# Cisco Unified Contact Center Enterprise Installation and Upgrade 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 NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: 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.

# CONTENTS


PREFACE

**Preface** xvii

Change History xvii

About This Guide xviii

Audience xviii

Related Documents xviii

Communications, Services, and Additional Information xix

Field Notice xix

Documentation Feedback xx

Conventions xx

CHAPTER 1

**Preparation** 1

Scenarios 1

Installation Scenario 1

Upgrade Scenarios 2

System Requirements 3

Platform Requirements 4

Network Requirements 5

Transport Layer Security Version 1.2 Required 5

Software License Requirements 5

Virtualization Requirements 5

ESXi Supportability 6

Compatibility Requirements 6

Java Requirements 7

CHAPTER 2

**Installation Overview** 9

Installation Tools 9

CHAPTER 3 Preinstallation 11

Preinstallation Task Flow 11

Preinstallation Tasks 11

Set up Active Directory 11

Set Up Virtual Machines 12

Verify Datastores 12

Configure HyperFlex M5 Series and M6 Series 12

Configure RAID for Cisco UCS C240 M5SX and Cisco UCS C240 M6SX 12

Download Unified CCE OVA Files 13

Create a Virtual Machine from the OVA 13

Allocate a Second Virtual Hard Drive 15

Mount ISO Files 16

Unmount ISO File 16

Set Up Third-Party Software 16

Install Microsoft Windows Server 16

Install Microsoft Windows 11 for Administration Client 18

Set Windows Locale 20

Install Vmware Tools 20

Initialize and Format Secondary Disk 21

Install Microsoft SQL Server 21

Increase Database and Log File Size for TempDB 25

Install Antivirus Software 25

Set Up Virtual Machines for Installation 27

Validate Network Adapter Settings and Power On 27

Configure Network Cards 27

Set Persistent Static Routes 28

Configure Private Ethernet Card 28

Configure Public Ethernet Card 29

Verification of the Downloaded ISO or Minor Release Installer 30

CHAPTER 4 Installation 31

Installation Task Flow 31

Installation Tasks 32

Install Unified CCE Software 33
Set up Organizational Units 34
Add a Domain 34
Add Organizational Units 34
Add Users to Security Groups 35
Add Unified CCE Instance 36
Set Up Unified CCE Central Controller and Administration and Data Server Components 36
Create Component Databases 36
Add Components to Unified CCE Instance 39
Set up Peripheral Gateways 44
Configure Peripheral Gateways in PG Explorer 44
Add Peripherals to Peripheral Gateways 45
Configure Peripheral Gateway Setup 48
Install Cisco JTAPI Client on PG 51
Set up CTI Server 53
Add CTI Server Component 54
Set CTI Server Properties 54
Set CTI Server Component Properties 54
Set CTI Server Network Interface Properties 56
Complete CTI Server Setup 56
Install Unified CCE Administration Client 56
Install Administration Client 56
Set Up Administration Client 57
Install Unified CCE Language Pack 58
Java Upgrades 58
Upgrade OpenJDKUtility 59
Upgrade Tomcat Utility 59
Install Tomcat 60
Silent Installation 60
Silent Installation Prerequisites for Unified CCE Release 12.5(1) 60
Perform a Silent Installation for Unified CCE Release 12.5(1) 61
Silent Installation Prerequisites for Unified CCE Release 12.6(2) 61
Perform a silent installation for Unified CCE Release 12.6(2) 62
Set Deployment Type in Unified CCE Administration Configuration 62

Cisco Finesse Server Installation 63
Installation Task Flow 63
Install Finesse on Primary Node 64
Configure Contact Center Enterprise Administration and Data Server settings 67
Contact Center Enterprise CTI Server Settings 68
Restart Cisco Finesse Tomcat 71
Validate Configuration 71
Configure Cluster Settings 72
Install Finesse on Secondary Node 72
Check Replication Status 75
Install Cisco Identity Service Standalone Deployment 75
Install Publisher/Primary Node of Cisco Identity Service 75
Set IdS Subscriber Node 77
Install Subscriber/Secondary Node of Cisco Identity Service 77
Live Data Standalone Installation 79
Install Publisher/Primary Node of Live Data 79
Set Live Data Secondary Node 80
Install Subscriber/Secondary node of Live Data 81
Configure Live Data Machine Services 82
Configure Live Data for Unified Intelligence Center Data Sources 83
Configure Cross Origin Resource Sharing (CORS) for Live Data 83
Restart Live Data 84
Set Up Certificates for Live Data 84
Install Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS) 84
Install Publisher/Primary Node of Co-resident Deployment (Cisco Unified Intelligence Center with Live Data and IdS) 85
Install Subscriber/Secondary Node of Co-resident Deployment (Cisco Unified Intelligence Center with Live Data and IdS) 87
Add Coresident (Cisco Unified Intelligence Center with Live Data and IdS) Machine Type to the System Inventory 88
Configure Live Data Unified Intelligence Center Data Sources 89
Restart Live Data 89
Install Cloud Connect 89
Install Publisher or Primary Node of Cloud Connect 90
Set Subscriber or Secondary Node of Cloud Connect 91

