8447=astproxy.cisco.com:8447
livedata-LL.autobot.cvp:12005=astproxy.cisco.com:12005
livedata-LL.autobot.cvp:12008=astproxy.cisco.com:12008
cuic-PQR.autobot.cvp:8444=astproxy125.cisco.com:8444
cuic-PQR.autobot.cvp:8447=astproxy125.cisco.com:8447
livedata-ABC.autobot.cvp:12005=astproxy125.cisco.com:12005
livedata-ABC.autobot.cvp:12008=astproxy125.cisco.com:12008
ids.autobot.cvp:8553=astproxy.cisco.com:8553
ids2.autobot.cvp:8553=astproxy125.cisco.com:8553
finads-WXY.finesse.com:443=astproxy-idp.cisco.com:443
fincup1-WX.cisco.com:5280=astproxy.cisco.com:5280
fincup2-PQ.cisco.com:5280=astproxy125.cisco.com:15280
fincup3-RST.cisco.com:5280=astproxy.cisco.com:25280
```

## Add Proxy IP by Using CLI

The administrator must use CLI to add the list of trusted reverse-proxy IP addresses and their corresponding hostnames. This must be done on all the nodes of Finesse, IdS, CUIC, and LiveData (12.6(1) ES01 and above). These components consider only requests from the configured hosts or IP addresses as valid.



- Note**
- Ensure to add the hostnames that are resolvable from the respective components from where the CLI is run.
  - Ensure to add both public and private IP addresses of the reverse-proxy.
  - The allowed hosts must not contain the hostname or IP address of the load balancer. It should contain only the internal and external hostname and IP address of the reverse-proxy.

The following is an example of the CLI to add the hosts and IP addresses:

```
admin:utils system reverse-proxy allowed-hosts add 10.78.95.178
Source 10.78.95.178 successfully added
admin:utils system reverse-proxy allowed-hosts add proxy.xyz.com
Source proxy.xyz.com successfully added
```

```
Restart Cisco Web Proxy Service for the changes to take effect: utils service restart Cisco
Web Proxy Service
```

If the added hostname is not resolvable from a component, the following error is displayed:

```
admin:utils system reverse-proxy allowed-hosts add xyz.com
```

```
Either IPv4 address or hostname is invalid or is not resolvable. Now validating IPv6 address
for source xyz.com
```

```
Operation failed, please enter valid source(s). Source xyz.com is invalid
```

After adding proxy hosts as trusted hosts through CLI on individual nodes, you must upload proxy server certificates to the Tomcat trust store of the respective components. This is required for proxy authentication to work. Otherwise, the traffic from proxy will be rejected by the components. For information about generating proxy certificates and uploading to the Tomcat trust store, see the *Set up Nginx reverse proxy certificate* and *Generate and Copy CA Certificates of VOS Components* sections in the [Security Guide for Cisco Unified ICM/Contact Center Enterprise](#).



- Note** If you are upgrading from 12.6(1) ES01, you must copy and upload proxy server certificates to the Tomcat trust store of the respective components. The certificates are required at the component server to verify and allow TLS connections from the proxy.

The following is an example of the CLI to view the list of allowed hosts and IP addresses:

```
admin:utils system reverse-proxy allowed-hosts list
```

```
Source proxy.xyz.com successfully added list
```

```
The following source(s) are configured:
```

```
1. 10.78.95.178
```

```
2. proxy.xyz.com
3. proxy125.xyz.com
```

The following is an example of the CLI to delete an entry from the list of allowed hosts and IP addresses. This command lists all the configured proxy hosts and IP addresses, and gets user input to delete specific or all proxy hosts and IP addresses.

```
admin:utils system reverse-proxy allowed-hosts delete
Select the reverse-proxy source IP to delete:
```

```
1) 10.78.95.178
2) proxy.xyz.com
3) proxy125.xyz.com
4) all
5) quit
```

```
Please select an option (1 - 5 or "q"): 1
```

```
Delete operation successful
```

## Configure Reverse-Proxy Host Verification

You can configure SSL certificate verification for communication between reverse-proxy host and the Cisco Web Proxy Service by running the following CLI command on both publisher and subscriber nodes of Finesse:

### **utils system reverse-proxy client-auth**

This command has the following parameters:

- enable
- disable
- status

By default, the host authentication is enabled.

The following is an example of the CLI to view the status of the host authentication:

```
admin:utils system reverse-proxy client-auth status
```

```
SSL certificate verification for connections established from reverse proxy hosts is disabled
```

The following is an example of the CLI to enable the host authentication:

```
admin:utils system reverse-proxy client-auth enable
```

```
SSL certificate verification enabled for connections established from reverse proxy hosts
```

```
Restart Cisco Web Proxy Service for the changes to take effect:
```

```
utils service restart Cisco Web Proxy Service
```




---

**Note** After enabling the reverse-proxy host authentication, browser-based clients that connect to Finesse Desktop via LAN hostname must select a client certificate. A pop-up is displayed on systems where client certificates are installed. Clients can choose any of the certificates listed in the pop-up, and continue to connect to Finesse.

---

The following is an example of the CLI to disable the host authentication:

```
admin:utils system reverse-proxy client-auth disable
```

```
SSL certificate verification disabled for connections established from reverse proxy hosts
```

```
Restart Cisco Web Proxy Service for the changes to take effect:
utils service restart Cisco Web Proxy Service
```

## Configure Proxy Mapping by Using CLI

The Proxy-config map file can be configured in the Finesse, IdS, and CUIC servers using the `utils system reverse-proxy config-uri` command. If the URL is configured to use HTTPS protocol, Finesse, IdS, and CUIC must have the certificate (certificate of the web server hosting the URL) uploaded in `/cmplatform`. The administrator can configure a maximum of two URLs. The URL that is added first takes precedence and that URL is polled to detect changes in the mapping file. When the URL is not accessible, the alternate URL is used. The following is an example of the CLI to list the configured Proxy-config map URLs:

```
admin:utils system reverse-proxy config-uri list
```

```
Currently no source is configured
```

The following is an example of the CLI to configure the Proxy-config map URL on the Finesse, IdS, and CUIC servers:

```
admin:utils system reverse-proxy config-uri add https://saproxy.xyz.com:10000/proxyconfig.txt
```

```
Operation failed, please enter valid source(s). Source
https://saproxy.xyz.com:10000/proxyconfig.txt is invalid
```

```
admin:utils system reverse-proxy config-uri add https://saproxy.xyz.com:10000/proxymap.txt
```

```
Source https://saproxy.xyz.com:10000/proxymap.txt successfully added
```

```
admin:utils system reverse-proxy config-uri list
```

```
The following source(s) are configured:
```

```
1. https://saproxy.cisco.com:10000/proxymap.txt
```

The following is an example of the CLI to delete existing Proxy-config map URLs. This command lists all the configured Proxy-config URLs and gets user input to delete specific or all Proxy-config URLs:

```
admin:utils system reverse-proxy config-uri delete
```

```
Select the reverse-proxy source URI to delete:
```

```
1) https://saproxy.xyz.com:10000/proxymap.txt
2) all
q) quit
```

```
Please select an option (1 - 2 or "q"): 1
```

```
Delete operation successful
```

The following is an example of the CLI to set the Proxy-config update frequency (in minutes). Based on the set frequency, the local file system of Finesse, IdS, and CUIC are updated with the content from the Proxy-config map file. Before configuring the URL, this command does not return any value. After configuring the Proxy-config map URL, by default it returns one minute as the value.

```
admin:utils system reverse-proxy show-config-update-frequency
```

```
No config-uri configured
```

```
admin:utils system reverse-proxy config-uri add https://saproxy.xyz.com:10000/proxymap.txt
```

```
Source https://saproxy.xyz.com:10000/proxymap.txt successfully added

admin:utils system reverse-proxy show-config-update-frequency
1 minute

admin:utils system reverse-proxy set-config-update-frequency 5

admin:utils system reverse-proxy show-config-update-frequency
5 minutes
```

## Configure CORS and Frame-Ancestors

Add both the primary and secondary reverse-proxy origins on publisher and subscriber nodes of Finesse and CUIC. If you change Cross-Origin Resource Sharing (CORS) allowed list and frame-ancestors, you must restart Finesse Notification and Tomcat services. For information about restarting Finesse notification service, see the *Cisco Finesse Services* section in [Cisco Finesse Administration Guide](#).

- Administrators must add the list of proxy server origins on the allowed list of CORS origins, if the CORS setting is enabled on Finesse, CUIC, and Live Data .
- Frame-ancestors are added automatically while adding the reverse-proxy trusted hosts in Finesse servers.
- Administrators must add frame-ancestors while adding reverse-proxy trusted hosts in CUIC servers.
- Administrators must delete the corresponding allowed list of CORS and frame-ancestors entries while deleting the trusted hosts of a reverse-proxy.




---

**Caution** If you do not delete the corresponding CORS and frame-ancestors entries, it becomes a security vulnerability.

---




---

**Note** CORS and frame-ancestors are not applicable to IdS.

---

For information about deleting CORS see the *Cross-Origin Resource Sharing (CORS)* section in the [Cisco Finesse Administration Guide](#).

For more information about configuring CORS, see the Live Data CORS Configuration section in [Cisco Unified Contact Center Enterprise Installation and Upgrade Guide](#).

For information about deleting frame-ancestors see the *Supported Content Security Policy Directives* section in the [Cisco Finesse Administration Guide](#).

## Configure SSO

If SSO is enabled in Unified CCE, SSO must be configured for VPN-less access. Otherwise, agents and supervisors can't login to the Cisco Finesse desktop.

The steps to configure SSO are as follows:

1. Administrator must download proxy specific SAML SP metadata from IdS administration interface.
2. Add proxy relying party trust with IdP.
3. Add proxy redirect URIs to Finesse clients manually via IdS admin interface.



#### 4. Validate SSO configuration for reverse-proxy from IdS admin

For more information, see the [Single Sign-On](#).



#### Note

- Proxy configuration does not reflect in IdS in any one of the following scenarios:
  - IdP metadata is not uploaded
  - IdS is in maintenance mode
  - Maintenance mode is completed.
- If proxy configuration is changed for IdS hosts, administrator must reestablish trust on IdP for new IdS proxy hosts after downloading new metadata file from IdS admin. Administrator must reestablish **Relying Party Trusts** with IdP. For more information, refer to the Integrate Cisco IdS with AD FS
- If proxy configuration is changed for Cisco Finesse hosts, administrator must manually update the allowed Finesse client redirect URIs list on IdS admin interface. For more information, refer to the Configure the Cisco Identity Service. Client name is "Finesse" and the URLs that are to be added are as follows:
  - `https://<finesseReverseProxySideAHost:finesseReverseProxySideAPort>/desktop/ss0/authcode`
  - `https://<finesseReverseProxySideBHost:finesseReverseProxySideBPort>/desktop/ss0/authcode`
  -

## Serviceability

### Monitor Connected Agents and Supervisors

The reverse-proxy has to be monitored by using the proxy-specific features. For more information, refer to the specific reverse-proxy documentation.

Cisco Finesse allows administrators to view the list of currently connected agents and supervisors in `cfadmin`. The administrator can filter and see the agents and supervisors who are connected to the Finesse desktop based on the connection type. For example, agents and supervisors connected through the Contact Center network and those connected through reverse-proxy can be seen. For more information, see the *Connected Agents* section in *Cisco Finesse Administration Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html>. Administrators can also view the summary of connected users by using the following CLI command:

```
admin:utils finesse show_connected_users summary
```

```
Total Connected Users: 6
```

```
Desktop Users: 1
FIPPA Users: 2
Third-party Users: 3
```

```
Users connected to Finesse via LAN/WAN: 5
Users connected to Finesse via Proxy: 1
```

To view the complete list of signed-in users, log in to the Cisco Finesse Administration Console, and navigate to the Connected Agents tab.

To view the real-time list of connected users by using an API, see the *ConnectedUsersInfo* section in *Cisco Finesse Web Services Developer Guide* at <https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide>.

## API Modifications to Support Reverse-Proxy Deployments

### Finesse SystemInfo API

SystemInfo API is now secured when it is accessed through a reverse-proxy. The API is accessible with agent and supervisor credentials. The following field has been added to support this feature:

- **httpsPort:** HTTPS port has to be used for all Finesse API and desktop notifications.

For more information, see the *SystemInfo* and *ConnectedUsersInfo* sections in *Cisco Finesse Web Services Developer Guide* at <https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide>.

## HTTP Return codes returned by the reverse-proxy

These are the HTTP return codes returned by the proxy in exceptional scenarios. The HTTP error code and the situations in which these custom error codes are sent are as follows:

Error Code	Error	Reason
444	No Response	Accessing https ports with http requests.
401	Unauthorized	Authentication Failed - Note, even SystemInfo requires to be authenticated when accessed through reverse-proxy.
403	Forbidden	When restricted pages are accessed or the user is unauthorized.  <code>cfadmin/FIPPA/</code> , <code>test sso</code> , and some of the pages are restricted through reverse-proxy.
405	Method not allowed	Accessing URLs with invalid HTTP methods. For example, most of the Cisco IdS URLs support only GET, POST, and OPTIONS methods. Anything other than these methods results in this error.
412	Precondition Failed	Check the <b>User-Agent</b> field of the request header.  Reverse-proxy validates some of the pre-configured <b>User-Agent</b> headers that could be triggered from Bots.

Error Code	Error	Reason
417	Expectation Failed	The server can't meet the requirements of the <b>Expect request-header</b> field. Please check the referrer header field is populated as one of the valid configured referrer headers.  Please check the <b>NGX_VALID_REFERRERS</b> in the <b>core.env</b> file has all the valid referrer headers configured for the failed request.
421	Misdirected Request	Accessing URL that isn't supported through reverse-proxy. Reverse-proxy configured to support only a set of upstream URLs. Any URL other than that is requested results in this error.
429	Too Many Requests	The response status code indicates that the user has sent too many requests in a given amount of time ("rate limiting").  Need to check the configured LB and rate limiting configurations on the <b>core.env</b> file and component's envs.

## Historical and Real Time Gadgets

The Cisco Unified Intelligence Center release 12.6.1 ES02 and above, supports Historical and Real Time report gadgets in agent and supervisor desktops in VPN-less deployments. To configure the Historical and Real Time report gadgets, refer to the *Configure Historical Report Gadgets in Cisco Finesse* section in *Cisco Unified Intelligence Center User Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-user-guide-list.html>.

**Note**

- Stock reports and custom reports can be viewed in VPN-less supervisor desktop. However, before viewing the custom reports as gadgets in VPN-less supervisor desktop, run the command, **set cuic properties allow-proxy-custom-report on**.
- To configure the data set size for Historical report, run the command, **set cuic properties vpnless-response-size-ht**. By default, the data set size for HT is set to 8MB.
- To configure the data set size for Real Time report, run the command, **set cuic properties vpnless-response-size-rt**. By default, the data set size for RT is set to 300KB.

If the data set size is more than the configured value, the gadget will display the following error message:

```
Failed to load the gadget. Response size is more than allowed limit. Please contact your Administrator.
```

This limitation is applicable on VPN-less deployments only. For more information about configuring the data set size, see *set Cisco Unified Intelligence Center properties* section in *Administration Console User Guide for Cisco Unified Intelligence Center* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html>.

## Security Guidelines

For information about security guidelines, see the *Security Guidelines for Reverse-Proxy* 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>.

## Caveats

Reverse-proxy deployment allows agents and supervisors to concurrently access the Cisco Finesse desktop from both LAN and through reverse-proxy. After configuring the reverse-proxy, when the agents and supervisors access the Finesse desktop through LAN, all the features work seamlessly. However, when the Finesse desktop is accessed through the reverse-proxy, the caveats are as follows:

- Finesse IP Phone Agent (FIPPA) isn't supported.
- Administrative applications and the corresponding APIs of Finesse, IdS, and Cisco Unified Intelligence Center aren't supported.
- Multiple devices accessing the Finesse desktop through Network Address Translation (NAT) isn't supported.
- Multiple users accessing the VPN-less desktop from behind a common proxy isn't supported when multiple sites are involved.
- If threshold images are used in Live Data, Real Time, and Historical gadgets, add the reverse-proxy rules to allow images to be accessed through reverse-proxy. For more information on threshold images rules, refer to the [Nginx TechNote article](#) section.
- After upgrading Finesse to 12.6(1), Cisco Unified Intelligence Center must be upgraded to 12.6(1) for the Live Data (LD) gadgets to work. Refer to the [Unified CCE Compatibility Matrix](#) for general

compatibility between CUIC and Finesse when accessed through the Contact Center network or the reverse-proxy.

- Third-party gadgets on the Finesse desktop could be incompatible with the reverse-proxy deployment. For more information on gadget compatibility, see the [Determine Gadget Compatibility, on page 259](#) section.
- **Finesse API Compatibility:**
  - Finesse Desktop supports only the WebSocket notification mechanism over reverse-proxy. For third-party servers, BOSH or XMPP over TCP communication through reverse-proxy isn't supported.
  - When the SystemInfo API is accessed through a reverse-proxy, the authorization headers are required.





## CHAPTER 18

# Webex Experience Management Integration

- Experience Management Overview, on page 275
- Experience Management Voice Survey, on page 276
- Provision Experience Management Service on Cloud Connect, on page 278
- Configure Unified CCE for Experience Management Voice, SMS and Email Survey, on page 279
- Configure Expanded Call Variables, on page 279
- Upload Audio Files for Questions in Experience Management, on page 281
- Configure Dialed Number and Call Type, on page 281
- Associate Survey to Call Type in Unified CCE Admin, on page 282

## Experience Management Overview



**Note** To enable this feature in Unified CCE, install the following patches:

- ICM 12.5(1)\_ES7
- CVP 12.5(1)\_ES6
- Cloud Connect 12.5(1)ES1
- Finesse 12.5(1)ES2

Cisco Webex Experience Management is a Customer Experience Management (CEM) platform that allows you to see your business from your customers' perspective. To know more about Webex Experience Management, see <https://xm.webex.com/docs/ccoverview/>.

With Webex Experience Management, Unified CCE supports:

- Customer experience surveys - Set up and send surveys to customers, after an interaction, to collect feedback about their interaction.
- Experience Management Post Call Survey
- Customer Experience Journey (CEJ) gadget - Displays all the past survey responses from a customer in a chronological list. The agent and supervisor use this gadget to gain context about the customers past experiences with the business and engage with them appropriately.

- Customer Experience Analytics (CEA) gadget - Displays the overall experience of the customer interaction with agents using industry-standard metrics such as NPS, CSAT, and CES or other KPIs tracked within Experience Management. This gadget is available for agents and supervisors.

## Experience Management Voice Survey

Experience Management post-call survey is used to determine whether the customers are satisfied with their voice call experiences. You can configure Experience Management to initiate this survey when an agent disconnects from the caller. The survey can be done in three modes—voice, SMS, or email.

The CCE script enables or disables voice call survey for each call by testing for conditions and setting an expanded call variable that controls Experience Management. For example, the script can invoke a prompt that asks callers whether they want to participate in a survey. Based on the caller's response, the script sets the expanded call variable that controls whether the call gets transferred to the voice call survey Dialed Number.

You can send post call survey links through email or SMS also. After every call, the customer is provided with a choice to participate in the survey and answer few questions over email or their phone. For more information on how to configure or to associate the survey, refer to the section [Configure Unified CCE for Experience Management Voice, SMS and Email Survey, on page 279](#).

The Experience Management Post Call Survey call works just like a regular call from the Unified CCE point of view. Scripts are invoked, CVP refers the call to Experience Management, and the customer uses the keypad on a phone to respond to questions asked during the survey. During Experience Management Post Call Survey, the call context information is retrieved from the original customer call.




---

**Note** Experience Management supports G.711 u-law and G.711 a-law codecs.

---

## Experience Management Task Flow

To enable Experience Management Post Call Survey in Cisco Unified CCE, follow this task flow:

- 
- Step 1** Contact your Cisco representative to purchase Experience Management license. After the purchase, you need to provide relevant information about your organization to Experience Management Activation Team. To know more about the information that will be collected, see [Prerequisites](#).
- Step 2** Experience Management Activation Team performs the following actions:
- Creates accounts and provisions the same.
  - Creates default spaces and metric groups for your accounts. To know more about creating spaces, see [Space Creation](#).
  - Creates standard questionnaires for Experience Management Post Call Survey and publishes the same. To know more about creating questionnaires, see [Questionnaires](#).
- Step 3** After creating and provisioning the account, you will receive handover emails from the Experience Management Activation Team. The email contains credentials and other essential information for your account. To know more about provisioning details, see [Handover](#).



- Step 4** Initially, Spaces and Widgets are created by the Experience Management provisioning team. To know more about the different default Widgets, how to export and derive meaningful insights from them, see [Experience Management Gadgets](#).
- To know how to configure additional Widgets in Experience Management, see [Experience Management Gadgets](#).
- Step 5** Ensure that the Cloud Connect publisher and subscriber are installed. For more information, see the *Install Cloud Connect* section in *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html>.
- Step 6** Provision Experience Management service using CLI on Cloud Connect. For more information, see [Provision Experience Management Service on Cloud Connect, on page 278](#).
- Step 7** Configure Cloud Connect in Operations Console (NOAMP). For details see the section *Configure CVP Devices for Cloud Connect* in *Administration 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>.
- Step 8** Configure Post Call Survey in CVP. For more information, see [Configure Post Call Survey in CVP, on page 146](#).
- Step 9** Import the following certificates to the CVP Server:
- Cloud Connect certificate
  - Experience Management certificate
- For details, see the sections *Import Cloud Connect Certificate to Unified CVP Keystore* and *Import Experience Management Certificate to Unified CVP Call Server* in *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>.
- Step 10** Ensure that the threshold properties (in *ivr.properties* and *sip.properties* files) and proxy settings are configured in CVP for Experience Management. For details, see the section *Webex Experience Management Configuration* in *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>.
- Step 11** Configure Unified CCE Experience Management. For more information, see the topic [Configure Unified CCE for Experience Management Voice, SMS and Email Survey, on page 279](#).
- Step 12** Configure Dialed Number and Call Type for Incoming Call and Experience Management post call survey routing script. For more information, see [Configure Dialed Number and Call Type, on page 281](#).
- Step 13** Modify CCE scripts. For more information, see *Modify CCE Scripts for Experience Management Voice, SMS and Email Surveys* in *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>.
- Associate the CCE script with the Call Type created in the previous step.
- Step 14** Provision Cloud Connect on Cisco Finesse. For more information, see the *Cloud Connect Server Settings* topic at the [Cisco Finesse Administration Guide](#).
- Step 15** Add Experience Management gadgets into Finesse desktop layout. For more information, see [Cisco Webex Experience Management Gadgets](#).
-

# Provision Experience Management Service on Cloud Connect

Before provisioning Experience Management service on Cloud Connect, ensure to setup and enable Cloud Connect. For more information, see the *Cloud Connect Administration* section in [Administration Guide for Cisco Unified Contact Center Enterprise](#)

Provision Experience Management service using the following CLI on Cloud Connect.

```
set cloudconnect cherrypoint config
```

For more commands related to Experience Management service, see the *Cloud Connect CLI* section in the [Cisco Unified Contact Center Enterprise Installation and Upgrade Guide](#).

The partner hosted module which is a part of Experience Management Invitations solution is required to send surveys to customers over emails and SMS.

For information about *Partner Hosted Module Architecture* refer to <https://xm.webex.com/docs/cxsetup/guides/partnerarchitecture/>

For information about how to provision the infrastructure required to deploy the partner hosted components of the Experience Management Invitations module, see <https://xm.webex.com/docs/cxsetup/guides/partnerinfra/>.

For information about how to deploy the partner hosted components on the Experience Management Invitations module once the infrastructure is provisioned, see <https://xm.webex.com/docs/cxsetup/guides/partnerdeployment/>.

## Configuration Changes in Webex Experience Management

Any configuration changes done in the Webex Experience Management administration interface gets reflected in the on-premise Contact Center integrations after a maximum caching delay.

You observe the caching delay when:

- Modify the questionnaires.
  - Adding or removing questions.
  - Adding new stock prefill question.
  - Updating the tags associated with stock prefill questions. The specific tags that Contact Center integrations use.
- System configuration changes are made to the dispatch.

The maximum caching delay depends on the kind of configuration change. Because the on-premise systems cache, Webex Experience Management configuration, and the maximum delay depend on the cache invalidation period. In cache invalidation, the system invalidates or removes the data from the cache after a specific time interval.

### Types of Caches and Cache Invalidation

The different types of caches that are used in the on-premise systems are:

- **Prefill Cache** if any new tag is not in the cache it's updated. However, if any new questions get added with the tag it reflects only after a cache invalidation period of 24 hours. For example, tag -> List of Questions.



---

**Note** As the new questions are staff prefill questions, we do not expect it to change often. Hence a delay of 24 hours is acceptable.

---

- **All other caches** will be reflected after a cache invalidation period of 1 hour. For example, questionnaire -> hashScheme dispatchTemplate -> questionnaireDispatchSettings (As obtained from settings API)

The partner hosted module in the Experience Management Invitations solution maintains a cache with maximum delay of 1 hour for the Dispatches list, Settings, Delivery Policy, Active Questions, and Questionnaire APIs. For more information, see <https://xm.webex.com/docs/cxsetup/guides/partnerarchitecture/#43-caching-mechanism>.

## Configure Unified CCE for Experience Management Voice, SMS and Email Survey

Refer to the following procedures to enable the Experience Management voice, SMS and email survey:

- [Configure Expanded Call Variables, on page 279](#)
- [Upload Audio Files for Questions in Experience Management, on page 281](#)
- [Configure Dialed Number and Call Type, on page 281](#)
- [Associate Survey to Call Type in Unified CCE Admin, on page 282](#)

## Configure Expanded Call Variables

- 
- Step 1** In the **Configuration Manager** menu, select **Tools > List Tools > Expanded Call Variables List**. The **Expanded Call Variables List** window appears.
- Step 2** Click **Retrieve** to view the list of existing ECC variables.
- Step 3** Check if the *user.microapp.isPostCallSurvey* variable exists. If the variable does not exist, do the following to create a new variable:
- a) Click **Add**.
  - b) In the **Attributes** tab that appears, enter *user.microapp.isPostCallSurvey* in the **Name** field.
  - c) Set **Max Length** to 1.
  - d) Check the **Enabled** check box.
  - e) Click **Save**.

When your CCE routing scripts starts, the Post Call Survey field is **enabled** by default even if *user.microapp.isPostCallSurvey* has not yet been set in the script. You can turn off Post Call Survey field in the script

by setting `user.microapp.isPostCallSurvey` to `n`. You can later enable Post Call Survey in the same path of the script by setting this variable to `y`.

**Note** To enable Experience Management, `user.microapp.isPostCallSurvey` must be set to `y`.

**Step 4** Check if the `user.CxSurveyInfo` variable exists. If the variable does not exist, do the following to create a new variable:

- Click **Add**.
- In the **Attributes** tab that appears, enter `user.CxSurveyInfo` in the **Name** field.
- Set the **Max Length** to 133 for Type 10 VRUs. For all other routing clients, set **Max Length** to 80.
- Check the **Enabled** check box.

**Step 5** Click **Save**.

**Note** The newly created ECC variables are added to the default payload list. If you want to save the ECC variables to a different payload list, in the **Configuration Manager**, navigate to **Tools > List Tools > Expanded Call Variable Payload List** and add the ECC variables to the payload list of your choice.

**Step 6** Populate the **POD.ID** variable.

For more information on populating this variable, refer to the topic [Configure POD.ID](#).

**Step 7** Restart the active VRU PG (side A or B) to register the new ECC variable.

If the ECC variable already exists, you can skip this step.

**Note** The `user.microapp.isPostCallSurvey` setting takes effect on Unified CVP only when it receives a **connect** or temporary connect message. If you do not want the survey to run, without first reaching an agent (such as 'after hours of treatment'), set the `isPostCallSurvey` to `n` before the initial 'Run script request'.

## Configure POD.ID

Cisco provided variables are predefined, but for POD.ID, the maximum length should be set to 120.

You can modify the variables only if you have the edit access.

Populate the value in the script with multiple attributes in a key-value pair format. Each key-value pair is separated with a semi-colon. The following table displays the supported attributes:

**Table 18: Variables and their descriptions**

Attribute	Description	Applicable
cc_CustomerId	Unique ID for a customer across multiple channels	Chat and Email surveys for Digital Channels
Email	Email ID of the caller for Email surveys	Email survey for voice channel
Mobile	Phone number for SMS surveys	SMS survey for voice channel

Attribute	Description	Applicable
cc_language	Language of the survey For the list of supported languages, refer to the Webex Experience Management documentation at <a href="https://xm.webex.com/docs/user/getting-help/#cloudcherry-language-support">https://xm.webex.com/docs/user/getting-help/#cloudcherry-language-support</a>	Email, SMS, and Voice surveys for voice channel
Optin	Whether to opt in or opt out of the survey	Email, SMS, and Voice surveys for voice channel

Example: `cc_CustomerId=xxx;Email=xx;Mobile=xxx;cc_language=xxx;Optin=yes/no`

For more information on **Expanded Call Context Variables**, see the chapter *Configure Variables* in 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>.

You can also configure POD.ID from CVP Call Studio. For more information, refer to the topic *Configure Call Studio App Data Format* in 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>.

## Upload Audio Files for Questions in Experience Management

Experience Management allows you to upload the audio files for post call survey.



**Note** To run post-call voice survey, you must either configure *Text-To-Speech(TTS)* in the voice browser or upload audio prompts in Experience Management.

Create and configure the questionnaires in Experience Management for sending IVR surveys to the customer. For more information on Experience Management, refer to <https://xm.webex.com/docs/ccoverview/>

For more information on how to create and modify the questionnaires, refer to <https://xm.webex.com/docs/cxsetup/questionnaires/>.

## Configure Dialed Number and Call Type

**Step 1** In **Configuration Manager**, navigate to **Tools > List Tools > DialedNumber/Script Selector List**.

**Step 2** In **DialedNumber/Script Selector List** create **Incoming Dialed Number** and **Post Call Survey Dialed Number**.

For more information on how to create a PCS Dialed Number, refer to the section *Configure ICM for Post Call Survey* in *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>.

- Step 3** Click **Save**. You will be re-directed to the **Configuration Manager** window.
- Step 4** In **Configuration Manager**, navigate to **Tools > List Tools > Call Type List**.
- Step 5** In **Call Type List** create the **Call Type**. You should associate to the incoming call script and PCS script.
- You should associate the incoming call type with the survey from CCEAdmin.
- For more information, refer to the topic [Associate Survey to Call Type in Unified CCE Admin, on page 282](#).
- 

## Associate Survey to Call Type in Unified CCE Admin

You can associate the Call Type to the survey only if you have added **Cloud Connect** in the **Inventory** page and configured the survey in **Webex Experience Management** portal.



**Note** Only one survey can be associated to a Call Type.

---

Call Types are created and managed in **Configuration Manager** tool and the survey is associated using the **CCE Admin** tool.

---

- Step 1** In **Unified CCE Administration**, navigate to **Overview > Call Settings > Route Settings > Call Types**.
- The list of all the **Call Types** are displayed.
- For more information on Call Types, refer to the **Help** in **ConfigManager > List Tools > Call Types**.
- Step 2** Click on the **Call Type** which you want to associate to the Survey. Associate the survey with the last call type before the call is first connected to an agent.
- Step 3** Select the **Enable Experience Management** check box to associate the **Webex Experience Management** survey.
- The **Experience Management** tab is enabled with the following options:
- **Inline Survey** (post-call voice survey)
  - **Deferred Survey** (post-call Email and SMS survey)
- Step 4** Click on the **magnifying glass** icon, and the configured surveys will be populated in the pop-up window.
- Step 5** Select the survey from the pop-up window and click **Save**.
-



## CHAPTER 19

# Webex Experience Management Digital Channel Survey

---

- [Overview, on page 283](#)
- [Digital Channel Survey , on page 283](#)
- [Provision Cloud Connect for Digital Channel Survey, on page 285](#)
- [Configure Unified CCE for Digital Channel Survey , on page 285](#)
- [Configure Expanded Call Variables , on page 285](#)
- [Configure Call Type, Dialed Number, and Survey Association, on page 287](#)

## Overview

Digital Channel Survey is initiated when the agent responds to an email/chat from a customer using the Enterprise Chat and Email gadget. Cisco Webex Experience Management is a Customer Experience Management (CEM) platform that allows you to see the business from your customers perspective. It provides customer journey experience using the CEJ omni-channel gadget. To learn more about Webex Experience Management, see <https://xm.webex.com/docs/ccoverview/>.

With Webex Experience Management, Unified CCE supports:

- Customer experience surveys - Set up and send surveys to customers, after an interaction, to collect feedback about their interaction.
- Customer Experience Journey (CEJ) gadget - Displays all the past survey responses from a customer in a chronological list. The agent and supervisor use this gadget to gain context about the customers past experiences with the business and engage with them appropriately.
- Customer Experience Analytics (CEA) gadget - Displays the overall experience of the customer interaction with agents using industry-standard metrics such as NPS, CSAT, and CES or other KPIs tracked within Experience Management. This gadget is available for agents and supervisors.

## Digital Channel Survey

Email and chat inline surveys are used to determine whether customers are satisfied with their interaction with the agent in resolving their query over an email or chat. The feedback collected through the survey is used by the agents to gain context about the customer in their subsequent interactions and to also improve

their own performance. You can configure Enterprise Chat and Email to initiate this survey when the agent sends an email or terminates a chat conversation with a customer. The survey is sent inline in the agents email response to customers who contact them via email, and within the chat window for customers who contact them via chat.

## Digital Channel Survey Task Flow (Email/Chat)

To enable Experience Management inline surveys with Enterprise Email and Chat in Cisco Unified CCE, perform the following procedure:

- 
- Step 1** Contact your Cisco representative to purchase Experience Management license. Provide relevant information about your organization to Experience Management Activation Team. To know more about the information that will be collected, see [Prerequisites](#).
- Step 2** Experience Management Activation Team performs the following actions:
- Creates account and provisions the same.
  - Creates default spaces and metric groups for your accounts. To know more about creating spaces, see [Space Creation](#).
  - Creates default questionnaires in Experience Management suited for inline email and chat survey. To know more about creating your own questionnaires or editing the default ones, see [Questionnaires](#).
- Step 3** After creating and provisioning the account, you will receive handover emails from the Experience Management Activation Team. The email contains credentials and other essential information for your account. To know more about provisioning details, see [Handover](#).
- Step 4** Initially, Spaces and Widgets are created by the Experience Management provisioning team. To know more about the different default Widgets and how to export and derive meaningful insights from them, see [Cisco Webex Experience Management Gadgets](#).
- To know how to configure other Widgets in Experience Management, see [Basic Widget](#) and [Composite Widgets](#).
- Step 5** Ensure that the Cloud Connect publisher and subscriber are installed. For more information, see the *Install Cloud Connect* section in *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html>
- Step 6** Provision Experience Management service using CLI on Cloud Connect. For more information, see [Provision Cloud Connect for Digital Channel Survey, on page 285](#).
- Step 7** Ensure that the Enterprise Chat and Email (ECE) is installed and configured, see the *Webex Experience Manager Integration* in *Enterprise Chat and Email Administrator's Guide to Administration Console* at <https://www.cisco.com/c/en/us/support/contact-center/enterprise-chat-email-12-5-1/model.html>.
- Step 8** Configure Unified CCE Experience Management integration. For more information, see [Configure Unified CCE for Digital Channel Survey , on page 285](#).
- Step 9** Configure Call Type and Dialed Number. For more information, see [Configure Call Type, Dialed Number, and Survey Association, on page 287](#).
- Step 10** Modify CCE Scripts. For more information, see *Modify CCE Scripts for Experience Management Digital Channel Surveys* in *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>.
- Associate the CCE script with the Call Type created in the previous step.
- Step 11** Provision Cloud Connect on Cisco Finesse. For more information, see the *Cloud Connect Server Settings* topic at the [Cisco Finesse Administration Guide](#).



- Step 12** Add Experience Management gadgets into Finesse desktop layout. For more information, see [Cisco Webex Experience Management Gadgets](#).

## Provision Cloud Connect for Digital Channel Survey

Before provisioning Cloud Connect for Experience Management service, ensure to setup and enable Cloud Connect. For more information, see the *Cloud Connect Administration* section in [Administration Guide for Cisco Unified Contact Center Enterprise](#)



**Note** Ensure that you have installed the self-signed certificates for Cloud Connect. For more information, see the *Self-Signed Certificates* section in the [Cisco Unified Contact Center Enterprise Installation and Upgrade Guide](#).

Provision Experience Management service using the following CLI on Cloud Connect.

```
set cloudconnect cherrypoint config
```

For more commands related to Experience Management service, see the *Cloud Connect CLI* section in the [Cisco Unified Contact Center Enterprise Installation and Upgrade Guide](#).

## Configure Unified CCE for Digital Channel Survey

Refer to the following procedures to enable the Experience Management email and chat survey:

- [Configure Expanded Call Variables](#) , on page 285
- [Configure Call Type, Dialed Number, and Survey Association](#), on page 287
- [Associate Survey to Call Type in Unified CCE Admin](#), on page 287

## Configure Expanded Call Variables

- Step 1** In the **Configuration Manager** menu, select **Tools > List Tools > Expanded Call Variable List**. The **Expanded Call Variable List** window appears.
- Step 2** Click **Retrieve** to view the list of existing ECC variables.
- Step 3** Check if the *user.microapp.isPostCallSurvey* variable exists. If the variable does not exist, do the following to create a new variable:
- a) Click **Add**.
  - b) In the **Attributes** tab that appears, enter *user.microapp.isPostCallSurvey* in the **Name** field.
  - c) Set **Max Length** to 1.
  - d) Check the **Enabled** check box.
  - e) Click **Save**.

When your CCE routing scripts starts, you can turn off Post Call Survey field in the script by setting `user.microapp.isPostCallSurvey` to `n`. You can later enable Post Call Survey in the same path of the script by setting this variable to `y`.

**Note** In the script, set the `user.microapp.isPostCallSurvey` before routing it to the agent.

**Note** To enable Experience Management, `user.microapp.isPostCallSurvey` must be set to `y`.

**Step 4** Check if the `user.CxSurveyInfo` variable exists. If the variable does not exist, do the following to create a new variable:

- a) Click **Add**.
- b) In the **Attributes** tab that appears, enter `user.CxSurveyInfo` in the **Name** field.
- c) Set **Max Length** to 80.
- d) Check the **Enabled** check box.

**Step 5** Click **Save**.

**Note** The newly created ECC variables are added to the default payload list. If you want to save the ECC variables to a different payload list, in the **Configuration Manager**, navigate to **Tools > List Tools > Expanded Call Variable Payload List** and add the ECC variables to the payload list of your choice.

**Note** You can use several ECC payloads in the same call flow, but only one ECC payload has scope at a given moment. For more information, see *ECC Payloads* sections in *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>

**Step 6** Populate the **POD.ID** variable.

For more information on populating this variable, refer to the topic [Configure POD.ID](#), on page 286.

## Configure POD.ID

Cisco provided variables are predefined, but for POD.ID, the maximum length should be set to 120. Enable the POD.ID variable to edit its length.

You can modify the variables only if you have the edit access.

Populate the value in the script with multiple attributes in a key-value pair format. Each key-value pair is separated with a semi-colon. These attributes are sent to the Webex Experience Management as prefills when ECE initiates the survey. The following table displays the supported attributes:

**Table 19: Variables and their descriptions**

Attribute	Description	Applicable
cc_CustomerId	Unique ID for a customer across multiple channels	Chat and Email surveys for Digital Channels
Email	Email ID of the customer for Email survey across multiple channels	Chat and Email surveys for Digital Channels
Mobile	Phone number for Chat surveys	Chat and Email surveys for Digital Channels

Example: `cc_CustomerId=xxx;Email=xx;Mobile=xxx;`

For more information on setting the ECC variables used in the example, see *Modify CCE Scripts for Experience Management Digital Channel Surveys* in *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>.

For more information on **Expanded Call Context Variables**, see the chapter *Configuring Variables* in 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>.

## Configure Call Type, Dialed Number, and Survey Association

- 
- Step 1** In ICM Configuration Manager, navigate to **Tools > List Tools > Call Type List** to create a Call Type.
- Step 2** Associate the survey with the last call type before the email/chat is handled by the agent.
- For more information, refer to the topic [Associate Survey to Call Type in Unified CCE Admin, on page 287](#).
- Step 3** Create a Dial Number in ICM Configuration Manager and associate it with Call type (created in Step 1) for email and chat.
- 

## Associate Survey to Call Type in Unified CCE Admin

You can associate the survey to the Call Type only if you have added **Cloud Connect** to the **Inventory** page in **CCE Admin** and configured the survey in **Webex Experience Management** portal.



---

**Note** Only inline surveys can be associated to a Call Type associated with digital channels.

---

Call Types are created and managed in **Configuration Manager** tool and the survey is associated using the **CCE Admin** tool.

---

- Step 1** In **Unified CCE Administration**, navigate to **Overview > Call Settings > Route Settings > Call Type**.  
The list of all the **Call Type** are displayed.  
For more information on Call Types, refer to the **Help** in **Configuration Manager > Tools > List Tool > Call Type List**.
- Step 2** Click on the **Call Type** which you want to associate to the Survey.
- Step 3** Select the **Enable Experience Management** check box to associate the **Webex Experience Management** survey.
- a) The Experience Management tab is enabled with the following options:
- Inline Survey
  - Deferred Survey

**Step 4** Select **Inline Survey** for email and chat.

- Click on the **magnifying glass** icon, and the configured surveys will be populated in the pop-up window.

**Step 5** Select the survey from the pop-up window and click **Save**.

---



## CHAPTER 20

# Whisper Announcement

---

- [Capabilities, on page 289](#)
- [Deployment Tasks, on page 290](#)
- [How Whisper Announcement Works, on page 297](#)

## Capabilities

Whisper Announcement plays a brief, prerecorded message to an agent just before the agent connects with each caller. The announcement plays only to the agent; the caller hears ringing (based on existing ring tone patterns) while the announcement plays.

The content of the announcement can contain information about the caller that helps prepare the agent to handle the call. The information can include caller language preference, choices the caller made from a menu (Sales, Service), customer status (Platinum, Gold, Regular), and so on.

After Whisper Announcement is enabled, the played announcements are specified in the call routing scripts. The determination of which announcement to play is controlled in the script and is based on various inputs, such as the dialed number, a customer ID look up in your customer database, or selections you made from a VRU menu.

## Functional Limitations

Whisper Announcement is subject to these limitations:

- Announcements do not play for outbound calls made by an agent. The announcement plays for inbound calls only.
- For Whisper Announcement to work with agent-to-agent calls, use the `SendToVRU` or `TranslationRouteToVRU` node before you transfer the call to the agent. Transfer the call to Unified CVP before you transfer the call to another agent. Then, Unified CVP can control the call and play the announcement, regardless of which node transfers the call to Unified CVP.
- Announcements do not play when the router selects the agent through a label node.
- CVP Refer Transfers do not support Whisper Announcement.
- Whisper Announcement supports Silent Monitoring with this exception: For Unified Communications Manager-based Silent Monitoring, supervisors cannot hear the announcements themselves. The supervisor desktop dims the Silent Monitor button while an announcement plays.

- Only one announcement can play for each call. While an announcement plays, you cannot put the call on hold, transfer, or conference; release the call; or request supervisor assistance. These features become available again after the announcement completes.
- The codec settings for Whisper Announcement recording and the agent's phone must match. For example, if Whisper Announcement is recorded in G.711 ALAW, the phone must also be at G.711 ALAW. If Whisper Announcement is recorded in G.729, the phone must support or connect using G.729.
- Forking happens in Gateway in NBR only when a caller is connected to the agent (with two-way audio). Whisper announcement is played only with one way audio with agent (before connecting to the caller).
- In an IPv6-enabled environment, Whisper Announcement might require extra Media Termination Points (MTPs).

## Deployment Tasks

The following list shows the high-level tasks that are required to deploy Whisper Announcement. Individual steps are covered in more detail in later sections.

1. Ensure your deployment meets the baseline requirements for software, hardware, and configuration described in the System Requirements and Limitations section. See the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html>.
2. [Create Whisper Announcement Audio Files, on page 290.](#)
3. [Deploy Whisper Announcement Audio Files to Media Server, on page 291.](#)
4. [Configure Whisper Service Dialed Numbers, on page 291.](#)
5. [Add Whisper Announcement to Routing Scripts, on page 292.](#)
6. [Fail-Safe Timeout for Whisper Announcement in Unified CCE, on page 295.](#)

Example scripts that enable Whisper Announcement are installed with your system. For information about these scripts and how to access them, see [Whisper Announcement Sample Scripts, on page 296.](#)

## Create Whisper Announcement Audio Files

You must create audio files for each different Whisper Announcement you want to use on your system; for example, “Sales, English” or “Soporte Técnico en Español.” Create the files using the recording tool of your choice.

When recording your files, follow these rules:

- The media files must be in wave (.wav) format. Your wave files must match Unified CVP encoding and format requirements (G729, CCITT G.711 A-Law and U-law 8 kHz, 8 bit, mono).
- To avoid cutting off files when they are played, make sure they do not exceed the Whisper Announcement play limit (15 seconds).
- Test your audio files. Ensure that they are not cut off and that they are consistent in volume and tone.

- To reduce the likelihood of scripting errors, decide ahead of time on a file-naming convention that is easy for you and others to remember. For example, `en_sales.wav`, `sp_support.wav`.

## Deploy Whisper Announcement Audio Files to Media Server

Deploy your whisper audio files to your Unified CVP media server using whatever file-transfer method you prefer. The most important consideration is where on the server to place the files. HTTP requests for media server audio files are constructed as

```
http://<media_server>/<locale_directory>/<application_directory>/<file_name>.
```

The CVP defaults for the locale and application directories are `en-us/app`. Unified CCE automatically adds `en-us/app` to the server name when making HTTP requests for media files.

For example, if:

- The script node that defines the media server has a value of `http://myserver.mydomain.com` and
- The script node that defines the audio file to play has a value of `en_sales.wav`

Then the HTTP request for the file is automatically constructed as

```
http://myserver.mydomain.com/en-us/app/en_sales.wav
```

If you store your files in a different locale and application directory, your routing scripts must include variable nodes that define those alternate locations. Make note of the directories in which you place your files and communicate the locations to your script authors.

Make sure that the directories in which you deploy your files have the appropriate permissions to allow Read access.

### CVP with the Streaming Audio (Helix) and Whisper Announcement

You must set the `user.microapp.media_server` variable, to point to the whisper announcement .wav file, for the CVP Whisper Announcement feature to work while Streaming Audio feature (using Helix) is also on. This is achieved by setting the `Call.WhisperAnnouncement` variable to the complete URL of the whisper announcement wav file. The `Call.WhisperAnnouncement` variable should be put in using the `http://<VXMLserverip>:7000/CVP/audio/XXX.wav` URL format.

## Using a Default Media Server

Optionally, CVP lets you define a default media server. (You do this in the CVP Operations Console; see your CVP documentation for more information.) If a default media server is defined in CVP, script authors need not identify the media server in their call routing scripts provided the files that they request are available from that server.

## Configure Whisper Service Dialed Numbers

For Whisper Announcement, Unified CVP uses two different dialed numbers when transferring a call to an agent:

- The first number calls the ringtone service that the caller hears while the whisper plays to the agent. The CVP default for this number is 91919191.
- The second number calls the whisper itself. The Unified CVP default for this number is 9191919100.




---

**Note** Whisper Announcement dialed number is always an extension of the Ringtone dialed number with an extra two zeros at the end.

---

For Whisper Announcement to work, your dial plan must include both of these numbers. The easiest way to ensure coverage is through the use of wild cards such as 9191\*.

## Configure Dialed Numbers

You configure the dialed numbers for Whisper Announcement in the Unified CVP Operations Console at **System > Dialed Number Pattern > Add new**. For the Dialed Number Pattern Types, select **Enable Local Static Route**. Once **Enable Local Static Route** is checked, select either **Route to Device** or **Route to SIP Server Group** for VXML gateways. Then save and deploy the dialed number.

It may be necessary to override the dialed number plan for the default Whisper DN, if the default DN conflicts with the overall dial number plan.

### Change the Whisper Announcement Default Dialed Number

To override the DN pattern from the SIP subsystem level in CVP OAMP:

- 
- Step 1** Select **Device Management > Unified CVP Server**.
  - Step 2** Select the Call Server on which to override the default whisper DN.
  - Step 3** Select the SIP tab.
  - Step 4** Override the default value of 91919191 configured under the **DN on the Gateway to play the ringtone** field.
  - Step 5** Click **Save & Deploy**.
- 

## Configure Ringtone Dialed Number

To configure the Ringtone dialed number in the CVP Operations Console:

1. Select **Device Management > Unified CVP Server**.
2. Select the Call Server on which you want to configure the settings.
3. Select the SIP tab.
4. In the **DN on the Gateway to play the ringtone** field, configure the default Ringtone dialed number Pattern.

### Dialed Number in the Dial-Peer

In addition to configuring the dial plan in Unified CVP, examine your IOS dial-peer. Make sure that the dialed number setting in your dial-peer configuration accommodates both of the whisper service dialed numbers.

## Add Whisper Announcement to Routing Scripts

To enable Whisper Announcements, use the Script Editor to modify your routing scripts as follows:



- Specify the WhisperAnnouncement call variable
- Specify the Unified CVP media server and location of whisper audio files
- Specify other required variables

For more information, see [Whisper Announcement Sample Scripts, on page 296](#).

## Specify WhisperAnnouncement Call Variable

To include Whisper Announcement in a script, insert a Set Variable node that references the WhisperAnnouncement call variable. The WhisperAnnouncement variable causes a whisper to play and specifies the audio file it should use. Typically, you use a single whisper prompt for a single call type. As a result, you use only one WhisperAnnouncement set node for each script. However, as needed, you can set the variable at multiple places in your scripts to allow different announcements to play for different endpoints. For example, for skills-based routing, you can specify the variable at each decision point used to select a particular skill group or Precision Queue.



---

**Note** Only one Whisper Announcement can play for each call. If a script references and sets the WhisperAnnouncement variable more than once in a single path through a script, the last value to be set is the one that plays.

---

Use these settings in the Set Variable node for Whisper Announcement:

- Object Type: Call.
- Variable: Must use the WhisperAnnouncement variable.
- Value: Specify the filename of the whisper file. For example: “my\_whisper.wav” or “my\_whisper”.
  - Specify the filename only, not its path.
  - You must enclose the filename in quotation marks.
  - The filename is not case sensitive.
  - The filename cannot include spaces or characters that require URL encoding.
  - The .wav extension is optional. If you omit it, Unified CVP adds it automatically in the HTTP request.

## Specify Unified CVP Media Server Information

If you define a default media server in your CVP Operations Console and it is the server from which you serve your whisper files, then you need not specify the media server in your routing scripts. However, if you do not define a default media server, or if you store your whisper file on a server other than the default, then your scripts must include a Set Variable node that identifies that server.

To specify your media server, use the following settings in the Set Variable node:

- Object Type: Call.
- Variable: Must use the user.microapp.media\_server ECC variable.

- Value: Specify the HTTP path to the server. For example: “http://myserver.mydomain.net.” You must enclose the path in quotes.
- Alternately you can specify an IP address in place of a DNS. Include the listening port number if the media server web server listens on a port other than 80 (for HTTP) or 443 (for HTTPS).

### Specify Whisper File Locale and Application Directories

CVP uses a default storage directory for media files: <web\_server\_root>/en-us/app. To take advantage of this, Unified CCE call routing scripts automatically add “en-us/app,” to the server name when constructing HTTP requests for media files. For example:

- If the script node that defines the media server has a value of “http://myserver.mydomain.com” and...
- The script node that defines which audio file to play has a value of “en\_sales.wav,” then...
- The HTTP request for the file is automatically constructed as

http://myserver.mydomain.com/en-us/app/en\_sales.wav

If your whisper audio files are stored in a different locale directory, you must add a Set Variable node to your script that identifies the locale directory. Similarly, if your whisper files are stored in a different application directory, you must add a Set Variable node that identifies that directory.

#### *Specify Locale Directory*

Use these settings in the Set Variable node to specify your locale directory:

- Object Type: Call.
- Variable: Must use the user.microapp.locale ECC variable.
- Value: Specify the directory name. For example: “pt-br,” You must enclose the path in quotes.

#### *Specify Application Directory*

Use these settings in the Set Variable node to specify your application directory:

- Object Type: Call.
- Variable: Must use the user.microapp.app\_media\_lib ECC variable.
- Value: Specify the directory name. For example: to use a directory “wav\_files” in place of the default directory “app,” enter “wav\_files.” To use a sub-directory “wav\_files” “app,” enter “app/wav\_files.” You must enclose the path in quotes.

#### *Variable Length for Media Server Locale and Application Directory Variables*

If you do include Set Variable nodes for the media server, locale, or application directories, ensure that the values you set for them do not exceed the Maximum Length settings for their corresponding ECC variables.

For example, if you include a Set Variable node for the media server with a value of “http://mysubdomain.mydomain.co.uk,” the string is 33 characters long. Therefore, the Maximum Length setting for the user.microapp.media\_server ECC variable must be 33 or greater. If it is not, you must increase the Maximum Length setting. Otherwise, the server name is truncated in the HTTP request for the file and the file is not found. You configure ECC variables in the Unified CCE Configuration Manager at List Tools > Expanded Call Variables List.

## Test Whisper Announcement File Path

To test the path to the whisper file that you defined in your script variables, enter the complete URL into a browser. The .wav file should play. For example:

- If your script includes: default media server + default locale + default application directory + whisper.wav, then the path is “http://<default\_media\_server>/en-us/app/whisper.wav”
- If your script includes: http://my\_server.my\_domain.com + default locale + “app/wav\_files” + whisper.wav, then the path is “http://my\_server.my\_domain.com/en-us/app/wav\_files/whisper.wav”

## Other Script Settings That Are Required for Whisper Announcement

These additional settings are required for Whisper Announcement to work:

- Enable Target Requery on all script nodes that follow the WhisperAnnouncement variable and target an agent. These include Queue (to Skill Group or Precision Queue), Queue Agent, Route Select, and Select. If Target Requery is not enabled, the Whisper Announcement does not play.
- When you run an agent transfer or a conference script, use a SendToVRU, a TranslationToVRU, or a Run Script Request node before you target an agent.

## Fail-Safe Timeout for Whisper Announcement in Unified CCE

Unified CVP sends one message to Unified CCE each time a Whisper Announcement begins and a second message when the announcement ends. The time stamps from these messages are used to calculate Whisper Announcement data in Unified CCE reports.

If Unified CVP fails to send a Whisper Announcement end message to Unified CCE, the following occurs:

- Unified CCE cannot accurately calculate the whisper length, thus skewing report data.
- The agent cannot control the call (for example, put it on hold or transfer it) because these controls are disabled while a Whisper Announcement is playing.

To prevent this, Unified CCE has a Whisper Announcement timeout setting. The value for this setting represents the maximum Whisper Announcement play time that Unified CCE uses to calculate its report data.

The default is 20 seconds. This default is based on the default Whisper Announcement play time (specified in Unified CVP) of 15 seconds. The extra 5 seconds in the Unified CCE fail-safe timeout is a buffer against latency. If you modify the maximum Whisper Announcement play time in Unified CVP, modify the Unified CCE Whisper Announcement fail-safe timeout accordingly.

The Unified CCE Whisper Announcement fail-safe timeout value should be equal to or greater than the maximum Whisper Announcement play time setting in Unified CVP. Otherwise, Whisper Announcement play time in Unified CCE reports are under-reported.

To change the fail-safe timeout value, complete the following steps for the Unified CCE peripheral by using the PG explorer tool:

- 
- Step 1** In Unified CCE Configuration, select **Tools > Explorer Tools > PG Explorer**.
  - Step 2** Click **Retrieve** to return a list of PGs (Peripheral Gateways).
  - Step 3** Double-click the agent PG to expand it, and select the peripheral with client type **CUCM** or **UCCE system**.
  - Step 4** On the **Peripheral** tab, enter the following text in the **Configuration Parameters** field:

```
/WHSTMOUT <value in seconds>
```

**Step 5** Once you are finished, click **Save**.

## Whisper Announcement Sample Scripts

Unified CCE includes sample routing scripts that demonstrate Whisper Announcement. You can use them as learning tools and as models for your own Whisper Announcement scripts. They are the following:

- **WA.ICMS**—This script plays a Whisper Announcement.
- **WA\_AG.ICMS**—This script plays both a Whisper Announcement and an Agent Greeting to play on the same call flow.

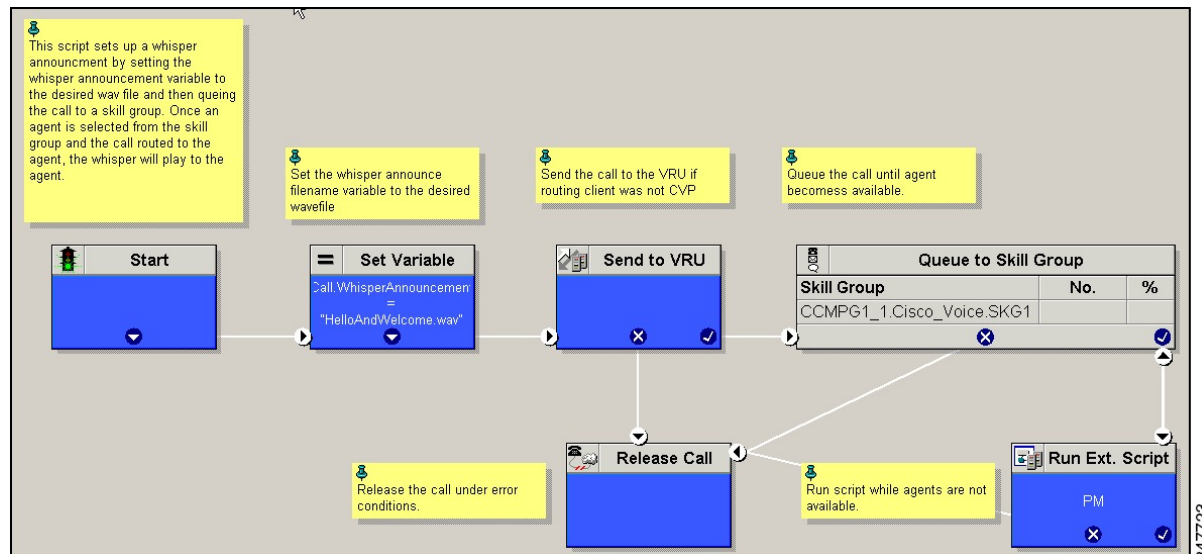
The script files are located in the `c:\icm\bin` directory. In Unified CCE Script Editor, they are installed to the application root directory.



**Note** To use these scripts you must have a default media server configured in Unified CVP, and have the Whisper file stored in the default location on the media server. For that reason, they do not include variables that specify the media server, locale, or application directories.

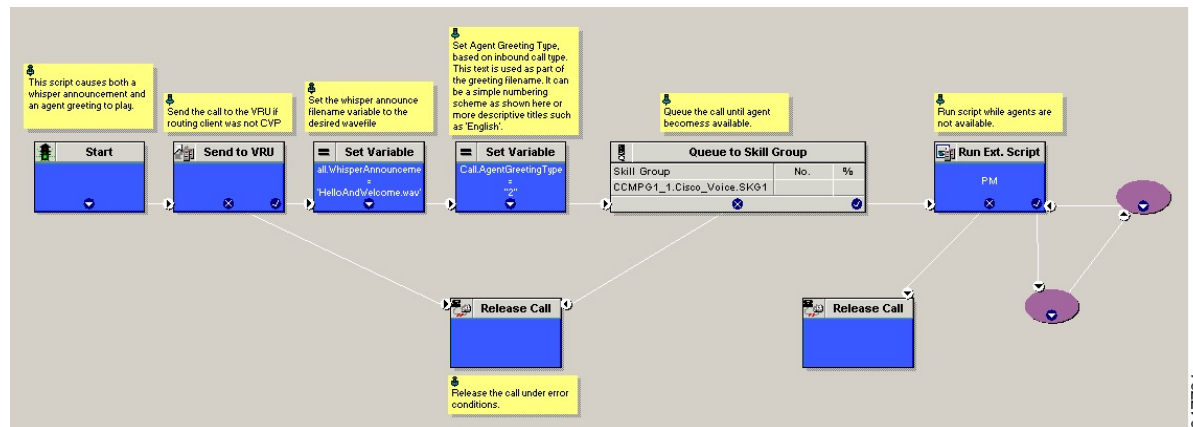
### WA.ICMS Script

This script sets up a Whisper Announcement by setting the Whisper Announcement variable to the desired wave file and then queuing the call to a skill group or Precision Queue. After an agent is selected from the skill group or Precision Queue and the call routed to the agent, the whisper plays to the agent.



### WA\_AG.ICMS Script

This script causes both a Whisper Announcement and an Agent Greeting to play.



347721

## Import Sample Whisper Announcement Scripts

To view or use the sample Whisper Announcement scripts, you must first import them into Unified CCE Script Editor. Follow this procedure to import the scripts:

**Step 1** Open Script Editor.

**Step 2** Select **File > Import Script** and select the first of the two scripts to import.

In addition to importing the script, Script Editor tries to map imported objects. Some objects that are referenced in the sample scripts, such as the external Network VRU scripts or the skill groups or Precision Queues, do not map successfully. You must create these maps manually or change these references to point to existing Network VRU scripts, skill groups, and Precision Queues in your system.

**Step 3** Repeat steps 2 and 3 for the remaining script.

## How Whisper Announcement Works

### Whisper Announcement Audio File

You store and serve your Whisper Announcement audio files from the Cisco Unified Contact Center Enterprise (Unified CCE) media server. This feature supports only the wave (.wav) file type. The maximum play time for a Whisper Announcement is subject to a timeout. Playback terminates at the timeout regardless of the actual length of the audio file. The default timeout is 15 seconds. In practice, you may want your messages to be much shorter than that, 5 seconds or less, to shorten your call-handling time.

### While a Whisper Announcement Is Playing

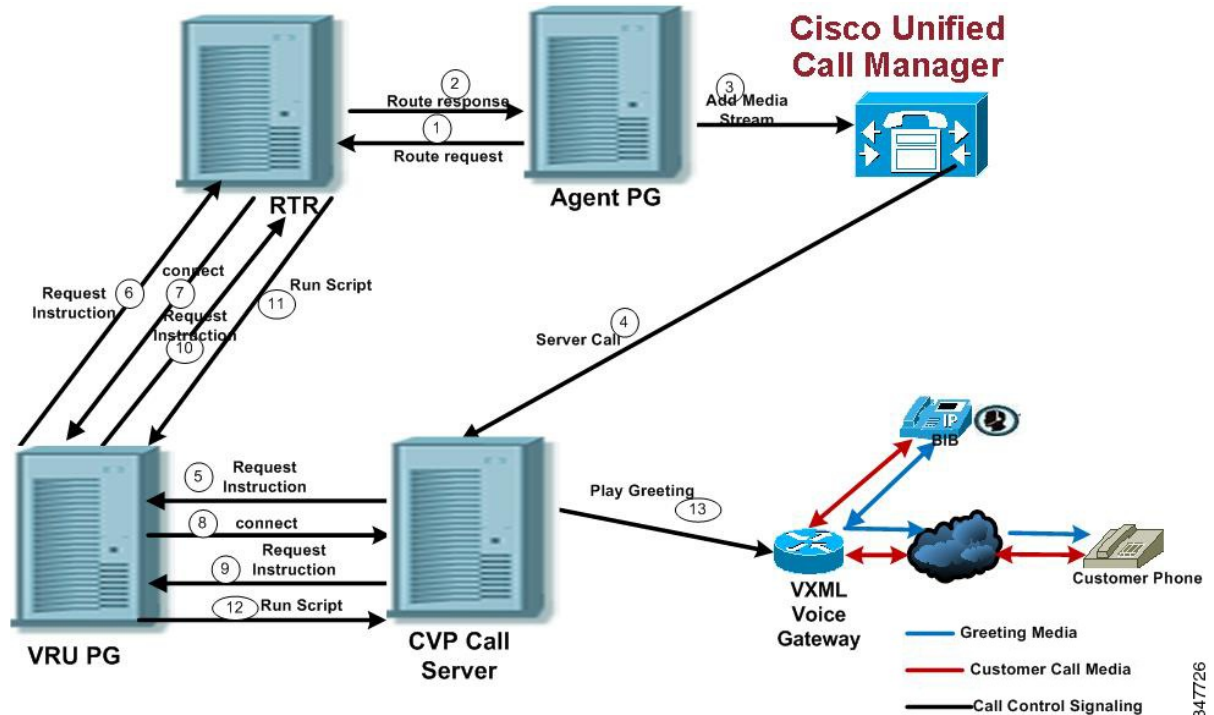
Only one Whisper Announcement can play for each call. While a Whisper Announcement is playing, you cannot put the call on hold, transfer, conference, or release the call, or request supervisor assistance. These features become available again after the whisper is complete.

## Whisper Announcement with Transfers and Conference Calls

When an agent transfers or initiates a conference call to another agent, the second agent hears an announcement if the second agent's number supports Whisper Announcement. In the case of consultative transfers or conferences, while the whisper plays, the caller hears whatever generally plays during hold. The first agent hears ringing. In the case of blind transfers, the caller hears ringing while the whisper announcement plays.

### Whisper Announcement Call Flow

Following is a Whisper Announcement call flow diagram accompanied by a description of the steps.



1. CVP receives a new call from the PSTN.
- 2 - 3. CVP sends the new call to the VRU PIM and the VRU PIM sends the new call to the Unified CCE router.
4. If an agent is available, the router reserves the agent.
- 5 - 6. The router sends a label with a whisper prompt to CVP.
7. CVP sends the call to Unified CM.
- 8 - 9. The agent receives and answers the call.
10. Unified CM sends the established event to the agent PIM. The agent PIM holds the event until the Whisper Announcement is done playing.
11. CVP tells the VXML gateway to play ringback to the caller and the Whisper Announcement to the agent. After the Whisper Announcement plays, CVP connects the agent to the customer and notifies Unified CCE.
12. The agent PIM gets notification that Whisper Announcement is complete and sends the established event to the agent desktop.

## Reporting and Serviceability

Whisper time is not specifically broken out in Unified CCE reports. In agent, skill group, and Precision Queue reports, the period during which the announcement plays is reported as Reserved agent state time. In the Termination Call Detail records, it is treated as Ring Time.

Serviceability for Whisper Announcement includes system events to indicate reasons for Whisper Announcement failures and counters to track the number of failed whisper events.

### Component Failure and Whisper Announcement

#### *Failure to Access CVP Media Server*

If the connection to the CVP media server fails, or if a requested whisper audio file cannot be found, the call proceeds without Whisper Announcement.

### Whisper Announcement in Agent Desktop Software

No configuration is needed to integrate Whisper Announcement with agent desktop software. While a whisper is playing, software on the agent desktop shows the call in the Ring state. Desk phones show the call in the Talking state.

### Using Agent Greeting with Whisper Announcement

You can use Agent Greeting along with the Whisper Announcement feature. Consider the following when you use them together:

- On the call, the Whisper Announcement always plays first before the greeting.
- To shorten your call-handling time, you may want to use shorter whispers and greetings than you might if you were using either feature by itself. A long whisper followed by a long greeting means a long wait before an agent handles a call.
- Usually, agents that use Whisper Announcement handle different types of calls: for example, "English, Gold Member, Activate Card, Spanish, Gold Member, Report Lost Card, English, Platinum Member, Account Inquiry." Ensure the greetings your agents record are generic enough to cover the range of customer calls they handle.







## APPENDIX **A**

# Reverse Proxy Automated Installer

---

- [Introduction](#), on page 301
- [Prerequisites](#), on page 301
- [Background Information](#), on page 302
- [Reverse-Proxy Installer](#), on page 303
- [Install and Operations](#), on page 306
- [Use configurations with custom NGINX installation](#), on page 323
- [Upstream component configuration specifics](#), on page 324
- [Security](#), on page 325
- [Frequently Asked Questions](#), on page 329

## Introduction

Download the reverse-proxy installer and associated artifacts from [https://software.cisco.com/download/home/283613135/type/284259728/release/12.6\(2\)](https://software.cisco.com/download/home/283613135/type/284259728/release/12.6(2))

The content in this chapter is provided as a guidance for customers to install and configure the reverse-proxy artifacts provided by Cisco. We ship an embedded Nginx based OpenResty® reverse-proxy.

For information on the deployment details and the pre-requisites required, see the [VPN-less access to Finesse desktop](#), on page 247 section.

We don't support install or configuration requests for custom reverse-proxy images and network configurations related issues. Queries that are related to this subject can be discussed on [Cisco community forums](#).

For older format of VPN-less Finesse, see [Cisco Finesse 12.6 ES07 Readme](#).

## Prerequisites

### Requirements

We recommend that you have knowledge of the following:

- Cisco Unified Contact Center Enterprise (Unified CCE) Release
- Cisco Finesse

- Linux administration
- Network administration and Linux network administration

## Components Used

The information in this section is based on the following software and hardware versions:

- Cisco Finesse - 12.6 ES07 and above
- Cisco Unified Intelligence Center - 12.6 ES03 and above
- Cisco Identity Service - 12.6 ES03 and above
- Cisco Unified CCE and Packaged CCE - 12.0 and above
- Cisco Cloud Connect-12.6(2)
- ADFS 3.0 for being used as IDP in SSO deployments



---

**Note** To use VPN-Less access to Finesse desktop feature, you must upgrade Finesse, Cisco IdS, and Cisco Unified Intelligence Center to releases mentioned above.

If you are using LiveData 12.6(1), you must upgrade LiveData to releases mentioned above.

Packaged CCE and Unified CCE 2k deployments must be on 12.6 version of CCE to support the coresident deployment of Livedata (LD) and Cisco Unified Intelligence Center.

---

## Background Information

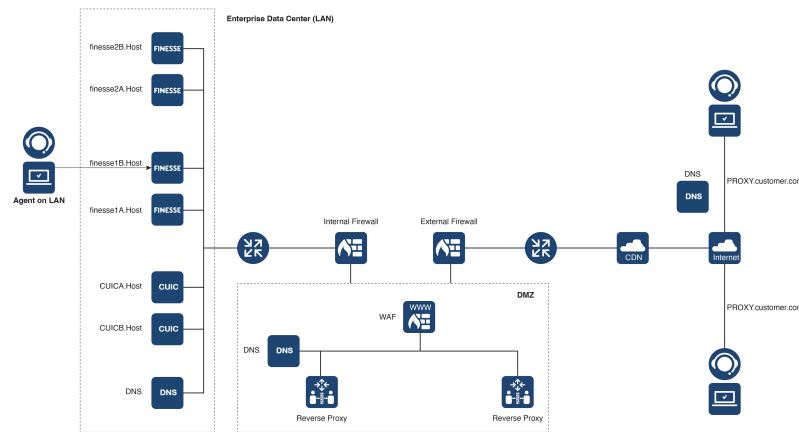
This deployment model is supported for the Unified CCE and Packaged CCE solutions.

Deployment of a reverse-proxy is supported (available from 12.6 ES07) as an option to access the Cisco Finesse desktop without connecting to a VPN. This feature provides the flexibility for agents to access the Finesse desktop from anywhere through the Internet.

To enable this feature, a reverse-proxy pair must be deployed in the Demilitarized Zone (DMZ).

Media access remains unchanged in reverse-proxy deployments. To connect to the media, agents can use Cisco Jabber over MRA solution or the Mobile Agent capability of Unified CCE with a Public Switched Telephone Network (PSTN) or mobile endpoint. The following diagram shows how the network deployment looks when you access two Finesse clusters and two Cisco Unified Intelligence Center nodes through a single HA pair of reverse-proxy nodes.

Concurrent access from agents on the Internet and agents who connect from LAN is supported as shown in the following image:



**Note** For more information on how to select an appropriate reverse-proxy that supports this deployment, see the section [Minimum and additional requirements](#) at *Security Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.6(1)*.

Before you read this section, it is suggested to refer to the [VPN-less access to Finesse desktop](#) section. Also, see the *Security Considerations for Mobile Agent Deployments* section in *Security Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.6(1)*.

## Reverse-Proxy Installer

The Reverse-Proxy Installer (referred to as Installer in this document) is an automated tool to make the reverse-proxy deployment for Cisco Unified Contact Center a simple and error free exercise.

This Installer replaces the older VPN-less Finesse configuration provided as part of the 12.6 ES 01 and ES07 releases. This required manual installation of the proxy along with editing of the provided rules for creating a VPN-less deployment.

The following are the Cisco Unified Contact Center solution components which are supported by the reverse-proxy Installer:

- Cisco Finesse
- Cisco Identity Service
- Cisco Unified Intelligence Center
- Cisco Unified Cloud Connect

### Installer Components

#### Reverse-proxy within container

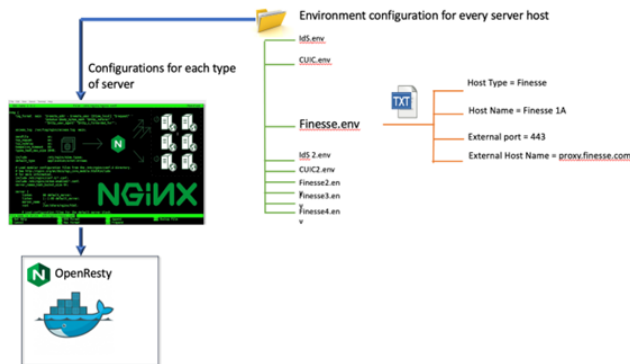
The Installer deploys the latest load-tested and qualified OpenResty® reverse-proxy binary, in a docker container and adds it within the required configurations automatically. (Follow the process in the sections below).

This makes it very easy to run the reverse-proxy configuration that is required to support the VPN-less infrastructure. This simplifies the deployment immensely, without requiring compilation or the knowledge of NGINX configuration. You don't need to know how to compile or install the open source NGINX.

Containerized proxy instances are also more secure as it is locked down and provides an additional barrier for an intruder to overcome compared to a proxy process running on a bare metal operating system.

### Proxy Configuration Environment Files and Templates

The proxy configuration is split into environment configuration and proxy rule configurations is also known as templates.



The simple and unique environment values which differentiate each upstream component server is collated within the respective environment files, with one file for each upstream component server. These are automatically combined into the proxy rules for each unique type of upstream component server (For example: Cisco Finesse, Cisco Identity Service, and so on) by the Installer. These and are then pushed into the OpenResty® NGINX proxy which then proceeds to deploy these rules.

This allows easy instantiation of any number of supported upstream component server hosts as required by adding new environment files corresponding to new servers.

The proxy configuration rules, known as rule templates, contain the necessary NGINX rules to access the server and you don't have to understand or change them.

This also makes Installer upgrades easy as the environment files containing the configurations are rarely changed and can be persisted through multiple Installer changes without requiring much NGINX expertise.

#### Sample environment files

The Installer archives come with a sample environment that can be used as a starting point to create a new VPN-less Finesse deployment.

Each file the Installer contains is an environment for a unique type of upstream host natively supported by the configurations or reverse-proxy rules provided, such as Finesse, Unified Intelligence Center and Cisco IdS.

The administrator should clone this directory and create multiple copies of each environment corresponding to each upstream component host which has to be exposed via the proxy and supply this directory location to the Installer which will then proceed to instantiate each host configuration based on the supplied parameters contained in the environment file.

Reverse Proxy Installer components	Directory/ File Name	Description
Reverse proxy instance	<i>reverse-proxy-openresty-container/</i>	Contains the docker container image that is used to create the container instance. This contains the OpenResty® NGINX proxy and other dependent libraries and modules  <b>OpenResty® version packaged:</b> Latest CentOS version 7 based OpenResty® available in the docker hub.
Component Configuration Templates	<i>reverse-proxy-openresty-configs/</i>	Contains the OpenResty® configuration templates.  These templates are used to generate final OpenResty® configurations from provided deployment configuration data.
Host OS configurations:	<i>reverse-proxy-os-configs/</i>	These templates are used to generate the final OpenResty® configurations from the deployment configuration data provided.  Contains the OS configurations for hardening the host. CentOS version 7 is the only supported OS.  You must manually install the OS configurations using the <code>install_os_settings.sh</code> that is available in this directory.  <b>Note</b> The OS configurations are tested with OpenResty® version 1.19. These configurations are expected to work with other distributions. You may need to make some minor updates as required.
Installer configuration	<i>installer.env</i>	Contains the configuration data for the reverse-proxy Installer.
Proxy configuration	<i>sample_envs/</i>	Contains the sample <code>env</code> configuration data for reference. Use this sample <code>env</code> when you are preparing the configuration data for your deployment.

Reverse Proxy Installer components	Directory/ File Name	Description
Launcher scripts	<i>proxy_launcher.sh</i>	Launcher script to perform the <b>start stop reload clear_cache</b> operations for a given Installer instance.
version.txt:		Contains Installer versions.  Reverse-proxy Installer creates all the configurations afresh on every restart and no configuration is retained. Any additional changes made to the existing proxy configurations are lost after the restart.

## Upgrade notes for 12.6(1) ES01-7 based reverse proxy configurations

The configuration formats have been modified with the new Installer-based configuration and can't be reused as is. The information contained, however, can be easily extracted and plugged into the new Installer configuration, and the format will not be changed further.

The CLI configurations and proxy-map data need not be altered. However, as previously described, the manner in which the upstream component server hosts and their associated configurations are provided to the reverse-proxy instance has now changed. For more information, see the *Environment Files and Templates* section in [Reverse-Proxy Installer, on page 303](#)

The following are some important points to consider when you upgrade your reverse-proxy instance using the automated Installer:

- The data required in the component host environment will match the individual values replaced in the template configurations using the `## Must-Change` notations from the older configurations. This can be used as a reference to fill the data if required.
- `Tmpfs` is not used in the new Installer, and earlier configurations that were run with "`tmpfs`" can be ignored. However, disk subsystem slowness can impact the proxy performance and needs to be efficient.

# Install and Operations

## Setup reverse-proxy

To setup the reverse-proxy server, refer to the following sections:

### Related Topics

[Proxy Hardware requirements](#), on page 307

[Prepare Host](#), on page 307

[Install the reverse proxy Installer package](#), on page 308

[Configure Host OS](#), on page 308

[Configure proxy hardware resources and other critical runtime options](#), on page 309

[Configure SSL certificates](#), on page 309

[Configure the Mapping File](#)

[Configure deployment environment configurations](#), on page 315

## Proxy Hardware requirements

The following are the hardware requirements to set up a reverse-proxy server for a 2K cluster. This includes Cisco Finesse, Cisco Identity Server (IdS), Cisco Unified Intelligence Center, Live Data, Enterprise Chat and Email, and Cisco Cloud Connect:

- CPU: 2vCPU for 2000 agents and 4vCPU for 4000 agents Deployment.
- Memory: 8 GB
- Disk: 80 GB
  - Cache disk space requirements for specific components:
    - **Finesse: 3 GB for one upstream**
    - **CUIC: 200 MB for one upstream**
    - **IdS: There's nothing cached.**
- Ethernet interfaces must be gigabit speed and connected to gigabit ethernet switches. 10/100 ethernet isn't supported.




---

**Note** Disk slowness can hamper the proxy performance. Please monitor the solution to ensure that the disk has adequate IO throughput.

Running the linux command `dd if=/dev/zero of=/root/junk bs=2k count=1000 oflag=dsync` should show a minimum of 5 MB per second of throughput and completion time of less than 0.3 seconds to write the data out.

---

## Prepare Host

Steps to prepare the host are as follows:

**Step 1** Install the latest build of CentOS Linux 7.x (7.9 or later).

**Step 2** To Install the **envsubst utility**, run the command `yum install gettext`.

**Step 3** Install the Docker. For instructions, see the Docker documentation at <https://docs.docker.com/get-docker/>

**Note** Uninstall podman on CentOS or RHEL. If already installed the podman conflicts with the Docker installation. Run the `yum erase podman buildah` command to uninstall the podman.

**Step 4** Perform the post-installation steps to manage the Docker. For instructions, see the Post-installation steps for Linux section at <https://docs.docker.com/engine/install/linux-postinstall>.

- Step 5** Run the **yum install logrotate -y** command to install **logrotate** on the host.
- Step 6** Run the following commands to uninstall or stop the firewall daemon service on CentOS:
- **sudo systemctl stop firewalld**
  - **sudo systemctl disable firewalld**
  - **sudo systemctl mask --now firewalld**
- Step 7** Run the following commands to install the iptables service on CentOS:
- **sudo yum install iptables-services -y**
  - **sudo systemctl start iptables**
  - **sudo systemctl enable iptables**

---

## Install the reverse proxy Installer package

To install the package:

- 
- Step 1** Download or copy the Installer zip on the host.
- Step 2** Extract the archive (.zip) to the location where you need the Installer to be running from.
- 

## Configure Host OS

The following are the OS hardening configurations for the reverse-proxy host that are included in the `Installer/reverse-proxy-os-configs/` folder:

- Kernel hardening configurations that is **sysctl** configurations
- Logrotate config
- CentOS version 7

The Installer script is provided to install the required configurations automatically. Various options can be provided in the script to control the installation and configuration.

Run the **install\_os\_settings.sh** script with the required options. The different options are as follows:

```
USAGE: ./install_os_settings.sh [OPTIONAL_ARGS]
OPTIONAL_ARGS: -k -l -i -p <source-ip1> -p <source-ip2> ... -s <interface1> -s <interface2>
... -r <interfacel:source-ip1> -r <interfacel:source-ip2> -r <interface2:source-ip1> ...
-k: configure kernel hardening
-l: configure logrotate for given log directory
-i: configure iptables
-p: allowed source ip for ICMP ping messages. By default ICMP ping is blocked for all hosts.
This option is ignored if -i or iptables configuration option is not given
-s: network interface name to allow SSH access to. By default ssh access is blocked for all
hosts. This option is ignored if -i or iptables configuration option is not given
-r: disable rate limits for a source-ip on an interface. Provide value as INTERFACE:SOURCE_IP.
By default rate limits applies for all. This option is ignored if -i or iptables
configuration option is not given
```



```
Example usage: ./install_os_settings.sh -k -l ~/reverse_proxy/proxy25.autobot.cvp/logs -i
-p allowed.host.for.ping.1 -p allowed.host.for.ping.2 -s ssh_interface1 -s ssh_interface2
-s -s ssh_interface3 -r interface1:host1 -r interface1:host2 -r interface2:host1
```



**Note** If you're installing the reverse-proxy to proxy a specific component, for example Cloud Connect, you must not install the iptable rules for other components. As an administrator, you must select the component rules and the port values to be installed and configured for the iptables. The port value may change depending on the deployment. The script doesn't control the customization of iptable rules.

## Configure proxy hardware resources and other critical runtime options

The Installer script `installer/proxy_launcher.sh` that is used to deploy the reverse-proxy takes the following input arguments:

- `installer.env`: Path to `installer.env` file containing Installer configuration data.
- `proxy_env_dir/`: Path to `proxy_env_dir/` file containing proxy configuration data.



**Note** The `installer.env` file contains properties to configure Installer options. The sample file is provided in the Installer package. Use it as a reference to prepare the actual configuration.

The steps to configure the proxy hardware resources and other runtime options are as follows:

- Step 1** Copy the sample file `installer.env` to any other directory, and rename it. If there are multiple proxy instances running on the same host, use the proxy name or the customer name that maps to a particular proxy instance.
- Step 2** Modify the installer options as required. Options are included in the configuration file with their intended purpose.

## Configure SSL certificates

The environment configuration file for each component includes an **SSL CONFIG** section that has configurations to set up the SSL connector for the component. In addition, the configurations are used to configure the following:

- Either custom certificates that you have generated manually or certificates that the Installer has generated can be used for reverse proxy.
  - If you choose to use the custom certificate that is either CA-signed or self-signed, which you've generated, place the certificate inside the `ssl` directory mentioned in the option `HOST_SSL_VOL` (defaults to `${HOST_WORKING_DIR}/ssl`).
  - You can also allow the Installer to generate the self-signed certificate. When starting the `Installer/proxy_launcher.sh` script, set the **CREATE\_SELF\_SIGNED\_SSL\_CERT** option to true. For more information, see [Configure proxy hardware resources and other critical runtime options](#). If the required certificate and key names aren't present in the `ssl` directory, the Installer generates the certificate and includes it in the `ssl` directory mentioned in the option `HOST_SSL_VOL` (defaults to `${HOST_WORKING_DIR}/ssl`). The Installer doesn't overwrite the existing files.

These certificates are used to configure the SSL connector for individual component configurations.

- Supported TLS protocol versions
- Supported TLS ciphers
- SSL session cache size and timeout
- SSL stapling configurations
- Mutual TLS authentication for upstream connections: By default, this option is disabled. To enable this option, modify the following configurations:
  - Set the `NGX_PROXY_SSL_VERIFY` option to "on"
  - `NGX_PROXY_SSL_TRUST_CERT` → Trust file containing certificate of upstream being proxied. Certificate from this file will be verified by NGINX against what is provided by upstream during the TLS handshake.




---

**Note** Self-signed certificates are to be used only for testing and development purposes and CA-signed certificates are mandatory for production deployments. If the certificate received from the CA isn't a certificate chain containing all the respective certificates, compose all the relevant certificates into a single certificate chain file.

---

## Create CA-signed Certificates

To create a CA-signed certificate, perform the following steps:

---

**Step 1** Create a working directory under the proxy installer and navigate into it, using the following commands:

```
mkdir sslwork
cd ./sslwork
```

**Step 2** Create an OpenSSL configuration file using the following command:

```
nano sslcert.cnf
```

**Step 3** Modify the OpenSSL configuration file to add the below contents in the configuration file and save:

The following are the contents of a sample configuration:

**Note** The Subject Alternative Name (SAN) of a DNS server allows for the specification of multiple alternate names. This is particularly beneficial when you want to use multiple Fully Qualified Domain Names (FQDNs) under a single certificate. Ensure that you update the content as required for your environment.

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req

[req_distinguished_name]
countryName = Country Name (2 letter code)
countryName_default = US
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = North Carolina
```

```

localityName = Locality Name (eg, city)
localityName_default = Research Triangle Park
organizationName = Company Name
organizationName_default = Cisco Systems Inc
organizationalUnitName = Organizational Unit Name (eg, section)
organizationalUnitName_default = Cisco TAC
commonName = mddesktop1.cisco.com
commonName_max = 64

[v3_req]
Extensions to add to a certificate request
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = desktop1.cisco.com
DNS.2 = cuic1.cisco.com
DNS.3 = sso1.cisco.com
DNS.4 = digitalrouting.cisco.com

```

**Step 4** Save and exit the configuration file.

**Step 5** To create a certificate signing request with Open SSL, use the following command:

```
openssl req -out reverseproxy.csr -newkey rsa:2048 -nodes -keyout reverseproxy.key -config sslcert.cnf
```

Enter the details of the configuration as shown below in the sample prompt:

```

Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'reverseproxy.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) [US]:US
State or Province Name (full name) [North Carolina]:Illinois
Locality Name (eg, city) [Research Triangle Park]:Chicago
Company Name [Cisco Systems Inc]:
Organizational Unit Name (eg, section) [Cisco TAC]:
mddesktop1.cisco.com []:desktop1.cisco.com

```

**Step 6** After you generate the Certificate Signing Request (CSR) file (reverseproxy.csr), do the following:

- a. Submit the CSR to the Certificate Authority (CA) for signing. The CA will verify the information in the CSR and issue the certificate.
- b. Download the signed certificate in Base64 format when the certificate is ready.

**Step 7** Copy the contents of the certificate back to the reverse proxy in the `sslwork` directory into a file name `reverseproxy.crt`

**Note** Ensure that the reverse proxy installer is stopped.

**Step 8** Modify the `installer.env` file you are using for your proxy to change `CREATE_SELF_SIGNED_SSL_CERT=false`

**Step 9** To ensure your proxy setup works correctly, you need to copy the certificate and private key to the appropriate working directory. Follow the below steps:

- a. Ensure that the certificate (`reverseproxy.crt`) and private key (`reverseproxy.key`) are located in the source directory: `~/proxy/sslwork/`.
- b. The destination directory where these files need to be copied is: `~/proxy/work/container/ssl/`. If this directory does not exist, create it using the following command: `mkdir -p ~/proxy/work/container/ssl/`
- c. To copy the certificate and private key to the working directory for your install, use the following commands:
 

```
cp ~/proxy/sslwork/reverseproxy.crt ~/proxy/work/container/ssl/reverseproxy.crt
cp ~/proxy/sslwork/reverseproxy.key ~/proxy/work/container/ssl/reverseproxy.key
```

- Note** When deploying the reverse proxy, the location where the proxy runs depends on the configuration in the `installer.env` file. Ensure that the SSL files are in the `ssl` directory within the respective working directory.
- For default configuration, the proxy runs in `~/reverse_proxy/${CONTAINER_NAME}` and the SSL files must be placed in `~/reverse_proxy/${CONTAINER_NAME}/ssl`
  - For custom configuration, the proxy runs in `/usr/local/proxy/work/${CONTAINER_NAME}` and the SSL files must be placed in `/usr/local/proxy/work/${CONTAINER_NAME}/ssl`

**Step 10** Start the proxy and validate that the new certificate is being used.

---

### Create Custom Diffie-Hellman Parameter

1. Create a custom Diffie-Hellman parameter by using the following commands:

```
openssl dhparam -out /usr/local/openresty/nginx/ssl/dhparam.pem 2048
chmod 400 /usr/local/openresty/nginx/ssl/dhparam.pem
```

2. Modify the server configuration to use the new parameters in the file `/usr/local/openresty/nginx/conf/conf.d/ssl/ssl.conf` by using the following command:

```
ssl_dhparam /usr/local/openresty/nginx/ssl/dhparam.pem;
```

### Enable OCSP Stapling



- Note** To enable the Online Certificate Status Protocol (OCSP) stapling, the server should be using a CA-signed certificate. Also, the server should have access to the CA which signed the certificate.

Use the following parameters to configure stapling **NGX\_SSL\_STAPLING & NGX\_SSL\_STAPLING\_VERIFY** on the respective component's `env` files. By default, they are set to **"off"**.

---

### Configure mutual TLS authentication between reverse-proxy and components

The **mutual TLS (mTLS)** is a standard security requirement for connections established from DMZ into the data center. For more information, see Nginx CIS benchmarks-<https://www.cisecurity.org/benchmark/nginx>

For mTLS, both the server and client must be pre-configured with mutual information about each other. Also, the mutual certificates must be properly verified. So the term **"mutual TLS (mTLS)"**. A properly configured proxy server will be able to circumvent TCP rate limits and provide the client IP to the server for logging

purposes. As a result, it's critical to verify the proxy identity before connecting as a reverse-proxy. For security reasons, by default this feature is turned on.

This requires the upstream component certificates to be made available to the proxy and vice-versa. By default, reverse-proxy establishes verified TLS connections to the upstream server and it's the proxy verification at the client which is optional. So, this must be enabled at the upstream client server.

### Enabling mutual TLS

The mTLS must be enabled at the upstream component servers using the provided CLI.

Use the **utils system reverse-proxy client-auth enable** CLI to enable proxy certificate verification at the upstream component server.

After running the CLI, upload the proxy SSL certificate corresponding to the reverse-proxy hostname that is used to connect to the same server. This can be used to verify TLS connections when the reverse-proxy attempts to establish an upstream connection.

## Configure the Mapping File

Refer to [Host-Mapping file for network translation, on page 255](#).

### Use reverse-proxy as the Mapping File server

The following steps are required only if the reverse-proxy is also used as the proxy mapping file host:

1. Configure the reverse-proxy hostname in the domain controller used by the Finesse, Cisco Unified Intelligence Center, and IdS hosts such that its IP address can be resolved.
2. Upload the generated OpenResty® Nginx signed certificates on both the nodes under `tomcat-trust-of-cmplatform` and restart the server.
3. Update the **Must-change** values in `<NGINX_HOME>/html/proxymap.txt`.
4. Reload OpenResty® Nginx configurations with the `nginx -s reload` command.
5. Use the `curl` command to validate if the configuration file is accessible from another network host.

### CentOS 8 Kernel Hardening

If the operating system is CentOS 8 and the installations use a dedicated server for hosting the proxy, harden the kernel by using the following `sysctl` configurations:

```
Configurations for kernel hardening - CentOS8. The file path is /etc/sysctl.conf
Note that the commented configurations denote that CentOS 8's default value matches
the recommended/tested value, and are not security related configurations.

Avoid a smurf attack
net.ipv4.icmp_echo_ignore_broadcasts = 1
Turn on protection for bad icmp error messages
net.ipv4.icmp_ignore_bogus_error_responses = 1

Turn on syncookies for SYN flood attack protection
net.ipv4.tcp_syncookies = 1

Turn on and log spoofed, source routed, and redirect packets
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1

Turn off routing
```

```
net.ipv4.ip_forward = 0
net.ipv4.conf.all.forwarding = 0
net.ipv6.conf.all.forwarding = 0

net.ipv4.conf.all.mc_forwarding = 0
net.ipv6.conf.all.mc_forwarding = 0

Block routed packets
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
net.ipv6.conf.all.accept_source_route = 0
net.ipv6.conf.default.accept_source_route = 0

Block ICMP redirects
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0

Filter routing packets with inward-outward path mismatch(reverse path filtering)
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1

Router solicitations & advertisements related.
net.ipv6.conf.default.router_solicitations = 0
net.ipv6.conf.default.accept_ra_rtr_pref = 0
net.ipv6.conf.default.accept_ra_pinfo = 0
net.ipv6.conf.default.accept_ra_defrtr = 0
net.ipv6.conf.default.autoconf = 0
net.ipv6.conf.default.dad_transmits = 0
net.ipv6.conf.default.max_addresses = 1
net.ipv6.conf.all.accept_ra = 0
net.ipv6.conf.default.accept_ra = 0

Backlog - increased from default 1000 to 5000.
net.core.netdev_max_backlog = 5000

Setting syn/syn-ack retries to zero, so that they don't stay in the queue.
net.ipv4.tcp_syn_retries = 0
net.ipv4.tcp_synack_retries = 0

Max tcp listen backlog. Setting it to 511 to match nginx config
net.core.somaxconn = 511

Reduce the duration of connections held in TIME_WAIT(seconds)
net.ipv4.tcp_fin_timeout = 6

Maximum resources allotted
fs.file-max = 2019273
kernel.pid_max = 4194304
net.ipv4.ip_local_port_range = 32768 60999

TCP window size tuning
net.ipv4.tcp_window_scaling = 1
net.core.rmem_default = 212992
net.core.rmem_max = 212992
net.ipv4.tcp_rmem = 4096 87380 6291456
net.ipv4.udp_rmem_min = 4096
net.core.wmem_default = 212992
net.core.wmem_max = 212992
```

```
net.ipv4.tcp_wmem = 4096 16384 4194304
net.ipv4.udp_wmem_min = 4096
vm.lowmem_reserve_ratio = 256 256 32 0 0
net.ipv4.tcp_mem = 236373 315167 472746

Randomize virtual address space
kernel.randomize_va_space = 2

Congestion control
net.core.default_qdisc = fq_codel
net.ipv4.tcp_congestion_control = cubic

Disable SysReq
kernel.sysrq = 0

Controls the maximum size of a message, in bytes
kernel.msgmnb = 65536

Controls the default maximum size of a message queue
kernel.msgmax = 65536

Controls the eagerness of the kernel to swap.
vm.swappiness = 1
```

Reboot the server after you make the recommended changes.

## Configure deployment environment configurations

The environment configuration data is the main input that the Installer needs to generate the actual proxy configurations from the templates. There is a sample environment data, `Installer/sample-envs/` that is provided within the `installer.zip`. The sample environment data contains up-to-date reference **envs** for all supported components. The following are the contents of the sample **env** directory:

```
installer/sample_envs/
|- core.env
|- dirs.env
|- finesse.env
|- ids.env
|- cuic.env
|- livedata.env
|- chat.env
|- cloudconnect.env
```

These property files are divided into three categories:

- The `core.env` : **Mandatory**: File containing OpenResty® NGINX core configurations data. This is required to configure OpenResty® NGINX core configurations.

This environment configuration file contains data for *reverse-proxy core configuration template files*. Core configuration files include details specific to the running NGINX instance and is applied generally to all the components until or unless it is overridden at the component level.

The core configuration template file includes:

- `cache.conf`: Template file containing cache configurations
- `common.conf`: Template file containing common configurations
- `logging.conf`: Template file containing logging configurations
- `maps.conf`: Template file containing constants and other variable configurations
- `rate_limit.conf`: Template file containing rate limit configurations

- `static.conf`: Template file containing static configurations
- `ssl_config.conf`: Template file containing ssl connector configurations for common server blocks such as status endpoint and static files endpoint

Values provided in the `core.env` file is used to substitute all the place holders in the above files.

- `dirs.env`: **Mandatory**: File containing various OpenResty® NGINX directory paths as per OpenResty® installation. This is required to configure directory paths in the configuration templates.

This environment data contains information regarding the OpenResty® installation directory structure. The default values are included as per the default OpenResty® installation.

```

• # Directory location for various openresty folders required to
• # configure configurations accordingly.
•
• # Home directory for openresty nginx installation
NGX_HOME="/usr/local/openresty/nginx"
• # Openresty directory containing static resources
NGX_HTML_DIR="${NGX_HOME}/html"
• # Openresty directory containing lua resources
NGX_LUA_DIR="${NGX_HOME}/lua"
• # Cache directory where various resources for components will be cached
NGX_CACHE_DIR="${NGX_HOME}/cache"
• # Openresty directory containing SSL resources like certs, keys etc.
NGX_SSL_DIR="${NGX_HOME}/ssl"
• # Openresty directory where openresty logs will be put
NGX_LOG_DIR="${NGX_HOME}/logs"
• # Openresty directory containing NGINX configurations - core configs, components
 configs etc.
NGX_CONF_DIR="${NGX_HOME}/conf"

```

- `component envs`: **Optional**: Files containing configuration data for proxied solution components such as Finesse, Cisco IdS, Unified Intelligence Center, Live Data, Cisco IM&P, and so on. One environment configuration file must be created per upstream solution component that is being proxied.

Some properties are mandatory in component environment config files, without which the configurations are generated for those components. The properties are as follows:

- `TEMPLATE_TYPE`: Defines which type of upstream component is being configured, so that the correct templates can be referred to generate the actual configurations. The value can be `finesse`, `ids`, `cuic`, `livedata`, or `chat`
- `NGX_COMP_DIR_NAME`: Defines the output directory where configuration files for the component will be generated. The final output location for the files will be `./configs_out/conf/components/<NGX_COMP_DIR_NAME>/. Also, this directory is used to form the file including the paths in various configuration files of the component.`




---

**Note** Ensure that each environment configuration file has a unique output directory name (`NGX_COMP_DIR_NAME`) and hostname (`NGX_COMP_HOSTNAME`).

---

Other properties are different for different components and the default values for all the components are provided in their respective `env` files.

The following are the steps to configure these options:



- 
- Step 1** Copy the **installer/sample-envs/** directory and the **installer/installer.env** file to a separate directory and modify it.
- Step 2** After the files are copied to a new directory at **~/proxy\_config/proxy\_instance\_name**, rename the files such that they can be mapped to a running proxy instance.
- Step 3** Modify the **core.env** file for OpenResty® configuration.  
For most of the options the default values can be used. However, for some of the options you must change the values as per the deployment.
- Step 4** Validate all the property values given in the **core.env** file.  
**Note** Do Not Rename this file.
- Step 5** Provision is available in the **dirs.env** file to deploy the configurations on a custom NGINX installation. If you choose to use the Installer as is, avoid modifying the **dirs.env** file.  
**Note** Do Not Rename this file.
- Step 6** Retain the **.env** files of components that you require and delete the remaining files.  
For example, for a proxied Finesse cluster running on non-ss0 mode with Live Data and Unified Intelligence Center reports, you must retain the **finesse.env**, **cuic.env**, and **livedata.env** files. You must delete the remaining files **chat.env**, **ids.env** and **cloudconnect.env**. The remaining **.env** files present in the directory is processed by the Installer.
- Step 7** Rename the component **.env** files as per their hostnames, as it is easy to identify them. Modify the component **.env** file values as per the requirement of the deployment. Generally, you can modify only the hostname values as per the deployment and retain the default values for the other options.
- Step 8** Property description in all the **.env** files should be self-explanatory and it should provide the information regarding the purpose and the usage of a given property. Also, **Do not modify any property name** or **Delete any property from the .env file**.  
**Note** All the properties are essential for the Installer, and in case of any missing property, the Installer will not be able to open the proxy instance. Override or change the default values only for the required properties.
- 

## Add or Remove the Unified CCE solution component

Any number of Unified CCE solution components can be proxied through the installer.

To add or remove any of the component proxies, the corresponding component environment configuration file must be available in the **env** directory. The Installer generates the proxy configurations for all the required components from the beginning as per the contents in the **env** directory.

## Configure Auth URL for components

The component configuration file has an option to redirect to Finesse nodes' authorization url (auth url) to perform the authentication at the proxy. Configure this for the component configuration files as per the deployment, to redirect them to the same cluster Finesse node which contains user data. For more information, see `NGX_AUTH_URL=` <https://reverseproxy.host.domain:8445/finesse/api/UserAuth>.

## Multi-cluster deployment

The reverse-proxy installer supports Unified CCE or Packaged CCE that are larger than 2k deployments. These deployments must expose multiple Finesse nodes to the Agents over the internet and needs extra CUIC nodes.

These additional nodes are supported by multiple pairs of reverse-proxy or by configuring the extra nodes. The extra nodes work as added upstream servers on the same proxy pair using a single HA pair of the reverse-proxy.

Adding more upstream servers is as simple as creating a new environment (env) file. The **env** file corresponds to the upstream server type and modify specific details such as its hostname.

For example, a deployment containing three Finesse clusters must have three Finesse **env** files in the **env** directory as follows:

- Side A proxy **env** directory:
  - finesse1a.env
  - finesse2a.env
  - finesse3a.env
- Side B proxy **env** directory:
  - finesse1b.env
  - finesse2b.env
  - finesse3b.env

You can extend the same for multiple clusters of other components as required.

Consider multi-cluster deployments for the port and the hostname management. The prerequisite for the installer to communicate through proxy is that the hostname and the port pair are unique for a component across all other components.

To plan the hosts and ports used in the individual component **env** files, see the [Port management](#) section.

## Starting the reverse-proxy

To start the proxy instance from the Installer, we must open the script with the required `installer.env` file from the `proxy_env_dir/` path as input arguments. Check the following steps:

```
USAGE: ./proxy_launcher.sh [options...] (start|stop|reload|clear_cache)
Options: -e <ENV-DIR> -i <INSTALLER-ENV-FILE1> -i <INSTALLER-ENV-FILE2> ...
INSTALLER-ENV-FILE: Mandatory : Installer env files ... Multiple files can be provided to
override base env
ENV-DIR: Mandatory for start, Optional for other actions : Reverseproxy environment config
data directory
Example usage: ./proxy_launcher.sh -e /path/to/env/dir -i /installer/env/1 -i
/installer/env/override/1 -i /installer/env/override/2 start
```

When the command **start** is initiated, the Installer performs the following:

- 
- Step 1** Validates if the input arguments are correct, directories and the mandatory files are available.
  - Step 2** Creates the required working directory, and volume mounts on the host as per the **Installer.env** file entries.
  - Step 3** Generates the required OpenResty® configurations and runs the command `run.sh` inside the `reverse-proxy-openresty-configs/` directory.
  - Step 4** Modifies the generated configurations to their respective directories inside the working directory.

- Step 5** Creates the self-signed SSL certificate for the reverse-proxy to use it if necessary. Configures it in the `installer.env` file.
- The SSL certificate is generated only if there's no other file with the same filename in the directory or no other file is overwritten.
- Note** Load docker image is provided as part of the Installer. This can be overridden from the `installer.env` file. You can also choose to load a different image.
- Step 6** It runs the container with the required arguments as per the Installer configuration data.

## Serviceability

### Bootstrap checks or validations

The Installer validates the configurations that are provided through the `.env` files and stops the deployment if it identifies certain common errors. This is done to prevent lengthy debugging on the configurations provided, which can be easily identified in the validation phase.

The following are the errors which are currently identified and reported during the validation phase.

Scenario	Sample Error Message
An unknown template type is mentioned on the <code>.env</code> file which isn't known to the Installer.	[ERROR]: Unknown TEMPLATE_TYPE cuic_1230 found in file cuic.env. Exiting.
The <code>.env</code> file doesn't contain the property <code>TEMPLATE_TYPE</code> which identifies the type of upstream component.	[ERROR]: TEMPLATE_TYPE variable missing in file cuic.env. Exiting.
A particular variable isn't present in the primary <code>.env</code> file for the template type. However, it's available in a particular <code>.env</code> file that is being processed in the custom <code>env</code> directory.	[ERROR]: Below unused variable found in <code>./sample_envs/</code> . Exiting. <b>NGX_FIN_TEST_HOSTNAME</b>
The <code>NGX_LOAD_BALANCER_IPS</code> contains values which can't be parsed as a valid IP.	[ERROR]: <b>NGX_LOAD_BALANCER_IPS</b> should contain only IP addresses. Exiting.
The <code>NGX_LOAD_BALANCER_REAL_IP_HEADER</code> is configured but the <code>NGX_LOAD_BALANCER_IPS</code> isn't configured.	[ERROR]: <b>NGX_LOAD_BALANCER_REAL_IP_HEADER</b> should be configured only when <b>NGX_LOAD_BALANCER_IPS</b> is configured. Exiting.
The <code>NGX_LOAD_BALANCER_REAL_IP_HEADER</code> is empty but the <code>NGX_LOAD_BALANCER_IPS</code> is configured.	[ERROR]: <b>NGX_LOAD_BALANCER_REAL_IP_HEADER</b> is empty. It should contain header details when <b>NGX_LOAD_BALANCER_IPS</b> is configured, Exiting.
One of the mandatory variables isn't configured. (Currently, limited to host and port of the upstream).	[ERROR]: <b>NGX_PRXY_CHAT_HOSTNAME</b> 's value is not configured. Exiting.