Install Subscriber or Secondary Node of Cloud Connect 91
Initial Configuration for Cloud Connect 92
Install VMware Tools for VOS 93

CHAPTER 5 **Initial Configuration** 95
Initial Configuration Overview 95
Initial Configuration Task Flow 95
Initial Configuration Tasks 96
Configure Permissions in the Local Machine 96
Configure Registry Permissions 96
Configure AW-HDS Database Permissions 96
Configure Folder Permissions 97
Configure Cisco Unified Contact Center Enterprise 97
Access Configuration Manager tool 98
Configure Media Routing Domain 98
Configure Trunk Groups 99
Configure Network VRU Bank 100
Configure services 101
Configure dialed numbers 102
Configure call types 104
Configure Variables 105
Configure Users 109
Configure Network VRUs 116
Configure scripts 117
Configure Agent Targeting Rules 120
Configure translation routes 120
Configure Skill Groups or Precision Routing 122
Configure Precision Routing 125
Configure routes 131
Perform Bulk Configuration 132
Configure Cisco Unified Intelligence Center 137
Sign In to Administration Console 137
Configure SQL User Account 138
Configure Data Sources 138

Download Report Bundles 142
Import Report Bundles 143
Configure Unified Intelligence Center Administration 143
Configure Cisco Unified Customer Voice Portal 144
Configure Unified CVP Server 144
Configure Unified CVP Reporting Server 145
Configure Unified CVP Operations Console 148
Configure Cisco Unified Communications Manager 162
Set Up Device Pool 162
Set Up Unified Communications Manager Groups 162
Set Up CTI Route Point 163
Set Up Trunk 163
Set Up Application User 164
Set Up SIP Options 164
Set Up Route Pattern 165
Set Up Conference Bridge 165
Set Up Media Termination Point 165
Set Up Transcoder 166
Set Up Media Resource Group 166
Set Up and Associate Media Resource Group List 166
Set Up Enterprise Parameters 167
Configure Mobile Agent 167
Configure Local Trunk 168
Configure Outbound Dialer 169
Configure A-Law Codec 170
Configure Support for Multiline Agent Control 170
Configure Caller-Specific Music on Hold 171
Configure Cisco Finesse 172
Configure Contact Center Enterprise CTI Server Settings 172
Configure Contact Center Enterprise Administration and Data Server Settings 173
Configure Cluster Settings 174
Restart Cisco Finesse Tomcat 175
Check Replication Status 175
Ensure Agents Have Passwords 175

Ensure Logout Non-Activity Time for Agents is Configured 176
Ensure Agents Can Sign in to Desktop 176
Obtain and Upload CA Certificate 177
Deploy Certificate in Browsers 179
Accept Security Certificates 180
Browser Settings for Firefox 183
Browser Settings for Chrome 183
Configure DNS on Clients 183
Live Data Reports 184
Initial Configuration Troubleshooting 190

CHAPTER 6 **Upgrade Overview** 193
Upgrade Overview 193
Multistage Upgrade Workflow for 2000 Agents Deployment 196
Upgrade Flowcharts 202
Multistage Upgrade Workflow for 4000 Agents and above Deployments 209
Upgrade Flowcharts 214
Data Migration Considerations 223
Enable and Disable TDE on a Database 225
Silent Upgrade 226
Unified CCE Upgrade Overview 226
Upgrade Prerequisites 227
Upgrade CCE Minor/Maintenance Release Software 227
Custom Truststore to Store Component Certificates 227
Upgrade Cloud Connect 228