Scenario	Sample Error Message
Same variable is encountered more than once in the <code>.env</code> file that is being processed.	[ERROR]: <b>NGX_PRXY_CLOUDCONNECT_HOSTNAME</b> 's value is configured in multiple places. Exiting.
Mandatory variable is configured more than once.	[ERROR]: <b>NGX_FIN_HOSTNAME</b> 's configured more than one time. Exiting.
Duplicate environment variable.	[ERROR]: Following variables were found to be duplicate in file <code>sample_env/finesse.env</code> . Exiting.
More than one version for Unified Intelligence Center or LiveData is configured.	[ERROR]: Multiple versions of env files detected for Unified Intelligence Center, retain one type and retry. Exiting.
More than one Cisco IdS instance is configured. (Each side of the proxy should have only a single instance of IdS configured).	[ERROR]: Number of Cisco IdS instance should not be more than 1. Exiting.
The <code>.env</code> file is not readable.	[ERROR]: File <code>sample_env/core.env</code> does not exist or does not have appropriate permissions. Exiting.
The primary template is altered. This is just a warning, it won't exit the installation.	[!!! WARNING !!!] Primary templates have been altered. Note: Some of the pre-install checks that are based on the templates configurations will be skipped.
The primary <code>env</code> file is altered. This is just a warning. It won't exit the installation.	[!!! WARNING !!!] Primary <code>master_env</code> have been altered. Note: Some of the pre-install checks that are based on the templates configurations will be skipped.
The custom <code>env</code> directory which is passed as a run time option to the Installer is missing.	[ERROR]: Directory <code>sample_env/core</code> doesn't exist. Exiting.
Certificate-based authentication is enabled for a particular upstream server (Using <code>NGX_PRXY_SSL_VERIFY="on"</code> ), without defining the certificate path.	[ERROR]: Mutual Transport Layer Security validation is enabled for <code>finesse</code> , but the upstream server certificate path in <code>NGX_PRXY_SSL_TRUST_CERT</code> is empty. Exiting.
Certificate-based authentication is enabled for a particular upstream server. (Using <code>NGX_PRXY_SSL_VERIFY="on"</code> ). However, the certificate isn't present, nonreadable, or empty.	[ERROR]: Mutual TLS validation is enabled for <code>Finesse</code> , but the upstream server certificate <code>/opt/cisco-proxy/enterprise-features/proxy/ssl/trust/finesse.trust.ct</code> is not present, not readable or invalid. Exiting.

## Launcher logs

Proxy instance launcher logs can be located at `/${HOST_WORKING_DIR}/logs/openresty_launcher.log`. During the NGINX startup, check the logs to see if there are any error information inside the container instance.

`Openresty pid` file is also located in the same folder at `/${HOST_WORKING_DIR}/logs/openresty.pid`.

## Access and error logs

You can locate the Nginx access and error logs for a given proxy instance at the `logs` directory inside the proxy working directory as `${HOST_WORKING_DIR}/logs/access.log` and `${HOST_WORKING_DIR}/logs/error.log`. Check these log files for any debugging information about the OpenResty® startup.

To identify the Digital Routing task requests, the reverse-proxy server generates access logs with the `trackingId` field. The following is the snippet of the `access.log` with the `trackingId` field:

```
[09/Feb/2023:07:24:25 +0000] conn_stats:"7 : 1" client:"35.168.152.254"
host:"pccedrdmzproxy-cc.cisco.com" host_addr:"173.39.15.27"
host_to_upstream:"pccedrdmzproxy-cc.cisco.com->10.10.10.95:8445"
user:"- " server_block:"173.39.15.27:443" request:"POST /drapi/v1/tasks HTTP/1.1" requestid:"- "
server_cache_bypass:"- " cookie:"- " user_agent:"Apache-HttpClient/4.5.2 (Java/1.8.0_242)"
referer:"- " cache_status:"- " rsp_status:"201 (201)" body_bytes_sent:"56"
time_taken:"0.021 (0.022)" up_connect_time:"0.002" up_header_time:"0.022" up_bytes_sent:"1297"
up_bytes_rcvd:"852" trackingId:"WebexConnect_ea54eac0-1d2a-4e09-9fa2-cb212dad13df"
```

If there are failures in the Digital Routing task requests, the reverse-proxy server generates error logs with the `trackingId` field only when you set the trace level to debug.

To enable the debug trace level for the reverse-proxy server:

1. In the "`<reverse_proxy_installed_dir>/conf`" directory, locate and open the `nginx.conf` file.
2. In the `nginx.conf` file, find the statement `[error_log ${NGX_LOG_DIR}/error.log info;]`.
3. Change the trace level from `info` to `debug` as follows: `[error_log ${NGX_LOG_DIR}/error.log debug;]`.
4. Reload the reverse-proxy server for the change to take effect.

The following is the snippet of the `error.log` with the `trackingId` field:

```
2023/02/14 08:01:59 [debug] 206#206: *5 [lua] log_dr_requests.lua:4: conn_stats:5:1
client:172.16.102.61 host:173.39.15.27 host_addr:173.39.15.27
host_to_upstream:173.39.15.27->10.10.10.95:8445
user:nil server_block:pccedrdmzproxy-cc.cisco.com:443 request:GET /drapi/v1/tasks?from=0
HTTP/1.1 requestid:nil server_cache_bypass:nil cookie:nil user_agent:PostmanRuntime/7.29.2
referer:nil
cache_status:nil rsp_status:200 (200) body_bytes_sent:46 time_taken:0.004 (0.005)
up_connect_time:0.002 up_header_time:0.005 up_bytes_sent:3411 up_bytes_rcvd:733
trackingId:WebexConnect_ea54eac0-1d2a-4e09-9fa2-cb212dad13df
```

## IP blocking logs

A separate log file is maintained to track the IPs that block the running proxy instance at `${HOST_WORKING_DIR}/logs/blocking.log`. This file can be supplied to the tools such as *fail2ban* to automate the blocking of IP addresses at IP table level.

Client IPs are blocked if a client makes several failed authentication requests in a given time interval.

## Syslogs

Syslogs are released by the reverse-proxy. By default, syslogs are pushed to the local endpoint. However, proxies can be configured to push this to the remote endpoint.

Syslogs are released when the client IP is blocked by the reverse proxy.

## Reloading configuration and clearing cache

### Static file hosting

Reverse-proxy provides provision to host the static files as required at `${HOST_WORKING_DIR}/html`. You can add any of the static files that must be accessed through proxy such as *proxymap.txt*. These files are accessible through a static file access endpoint provided by the proxy. The endpoint hostname and the port are configurable through the *core.env* file.

By default, you can access the static files deployed on the reverse-proxy at the URL `https://[ip-of-proxy-host]:10000/staticfile`.

To configure access from a different port, use the `NGX_PRXY_STATIC_FILES_PORT` option provided in the **core.env** file.

The static file port isn't opened by default in the IP tables. If necessary, it must be explicitly opened by the administrator. The same must be opened in the DMZ firewall to access from the internet.




---

**Note** While enabling access to this port over the internet, you must be cautious as this port isn't covered under DOS preventive measures.

---

### Reverse-proxy caching

Each and every proxy instance caches the files as specified by different components inside the `${HOST_WORKING_DIR}/cache` directory. Inside the cache directory, every upstream has a separate directory where the cache files for that upstream is present. The sample on how the cache is maintained is as follows:

```

${HOST_WORKING_DIR}/cache
|- client_temp
|- proxy_temp
|- finesse125.autobot.cvp
|- desktop
|- layout
|- openfire
|- rest
|- shindig
|- cuic126.autobot.cvp
|- cuic
|- cuicdoc

```

To get the latest upstream resources, the cache has to be cleared. Administrator can either do this manually by clearing all the files inside each and every directory as required or can run the script provided inside the container to clear the cache automatically.

```

docker exec <PROXY_INSTANCE_NAME>
 /usr/local/openresty/nginx/sbin/openresty_launcher.sh clear_cache

```

Caching behaviors such as cache expiration, cache sizes, and so on, can be configured from the individual component **env** files. The configuration options for different components' **env** files are as follows:

- Finesse
  - `NGX_FIN_DESKTOP_CACHE_SIZE`
  - `NGX_FIN_DESKTOP_CACHE_MAX_SIZE`
  - `NGX_FIN_DESKTOP_CACHE_INACTIVE_DURATION`

- NGX\_FIN\_SHINDIG\_CACHE\_SIZE
  - NGX\_FIN\_SHINDIG\_CACHE\_MAX\_SIZE
  - NGX\_FIN\_SHINDIG\_CACHE\_INACTIVE\_DURATION
  - NGX\_FIN\_OPENFIRE\_CACHE\_SIZE
  - NGX\_FIN\_OPENFIRE\_CACHE\_MAX\_SIZE
  - NGX\_FIN\_OPENFIRE\_CACHE\_INACTIVE\_DURATION
  - NGX\_FIN\_REST\_CACHE\_SIZE
  - NGX\_FIN\_REST\_CACHE\_MAX\_SIZE
  - NGX\_FIN\_REST\_CACHE\_INACTIVE\_DURATION
  - NGX\_FIN\_LAYOUT\_CACHE\_SIZE
  - NGX\_FIN\_LAYOUT\_CACHE\_MAX\_SIZE
  - NGX\_FIN\_LAYOUT\_CACHE\_INACTIVE\_DURATION
- CUIC
    - NGX\_CUIC\_CACHE\_SIZE
    - NGX\_CUIC\_CACHE\_MAX\_SIZE
    - NGX\_CUIC\_CACHE\_INACTIVE\_DURATION
    - NGX\_CUICDOC\_CACHE\_SIZE
    - NGX\_CUICDOC\_CACHE\_MAX\_SIZE
    - NGX\_CUICDOC\_CACHE\_INACTIVE\_DURATION

## Use configurations with custom NGINX installation

The proxy Installer package can be deployed as a standalone. However, you can use the following steps to deploy only the generated configuration with the third-party NGINX installations:

- 
- Step 1** Navigate to the directory **reverse-proxy-openresty-configs/** inside the proxy Installer.
  - Step 2** For third-party NGINX installations, ensure to change the **dirs.env** as per the NGINX installation directory structure.
  - Step 3** Generate the configurations by running the command **./run.sh <ENV-DIR>** where the **ENV-DIR** is the path of the directory containing the environment configuration data files.
  - Step 4** Copy the **conf, html, lua** folders from the **~/configs-out** directory to the **NGX\_HOME** directory.

**Note** This requires NGINX installation with Lua support.

---

# Upstream component configuration specifics

## Verifying Reverse-Proxy Configuration

### Finesse

---

- Step 1** From the DMZ, open `https://<reverseproxy:port>/finesse/api/SystemInfo` and check if it's reachable.
- Step 2** Check if the `<host>` values in both `<primaryNode>` and `<secondaryNode>` are valid in the reverse-proxy hostnames. It shouldn't be the Finesse hostnames.
- Note**
- If CORS status is **enabled**, you must explicitly add the reverse-proxy domain name to the list of CORS trusted domain names.
  - Reverse-proxy supports a maximum of 8000 folders (including sub-directories) in the `finesse/3rdpartygadget` folder.
- 

### Cisco Unified Intelligence Center and LiveData

---

- Step 1** If you find the Finesse hostnames in the response instead of reverse-proxy hostnames, validate the proxy-mapping configurations. Also, check if the allowed hosts are properly added in Finesse servers as described in the [Populate Network Translation Data](#) section.
- Step 2** If the LiveData gadgets load properly in the Finesse Desktop, the CUIC and LiveData proxy configurations are correct.
- Step 3** To validate the Cisco Unified Intelligence Center and LiveData configurations, make the HTTP requests from the DMZ to the following URLs and check if they are reachable:
- `https://<reverseproxy:cuic_port>/cuic/rest/about`
  - `https://<reverseproxy:ldweb_port>/livedata/security`
  - `https://<reverseproxy:ldsocketio_port>/security`
- 

### Cisco Identity Service

To validate the Cisco IdS configuration, perform the following steps:

---

- Step 1** Log in to the Cisco IdS Admin interface at `https://<ids_LAN_host:ids_port>:8553/idsadmin` from the LAN because the admin interface isn't exposed over reverse-proxy.
- Step 2** Choose **Settings > IdS Trust**.
- Step 3** Verify that the proxy cluster publisher node is listed on the Download SP metadata page, and click **Next**.
- Step 4** Verify that the IDP proxy is correctly displayed (if configured on the Upload IDP metadata page) and click **Next**.



- Step 5** Initiate test SSO through all proxy cluster nodes from the Test SSO page and validate that all are successful. This requires client system connectivity to reverse-proxy nodes.
- 

# Security

## Authentication



**Note** Authentication isn't enabled for Digital Channel requests accepted by the proxy.

---

Proxy supports the authentication at the Edge. Authentication is supported for Single Sign-On (SSO) and Non-SSO deployments. Authentication is enforced for all the requests and the protocols that are accepted by the proxy before they are forwarded to the upstream component servers.

The authentication is enforced by the component servers locally. All authentication uses the common Finesse sign-in credentials to authenticate the requests. Persistent connections, such as websockets which rely on application protocols such as Extensible Messaging and Presence Protocol (XMPP) for authentication, the connections are authenticated at the proxy by validating the IP address. Connections from an IP address are allowed only if there's a successful application authentication made from the IP address, before initiating the websocket connection.

### Non-SSO authentication

Non-SSO authentication doesn't require any extra configurations. It works without the NGINX configuration scripts after the required script replacements are made. Authentication relies on the username and password used to sign in to Finesse.

Access to all the endpoints are validated with Finesse authentication services. The list of valid users is cached at the proxy locally (updates the cache every 15 minutes), which is used to validate the user in a request. User credentials are validated by forwarding the request to the configured Finesse URI and thereafter the credential hash is cached locally (cached 15 minutes) to authenticate new requests locally. If there's any change to the username or password, it takes effect only after 15 minutes.

### SSO authentication

SSO authentication for Cisco IdS 12.6(1) (latest ES) requires that the administrator configure the Cisco IdS token encryption key at the NGINX server within the configuration file. You can obtain the Cisco IdS token encryption key from the Cisco IdS server with the **show ids secret** CLI command. The key has to be configured as part of the **core.env** (**NGX\_JWT\_SECRET option**) file that the administrator has to perform in the scripts before the SSO authentication can work.

For Cisco IdS in 12.6.(2) and above this need not be configured, as the proxy automatically add this information from the backend. For more information on Single Sign-On, see [Cisco Unified Contact Center Enterprise Features Guide](#).

The SSO user guide for the Cisco IdS SAML configurations to be performed for the proxy resolution to work for Cisco IdS. After SSO authentication is configured, a valid pair of tokens can be used to access any of the endpoints in the system. The proxy configuration validates the credentials by intercepting the token retrieval

requests made to Cisco IdS or by decrypting valid tokens and thereafter caching them locally for further validations.

### Authentication for Websocket connections

Websocket connections can't be authenticated with the standard authorization header, as custom headers aren't supported by original websocket implementations in the browser. Application-level authentication protocols, where the authentication information contained in the payload doesn't prevent websocket connection establishment. So, malicious entities can render DOS or DDOS attacks just by creating innumerable connections to overwhelm the system.

To mitigate this possibility, the NGINX reverse-proxy configurations provided have specific checks to allow the websocket connections to be accepted ONLY from those IP addresses which have successfully made an authenticated REST request before establishing the websocket connection. It implies that the clients which attempt to create websocket connections before a REST request is issued, gets an authorization failed error and isn't the supported usage scenario.

## Validating unauthenticated static resources

All valid endpoints that can be accessed without any authentication are actively tracked in the ES04 scripts. If invalid URIs are requested to these unauthenticated paths, they are rejected without sending the requests to the components' servers.

## Brute Force attack prevention

The proxy authentication scripts actively prevent brute force attacks which can be used to guess the user password. It does this by blocking the IP address which is used to access the service. After some failed attempts in a short time, these requests are rejected with the HTTP error 418. You can access the details of the blocked IP addresses from the `${HOST_WORKING_DIR}/logs/blocking.log` and `${HOST_WORKING_DIR}/logs/error.log` files.

You can configure the threshold for failed requests, the time interval for the threshold, and the blocking duration. The configurations are present in the `core.env` file. The following are the options:

- **NGX\_CLIENT\_LOCK\_THRESHOLD**: Request authorization failure threshold for a source IP
- **NGX\_CLIENT\_LOCK\_DURAION**: Request authorization failure threshold over a given interval for a source IP
- **NGX\_CLIENT\_BLOCK\_DURAION**: Sets the duration (in seconds) of blocking a client to avoid brute force attack

## Attack Detection Parameters

Configurations are present in the `<nginx-install-directory>/conf/conf.d/maps.conf` file.

```
These two constants indicate five auth failures from a client can be allowed in thirty
seconds.
if the threshold is crossed,client ip will be blocked.
map $host $auth_failure_threshold_for_lock {
Must-change Replace below two parameters as per requirement
default 5 ;
}
map $host $auth_failure_counting_window_secs {
```

```
Must-change Replace below two parameters as per requirement
default 30;
}
This indicates duration of blocking a client to avoid brute force attack
map $host $ip_blocking_duration {
Must-change Replace below parameter as per requirement
default 1800;
}
```

## Logging

You can find the IP addresses that are blocked.

---

To find the IP addresses that are blocked, run the following commands from the directory *{HOST\_WORKING\_DIR}/logs/*.

```
grep "will be blocked for" blocking.log
grep "IP is already blocked." error.log
2021/10/29 17:30:59 [emerg] 1181750#1181750: *19 [lua] block_unauthorized_users.lua:153:
_redirectAndSendError(): 10.68.218.190 will be blocked for 30 minutes for exceeding retry limit.,
client: 10.68.218.190, server: saproxy.cisco.com, request: "GET
/finesse/api/SystemInfo?nocache=1636456574482 HTTP/2.0", host: "saproxy.cisco.com:8445", referrer:
"https://saproxy.cisco.com:8445/desktop/container/?locale=en_US&"

2021/10/29 19:21:00 [error] 943068#943068: *43 [lua] block_unauthorized_users.lua:53: 10.70.235.30
:: IP is already blocked..., client: 10.70.235.30, server: saproxy.cisco.com, request: "GET
/finesse/api/SystemInfo?nocache=1635591686497 HTTP/2.0", host: "saproxy.cisco.com:8445", referrer:
"https://saproxy.cisco.com:8445/desktop/container/?locale=en_US"
```

**Note** It's recommended that the customers integrate with Fail2ban or similar to add the ban to the IP table or firewall rules.

---

## Caching CORS headers

When the first option request is successful, then the following response headers are cached at the proxy for five minutes. These headers are cached for each respective upstream server.

- access-control allow-headers
- access-control-allow-origin
- access-control-allow-methods
- access-control-expose-headers and
- access-control-allow-credentials

## Install and configure Fail2ban

Fail2ban scans log files and bans IPs that show the malicious signs such as too many password failures, seeking for exploits, and so on. Generally, Fail2Ban is used to update the firewall rules to reject the IP addresses for a specified amount of time. It can also be configured for any arbitrary actions such as sending an email. For more information, see <https://www.fail2ban.org/>.

Fail2ban can be configured to monitor the blocking log to identify the IP addresses that are blocked by NGINX on detecting brute force attacks, and ban them for a configurable duration.

The following are the steps to install and configure Fail2ban on a CentOS reverse-proxy:

---

**Step 1** Install the Fail2ban using **yum**.

```
yum update && yum install epel-release
yum install fail2ban
```

**Step 2** Create a local jail.

Jail configurations allow the administrator to configure various properties such as the ports that are to be banned from being accessed by any blocked IP address. The duration for which the IP address stays blocked, the filter configuration used for identifying the blocked IP address from the log file monitored, and so on.

Use the following steps to add a custom configuration for banning the IP addresses that are blocked from accessing the upstream servers:

- Navigate to the Fail2ban installation directory (in this example `/etc/fail2ban`) `cd /etc/fail2ban`.
- Create a copy of **jail.conf** into **jail.local** to keep the local changes isolated in **cp jail.conf jail.local**.
- Add the following jail configurations to the end of the **jail.local** file. Substitute the ports in the template with the actual ones. Update the ban time configurations as required.

```
Jail configurations for HTTP connections.
[finesse-http-auth]
enabled = true
The ports to be blocked. Add any additional ports.
port = http,https,<finesse-ports>,<cuic-ports>,<any-other-ports-to-be-blocked>
Path to nginx blocking logs.
logpath = ${HOST_WORKING_DIR}/logs/blocking.log
The filter configuration.
filter = finesseban
Block the IP from accessing the port, once the IP is blocked by lua.
maxretry= 1
Duration for retry set to 3 mins. Doesn't count as the maxretry is 1
findtime= 180
Lock time is set to 3 mins. Change as per requirements.
bantime = 180
```

**Step 3** Configure a filter. A filter tells Fail2ban what to look for in the logs to identify the host to be banned. The steps to create a filter are as follows:

- Create **filter.d/finesseban.conf**. touch **filter.d/finesseban.conf**
- Add the following lines into the file `filter.d/finesseban.conf` [Definition] # The regex match that would cause blocking of the host. `failregex = <HOST> will be blocked for`

**Step 4** Start Fail2ban. Run the **fail2ban-client start** command to start Fail2ban.

Open the Fail2ban log files and verify that there are no errors. By default, logs for Fail2ban go into the `/var/log/fail2ban.log` file.

**Step 5** Validate static resource URLs. All valid endpoints which can be accessed without authentication are actively tracked in the proxy scripts.

Requests to these unauthenticated paths are actively rejected, if an invalid URI is requested, without sending these requests to the upstream server.

---

# Frequently Asked Questions

## Why does the proxy launcher fail to restart the Reverse Proxy?

The environment settings are incorrect. Correct any errors in the environment data and retry. The log file is stored at `${HOST_WORKING_DIR}/logs/openresty_launcher.log`. Using the command `docker ps -a`, see if the container is up and running.

## How can I solve the OpenResty® launch error?

Some error during OpenResty® start. Fix any of the errors listed in the error log file available at `${HOST_WORKING_DIR}/logs/error.log` and try to restart.

## Why is the content not refreshed to the end user?

Cache is not updated with latest contents. Run the following command to clear the cache:

```
docker exec <PROXY_HOSTNAME> /usr/local/openresty/nginx/sbin/openresty_launcher.sh
clear_cache. The error log file available at ${HOST_WORKING_DIR}/logs/access.log
```

## Why is configuration generation from templates unsuccessful?

Failed to validate while generating the configuration. Correct any problems or failures reported on the console or in the error file. The error file as follows "Configuration generation from templates fails".

## How can I fix problems or failures reported on the console or in the error file?

Reverse proxy is not included in the authorized list. Use this list of CLI Reverse Proxy authorized hosts and confirm if the list of Reverse Proxy authorized host names configured on Cisco IdS and Finesse boxes. This must contain the Reverse Proxy hostname and the allowed IP address.

## What causes intermittent failures of Finesse REST API?

Because of the NGINX proxy rate limit issue, gadgets are not loading in the Finesse desktop. This results in intermittent Finesse REST API failures.

## How do I determine which OpenResty® version is being used in the Installer?

Run the following command in the proxy instance to check the OpenResty® version on the Installer:

```
docker inspect <proxy_instance_name> | grep resty_rpm_version | cut -d ":" -f2
```

## Why does proxy send HTTP error code 4xx ?

Refer to the HTTP [HTTP Return codes returned by the reverse-proxy, on page 270](#) section.

## Environment Files

The Reverse Proxy Installer behavior is driven using user-editable configuration files called environment files (.env). The environment file contains configuration data in the form of **key=value** pairs, which are referred to as properties. Each upstream component has custom environment files and properties specific to the respective component. The Installer also has its own specific environment files, used to customize its behavior. Reverse proxy installation requires the administrator to modify the properties to match the deployment. The following tables list and describe these properties, with their default values and guidance about changing them:



**Note** [Reverse Proxy Automated Installer, on page 301](#) is a per-requisite reading for this chapter.

## Installer env properties

The installer runs the container (which is in a docker), that contains the proxy. The properties determine the configuration of the container like the resources made available to it and the network configurations and such. By default, the properties are set to 2000 users deployment. Deployments which are bigger or smaller than 2000 users must verify these values and modify them appropriately.

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>CONTAINER_NAME</p> <p>Specifies the name of the reverse-proxy container—generally the reverse-proxy hostname.</p> <p><b>Default:</b> proxy25.autobot.cvp</p>	Yes	When you change the name of the container.
<p>CONTAINER_NETWORK_MODE</p> <p>Specifies the network mode of the container.</p> <p><b>Default:</b> host</p>	Yes, If required.	<p>If you use the host network mode for a container, the network stack for that container isn't isolated from the Docker host. <sup>3</sup></p> <p>The other value is <b>bridge</b>. A bridge network creates a separate network for containers to communicate with each other, even if it is isolated from other networks on the host. This is useful when you want to deploy multiple containers on a single host and communicate with each other, but not with the outside world.</p>
<p>CONTAINER_DNS_RESOLVER</p> <p>Specifies a list of DNS servers separated by the   symbol.</p> <p><b>Default:</b> 1.1.1.1 8.8.8.8</p>	Yes	If an IP address changes, update the list.

Property Name, Description, and Default	Change Recommended?	When to Change?
<p><b>CONTAINER_DNS_SEARCH_DOMAIN</b></p> <p>Specifies a DNS search domain to use when resolving hostnames inside the container. This property takes one or more domain names as arguments, separated by commas.</p> <p>In this example, the DNS search domain is <code>example.com</code>. Inside the container, the DNS resolver appends the search domain to the hostname and attempts to resolve it. If you ping the webserver inside the container, the DNS resolver tries to resolve <code>webserver.example.com</code>; if that fails, it tries to resolve <code>webserver</code>.</p> <p><b>Default:</b> <code>search.domain.1 search.domain.2</code></p>	Yes	—
<p><b>CREATE_SELF_SIGNED_SSL_CERT</b></p> <p>Specifies whether to create a self-signed certificate during the reverse-proxy installation.</p> <p><b>Default:</b> <code>TRUE</code></p>	Yes, If required.	If the CA-signed certificates are present, you don't need to install self-signed certificates during the installation. In this case, change to <code>FALSE</code> .
<p><b>CERTIFICATE_COMMON_NAME</b></p> <p>Specifies the common name for the certificate.</p> <p>This value is required to create self-signed certificates. Used on the next property.</p> <p><b>Default:</b> <code>*.cisco.com</code></p>	Yes, If required.	Required only for creating self-signed certificates.
<p><b>CERTIFICATE_SUBJECT</b></p> <p>Specifies the subject line to be used on the self-signed certificate.</p> <p><b>Default:</b> <code>/C=IN/ST=KA/L=BLR/O=Cisco/OU=CCBU/CN=\${CERTIFICATE_COMMON_NAME}</code></p>	Yes, If required.	Required only for creating self-signed certificates.
<p><b>SSL_CERT_NAME</b></p> <p>Specifies the name of the certificate file to be auto-generated.</p> <p><b>Default:</b> <code>reverseproxy.crt</code></p>	Yes, If required.	Required only for creating self-signed certificates.
<p><b>SSL_KEY_NAME</b></p> <p>Specifies the name of the key file to be auto-generated.</p> <p><b>Default:</b> <code>reverseproxy.key</code></p>	Yes, If required.	Required only for creating self-signed certificates.
<p><b>SSL_CERT_KEY_LENGTH</b></p> <p>Specifies the certificate key length to create the self-signed certificate.</p> <p><b>Default:</b> <code>2048</code></p>	Yes, If required.	Required only for creating self-signed certificates.
<p><b>SSL_CERT_EXPIRY_IN_DAYS</b></p> <p>Certificate expiry in days, to be specified in the self-signed certificate.</p> <p><b>Default:</b> <code>1095</code></p>	Yes, If required.	Required only for creating self-signed certificates.