CHAPTER 7 **Common Ground Upgrade** 231
Preupgrade Overview 231
Common Ground Preupgrade Task Flow 232
Common Ground Preupgrade Tasks 234
Disable Configuration Changes 234
Virtual Machine Snapshot for Unified CCE Component Virtual Machines 234
VM Hardware Version Upgrade 234

Increase the Provisioned Disk Size for Unified Intelligence Center VMs (Standalone and Coresident) 235
Common Ground Upgrade Task Flow 236
Common Ground Upgrade Tasks 239
Migrate Unified CCE Logger Database and Upgrade Logger 239
Upgrade Unified CCE Call Router 241
Migrate HDS Database and Upgrade Unified CCE Administration & Data Server 241
Upgrade Unified CCE Administration Client 242
Enable Configuration Changes 243
Upgrade Peripheral Gateways 243
Upgrade Outbound Option Dialer 244

CHAPTER 8 **Common Upgrade Tasks** 245
Upgrade Voice and Data Gateways 245
Bring Upgraded Side A into Service 246
Verify Operation of Upgraded Side B Call Router and Logger 247
Disable Outbound Options High Availability (If Applicable) 249
Upgrade Cisco JTAPI Client on PG 250
Database Performance Enhancement 250
Performance Enhancement of TempDB 250
Performance Enhancement of Logger Database 251
Performance Enhancement of AW-HDS Database 252
Improve Reporting Performance 252
Reduce Reserved Unused Space for HDS and Logger 252
Update User Role 253
Certificates for Unified Contact Center Enterprise Web Administration 253
CA Certificates 253
Generate CSR 255
Create Trusted CA-Signed Server or Application Certificate 255
Import CA Certificate into AW Machines 256
Upload and Bind CA-Signed Certificate 257
Self-signed Certificates 258
Import Unified CCE Component Certificates 259
Import VOS Components Certificate 261

Certificates for Live Data 261
Certificates and Secure Communications 261
Self-Signed Certificates and Third-Party CA Certificates 262
Produce Certificate Internally 264
Set Up CA Certificate for Firefox Browser 265
Change Java Truststore Password 266

CHAPTER 9 Technology Refresh Upgrade 267
Preupgrade Overview 267
Technology Refresh Preupgrade Task flow 268
Disable Configuration Changes 268
Export the Server Registry 268
Technology Refresh Upgrade Task Flow 269
Technology Refresh Upgrade Tasks 272
Migrate the Logger Database and Upgrade the Logger 272
Upgrade Unified CCE Call Router 275
Migrate the HDS Database and Upgrade the Unified CCE Administration & Data Server 276
Synchronizing or Updating Configuration and Historical Data from Production Server to Staged Server During Cut Over 278
Upgrade Peripheral Gateways 279
Upgrade Outbound Option Dialer 280
Upgrade Unified CCE Administration Client 280

CHAPTER 10 Upgrade from a Standalone Deployment to a Coresident Deployment 281
Set Deployment Type in Unified CCE Administration Configuration 281
Install Publisher/Primary Nodes of VOS-Based Contact Center Applications 282
Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications 283
Set Up the System Inventory 285
Configure Live Data with AW 285
Configure Live Data Unified Intelligence Center Data Sources 286
Restart Live Data 286

CHAPTER 11 Uninstallation 287
Uninstallation of Unified ICM/CCE base version 12.5(1) 287

Prerequisite for Uninstallation of CCE 12.6(2) Maintenance Release 287
Uninstall Unified CCE 12.6(2) 288

CHAPTER 12 Testing 289
Testing Overview 289
Testing Tasks 289
Verify Upgrade to Cisco Unified Customer Voice Portal 289
Verify IOS Gateway Upgrade 290
Verify Upgrade to Cisco IOS-Based Transcoders and Conference Bridges 291
Verify Upgrade to Cisco Unified CCE Router and Logger 291
Verify Upgrade to Cisco Real Time Administration Workstation, Historical Database Server 292
Verify Upgrade to Peripheral Gateways 293
Verify Redundancy 293
Verify Upgrade to Cisco Unified Communications Manager 293

CHAPTER 13 CCE Orchestration 295
Overview 295
Email Notification 295
Orchestration in CCE Deployment 296
System Requirements 296
Orchestration Support using Cloud Connect Server 297
Parallel Running of CLI 297
Orchestration Deployment Task Flow 298
Administration Task Flow 298
Maintenance Task Flow 299
Deployment Tasks 299
Generate the Artifactory API Key 299
CLI to configure proxy for orchestration 300
CLI to configure artifactory URL and API key 301
Onboard VOS Nodes to Orchestration Control Node 305
Onboard Windows nodes to orchestration control node 306
Add Deployment Type and Deployment Name 308
Validate Onboarded Nodes for Orchestration 308
Configure Email Notification 309

Configure Windows Server for Updates (Optional) 311
Administration Tasks 311
Check Installed Software Version and Patches 311
Install or Rollback Patch or Upgrade Cloud Connect Server 312
List Available Patches for Specific Node or Group of Nodes 313
Install Patch to Specific Node or Group of Nodes 313
Roll Back Patch from Specific Node or Group of Nodes 314
Install Windows Updates to Specific Node or Group of Nodes 315
Roll Back Windows Update from Specific Node or Group of Nodes 317
Enable or Disable Compatibility Enforcement 318
Initiate maintenance mode for a specific node(s) 319
List Available Upgrade Options 320
Upgrade a Specific Node or Group of Nodes or All Nodes 320
Perform Switch Forward on Specific VOS Node or Group of Nodes 322
Roll Back Upgrade from Specific Node or Group of Nodes 322
Check Status 323
Check Last Known Orchestration Operation Status on Remote Node 324
Start Unified ICM Services 324
Maintenance Tasks 325
CLI to configure software download schedule 325
CLI to configure the bandwidth for Orchestration software download 325
Enforce software download from Cisco hosted software artifactory 327
Update VOS Nodes Onboarded to Orchestration Control Node 327
Remove VOS Nodes from Orchestration Control Node 327
Update Windows Nodes Onboarded to Orchestration Control Node 328
Validate Updated Nodes Onboarded for Orchestration 328
Configure Email Configuration 328
Delete Configuration for Email Notification 329
Unsubscribe Email Notification 330
Export and Import of Nodes Managed by Orchestration Control Node 330
Export Current Patch Level Details 331
Serviceability 332
Enable and View Windows Open SSH Logs 333
Configure SSH public key on Windows nodes 333

Self-Signed Certificate 334
Get Tomcat Certificate from Cloud Connect Server 334
Import Cloud Connect Server Tomcat Certificate to VOS Nodes 335
Things to Know 335

APPENDIX A **CLI Commands during Installation and Upgrade** 337
Live Data CLI Commands 337
Supported Character Set for Live Data Installation CLI Commands 337
Privilege Levels for Live Data Commands 338
Live Data AW DB Access 338
set live-data aw-access 338
unset live-data aw-access 339
show live-data aw-access 339
Live Data Cluster Configuration 339
set live-data secondary 339
unset live-data secondary 340
show live-data secondary 340
Live Data Reporting Configuration 340
set live-data reporting-interval 340
show live-data reporting-interval 341
unset live-data reporting-interval 341
Live Data Services Registration 341
set live-data cuic-datasource 341
show live-data cuic-datasource 342
unset live-data cuic-datasource 343
set live-data machine-services 343
show live-data machine-services 344
set live-data network-buffer 344
show live-data network-buffer 345
unset live-data network-buffer 345
show live-data appd-monitoring status 345
set live-data appd-monitoring enable 345
set live-data appd-monitoring disable 346
Live Data CORS Configuration 346

utils live-data cors status 346
utils live-data cors enable 347
utils live-data cors disable 347
utils live-data cors allowed_origin list 347
utils live-data cors allowed_origin add 347
utils live-data cors allowed_origin delete 348
utils live-data cors allowed_headers list 348
utils live-data cors allowed_headers add 348
utils live-data cors allowed_headers delete 349
utils live-data cors exposed_headers list 349
utils live-data cors exposed_headers add headers 349
utils live-data cors exposed_headers delete 350
Transport Layer Security CLI Commands 350
TLS Server Minimum Version 350
set tls server min-version 350
show tls server min-version 350
TLS Client Minimum Version 351
set tls client min-version 351
show tls client min-version 351
Cloud Connect CLI Command 351
set cloudconnect subscriber 351
show cloudconnect subscriber 351
unset cloudconnect subscriber 352
set cloudconnect cherrypoint config 352
show cloudconnect cherrypoint config 353
utils cloudconnect cherrypoint test-connectivity 353
set cloudconnect digitalrouting config 353
show cloudconnect digitalrouting config 353
show cloudconnect digitalrouting status 354
utils cloudconnect reinit services 354