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>AUTO_RESTART_CONTAINER</b> Toggles auto-restart of the reverse-proxy container when the host system reboots. <b>Default: 0</b>	Yes	Enable this property only when the reverse-proxy is in working condition. <a href="#">4</a>
<b>NOFILE_LIMIT</b> Specifies the initial and maximum number of open file descriptors that a container can have. Option in Docker is used to set system resource limits on a container. <b>Default: nofile=102400:102400</b>	Yes, If required.	nofile=204800:204800 for a 4000 deployment.
<b>CPU_LIMIT</b> Specifies the number of CPUs that a container can use. <b>Default: 2</b>	Yes, If required.	4 for 4000 deployment
<b>MEM_LIMIT</b> Specifies the maximum amount of memory that a container can use, in bytes or using a human-readable format. <b>Default: 4G</b>	Yes, If required.	8G for 4000 deployment
<b>MEM_SWAP_LIMIT</b> Specifies the maximum amount of memory and swap for a container—in bytes or using a human-readable format such as 1G for 1 gigabyte. <b>Default: 8G</b>	Yes, If required.	
<b>MEM_RES</b> Sets a soft limit on the minimum amount of memory to be available for the container. <b>Default: 2G</b>	Yes, If required.	4G for 4000 deployment

<sup>3</sup> The container shares the host networking namespace, and the container doesn't allocate its own IP address. For example, if you run a container which binds to port 80 and you use host networking, the container application is available on port 80 on the host IP address.

<sup>4</sup> If enabled and the container stops because of miss-configuration, setting the value with 1 keeps trying to restart the container. Also, the reverse-proxy container keeps running, until it is explicitly stopped.




---

**Note** Ensure that the host has adequate resources to run the container with the modified resource constraints.

---



### Installer env properties that aren't recommended to be altered



**Note** These properties are provided for reference and they are available in the configuration to provide flexibility, to adjust the behavior if necessary, and in exceptional situations. It isn't recommended to change casually without extensive testing.

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>CONTAINER_IMAGE</p> <p>A Docker image is a read-only template that contains a set of instructions for creating a container that can run on the Docker platform.</p> <p><b>Default:</b> reverse-proxy-openresty-container:12.6(2)</p>	No	Never
<p>HOST_WORKING_DIR</p> <p>Specifies the working directory of the container</p> <p><b>Default:</b> ~/reverse_proxy/\${CONTAINER_NAME}</p>	No	
<p>NGX_HOME</p> <p>Specifies the home directory of the NGINX server inside the container.</p> <p><b>Default:</b> /usr/local/openresty/NGINX</p>	No	
<p>HOST_CACHE_VOL</p> <p>Specifies the host system directory used to mount on the container.<sup>5</sup> Mapped with the following container directory: NGX_CACHE_DIR.</p> <p><b>Default:</b> \${HOST_WORKING_DIR}/cache</p>	No	
<p>HOST_SSL_VOL</p> <p>Specifies the host system directory used to mount on the container. Mapped to the following container directory: NGX_SSL_DIR</p> <p><b>Default:</b> \${HOST_WORKING_DIR}/ssl</p>	No	
<p>HOST_LOGS_VOL</p> <p>Specifies the host system directory used to mount on the container. Mapped to the following container directory: NGX_LOG_DIR</p> <p><b>Default:</b> \${HOST_WORKING_DIR}/logs</p>	No	
<p>HOST_CONF_VOL</p> <p>Specifies the host system directory used to mount on the container. Mapped with the container directory mentioned here: NGX_CONF_DIR</p> <p><b>Default:</b> \${HOST_WORKING_DIR}/conf</p>	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>HOST_HTML_VOL</p> <p>Specifies the host system directory used to mount on the container. Mapped to the following container directory: NGX_HTML_DIR</p> <p><b>Default:</b> \${HOST_WORKING_DIR}/html</p>	No	
<p>HOST_LUA_VOL</p> <p>Specifies the host system directory used to mount on the container. Mapped to the following container directory: NGX_LUA_DIR</p> <p><b>Default:</b> \${HOST_WORKING_DIR}/lua</p>	No	
<p>NGX_CACHE_DIR</p> <p>Specifies the container directory location mapped with the corresponding host system directory specified in the HOST_CACHE_VOL property.</p> <p><b>Default:</b> \${NGX_HOME}/cache</p>	No	
<p>NGX_SSL_DIR</p> <p>Specifies the container directory location mapped with the corresponding host system directory mentioned in the HOST_LOGS_VOL property.</p> <p><b>Default:</b> \${NGX_HOME}/ssl</p>	No	
<p>NGX_LOG_DIR</p> <p>Specifies the container directory location mapped with the corresponding host system directory mentioned in the HOST_LOGS_VOL property.</p> <p><b>Default:</b> \${NGX_HOME}/logs</p>	No	
<p>NGX_CONF_DIR</p> <p>Specifies the container directory location mapped with the corresponding host system's directory mentioned in the HOST_CONF_VOL property.</p> <p><b>Default:</b> \${NGX_HOME}/conf</p>	No	
<p>NGX_HTML_DIR</p> <p>Specifies the container directory location mapped with the corresponding host system directory mentioned in the HOST_HTML_VOL property.</p> <p><b>Default:</b> \${NGX_HOME}/html</p>	No	
<p>NGX_LUA_DIR</p> <p>Specifies the container's directory location mapped with the corresponding host system's directory mentioned on this property HOST_LUA_VOL.</p> <p><b>Default:</b> \${NGX_HOME}/lua</p>	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>MEM_SWAPPINESS</b> Controls how aggressively the kernel should swap memory pages of the container to disk when the container exceeds its memory limit. <b>Default:</b> 1	No	
<b>LOAD_CONTAINER_IMAGE_FROM_TAR</b> This property is commented out by default. The default value (when it's commented) is true. <b>Default:</b> This property is commented by default.	No	You can change the value to load the container image from a different location.
<b>REVERSE_PROXY_CONTAINER_IMAGE_TAR</b> Specifies the location of the container image tar file. This property is commented out by default. <code>\${SCRIPTPATH}</code> is the location of the <code>proxy_launcher.sh</code> script. <b>Default:</b> <code>\${SCRIPTPATH}//reverse-proxy-openresty-container/reverse-proxy-openresty-container.tar.gz</code>	No	
<b>RESTART_COND</b>	No	Not used.

<sup>5</sup> Volume mounting is a concept used in computer systems to make a directory or file from one file system available to another file system. It's a method for sharing data between containers in a Docker environment or between a container and the host system.

## Core properties

These are the basic properties that determine the behavior of the included OpenResty® Nginx proxy and control various aspects of its runtime behavior. It also contains request rates and various cache sizes setting for Nginx.

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>NGX_DNS_RSLVR</b> Specify the name servers used to resolve the names of upstream servers into addresses. Use spaces to separate multiple DNS server IP addresses. <b>Default:</b> 192.168.1.3 192.168.1.4 192.168.1.5	Yes	Update the entries with the IP addresses of the DNS servers.

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>NGX_JWT_SECRET</p> <p>OpenResty® Constants(defined in maps.conf) configuration. JWT secret pulled from IdS host using CLI "show ids secret"</p> <p>This secret is used to verify and validate tokens at proxy for authentication in SSO mode</p> <p>This secret is applicable only for IdS &lt; 12.6(2).</p> <p><b>Default:</b> TWSFbB9J6fBnu/D/hrHiQl2O0WEgrVj69ZiHJCtwahI=</p>	Yes, if IdS is running in < 12.6(2) version	Update it with the output of this command from IdS:  "show ids secret"
<p>NGX_SYSLOG_SVR_IP</p> <p>Specifies the syslog server IP to which NGINX pushes some specific notification logs when the access for an IP is blocked.</p> <p><b>Default:</b> 127.0.0.1</p>	Yes, if necessary.	The current syslog server is the current reverse-proxy. This can be changed to the IP for any syslog server, based on the configuration.
<p>NGX_VALID_REFERRERS</p> <p>Specifies the "Referrer" request header field values for which the request is allowed. Request is blocked for all other referrers. The value is case-sensitive.</p> <p>Include all reverse-proxy hostnames, IdS hostnames and ADFS hostname in this list. They are required for reverse-proxy and other functionality.</p> <p><b>Default:</b></p> <p>proxy_pub.host.domain proxy_sub.host.domain </p> <p>ids_pub.host.domain ids_sub.host.domain adfs.host.domain</p>	Yes	If not updated, the pages return with 417 HTTP error code. Make sure there are no typos in the hostnames.
<p>NGX_LOCALHOST_IPS</p> <p>Specifies the list of IPs assigned to the reverse-proxy host across all NICs. Include all public and private IPs for reverse-proxy in this list. Include the alternate side reverse-proxy's IP addresses as well.</p> <p><b>Default:</b> 192.168.1.69 192.168.1.169</p>	Yes	Update all the reverse-proxy IPs here.
<p>NGX_RATELIMIT_DISABLE_IPS</p> <p>Specifies a list of IP addresses for which rate limits aren't applied.</p> <p><b>Default:</b> 192.168.1.69 192.168.1.169 127.0.0.1</p>	Yes	All the IP address that should be allowed to exclude on rate-limiting.  Update the list with all the public and private IPs of both the primary and secondary reverse-proxy. It can also include any other load balancer or proxy which are forwarding requests to reverse-proxy.

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>NGX_LOAD_BALANCER_IPS</p> <p>Hostnames aren't supported as a permissible value in NGX_LOAD_BALANCER_IPS</p> <p>The list of entries should be   separated</p> <p># Example: "192.162.1.0/24 10.78.95.76"</p> <p>Alternatively, if the internet client connection is stopped at the reverse-proxy directly, these variables MUST be empty.</p>	Yes, If required.	If the load balancer forwards requests to the reverse-proxy, populate with the load balancer IP addresses.
<p>NGX_LOAD_BALANCER_REAL_IP_HEADER</p> <p>Devices must also send the end client IP alone, in a custom header.</p> <p>Add the name of the custom header used for this purpose to the NGX_LOAD_BALANCER_REAL_IP_HEADER variable. For example, "<b>X-Real-IP</b>".</p> <p>If you use the <b>X-Forwarded-For</b> as the field used to detect the client IP, include all trusted devices that can appear in this list in the NGX_LOAD_BALANCER_IPS variable. The first untrusted IP encountered is used as the client IP. We don't recommend using this field (<b>X-Forwarded-For</b>) for detecting the client IP.</p>	Yes, If required.	

#### Core properties that are not recommended to be altered



**Note** These properties are provided for reference and they are available in the configuration, to provide flexibility and adjust the behavior if necessary, in exceptional situations, and aren't recommended to be changed casually without extensive testing.

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>NGX_NUM_WKR_PRC</p> <p>OpenResty® NGINX core configurations.</p> <p>Specifies the number of worker processes. The value "auto" uses the number of available CPU cores.</p> <p><b>Default:</b> auto</p>	No	
<p>NGX_PID_FILE</p> <p>Defines a file that stores the process ID of the main process.</p> <p><b>Default:</b> openresty.pid</p>	No	
<p>NGX_WKR_CPU_AFFINITY</p> <p>Binds the worker processes to the sets of CPUs. The value "auto" binds worker processes automatically to the available CPUs.</p> <p><b>Default:</b> auto</p>	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>NGX_WKR_PRIORITY</p> <p>Defines the scheduling priority for worker processes like it's done by the nice command. A negative number means higher priority. The allowed range varies from -20 to 20.</p> <p><b>Default:</b> 0</p>	No	
<p>NGX_NUM_RLIMIT</p> <p>Changes the limit on the maximum number of open files (RLIMIT_NOFILE) for worker processes. Used to increase the limit without restarting the main process.</p> <p><b>Default:</b> 102400</p>	No	
<p>NGX_MULTI_ACCEPT</p> <p>If multi_accept is disabled, a worker process accepts one new connection at a time. Otherwise, a worker process accepts all new connections at a time.</p> <p><b>Default:</b> on</p>	No	
<p>NGX_NUM_WKR_CONN</p> <p>Specifies the maximum number of simultaneous connections that can be opened by a worker process.</p> <p><b>Default:</b> 10240</p>	No	
<p>NGX_SEND_FILE</p> <p>Enables or disables the use of <b>sendfile</b>.</p>	No	No
<p>NGX_TCP_NOPUSH</p> <p>Enables or disables the use of the TCP_NOPUSH socket option on FreeBSD or the TCP_CORK socket option on Linux. The options are enabled only when the <b>sendfile</b> is used.</p> <p><b>Default:</b> on</p>	No	
<p>NGX_MAP_HASH_BUCKET_SIZE</p> <p>Specifies the bucket size for the map variables hash tables.</p> <p><b>Default:</b> 128</p>	No	
<p>NGX_SERVERNAMES_HASH_BUCKET_SIZE</p> <p>Specifies the bucket size for the server names hash tables.</p> <p><b>Default:</b> 512</p>	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>NGX_JWT_EXPIRY</p> <p>Specifies the JWT token expiry in seconds as configured in the IdS host.</p> <p>Token cache expiry time in reverse-proxy. Reverse-proxy keeps the cached token for 2 hours for the default configuration of 1-hour access token expiry time configured in IdS.</p> <p><b>Default:</b> 7200</p>	No	
<p>NGX_IDS_PUBLIC_KEY_POLL_INTERVAL</p> <p>Specifies the IdS public key poll frequency in seconds.</p> <p>The frequency at which reverse-proxy polls the ids to get the public key value. The default is once in 5 minutes.</p> <p><b>Default:</b> 300</p>	No	
<p>NGX_CLIENT_LOCK_THRESHOLD</p> <p>If the threshold to detect DoS attacks is crossed in the specified interval, the client IP is blocked for the specified duration.</p> <p><b>Default:</b> 5</p>	No	
<p>NGX_CLIENT_LOCK_DURATION</p> <p>Specifies the request authorization failure threshold over a given interval for a source IP.</p> <p><b>Default:</b> 30</p>	No	
<p>NGX_CLIENT_BLOCK_DURATION</p> <p>Specifies the duration of blocking (in seconds) for clients to avoid brute force attacks.</p> <p>The block duration for the client IP is 30 minutes.</p> <p><b>Default:</b> 1800</p>	No	
<p>NGX_SYSLOG_SVR_PORT</p> <p>Specifies the port for the syslog server.</p> <p><b>Default:</b> 514</p>	No	Usually the syslog server listens on 514, if the syslog server is configured to listen on some other port then this can be changed.
<p>NGX_LOG_FILE</p> <p>Specifies the OpenResty® logging file.</p> <p><b>Default:</b> access.log</p>	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>NGX_LOG_FORMAT</p> <p>Specifies the OpenResty® NGINX access log format name as specified in logging.conf.</p> <p><b>Default:</b> info</p>	No	Not recommended to change on a production system. You can change it to the debug format in LAB setup for more detailed logging.
<p>NGX_LOG_BUFFER</p> <p>Specifies the OpenResty® NGINX access log buffer size. When this buffer is full or the flush interval is reached, the system writes the logs to the disk.</p> <p><b>Default:</b> 16k</p>	No	
<p>NGX_LOG_FLUSH_INTERVAL</p> <p>Specifies the OpenResty® NGINX access log flush interval. Logs are written to the disk after this interval is reached or the log buffer is full.</p> <p><b>Default:</b> 30s</p>	No	<p>Not recommended changing on production servers.</p> <p>For a LAB system, you can reduce this value to 1 to 5s so you can check the access.log file updates immediately.</p>
<p>NGX_PROXY_CACHE_LOCK</p> <p>Only one request at a time can populate a new cache element identified according to the <a href="#">proxy_cache_key</a> directive by passing a request to the server, which is enabled with reverse-proxy. Other requests of the same cache element either wait for a response to appear in the cache or the cache lock for this element to be released, up to the time set by the NGX_PROXY_CACHE_LOCK_TIMEOUT value.</p> <p><b>Default:</b> on</p>	No	
<p>NGX_PROXY_CACHE_LOCK_TIMEOUT</p> <p>Specifies the timeout for NGX_PROXY_CACHE_LOCK. When the time expires, the request is passed to the server, which is enabled with reverse-proxy; however, the response isn't cached.</p> <p><b>Default:</b> 30s</p>	No	
<p>NGX_PROXY_CACHE_LOCK_AGE</p> <p>If the last request passed to the server, which is enabled with reverse-proxy, for populating a new cache element hasn't completed for the specified time, one more request passes to the server, which is enabled with reverse-proxy.</p> <p><b>Default:</b> 5s</p>	No	



Property Name, Description, and Default	Change Recommended?	When to Change?
<p>NGX_PROXY_CACHE_BACKGROUND_UPDATE</p> <p>Allows starting a background sub request to update an expired cache item, while a stale cached response is returned to the client.</p> <p><b>Default:</b> on</p>	No	
<p>NGX_PROXY_CACHE_REVALIDATE</p> <p>Enables revalidation of expired cache items using conditional requests with the “If-Modified-Since” and “If-None-Match” header fields.</p> <p><b>Default:</b> on</p>	No	
<p>NGX_PROXY_CACHE_VALID</p> <p>Specifies the caching time for 200, 301, and 302 responses.</p> <p><b>Default:</b> 24h</p>	No	
<p>NGX_VARIABLES_HASH_BUCKET_SIZE</p> <p>Specifies the bucket size for the variables hash table.</p> <p><b>Default:</b> 128</p>	No	
<p>NGX_KEEPALIVE_TIMEOUT</p> <p>Specifies a timeout during which a keep-alive client connection stays open on the server side. The zero value disables keep-alive client connections.</p> <p><b>Default:</b> 20s</p>	No	
<p>NGX_SEND_TIMEOUT</p> <p>Specifies a timeout for transmitting a response to the client. The timeout is set only between two successive write operations, not for the transmission of the whole response.</p> <p><b>Default:</b> 10s</p>	No	
<p>NGX_CLIENT_HEADER_TIMEOUT</p> <p>Specifies the timeout for reading the client request header.</p> <p><b>Default:</b> 10s</p>	No	
<p>NGX_CLIENT_BODY_TIMEOUT</p> <p>Specifies a timeout for the reading the client request body. The timeout is set only for a period between two successive read operations, not for the transmission of the whole request body.</p> <p><b>Default:</b> 10s</p>	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>NGX_RESET_TIMEDOUT_CONNECTION</p> <p>Enables or disables resetting timed out connections and connections closed with the non-standard code 444.</p> <p><b>Default:</b> on</p>	No	
<p>NGX_CLIENT_HEADER_BUFFER_SIZE</p> <p>Specifies the buffer size for reading the client request header.</p> <p><b>Default:</b> 4K</p>	No	
<p>NGX_CLIENT_BODY_BUFFER_SIZE</p> <p>Specifies the buffer size for reading the client request body.</p> <p><b>Default:</b> 2k</p>	No	
<p>NGX_CLIENT_MAX_BODY_SIZE</p> <p>Specifies the maximum allowed size of the client request body.</p> <p><b>Default:</b> 15m</p>	No	
<p>NGX_LARGE_CLIENT_HEADER_BUFFER_NUM</p> <p>Specifies the maximum number of buffers used for reading a large client request header. Buffers are allocated only on demand.</p> <p><b>Default:</b> 2</p>	No	
<p>NGX_LARGE_CLIENT_HEADER_BUFFER_SIZE</p> <p>Specifies the maximum size of buffers used for reading a large client request header. A request line can't exceed the size of one buffer. Buffers are allocated only on demand.</p> <p><b>Default:</b> 8K</p>	No	
<p>NGX_UNDERSCORES_IN_HEADERS</p> <p>Enables or disables the use of underscores in client request header fields.</p> <p><b>Default:</b> on</p>	No	
<p>NGX_KEEPALIVE_REQUESTS</p> <p>Specifies the maximum number of requests that are served through one keep-alive connection.</p> <p>After the maximum number of requests are made, the connection is closed.</p> <p><b>Default:</b> 500</p>	No	
<p>NGX_HTTP2_MAX_CONCURRENT_STREAMS</p> <p>Specifies the maximum number of concurrent HTTP/2 streams in a connection.</p> <p><b>Default:</b> 150</p>	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>NGX_SERVER_TOKENS</p> <p>Enables or disables emitting NGINX version on error pages and in the “Server” response header field.</p> <p><b>Default:</b> off</p>	No	
<p>NGX_LIMIT_CONN_DRY_RUN</p> <p>Enables the dry-run mode for limiting HTTP connections. In this mode, the number of connections isn’t limited. However, in the shared memory zone, the number of excessive connections is considered as usual.</p> <p><b>Default:</b> off</p>	No	<p>On a production system, this should be always "off".</p> <p>If the system is running in lab mode, you can toggle this "on" to avoid rate limiting.</p>
<p>NGX_LIMIT_REQ_DRY_RUN</p> <p>Enables the dry-run mode for limiting HTTP requests. In this mode, the number of connections isn’t limited, however, in the shared memory zone, the number of excessive connections is considered as usual.</p> <p><b>Default:</b> off</p>	No	<p>On a production setup, this should be always "off".</p> <p>If the system is running in lab mode, you can toggle this "on" to avoid rate limiting.</p>
<p>NGX_LIMIT_CONN_LOG_LEVEL</p> <p>Specifies the desired logging level for cases when the server limits the number of connections.</p> <p><b>Default:</b> error</p>	No	
<p>NGX_LIMIT_REQ_LOG_LEVEL</p> <p>Specifies the desired logging level for cases when the server refuses to process requests due to rate exceeding, or delays request processing.</p> <p><b>Default:</b> error</p>	No	
<p>NGX_LIMIT_REQ_STATUS</p> <p>Specifies the status code to return in response to rejected requests due to HTTP request rate limits.</p> <p>This is the standard HTTP error code for rate-limiting errors.</p> <p><b>Default:</b> 429</p>	No	
<p>NGX_LIMIT_CONN_STATUS</p> <p>Specifies the status code to return in response to rejected requests due to HTTP connection rate limits.</p> <p><b>Default:</b> 503</p>	No	Error code returned when the connection limits are reached.

Property Name, Description, and Default	Change Recommended?	When to Change?
NGX_CHAT_REQUEST_RATE_LIMIT Specifies the HTTP request rate limit for chat access. <b>Default:</b> 30r/s	No	
NGX_IDS_REQUEST_RATE_LIMIT Specifies the HTTP request rate limit for IdS access. <b>Default:</b> 5r/s	No	
NGX_FIN_REQUEST_RATE_LIMIT Specifies the HTTP request rate limit for Finesse access. <b>Default:</b> 45r/s	No	
NGX_FIN_CLIENT_LOG_REQUEST_RATE_LIMIT Specifies the HTTP request rate limit for Finesse client log requests. <b>Default:</b> 5r/s	No	
NGX_FIN_SSO_VALVE_REQUEST_RATE_LIMIT Specifies the HTTP request rate limit for Finesse SSO valve requests. <b>Default:</b> 5r/s	No	
NGX_CUIC_REQUEST_RATE_LIMIT Specifies the HTTP request rate limit for CUIC access. <b>Default:</b> 50r/s	No	
NGX_CUIC_HISTORICAL_REPORT_REQUEST_RATE_LIMIT Specifies the HTTP request rate limit for CUIC historical report requests. <b>Default:</b> 16r/s	No	
NGX_CUIC_REALTIME_REPORT_REQUEST_RATE_LIMIT Specifies the HTTP request rate limit for CUIC realtime report requests. <b>Default:</b> 48r/s	No	
NGX_CUIC_REPORT_EXECUTION_REQUEST_RATE_LIMIT Specifies the HTTP request rate limit for CUIC report execution requests. <b>Default:</b> 12r/s	No	
NGX_LIVEDATA_REQUEST_RATE_LIMIT Specifies the HTTP request rate limit for livedata access. <b>Default:</b> 25r/s	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
NGX_CLOUDCONNECT_DR_TASK_REQUEST_RATE_LIMIT Specifies the HTTP request rate limit for DR API task request access. <b>Default:</b> 100r/s	No	
NGX_CLOUDCONNECT_USER_SYNC_CALLBACK_REQUEST_RATE_LIMIT Specifies the HTTP request rate limit for user sync callback request access. <b>Default:</b> 5r/m	No	
NGX_PRXY_STATIC_FILES_PORT Specifies the OpenResty® static content configuration. The reverse-proxy port is used to serve static files under the HTML directory. <b>Default:</b> 10000	No	This location serves the proxy-map information. You can change the port number if necessary.
NGX_PRXY_STATUS_IP Specifies the reverse-proxy IP used to access OpenResty® NGINX stats over the "/reverseproxy_status" endpoint Internal request is accessible from only the host system. <b>Default:</b> 127.0.0.1	No	
NGX_PRXY_STATUS_PORT Specifies the reverse-proxy port used to access OpenResty® NGINX stats over the "/reverseproxy_status" endpoint. <b>Default:</b> 10001	No	
NGX_USERTIMERTHREAD_SHRD_DICT_SIZE Specifies the LUA shared dictionary sizes used by reverse-proxy internally. <b>Default:</b> 100k	No	
NGX_USERLIST_SHRD_DICT_SIZE Specifies the LUA shared dictionary sizes used by reverse-proxy internally. <b>Default:</b> 50m	No	
NGX_CREDENTIALSSTORE_SHRD_DICT_SIZE Specifies the LUA shared dictionary sizes used by reverse-proxy internally. <b>Default:</b> 100m	No	
NGX_USERCOUNT_SHRD_DICT_SIZE Specifies the LUA shared dictionary sizes used by reverse-proxy internally. <b>Default:</b> 100k	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
NGX_CLIENTSTORAGE_SHRD_DICT_SIZE Specifies the LUA shared dictionary sizes used by reverse-proxy internally. <b>Default:</b> 100m	No	
NGX_BLOCKINGRESOURCES_SHRD_DICT_SIZE Specifies the LUA shared dictionary sizes used by reverse-proxy internally. <b>Default:</b> 100m	No	
NGX_TOKENCACHE_SHRD_DICT_SIZE Specifies the LUA shared dictionary sizes used by reverse-proxy internally. <b>Default:</b> 10m	No	
NGX_IPSTORE_SHRD_DICT_SIZE Specifies the LUA shared dictionary sizes used by reverse-proxy internally. <b>Default:</b> 10m	No	
NGX_DESKTOPURLLIST_SHRD_DICT_SIZE Specifies the LUA shared dictionary sizes used by reverse-proxy internally. <b>Default:</b> 10m	No	
NGX_DESKTOPPURLCOUNT_SHRD_DICT_SIZE Specifies the LUA shared dictionary sizes used by reverse-proxy internally. <b>Default:</b> 100k	No	
NGX_THIRDPARTYGADGETURLLIST_SHRD_DICT_SIZE Specifies the LUA shared dictionary sizes used by reverse-proxy internally. <b>Default:</b> 100m	No	
NGX_THIRDPARTYGADGETURLCOUNT_SHRD_DICT_SIZE Specifies the LUA shared dictionary sizes used by reverse-proxy internally. <b>Default:</b> 100k	No	
NGX_CORSHEADERSSTORE_SHRD_DICT_SIZE Specifies the LUA shared dictionary sizes used by reverse-proxy internally. <b>Default:</b> 100k	No	
NGX_TIMERTHREADSSTORE_SHRD_DICT_SIZE Specifies the LUA shared dictionary sizes used by reverse-proxy internally. <b>Default:</b> 100k	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>NGX_ALTERNATE_HOSTS_SHRD_DICT_SIZE</b> Specifies the LUA shared dictionary sizes used by reverse-proxy internally. <b>Default:</b> 100k	No	

## Directory (DIR) properties

The following table lists the directory properties and the default values for various OpenResty® folders.