APPENDIX B **Migrate from Co-resident Deployment to Standalone Deployment** 355
Upgrade from Co-resident to Standalone Deployments 355
Set up the System Inventory for Standalone Deployment 356

Upgrading Live Data for 24k Deployment Type 356

APPENDIX C **IPv6 Configuration 359**

Configure NAT64 for IPv6-Enabled Deployment 359

Configure DNS for IPv6 360

Determine IPv6 Translation of IPv4 Address for DNS Entry 360

Set Up IPv6 for VOS-Based Contact Center Applications 361

Set Up IPv6 Using Cisco Unified Operating System Administration 361

Set Up IPv6 for VOS-Based Applications Using the CLI 362

# Preface


- Change History, on page xvii
- About This Guide, on page xviii
- Audience, on page xviii
- Related Documents, on page xviii
- Communications, Services, and Additional Information, on page xix
- Field Notice, on page xix
- Documentation Feedback, on page xx
- Conventions, on page xx


## Change History

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

| Change | See | Date |
|---|---|---|
| **Initial Release of Document for Release 12.6(2)** | | April 2023 |
| Simplified upgrade using orchestration | CCE Orchestration | |
| | CLI to configure software download schedule | |
| | CLI to configure the bandwidth for Orchestration software download | |
| | Enforce software download from Cisco hosted software artifactory | |
| | CLI to configure proxy for orchestration | |
| | Serviceability enhancement for entitlement failure update in CLI to configure artifactory URL and API key | |
| Unified ICM upgrade path | Unified CCE Upgrade Overview | |
| Multistage upgrade | Multistage UpgradeWorkflow for 4000 Agents and above Deployments | |
| Java Upgrade | Java Requirements | |

# About This Guide

This guide describes how to install the components and software for a new Unified CCE system, or to upgrade an existing Unified CCE system.

# Audience

This guide is intended for users who install and upgrade Unified CCE contact centers.

The procedures assume that the system has been thoroughly designed and staged in preparation for the installation or upgrade.

# Related Documents

| Subject | Link |
|---|---|
| Design considerations and guidelines for deploying a Unified CCE solution, including its various components and subsystems. | Design Guide |

| Subject | Link |
|---|---|
| System diagrams, staging steps and sample test cases for supported models of Unified CCE. | Staging Guide |
| Pre-installation requirements and issues to address when you prepare for a Unified CCE installation. | Preinstallation and Planning |

# 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

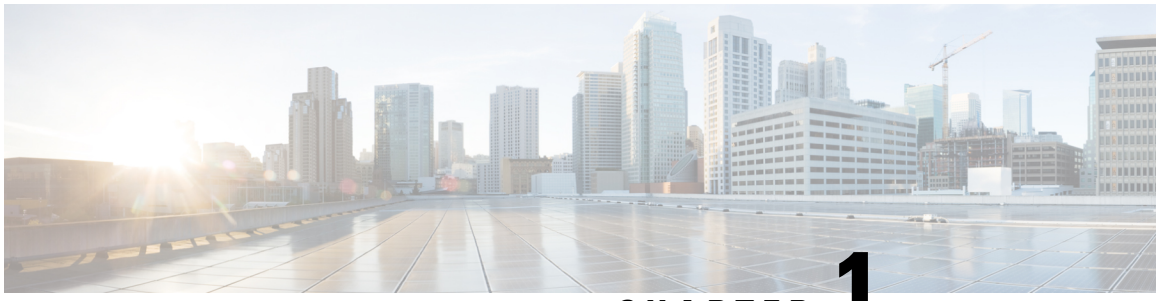
To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.

# Conventions

This document uses the following conventions:

| Convention | Description |
|---|---|
| **boldface** font | Boldface font is used to indicate commands, such as user entries, keys, buttons, folder names, and submenu names.<br>For example:<br>• Choose **Edit** > **Find**.<br>• Click **Finish**. |
| *italic* font | Italic font is used to indicate the following:<br>• To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills.<br>• A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*)<br>• A book title. Example: See the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*. |
| `window font` | Window font, such as Courier, is used for the following:<br>• Text as it appears in code or that the window displays. Example:<br>`<html><title>Cisco Systems, Inc. </title></html>` |
| `< >` | Angle brackets are used to indicate the following:<br>• For arguments where the context does not allow italic, such as ASCII output.<br>• A character string that the user enters but that does not appear on the window such as a password. |



CHAPTER 1

# Preparation


- Scenarios, on page 1
- System Requirements, on page 3


# Scenarios

Cisco Unified Contact Center Enterprise (Unified CCE) is supported only in a virtualized environment.