**Note** These properties are provided for reference and they are available in the configuration. They provide flexibility to adjust the behavior if necessary, in exceptional situations, and aren't recommended changing casually without extensive testing.

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>NGX_CACHE_DIR</b> Specifies the cache directory where various resources for components are cached. <b>Default:</b> \${NGX_HOME}/cache	No	
<b>NGX_CONF_DIR</b> Specifies the OpenResty® directory containing NGINX configurations, such as core and component configurations. <b>Default:</b> \${NGX_HOME}/conf	No	
<b>NGX_HOME</b> Specifies the home directory for OpenResty® nginx installation. <b>Default:</b> /usr/local/openresty/nginx	No	
<b>NGX_HTML_DIR</b> Specifies the OpenResty® directory <b>Default:</b> \${NGX_HOME}/html Directory containing static resources.	No	
<b>NGX_LOG_DIR</b> Specifies the OpenResty® directory where OpenResty® logs are stored. <b>Default:</b> \${NGX_HOME}/logs	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>NGX_LUA_DIR</b> Specifies the OpenResty® directory containing lua resources. <b>Default:</b> \${NGX_HOME}/lua	No	
<b>NGX_SSL_DIR</b> Specifies the OpenResty® directory containing SSL resources like certs and keys. <b>Default:</b> \${NGX_HOME}/ssl	No	

## Common Properties

### Common SSL-Related Properties

The following table lists SSL-related properties that are common across components.

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>NGX_PRXY_SSL_TRUST_CERT</b> Specifies a file with trusted CA certificates in the PEM format used to verify the certificate of the Finesse HTTPS server, which is enabled for reverse-proxy. <b>Default:</b> \${NGX_SSL_DIR}/upstreams_finesse_trust.crt	Yes, if necessary.	Point to the exact location of upstream Finesse's certificate for mutual trust establishment.
<b>NGX_SSL_CERT</b> SSL connector configuration for the component access. Specifies the location of a file with the certificate, for the given component, in the PEM format. <b>Default:</b> \${NGX_SSL_DIR}/reverseproxy.crt	Yes, if necessary.	Update the location of the Finesse reverse-proxy certificate.
<b>NGX_SSL_KEY</b> Specifies the location of a file with the secret key, for the given component, in the PEM format. <b>Default:</b> \${NGX_SSL_DIR}/reverseproxy.key	Yes, if necessary.	If the location of the file changes.



### Common SSL-Related properties that are not recommended to be altered



**Note** These properties are provided for reference and they are available in the configuration. They provide flexibility to adjust the behavior if necessary, in exceptional situations, and aren't recommended changing casually without extensive testing.

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>#NGX_SSL_DHPARAM</p> <p>Specifies a file with DH parameters for DHE ciphers.</p> <p><b>Default:</b> \${NGX_SSL_DIR}/dhparam.pem</p> <p>This property is disabled by default. Uncomment the parameter to use it.</p>	<p>No.</p> <p>Can be changed if necessary.</p>	<p>Enable for more security, to prevent affecting by an attack exploiting the Logjam vulnerability.</p> <p>For more information, see <i>Understanding Logjam and Future-Proofing Your Infrastructure</i> at: <a href="https://cisco.blogs.com">https://cisco.blogs.com</a></p>
<p>NGX_PROXY_SSL_VERIFY</p> <p>Enables or disables verification of the HTTPS server certificate, which is enabled for reverse-proxy.</p> <p><b>Default:</b> on</p>	<p>No</p>	<p>Changing this to off disables SSL verification of the requests.</p>
<p>NGX_PROXY_SSL_VERIFY_DEPTH</p> <p>Specifies the verification depth in the HTTPS server certificates chain, which is enabled for reverse-proxy.</p> <p>This is for DoS prevention. Building the chain might be an exponential algorithm with backoff, so with the openssl default of 100 a malicious backend might cause denial of service in nginx.</p> <p><b>Default:</b> 10; less than 4 is easy to break.</p>	<p>No</p>	
<p>NGX_SSL_CACHE_SIZE</p> <p>Specifies the SSL session cache size for session parameters storage for client connections.</p> <p>This cache is shared between all worker processes. The cache size is specified in bytes; one megabyte can store about 4000 sessions. Each shared cache should have an arbitrary name.</p> <p><b>Default:</b> 10m</p>	<p>No</p>	

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>NGX_SSL_CIPHERS</p> <p>Specifies the OpenSSL format for enabled ciphers.</p> <p><b>Default:</b> EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH</p>	No	This list contains all the strong ciphers available. You can update the list if ciphers are found to be vulnerable or to add new supported ciphers.
<p>NGX_SSL_PRFR_SRVR_CIPHERS</p> <p>Prefer server ciphers over client ciphers.</p> <p><b>Default:</b> on</p>	No	
<p>NGX_SSL_PROTO</p> <p>Specifies the TLS versions enabled for the connections. To specify multiple values, use space delimiters.</p> <p># Example: NGX_SSL_PROTO="TLSv1 TLSv1.1 TLSv1.2"</p> <p>Generally TLS version 1.2 is supported for the webapp requests. TLS v1 and TLS v1.1 aren't recommended.</p> <p><b>Default:</b> TLSv1.2</p>	No	
<p>NGX_SSL_SESSION_TICKETS</p> <p>Enables or disables session resumption through TLS session tickets.</p> <p><b>Default:</b> off</p>	No	Enable to resume sessions and avoid keeping a per-client session state. The TLS server encapsulates the session state into a ticket and forwards it to the client. The client can later resume a session using the obtained ticket.
<p>NGX_SSL_SSN_TIMEOUT</p> <p>Specifies a time during which a client may reuse the session parameters—how long each session lives in reverse-proxy.</p> <p><b>Default:</b> 30m</p>	No	
<p>NGX_SSL_STAPLING</p> <p>Enables or disables stapling of OCSP responses by the server.</p> <p>SSL stapling means that revocation information about the servers certificate (that is, the OCSP response) are included in the TLS handshake together with the server certificate.</p> <p><b>Default:</b> off</p>	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
<p><b>NGX_SSL_STAPLING_VERIFY</b></p> <p>Enables or disables the verification of OCSP responses by the server.</p> <p>Allows the presenter of a certificate to bear the resource cost involved in providing OCSP responses by appending ("stapling") a time-stamped OCSP response signed by the CA to the initial TLS handshake, eliminating the need for clients to contact the CA".</p> <p><b>Default:</b> off</p>	No	

## Cisco Finesse Properties

Property Name, Description, and Default	Change Recommended?	When to Change?
<p><b>NGX_PRXY_FIN_HOSTNAME</b></p> <p>Reverse-proxy hostname through which this Finesse host is accessed.</p> <p><b>Default:</b> reverseproxy.host.domain</p>	Yes	New installation or if the hostname of the reverse-proxy must be accessed from the internet changes.
<p><b>NGX_PRXY_FIN_PORT</b></p> <p>Specifies the reverse-proxy port over which this Finesse host are accessed.</p> <p><b>Default:</b> 8445</p>	Yes, if necessary.	New installation or if the port number of the reverse-proxy must be accessed from the internet changes.
<p><b>NGX_FIN_HOSTNAME</b></p> <p>Specifies the upstream Finesse hostname.</p> <p><b>Default:</b> finesse.host.domain</p>	Yes	New installation or if the hostname of the Finesse box changes.
<p><b>NGX_AUTH_URL</b></p> <p>Specifies the Finesse URL to fetch the users list to perform authentication at proxy.</p> <p><b>Default:</b> <a href="https://reverseproxy.host.domain:8445/finesse/api/UserAuth">https://reverseproxy.host.domain:8445/finesse/api/UserAuth</a></p>	Yes	Replace "reverseproxy.host.domain" with the FQDN of the reverse-proxy.

### Cisco Finesse properties that are not recommended to be altered



**Note** These properties are provided for reference and they exist in the configuration to provide flexibility to adjust the behavior if necessary, in exceptional situations and aren't recommended changing casually without extensive testing.

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>NGX_FIN_UPSTREAM_KEEPALIVE</p> <p>Specifies the proxy backend configurations for Finesse, and activates the cache for connections to an upstream IdS server. The value sets the maximum number of idle keep-alive connections to upstream servers that are preserved in the cache of each worker process. When this number is exceeded, the least recently used connections are closed.</p> <p><b>Default:</b> 128</p>	No	This default is the optimal value for keeping alive the upstream connection per component.
<p>TEMPLATE_TYPE</p> <p>Specifies the component template type—valid values are: chat, cuic, Finesse, ids, livedata, cuic_12.6(1), livedata_12.6(1), and idp-ads3.</p> <p><b>Default:</b> Finesse</p>	No	Never
<p>NGX_FIN_DESKTOP_CACHE_SIZE</p> <p>Specifies the proxy cache configuration for the Finesse desktop and the initial size of the Finesse desktop endpoints cache.</p> <p><b>Default:</b> 10m</p>	No	The default is the optimal value.
<p>NGX_FIN_DESKTOP_CACHE_MAX_SIZE</p> <p>Specifies the maximum size for the Finesse desktop endpoints cache. When the size exceeds or there isn't enough free space, it removes the least recently used data.</p> <p><b>Default:</b> 50m</p>	No	The default is the optimal value.
<p>NGX_FIN_DESKTOP_CACHE_INACTIVE_DURATION</p> <p>Specifies the content inactive duration for the Finesse desktop endpoints cache. Cached data that is not accessed during the time specified gets removed from the cache regardless of their duration.</p> <p><b>Default:</b> 3y</p>	No	The default is the optimal value. After this time, the cache contents expire.
<p>NGX_FIN_SHINDIG_CACHE_SIZE</p> <p>Specifies the proxy cache configuration for Finesse Shindig and the initial size of the Finesse Shindig endpoints cache.</p> <p><b>Default:</b> 10m</p>	No	
<p>NGX_FIN_SHINDIG_CACHE_MAX_SIZE</p> <p>Max size for Finesse shindig endpoints cache. When the size exceeds or there isn't enough free space, it removes the least recently used data.</p> <p><b>Default:</b> 500m</p>	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>NGX_FIN_SHINDIG_CACHE_INACTIVE_DURATION</p> <p>Specifies the content inactive duration for the Finesse desktop endpoints cache. Cached data that aren't accessed during the time specified get removed from the cache regardless of their freshness.</p> <p><b>Default:</b> 3y</p>	No	
<p>NGX_FIN_OPENFIRE_CACHE_SIZE</p> <p>Specifies the initial size of the Finesse openfire endpoints cache.</p> <p><b>Default:</b> 10m</p>	No	
<p>NGX_FIN_OPENFIRE_CACHE_MAX_SIZE</p> <p>Specifies the maximum size for the Finesse openfire endpoints cache. When the size exceeds or there isn't enough free space, it removes the least recently used data.</p> <p><b>Default:</b> 10m</p>	No	
<p>NGX_FIN_OPENFIRE_CACHE_INACTIVE_DURATION</p> <p>Specifies the content inactive duration for the Finesse desktop endpoints cache. Cached data that is not accessed during the time specified is removed from the cache regardless of their duration.</p> <p><b>Default:</b> 3y</p>	No	
<p>NGX_FIN_REST_CACHE_SIZE</p> <p>Specifies the initial size of the Finesse REST endpoints cache</p> <p><b>Default:</b> 10m</p>	No	
<p>NGX_FIN_REST_CACHE_MAX_SIZE</p> <p>Specifies the maximum size for the Finesse REST endpoints cache. When the size exceeds or there isn't enough free space, it removes the least recently used data.</p> <p><b>Default:</b> 1500m</p>	No	
<p>NGX_FIN_REST_CACHE_INACTIVE_DURATION</p> <p>Specifies the content inactive duration for the Finesse desktop endpoints cache. Cached data that is not accessed during the time specified, get removed from the cache regardless of their duration.</p> <p><b>Default:</b> 40m</p>	No	
<p>NGX_FIN_LAYOUT_CACHE_SIZE</p> <p>Specifies the initial size of the Finesse layout endpoints cache.</p> <p><b>Default:</b> 150m</p>	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>NGX_FIN_LAYOUT_CACHE_MAX_SIZE</p> <p>Specifies the maximum size for the Finesse layout endpoints cache. When the size exceeds or there isn't enough free space, the system removes the least recently used data.</p> <p><b>Default:</b> 300m</p>	No	
<p>NGX_FIN_LAYOUT_CACHE_INACTIVE_DURATION</p> <p>Specifies the inactive duration for content stored in the Finesse desktop endpoints cache. Cached data that aren't accessed during the time specified get removed from the cache regardless of their duration.</p> <p><b>Default:</b> 40m</p>	No	
<p>NGX_FIN_HTTP1_CONN_LIMIT</p> <p>Specifies the number of concurrent HTTP/1.1 connections allowed per source IP</p> <p><b>Default:</b> 12</p>	No	
<p>NGX_FIN_HTTP2_CONN_LIMIT</p> <p>Specifies the number of concurrent HTTP/2 streams allowed per source IP.</p> <p><b>Default:</b> 150</p>	No	
<p>NGX_FIN_DESKTOP_REQUEST_BURST_LIMIT</p> <p>Specifies the HTTP request burst limit for desktop endpoints</p> <p><b>Default:</b> 50</p>	No	
<p>NGX_FIN_SHINDIG_CORE_RPC_REQUEST_BURST_LIMIT</p> <p>Specifies the HTTP request burst limit for shindig rpc endpoints</p> <p><b>Default:</b> 40</p>	No	
<p>NGX_FIN_SHINDIG_IFR_REQUEST_BURST_LIMIT</p> <p>Specifies the HTTP request burst limit for shindig ifr endpoints</p> <p><b>Default:</b> 30</p>	No	
<p>NGX_FIN_SSOVALVE_REQUEST_BURST_LIMIT</p> <p>Specifies the HTTP request burst limit for SSO valve endpoints</p> <p><b>Default:</b> 5</p>	No	
<p>NGX_FIN_LIMIT_REQ_STATUS</p> <p>Specifies the HTTP response code to return when the HTTP request rate reaches the limit</p> <p><b>Default:</b> 429</p>	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>NGX_FIN_PROXY_BUFFER_SIZE</p> <p>Specifies the size of the buffer used for reading the first part of the response received from the server, which is enabled for reverse-proxy.</p> <p>Configurations are overridden from the common config for Finesse.</p> <p><b>Default:</b> 8k</p>	No	
<p>NGX_FIN_MAX_TEMP_FILE_SIZE</p> <p>Applies when buffering of responses from the server (which is enabled for reverse-proxy) is enabled. If the whole response doesn't fit into the buffers set by the NGX_FIN_PROXY_BUFFER_SIZE, the system saves part of the response in a temporary file.</p> <p><b>Default:</b> 100m</p>	No	

### Chat properties

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>NGX_PRXY_CHAT_PORT</p> <p>Specifies the reverse-proxy port over which this chat server is accessed.</p> <p><b>Default:</b> 5280</p>	Yes, if necessary.	New installation or if not changed, 5280 is the port for the chat server.
<p>NGX_PRXY_CHAT_HOSTNAME</p> <p>Specifies the reverse-proxy hostname over which this chat server is accessed.</p> <p><b>Default:</b> reverseproxy.host.domain</p>	Yes	New installation or if the chat hostname of the reverse-proxy is accessed from the the internet changes.
<p>NGX_CHAT_HOSTNAME</p> <p>Specifies the hostname of the chat server.</p> <p><b>Default:</b> chat1.host.domain</p>	Yes	New installation or if the host name of the upstream chat server changes.
<p>NGX_CHAT_HOST[1-8]_PROXY</p> <p>Required for substituting user home and backup node information in the log-in response.</p> <p>(Similar keys configurations exist for 4 HA clusters of chat servers.)</p> <p><b>Default:</b> reverseproxy.host.domain:5280/reverseproxy-sub.host.domain:15280</p>	Yes	New installation or if the chat server proxy hostname FQDN changes.

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>NGX_CHAT_HOST[1-8]</p> <p>Specifies the proxy access information for all chat nodes in the deployment. Required for substituting user home and backup node information in the log-in response.</p> <p>(Similar keys configurations exist for 4 HA clusters of chat servers.)</p> <p><b>Default:</b> chat[1-4].host.domain/chat[1-4]-sub.host.domain</p>	Yes	New installation or if the chat server upstream hostname FQDN changes.
<p>NGX_CHAT_BIND_PATH</p> <p>Specifies the binding URL for the chat server.</p> <p><b>Default:</b> httpbinding</p>	Yes	If the binding URL for the chat server changes.
<p>NGX_AUTH_URL</p> <p>Specifies the Finesse URL to fetch the users list to perform authentication at proxy.</p> <p><b>Default:</b> https://proxy.host.domain:8445/finesse/api/UserAuth</p>	Yes	New installation or if <a href="#">proxy.host.domain</a> is the hostname of the the reverse-proxy.

#### Chat properties that are not recommended to be altered



**Note** These properties are provided for reference and they are available in the configuration. They provide flexibility to adjust the behavior if necessary, in exceptional situations, and aren't recommended for changing casually without extensive testing.

Property Name, Description, and Default	Change Recommended?	When to change?
<p>TEMPLATE_TYPE</p> <p>Specifies the component template type—valid values are: chat, cuic, finesse, ids, livedata.</p> <p><b>Default:</b> chat</p>	No	
<p>NGX_CHAT_REQUEST_BURST_LIMIT</p> <p>Specifies the HTTP request burst limit.</p> <p><b>Default:</b> 10</p>	No	
<p>NGX_CHAT_PORT</p> <p>Specifies the port for the chat server.</p> <p><b>Default:</b> 5280</p>	No	New installation or if the port number for the upstream chat server is different.



Property Name, Description, and Default	Change Recommended?	When to change?
<b>NGX_CHAT_HTTP2_CONN_LIMIT</b> Specifies the number of concurrent HTTP/2 streams allowed per source IP. <b>Default: 30</b>	No	
<b>NGX_CHAT_HTTP1_CONN_LIMIT</b> Specifies the rate limit for desktop chat, the number of concurrent HTTP/1.1 connections allowed per source IP. <b>Default: 6</b>	No	

### Cloud Connect properties

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>NGX_PRXY_CLOUDCONNECT_PORT</b> Specifies the reverse-proxy port over which this Cloud Connect server is accessed. <b>Default: 443</b>	Yes, if necessary.	If there is a change in the port number.
<b>NGX_PRXY_CLOUDCONNECT_HOSTNAME</b> Specifies the reverse-proxy hostname over which this Cloud Connect server is accessed. <b>Default: reverseproxy.host.domain</b>	Yes	If there is a change in the chat hostname of the reverse-proxy that has must accessed from the internet.
<b>NGX_CLOUDCONNECT_HOSTNAME</b> Specifies the hostname for the Cloud Connect server and the hostname of the Publisher or Primary Cloud Connect node. (Conversely on the alternate side) <b>Default: cloudconnect.host.domain</b>	Yes	If there is a change in the FQDN for the upstream Cloud Connect server.
<b>NGX_CLOUDCONNECT_FAILOVER_HOSTNAME</b> Specifies the hostname of the Cloud Connect failover node and the hostname of the Subscriber or Secondary Cloud Connect node. (Conversely on the alternate side) <b>Default: cloudconct.failover.hostname</b>	Yes	If there is change in the FQDN of the alternate Cloud Connect server.
<b>NGX_CLOUDCONNECT_CLIENT_IPS</b> Creates a list of known IP addresses for clients connecting to Cloud Connect services like DigitalRouting and UserSync. <b>Default:</b> 35.161.238.252 35.166.68.236 34.240.73.178 3.9.155.97 54.206.189.15 52.62.185.51  13.210.45.137 52.40.46.90 52.214.81.91 3.9.151.19 3.105.22.233 52.17.23.194	Yes	Validate and update the list when there is a change in the IP addresses.

### Cloud Connect properties that are not recommended to be altered



**Note** These properties are provided for reference and they exist in the configuration to provide flexibility to adjust the behavior if necessary, in exceptional situations and aren't recommended changing casually without extensive testing.

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>TEMPLATE_TYPE</p> <p>Specifies the component template type—valid values are: chat, cuic, finesse, ids, livedata, cuic_12.6(1), livedata_12.6(1), and idp-ads3.</p> <p><b>Default:</b> cloudconnect</p>	No	
<p>NGX_CLOUDCONNECT_USER_SYNC_CALLBACK_REQUEST_BURST_LIMIT</p> <p>Specifies the HTTP request burst limit for user sync bulk requests.</p> <p><b>Default:</b> 10</p>	No	
<p>NGX_CLOUDCONNECT_UPSTREAM_KEEPALIVE</p> <p>Activates the cache for connections to the upstream Cloud Connect server.</p> <p>Specifies the maximum number of idle keepalive connections to upstream servers that are preserved in the cache of each worker process. When the count exceeds this number, the least recently used connections close.</p> <p><b>Default:</b> 150</p>	No	
<p>NGX_CLOUDCONNECT_LIMIT_REQ_STATUS</p> <p>Specifies the HTTP response code to return when the HTTP request rate reaches the limit.</p> <p><b>Default:</b> 429</p>	No	
<p>NGX_CLOUDCONNECT_HTTP2_CONN_LIMIT</p> <p>Specifies the number of concurrent HTTP/2 streams allowed per source IP.</p> <p><b>Default:</b> 250</p>	No	
<p>NGX_CLOUDCONNECT_HTTP1_CONN_LIMIT</p> <p>Specifies the number of concurrent HTTP/1.1 connections allowed per source IP—the rate limit for Digital Routing requests.</p> <p><b>Default:</b> 50</p>	No	
<p>NGX_CLOUDCONNECT_HEALTHCHECK_TIMEOUT</p> <p>Specifies the timeout for the health check API in milliseconds, if there is a failure.</p> <p><b>Default:</b> 2000</p>	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
NGX_CLOUDCONNECT_HEALTHCHECK_SSL_VERIFY Specifies whether to verify the SSL certificate for health checks. <b>Default:</b> FALSE	No	
NGX_CLOUDCONNECT_HEALTHCHECK_RISE Specifies the number of successive health check successes before turning up a peer. <b>Default:</b> 2	No	
NGX_CLOUDCONNECT_HEALTHCHECK_RESPONSE_CODES Generates a comma-separated list of valid HTTP status codes for the health check API. <b>Default:</b> {200}	No	
NGX_CLOUDCONNECT_HEALTHCHECK_INTERVAL Specifies the interval between health checks in milliseconds. <b>Default:</b> 2000	No	
NGX_CLOUDCONNECT_HEALTHCHECK_FALL Specifies the number of successive health check failures before turning down a peer. <b>Default:</b> 2	No	
NGX_CLOUDCONNECT_HEALTHCHECK_CONCURRENCY Specifies the number of concurrent health checks. <b>Default:</b> 2	No	
NGX_CLOUDCONNECT_HEALTHCHECK_API Specifies the active health check configurations for the DR API. The system uses this URL to check the health of the Cloud Connect. <b>Default:</b> /drapi/v1/ping	No	
NGX_CLOUDCONNECT_DR_TASK_REQUEST_BURST_LIMIT Specifies the HTTP request burst limit for digital routing tasks. <b>Default:</b> 200	No	

## Cisco IdS properties

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>NGX_PRXY_IDS_HOSTNAME</b> Specifies the reverse-proxy hostname over which this IdS host is accessed. <b>Default:</b> reverseproxy.host.domain	Yes	New installation or if the reverse-proxy IdS hostname changes.
<b>NGX_PRXY_IDS_PORT</b> Specifies the reverse-proxy port over which this IdS host is accessed. <b>Default:</b> 8553	Yes, If required.	New installation or if the reverse-proxy port changes.
<b>NGX_IDS_HOSTNAME</b> IdS server actual hostname <b>Default:</b> ids.host.domain	Yes	New installation or if the FQDN host name of the IdS server changes.

## Cisco IdS properties that are not recommended to be altered



**Note** These properties are provided for reference and they are available in the configuration. They provide flexibility to adjust the behavior if necessary, in exceptional situations, and aren't recommended changing casually without extensive testing.

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>TEMPLATE_TYPE</b> Specifies the component template type—valid values are: chat, cuic, finesse, ids, livedata, cuic_12.6(1), livedata_12.6(1), and idp-ads3. <b>Default:</b> ids	No	
<b>NGX_IDS_UPSTREAM_KEEPALIVE</b> Proxy backend configurations for IDS. Activates the cache for connections to the upstream IDP server. Specifies the maximum number of idle keepalive connections to upstream servers that are preserved in the cache of each worker process. When the count exceeds this number, the least recently used connections close. <b>Default:</b> 128	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>NGX_IDS_HTTP1_CONN_LIMIT</b> Rate limits configuration for IdS. Specifies the number of concurrent HTTP/1.1 connections allowed per source IP. <b>Default: 4</b>	No	
<b>NGX_IDS_HTTP2_CONN_LIMIT</b> Specifies the number of concurrent HTTP/2 streams allowed per source IP. <b>Default: 4</b>	No	
<b>NGX_IDS_REQUEST_BURST_LIMIT</b> Specifies the HTTP request burst limit. <b>Default: 4</b>	No	

### IdP Properties (ADFS 3.0)

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>NGX_PRXY_IDP_HOSTNAME</b> Specifies the reverse-proxy hostname over which this IdP host will be accessed. <b>Default: adfs-reverseproxy.host.domain</b>	Yes	New installation or if the FQDN of the reverse-proxy IdP host changes.
<b>NGX_PRXY_IDP_PORT</b> Specifies the reverse-proxy port over which this IdP host will be accessed. <b>Default: 443</b>	Yes, If required.	New installation or if unchanged, reverse-proxy uses the 443 port for CUIC.
<b>NGX_IDP_HOSTNAME</b> Specifies the CUIC server hostname. <b>Default: idp.host.domain</b>	Yes	New installation or if the FQDN of the IdP host changes.

### IdP Properties (ADFS 3.0) that are not recommended to be altered



**Note** These properties are provided for reference and they are available in the configuration. They provide flexibility to adjust the behavior if necessary, in exceptional situations, and are not recommended changing casually without extensive testing.