## Installation Scenario

The CCE components are supported on the following platforms in 12.6(2) release:

- Microsoft Windows Server 2016 and Microsoft SQL Server 2017
- Microsoft Windows Server 2019 and Microsoft SQL Server 2019

**Note** The cross combination of platforms is not supported. For example, Windows Server 2016 with SQL Server 2019 or Windows Server 2019 with SQL Server 2017.

In a virtualized environment, you can run Unified CCE on a VMware ESXi platform. Run the virtual machines (VMs) on Cisco Unified Computing System (UCS) C-series servers, or equivalent third-party servers.

Install the Unified CCE components after you configure the VMs.

You can use the OVA template to deploy the VMs before beginning with the installation of Unified CCE components.

**Note** Deploying VM with Guest Operating System 'Microsoft Windows Server 2019' on ESXi 7.0 using CCE OVA template displays a warning message, "The configured guest OS (Microsoft Windows Server 2016 or later (64-bit)) for this virtual machine does not match the guest that is currently running (Microsoft Windows Server 2019 (64-bit)). You should specify the correct guest OS to allow for guest-specific optimization". This warning message is informational only and has no detrimental effect on the system. This warning message is displayed only once and can be ignored.

The Unified CCE 12.6(2) installer is available as an add-on release to Unified CCE 12.5(1). Therefore, complete the installation of the base Unified CCE 12.5(1) before applying Unified CCE 12.6(2).

**Note** During Unified CCE installation on Windows Server 2019 and SQL Server 2019, do not select SQL Server Security Hardening optional configuration as part of the installation steps. Post the installation of Unified CCE 12.6(2), use the Security Wizard tool to apply SQL Server Security Hardening.

Common Ground Upgrade is not supported if the platform upgrade from Windows Server 2016 and SQL Server 2017 to Windows Server 2019 and SQL Server 2019 is planned as part of upgrade process.

Technology Refresh Upgrade is the supported upgrade option for platform upgrade. Fresh Install on Windows Server 2019 and SQL Server 2019 is supported. Fresh Install, Common Ground Upgrade, and Technology Refresh Upgrade is supported for Microsoft Windows Server 2016 and Microsoft SQL Server 2017 platform, where platform upgrade is not planned.

# Upgrade Scenarios

Upgrading to Unified CCE 12.6(2) from Unified CCE 12.5(1) is the same as upgrading or applying any other maintenance release. However, upgrading to Unified CCE 12.6(2) from Unified CCE 12.5(x) requires some database schema changes. The installer takes care of the schema changes during the upgrade. However, Unified CCE 12.6(2) doesn't have database schema update while upgarding from Unified CCE 12.6(1).

You can also upgrade from Unified CCE 12.0(1) to Unified CCE 12.5(1) and then to Unified CCE 12.6(2) by using one of the following two methods:

- **Common Ground Upgrades**: The Common Ground method is an in-place upgrade performed on your existing virtual machine which involves upgrading the Cisco Unified Contact Center Enterprise and all other associated software that is hosted on it. If your hardware meets the requirements for this release, you can perform a Common Ground upgrade without acquiring extra hardware.

**Note** Common Ground Upgrade isn't supported if the platform upgrade from Windows Server 2016 and SQL Server 2017 to Windows Server 2019 and SQL Server 2019 is planned as part of the upgrade process.

- **Technology Refresh Upgrades**: Use the Technology Refresh upgrade method to upgrade your hardware at the same time as the Cisco Unified Contact Center Enterprise system. When using the Technology Refresh method, you prepare a destination system on new hardware and then migrate data from your existing deployment to the new one.

  Follow the documented procedures to build a parallel network using new hardware and prestage it with configuration data to support the existing production network. Use the Enhanced Database Migration Tool (EDMT) to transfer data and perform a schema upgrade during the upgrade process. Don't use backup and restore procedures to perform the prestaged configuration on the parallel network.

Upgrade scenarios are considered at a component level; you can perform one type of upgrade on one component, and another type of upgrade on another component. However, the A and B sides of any given component must be running on identical hardware.

Follow the task flow and tasks for the upgrade scenario that applies to each individual component involved in the overall upgrade.

Upgrade to Unified CCE 12.6(2) by either of the methods is possible by employing an in-line upgrade (the process of specifying the Unified ICM 12.6(2) installer location, while running the Unified ICM 12.5(1) base installer). The system after upgrading to Unified CCE 12.5(1) and restarting, commences upgrading to Unified CCE 12.6(2).

**Note** The upgrade from Unified CCE 12.0(1) to 12.5(1) or 12.5(1) to 12.6(2) or 12.5(2) to 12.6(2) or 12.6(1) to 12.6(2) is specific to Unified CCE components (for example, Router, peripheral gateway, and so on).

Refer to the Fresh Install or Technology Refresh Upgrade section for details on prerequisites for installing Unified CCE components on the Windows Server 2019 and SQL Server 2019 platform.

**Note** While upgrading from previous versions of Unified ICM / Unified CCE using the base installer for the current release, make sure that there are no other Windows sessions that are active. These sessions may have inadvertently left open some Unified CCE tools like Configuration Manager. This can prevent the tools from getting upgraded appropriately and this can cause the tool to malfunction or assert. The installer logs indicate that some files were locked during the upgrade. To resolve the issue with these tools that weren't upgraded, you must rerun the base-installer and ensure that no other windows sessions are open.

# System Requirements

Before you start installation or upgrade activities, plan your Unified CCE contact center installation or upgrade. For system requirements, see the Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

By default, Windows Defender is enabled on Windows Server. For more information on Windows Defender antivirus compatibility, see https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/windows-defender-antivirus-compatibility.

Before proceeding with Unified ICM application installation, ensure that you follow the antivirus guidelines specified in the Section, Antivirus Guidelines of the 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.

Unified ICM installation can also take longer than expected due to scanning of files by Windows Defender. Based on your IT policy, either:

- Disable Windows Defender. For more information, see Disable Microsoft Defender Antivirus procedure in Microsoft documentation.

  -OR-

- Add the Unified ICM product folder **<ICM install directory:>\icm** to the exclusion list of Windows Defender. For more information, see https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/configure-extension-file-exclusions-windows-defender-antivirus.

On Logger, Rogger, AW, and HDS servers, the Unified CCE Installer adds BUILTIN\Administrators to SQL security logins and assigns **sysadmin** role to it. This is required for **Logger** and **Administration & Data Server** services to function appropriately.

Ensure that the system is ready, and meets all requirements for supported hardware and software.

This section provides a summary of the requirements for Unified CCE. If you have not confirmed all the information in this section, complete the planning phase before proceeding further.

For more information, see these documents:

- *Solution Design Guide for Cisco Unified Contact Center Enterprise* at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/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

# Platform Requirements

Server selection for Unified CCE in a virtualized environment involves several factors, including:

- The server and all related hardware must be supported for use in a virtualized Unified CCE system
- Minimum specifications for processing, memory, and storage
- Whether you want a packaged and tested Cisco configuration (Tested Reference Configuration or TRC) or a configuration that you base on Cisco-defined minimum requirements (Specs-based Configuration)
- Compatibility requirements for all hardware, and Cisco and third-party software including the VMware required to run and manage a virtual environment

Confirm that your hardware selection is supported for Unified CCE and meets all minimum specifications:

| Server | VMware required | For detailed requirements information, see |
|---|---|---|
| UCS C-series (TRC): | • VMware vSphere ESXi<br>• VMware vCenter (Optional) | *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 |
| UCS C-series (Specs-based): | • VMware vCenter<br>• VMware vSphere ESXi | |
| Third-party (Specs-based) | • VMware vCenter<br>• VMware vSphere ESXi | |

In addition to confirming that your servers meet minimum specifications, confirm that your server choice is compatible with all Cisco and third-party software.

# Network Requirements

Network requirements for virtualized Unified CCE systems vary widely, depending on the size and type of Unified CCE solution deployment. Confirm that you have clearly established all network requirements before you install or upgrade a Unified CCE contact center.

For more information, see *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.

# Transport Layer Security Version 1.2 Required

Contact center enterprise solutions require the use of TLS 1.2 only connections in this release. Our services accept incoming TLS connections only over TLS 1.2. All outgoing TLS connection use only TLS 1.2.

All clients that connect to either our web interfaces or databases must support TLS 1.2.

**Note** The older versions of the TLS/SSL are disabled by installer.

For more information see, *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.

# Software License Requirements

### Third-Party Products

**Note** For detailed information about the software editions and versions supported for this release, 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.