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>TEMPLATE_TYPE</p> <p>Specifies the component template type—valid values are: chat, cuic, finesse, ids, livedata, cuic_12.6(1), livedata_12.6(1), and idp-adfs3.</p> <p><b>Default:</b> idp-adfs3</p>	No	
<p>NGX_IDP_UPSTREAM_KEEPALIVE</p> <p>Proxy backend configurations for IDP. Activates the cache for connections to upstream IDP server</p> <p>Specifies the maximum number of idle keepalive connections to upstream servers that are preserved in the cache of each worker process. When the count exceeds this number, the least recently used connections close.</p> <p><b>Default:</b> 128</p>	No	

## Livedata Properties

### LiveData 12.6(1) Properties



**Note** Use livedata\_12.6(1).env when the upstream Livedata is still on Release12.6(1). Otherwise, use livedata.env.

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>NGX_PRXY_LD_HOSTNAME</p> <p>Specifies the reverse-proxy hostname over which this LD host is accessed.</p> <p><b>Default:</b> reverseproxy.host.domain</p>	Yes	If the reverse-proxy livedata host FQDN changes.
<p>NGX_PRXY_LD_PORT</p> <p>Specifies the reverse-proxy port over which this livedata host is accessed.</p> <p><b>Default:</b> 12005</p>	Yes, If required.	If there is a change in the reverse-proxy port for livedata.
<p>NGX_PRXY_LD_SCKT_IO_PORT</p> <p>Specifies the reverse-proxy port over which the socket IO endpoint of this livedata host will be accessed.</p> <p><b>Default:</b> 12008</p>	Yes, If required.	If there is a change in the reverse-proxy port for socket IO connections.
<p>NGX_LD_HOSTNAME</p> <p>Specifies the Livedata server hostname.</p> <p><b>Default:</b> livedata.host.domain</p>	Yes	If there is a change in the upstream livedata host FQDN.

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>NGX_LD_SIO_UPSTREAM_KEEPALIVE</b> Activates the cache for connections to the upstream livedata server socketio endpoint. <b>Default:</b> 128	No	—
<b>NGX_LD_BACKEND_FAILOVER</b> Livedata failover configuration. This is used to translate the location header during failover. For SideA LiveData, point to SideB LiveData and for SideB Livedata, point to SideA Livedata.	Yes	If there is a change in the FQDN or port.
<b>NGX_LD_BACKEND_PROXY_FAILOVER</b> Livedata proxy failover configuration. Each side points to the other side of the reverse-proxy node.	Yes	If there is a change in the FQDN or port.

#### LiveData 12.6(1) properties that are not recommended to be altered



**Note** These properties are provided for reference and they are available in the configuration. They provide flexibility to adjust the behavior if necessary, in exceptional situations, and aren't recommended changing casually without extensive testing.

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>TEMPLATE_TYPE</b> Specifies the component template type—valid values are: chat, cuic, finesse, ids, livedata, cuic_12.6(1), livedata_12.6(1), and idp-adfs3. <b>Default:</b> livedata_12.6(1)	No	—
<b>NGX_LD_WEB_UPSTREAM_KEEPALIVE</b> Proxy backend configurations for livedata. Activates the cache for connections to the upstream livedata server. Specifies the maximum number of idle keep alive connections to upstream servers that are preserved in the cache of each worker process. When the count exceeds this number, the least recently used connections close. <b>Default:</b> 128	No	—

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>NGX_LD_SIO_UPSTREAM_KEEPALIVE</b> Activates the cache for connections to the upstream livedata server socketio endpoint. <b>Default:</b> 128	No	—
<b>NGX_LD_HTTP1_CONN_LIMIT</b> Specifies the number of concurrent HTTP/1.1 connections allowed per source IP. <b>Default:</b> 12	No	—
<b>NGX_LD_HTTP2_CONN_LIMIT</b> Specifies the number of concurrent HTTP/2 streams allowed per source IP. <b>Default:</b> 150	No	—
<b>NGX_LD_REQUEST_BURST_LIMIT</b> Specifies the HTTP request burst limit. <b>Default:</b> 25	No	—
<b>NGX_LD_PROXY_BUFFER_SIZE</b> <b>Default:</b> 8k	No	—
<b>NGX_LD_MAX_TEMP_FILE_SIZE</b> <b>Default:</b> 100m	No	—

*LiveData 12.6(2) Properties*

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>NGX_PRXY_LD_HOSTNAME</b> Specifies the reverse-proxy hostname over which this LD host is accessed. <b>Default:</b> reverseproxy.host.domain	Yes	If the reverse-proxy livedata host FQDN changes.
<b>NGX_PRXY_LD_PORT</b> Specifies the reverse-proxy port over which this livedata host is accessed. <b>Default:</b> 443	Yes, If required.	If the reverse-proxy port for livedata changes.
<b>NGX_LD_HOSTNAME</b> Specifies the Livedata server hostname. <b>Default:</b> livedata.host.domain	Yes	If the upstream livedata host FQDN changes.



Property Name, Description, and Default	Change Recommended?	When to Change?
<b>NGX_LD_BACKEND_FAILOVER</b> Specifies the livedata failover configurations. This is used to translate the location header during failover. <b>Default:</b> hostname:port	Yes	For the SideA upstream LiveData, point to the upstream SideB LiveData.  For the SideB upstream, point to the upstream SideA.
<b>NGX_LD_BACKEND_PROXY_FAILOVER</b> Specifies the livedata failover node for this livedata host. This is used to translate the location header during failover. <b>Default:</b> hostname:port	Yes	Point to the other side of the reverse-proxy node.

### LiveData 12.6(2) properties that are not recommended to be altered



**Note** These properties are provided for reference and they exist in the configuration to provide flexibility to adjust the behavior if necessary, in exceptional situations and aren't recommended to be changed casually without extensive testing.

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>TEMPLATE_TYPE</b> Specifies the component template type—valid values are: chat, cuic, finesse, ids, livedata, cuic_12.6(1), livedata_12.6(1), and idp-ads3. <b>Default:</b> livedata	No	
<b>NGX_LD_WEB_UPSTREAM_KEEPALIVE</b> Proxy backend configurations for livedata. Activates the cache for connections to the upstream livedata server.  Specifies the maximum number of idle keepalive connections to upstream servers that are preserved in the cache of each worker process. When the count exceeds this number, the least recently used connections are closed. <b>Default:</b> 128	No	
<b>NGX_LD_SIO_UPSTREAM_KEEPALIVE</b> Activates the cache for connections to the upstream livedata server socketIO endpoint. <b>Default:</b> 128	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>NGX_LD_HTTP1_CONN_LIMIT</b> Specifies the number of concurrent HTTP/1.1 connections allowed per source IP. <b>Default:</b> 12	No	
<b>NGX_LD_HTTP2_CONN_LIMIT</b> Specifies the number of concurrent HTTP/2 streams allowed per source IP. <b>Default:</b> 150	No	
<b>NGX_LD_REQUEST_BURST_LIMIT</b> Specifies the HTTP request burst limit. <b>Default:</b> 25	No	
<b>NGX_LD_PROXY_BUFFER_SIZE</b> Sets the size of the buffer used for reading the first part of the response received from the server, which is enabled with reverse-proxy. <b>Default:</b> 8k	No	
<b>NGX_LD_MAX_TEMP_FILE_SIZE</b> When buffering of responses from the server (which is enabled with reverse-proxy) is enabled, and the whole response doesn't fit into the <code>NGX_LD_PROXY_BUFFER_SIZE</code> , a part of the response can be saved to a temporary file. <b>Default:</b> 100m	No	

## CUIC Properties

### Unified Intelligence Center 12.6(1) properties



**Note** Use this env file when the upstream Unified Intelligence Center is still on 12.6(1) release. Otherwise use `cuic.env`.

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>NGX_PRXY_CUIC_HOSTNAME</b> Specifies the reverse-proxy hostname over which this CUIC host is accessed. <b>Default:</b> reverseproxy.host.domain	Yes	If the reverse-proxy CUIC host FQDN changes.

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>NGX_PRXY_CUIC_PORT</b> Specifies the reverse-proxy port over which this cuic host is accessed. <b>Default:</b> 8444	Yes, If required.	New installation or if the port number changes.
<b>NGX_PRXY_CUIC_DOC_PORT</b> Specifies the reverse-proxy port over which this CUIC host doc endpoint is accessed. <b>Default:</b> 8447	Yes, If required.	New installation or if the port number changes.
<b>NGX_CUIC_HOSTNAME</b> Specifies the CUIC server hostname. <b>Default:</b> cuic.host.domain	Yes	If the upstream CUIC host FQDN changes.

#### Unified Intelligence Center 12.6(1) properties that are not recommended to be altered



**Note** These properties are provided for reference and they are available in the configuration. They provide flexibility to adjust the behavior if necessary, in exceptional situations, and aren't recommended changing casually without extensive testing.

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>TEMPLATE_TYPE</b> Specifies the component template type—valid values are: chat, cuic, finesse, ids, livedata, cuic_12.6(1), livedata_12.6(1), idp-ads3. <b>Default:</b> cuic_12.6(1)	No	Never
<b>NGX_CUIC_UPSTREAM_KEEPALIVE</b> Activates the cache for connections to the upstream CUIC server. Specifies the maximum number of idle keep alive connections to upstream servers that are preserved in the cache of each worker process. When this number exceeded, the least recently used connections are closed. <b>Default:</b> 128	No	—
<b>NGX_CUICDOC_UPSTREAM_KEEPALIVE</b> Activates the cache for connections to the upstream CUIC server doc endpoint. <b>Default:</b> 128	No	—

Property Name, Description, and Default	Change Recommended?	When to Change?
NGX_CUIC_CACHE_SIZE Specifies the initial size of the CUIC proxy cache. <b>Default:</b> 15m	No	—
NGX_CUIC_CACHE_MAX_SIZE Specifies the maximum size for the CUIC cache. When the size exceeds or there's not enough free space, the system removes the least recently used data. <b>Default:</b> 50m	No	—
NGX_CUIC_CACHE_INACTIVE_DURATION Specifies the content inactive duration for the CUIC cache. Cached data that is not accessed during the time specified get removed from the cache regardless of their freshness. <b>Default:</b> 3y	No	—
NGX_CUICDOC_CACHE_SIZE Specifies the initial size of the CUIC doc cache. <b>Default:</b> 15m	No	—
NGX_CUICDOC_CACHE_MAX_SIZE Specifies the maximum size for the CUIC doc cache. When the size exceeds or there isn't enough free space, the system removes the least recently used data. <b>Default:</b> 50m	No	—
NGX_CUICDOC_CACHE_INACTIVE_DURATION Specifies the content inactive duration for CUIC doc cache. Cached data that aren't accessed during the time specified get removed from the cache regardless of their freshness. <b>Default:</b> 3y	No	—
NGX_CUIC_HTTP1_CONN_LIMIT Specifies the number of concurrent HTTP/1.1 connections allowed per source IP. <b>Default:</b> 12	No	—
NGX_CUIC_HTTP2_CONN_LIMIT Specifies the number of concurrent HTTP/2 streams allowed per source IP. <b>Default:</b> 150	No	—

Property Name, Description, and Default	Change Recommended?	When to Change?
NGX_CUIC_REQUEST_BURST_LIMIT Specifies the HTTP request burst limit. <b>Default:</b> 100	No	—
NGX_CUIC_HISTORICAL_REPORT_CONN_LIMIT Specifies the number of concurrent connections allowed, per source IP, for CUIC historical reports endpoints. <b>Default:</b> 4	No	—
NGX_CUIC_HISTORICAL_REPORT_NEW_CONN_LIMIT Specifies the number of concurrent connections allowed, per source IP, for CUIC historical reports newRest endpoints. <b>Default:</b> 4	No	—
NGX_CUIC_HISTORICAL_REPORT_REQUEST_BURST_LIMIT Specifies the HTTP request burst limit for CUIC historical reports endpoints. <b>Default:</b> 4	No	—
NGX_CUIC_REALTIME_REPORT_CONN_LIMIT Specifies the number of concurrent connections allowed, per source IP, for CUIC realtime reports endpoints. <b>Default:</b> 4	No	—
NGX_CUIC_REALTIME_REPORT_NEW_CONN_LIMIT Specifies the number of concurrent connections allowed, per source IP, for CUIC realtime reports newRest endpoints. <b>Default:</b> 4	No	—
NGX_CUIC_REALTIME_REPORT_REQUEST_BURST_LIMIT Specifies the HTTP request burst limit for CUIC realtime reports endpoints. <b>Default:</b> 4	No	—
NGX_CUIC_REPORT_EXECUTION_REQUEST_BURST_LIMIT Specifies the HTTP request burst limit for CUIC reports execution endpoints. <b>Default:</b> 4	No	—

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>NGX_CUIC_PROXY_BUFFER_SIZE</b> Specifies the size of the buffer used for reading the first part of the response received from the server, which is enabled for reverse-proxy. <b>Default:</b> 8k	No	—
<b>NGX_CUIC_MAX_TEMP_FILE_SIZE</b> When buffering of responses from the server (which is enabled for reverse-proxy) is enabled, and the whole response doesn't fit into the buffers set by the <code>NGX_CUIC_PROXY_BUFFER_SIZE</code> , a part of the response is saved to a temporary file. <b>Default:</b> 100m	No	—

*Unified Intelligence Center 12.6(2) properties*

Property Name, Description, and Default	Change Recommended?	When to Change?
<b>NGX_PRXY_CUIC_HOSTNAME</b> Specifies the reverse-proxy hostname over which this cuic host is accessed. <b>Default:</b> reverseproxy.host.domain	Yes	If the reverse-proxy CUIC host FQDN changes.
<b>NGX_PRXY_CUIC_PORT</b> Specifies the reverse-proxy port over which this cuic host is accessed. <b>Default:</b> 443	Yes, If required.	If the reverse-proxy port changes.
<b>NGX_CUIC_HOSTNAME</b> Specifies the CUIC server hostname. <b>Default:</b> cuic.host.domain	Yes	If the upstream CUIC host FQDN changes.

**Unified Intelligence Center 12.6(2) properties that are not recommended to be altered**


---

**Note** These properties are provided for reference and they exist in the configuration to provide flexibility to adjust the behavior if necessary, in exceptional situations and aren't recommended changing casually without extensive testing.

---

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>TEMPLATE_TYPE</p> <p>Specifies the component template type—valid values are: chat, cuic, finesse, ids, livedata, cuic_12.6(1), livedata_12.6(1), and idp-ads3.</p> <p><b>Default:</b> cuic</p>	No	
<p>NGX_CUIC_UPSTREAM_KEEPALIVE</p> <p>Activates the cache for connections to the upstream CUIC server.</p> <p>Specifies the maximum number of idle keepalive connections to upstream servers that are preserved in the cache of each worker process. When the count exceeds this number, the system closes the least recently used connections.</p> <p><b>Default:</b> 128</p>	No	
<p>NGX_CUIC_CACHE_SIZE</p> <p>Specifies the initial size of the CUIC cache.</p> <p><b>Default:</b> 30m</p>	No	
<p>NGX_CUIC_CACHE_MAX_SIZE</p> <p>Specifies the maximum size for the CUIC cache. When the size exceeds the set maximum, or there isn't enough free space, the system removes the least recently used data.</p> <p><b>Default:</b> 100m</p>	No	
<p>NGX_CUIC_CACHE_INACTIVE_DURATION</p> <p>Specifies the content inactive duration for the CUIC cache. Cached data that aren't accessed during the time specified get removed from the cache regardless of their freshness.</p> <p><b>Default:</b> 3y</p>	No	
<p>NGX_CUIC_HTTP1_CONN_LIMIT</p> <p>Specifies the number of concurrent HTTP/1.1 connections allowed per source IP.</p> <p><b>Default:</b> 12</p>	No	
<p>NGX_CUIC_HTTP2_CONN_LIMIT</p> <p>Specifies the number of concurrent HTTP/2 streams allowed per source IP.</p> <p><b>Default:</b> 150</p>	No	
<p>NGX_CUIC_REQUEST_BURST_LIMIT</p> <p>Specifies the HTTP request burst limit.</p> <p><b>Default:</b> 100</p>	No	

Property Name, Description, and Default	Change Recommended?	When to Change?
<p>NGX_CUIC_HISTORICAL_REPORT_CONN_LIMIT</p> <p>Specifies the number of concurrent connections allowed per source IP for CUIC historical reports endpoints.</p> <p><b>Default: 4</b></p>	No	
<p>NGX_CUIC_HISTORICAL_REPORT_NEW_CONN_LIMIT</p> <p>Specifies the number of concurrent connections allowed per source IP for CUIC historical reports newRest endpoints.</p> <p><b>Default: 4</b></p>	No	
<p>NGX_CUIC_HISTORICAL_REPORT_REQUEST_BURST_LIMIT</p> <p>Specifies the HTTP request burst limit for CUIC historical reports endpoints.</p> <p><b>Default: 4</b></p>	No	
<p>NGX_CUIC_REALTIME_REPORT_CONN_LIMIT</p> <p>Specifies the number of concurrent connections allowed per source IP for CUIC realtime reports endpoints.</p> <p><b>Default: 4</b></p>	No	
<p>NGX_CUIC_REALTIME_REPORT_NEW_CONN_LIMIT</p> <p>Specifies the number of concurrent connections allowed per source IP for CUIC realtime reports new REST endpoints.</p> <p><b>Default: 4</b></p>	No	
<p>NGX_CUIC_REALTIME_REPORT_REQUEST_BURST_LIMIT</p> <p>Specifies the HTTP request burst limit for CUIC realtime reports endpoints.</p> <p><b>Default: 4</b></p>	No	
<p>NGX_CUIC_REPORT_EXECUTION_REQUEST_BURST_LIMIT</p> <p>Specifies the HTTP request burst limit for CUIC reports execution endpoints.</p> <p><b>Default: 4</b></p>	No	
<p>NGX_CUIC_PROXY_BUFFER_SIZE</p> <p>Configurations overridden from common config for CUIC.</p> <p>Specifies the size of the buffer used for reading the first part of the response received from the server, which is enabled for reverse-proxy.</p> <p><b>Default: 8k</b></p>	No	



Property Name, Description, and Default	Change Recommended?	When to Change?
<p data-bbox="131 289 574 321">NGX_CUIC_MAX_TEMP_FILE_SIZE</p> <p data-bbox="131 338 894 464">When buffering of responses from the server (which is enabled for reverse-proxy) is enabled, and the whole response doesn't fit into the buffers set by the NGX_CUIC_PROXY_BUFFER_SIZE, a part of the response is saved to a temporary file.</p> <p data-bbox="131 480 302 512"><b>Default:</b> 100m</p>	No	





## APPENDIX **B**

# Guidelines for Custom Reverse Proxy Deployment

This appendix provides you with guidelines for deploying an appropriate reverse proxy.



**Note** These guidelines are provided as best effort and Cisco does not claim support for any custom reverse proxy deployments.

- [Reverse proxy selection and configuration for digital channel interactions, on page 375](#)
- [Reverse proxy selection and configuration for VPN-less access to Finesse Desktop, on page 377](#)

## Reverse proxy selection and configuration for digital channel interactions

### Minimum and additional requirements

#### Minimum requirements

Contact Center administrators must select an appropriate reverse proxy. Any reverse proxy that meets the following minimum requirements can be used:

- Supports HTTP2/TLS 1.2.
- Has proper logging mechanism for easy debugging of issues and includes Tracking ID to easily track the task requests.
- Supports failover between the Cloud Connect nodes with health check.
- Supports X-Forwarded headers. The solution uses these headers to decide how to handle a request when front-ended with load balancer.

#### Additional Requirements

Some desirable requirements in a reverse-proxy are as follows:

- Consider deploying proxies that are built on non-blocking IO-based technology instead of the traditional thread-per-request architecture, to scale better.

- Apply rate limiting and configure allowed list of Webex Connect or Load balancer IPs.

### Performance and hardware recommendation

For details, see [Performance and Hardware Recommendations, on page 258](#).

## Configure custom reverse proxy

Install the host OS and reverse-proxy of your choice. Consider the following points while configuring the reverse-proxy:

- Configure SSL certificates as required.
- Configure the Mutual Transport Layer Security (mTLS) authentication between reverse proxy and Cloud Connect.
  - Add the list of trusted reverse proxy IP addresses and the corresponding hostnames on the publisher and subscriber nodes of Cloud Connect. For details, see [Add Proxy IP, on page 66](#).
  - Configure SSL certificate verification to establish communication between the reverse proxy host and the Digital Routing service. For details, see [Configure reverse proxy host verification, on page 67](#).
- Configure both nodes (publisher and subscriber) of Cloud Connect for task requests. Implement HTTP health check and failover to the subscriber node. The health check API that the Digital Routing service supports is `/drapi/v1/ping`.
- The DataConn callback requests are routed through the reverse proxy. Configure the DataConn requests to the upstream Cloud Connect publisher node. The DataConn service runs only on the publisher node of CloudConnect.

## Host header configuration

The following are the mandatory HTTP headers that reverse-proxy has to set along with the actual headers set by the client before forwarding the headers to the Finesse server.

**Table 20: Host header and description**

Header	Description
X-Client-IP	The reverse-proxy must populate this custom header as the client's IP address before forwarding it to Cloud Connect.
X-Real-IP	

Header	Description
Host	<p>The Host request header specifies the host and port number of the server to which the request is being sent. If no port is included, the default port for the service requested (for example, 443 for an HTTPS URL and 80 for an HTTP URL) is used. An HTTP/1.1 proxy ensures that any request message it forwards contains an appropriate Host header field to identify the service being requested by the proxy.</p> <p>This value is used by Cloud Connect to find if the request is sent via the allowed list of proxies configured in Cloud Connect.</p>
X-Forwarded-For	<p>The <b>X-Forwarded-For</b> (XFF) header is used for identifying the originating IP address of a client connecting to a web server through an HTTP proxy or a load balancer.</p> <p>The IP of the reverse-proxy has to be appended or set.</p> <p>Cloud Connect uses this header to find if the request is from the allowed list of reverse-proxies. When the request is forwarded through multiple reverse-proxies or load balancer, the values of all reverse-proxies are appended to the rightmost value of this header.</p>
X-Forwarded-Port	<p>The reverse-proxy should set the listening port on this header. Cloud Connect server receives all the requests internally via 8445 port.</p>
Connection	<p>Any Connection value in the HTTP header that is set by the client must be cleared and forwarded to the Cloud Connect server so that the server decides the connection management and not the client. This prevents security outages.</p>

# Reverse proxy selection and configuration for VPN-less access to Finesse Desktop

## Minimum and additional requirements

### Minimum requirements

Contact Center administrators must select an appropriate reverse-proxy. Any reverse-proxy that meets the following minimum requirements can be used:

- Supports HTTP2/TLS 1.2 and secure Websockets.

- Has proper logging mechanism for easy debugging of issues
- Supports multiple Finesse, IdS, and CUIC servers from a single reverse-proxy.
- Supports periodic revalidation of cached content. This is required because any updates or installations on the internal hosts don't require a manual intervention to clear the cached content of the proxy.
- Supports custom authentications or provides alternative mechanisms such as an enterprise login to prevent unauthenticated access of solution components.




---

**Note** When you use Cisco-provided reverse-proxy configuration, the requests are authenticated at the proxy before they are forwarded to the upstream servers. When you are configuring a custom reverse-proxy, you must create this authentication layer if they have to be as secure as the Cisco provided configuration. You should consider this configuration step while planning to implement VPN-less access to Finesse using a custom reverse-proxy.

---

- Enables caching of static resources with support for cache-control header to reduce DoS/DDoS attack vectors and to scale the proxy. Any proxy that needs to support more than a few hundred users and does not provide response caching features should be deployed with a Content Delivery Network (CDN) with support for cache-control headers so that load and security guidelines are met.




---

**Note** CDN deployment is also recommended with caching proxies such as OpenResty<sup>®</sup> Nginx to eliminate the impact of DDoS attacks.

---

- Supports X-Forwarded headers. These headers are used by the solution to decide how to handle a request.

### Additional Requirements

Some desirable requirements in a reverse-proxy are as follows:

- Consider deploying proxies that are built on non-blocking IO-based technology instead of the traditional thread-per-request architecture, to scale better.
- Consider proxies that provide response substitution capabilities which allow workarounds for custom gadgets as custom gadgets may not work with reverse-proxy directly.




---

**Note** Finesse Desktop Chat over reverse-proxy requires response substitution capability.

---

- Support for port-based forwarding can be used to reduce the cost of deployment by avoiding the need for multiple externally resolvable hostnames, public DNS records, and corresponding certificates for each internal server that has to be accessed.
- Support for custom plugin/modules, which can be used to enhance the authentication model and provide a more robust security posture.

### Performance and hardware recommendation

For details, see [Performance and Hardware Recommendations, on page 258](#).

## Configure Reverse-Proxy

Install the host OS and reverse-proxy of your choice. Consider the following points while configuring the reverse-proxy:

- Configure SSL certificates as required.
- Refer to the specific proxy documentation and configure the proxy rules for each service with the same host and port that is configured in the mapping file.
- IdS and IdP trust should be configured before proxy mapping configuration is done. Otherwise, proxy configuration changes will not be processed by IdS.
- For IdS hosts, if proxy configuration is changed, the administrator must re-establish trust on IdP for new IdS proxy hosts after downloading new metadata file from IdS admin.
- For Finesse hosts, if proxy configuration is changed, the administrator must manually add or update the allowed Finesse client redirect URIs from IdS administration interface.
- Whenever SAML certificate is regenerated or IdP metadata is uploaded, proxy configurations are generated afresh.

To secure the reverse-proxy, refer to the *Security Guidelines* section in the [Security Guide for Cisco Unified ICM/Contact Center Enterprise](#).

## Host Header Configuration

The following are the mandatory HTTP headers that reverse-proxy has to set along with the actual headers set by the client before forwarding the headers to the Finesse server.

**Table 21:**

Header	Description
X-Client-IP	The reverse-proxy should populate this custom header as the client's IP address before forwarding it to the Finesse server.  This is used to log the client's IP in the Finesse server.

Header	Description
Host	<p>The Host request header specifies the host and port number of the server to which the request is being sent. If no port is included, the default port for the service requested (for example, 443 for an HTTPS URL and 80 for an HTTP URL) is used. An HTTP/1.1 proxy ensures that any request message it forwards contains an appropriate Host header field to identify the service being requested by the proxy.</p> <p>This value is used by Finesse to find if the request is sent via the allowed list of proxies configured in Finesse.</p> <p>The hostname and port value of the reverse-proxy should be set. Otherwise, the Finesse validation fails and returns HTTP 400 Error.</p>
X-Forwarded-For	<p>The <b>X-Forwarded-For</b> (XFF) header is used for identifying the originating IP address of a client connecting to a web server through an HTTP proxy or a load balancer.</p> <p>The IP of the reverse-proxy has to be appended or set.</p> <p>Finesse uses this header to find if the request is from the allowed list of reverse-proxies. When the request is forwarded through multiple reverse-proxies, the values of all reverse-proxies are appended to the rightmost value of this header.</p>
X-Forwarded-Port	<p>The reverse-proxy should set the listening port on this header. Finesse server receives all the requests internally via 8445 port. This header value helps Finesse to set the valid configuration.</p>

The following are the standard headers manipulated by the proxy:

**Table 22:**

Header	Description
Connection	<p>Any Connection value in the HTTP header that is set by the client should be cleared and forwarded to the Finesse server. This has to be done so that the Finesse server decides the connection management and not the Finesse client. This prevents security outages.</p>
Accept-Encoding	<p>The reverse-proxy clears the Accept-Encoding header to have better control over compression aspects of the response.</p>