Before you begin an installation or upgrade of any part of your contact center, confirm the following:

- That you have all the required software products.
- That all the software versions are compatible with each other.
- That all software versions are also compatible with all hardware and VMware.

# Virtualization Requirements

You run the Unified Contact Center Enterprise solution on VMware ESXi platform.

The following requirements apply to VMware on virtual machines for Unified CCE:

- After you install the Unified CCE components on each VM, install the latest VMware Tools from your VMware host using the VMware Tool default settings.

**Note** Update the VMware Tools whenever you patch or upgrade ESXi.

**Note** Deploying VM with Guest Operating System 'Microsoft Windows Server 2019' on ESXi 7.0 using CCE OVA template displays a warning message, "The configured guest OS (Microsoft Windows Server 2016 or later (64-bit)) for this virtual machine does not match the guest that is currently running (Microsoft Windows Server 2019 (64-bit)). You should specify the correct guest OS to allow for guest-specific optimization". This warning message is informational only and has no detrimental effect on the system. The warning message is displayed only once and can be dismissed.

For more information, see *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.

# ESXi Supportability

For information on supported versions of ESXi for this release see *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.

As part of the Common Ground upgrade process, if there are no available overlapping supported ESXi versions, upgrade the Unified CCE software first if a back-out of the upgrade is required.

If the upgrade is successful and working, you can then proceed to upgrade ESXi to a supported version for final testing and restoring production operation.

# Compatibility Requirements

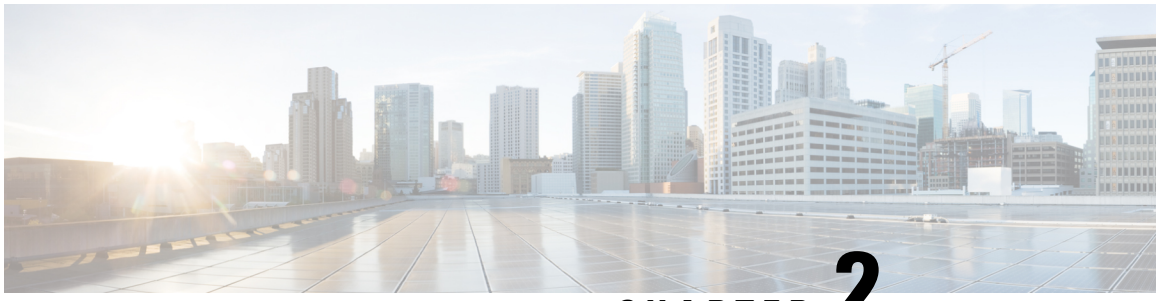
As part of the planning process, ensure that all hardware, Cisco software, third-party software, VMware, and firmware are compatible. Confirm that you meet all the following compatibility requirements:

| For this compatibility information | See |
|---|---|
| VMware and Cisco software components | *Virtualization Software Requirements* at http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-software-requirements.html |

| For this compatibility information | See |
|---|---|
| Required firmware | See the following:<br>*VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility/search.php.<br>For more information, see *Virtualization for Unified Contact Center Enterprise* at http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html.<br>Cisco Installation and Upgrade Guides at http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-installation-guides-list.html |
| Cisco software product intercompatibility | *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<br>**Note** Review the compatibility between different versions of the Cisco components to plan upgrades that occur across multiple maintenance windows. Components that are upgraded in one maintenance window must continue to operate with other components that are still at the previous version until the full upgrade is completed. |
| Windows OS and SNMP<br>• SNMP Service<br>• SNMP MI Provider | See the following:<br>*SNMP Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html<br>*Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html |
| Third party software products | *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 |

# Java Requirements

CCE has transitioned from Oracle to OpenJDK for the Java runtime environment (JRE). All CCE components require OpenJDK JRE version 1.8 (32-bit), update 352 or later. The 12.6(2) installer will install the required OpenJDK 1.8 version. If the existing Oracle JRE is not needed, you may uninstall it from the system manually.



CHAPTER 2

# Installation Overview


- Installation Tools, on page 9


# Installation Tools

During installation, use one or all of the following tools, as required:

- ICM-CCE-Installer—The main Unified CCE Installer copies all files into relevant folders, creates the base registries, and installs needed third-party software such as JRE and Apache Tomcat. It uses the Microsoft .NET Framework which is an integral software of Windows Server.

**Note** Optionally, you can update the JRE installed by the Unified CCE Installer with a later version of the JRE. See Java Upgrades, on page 58.

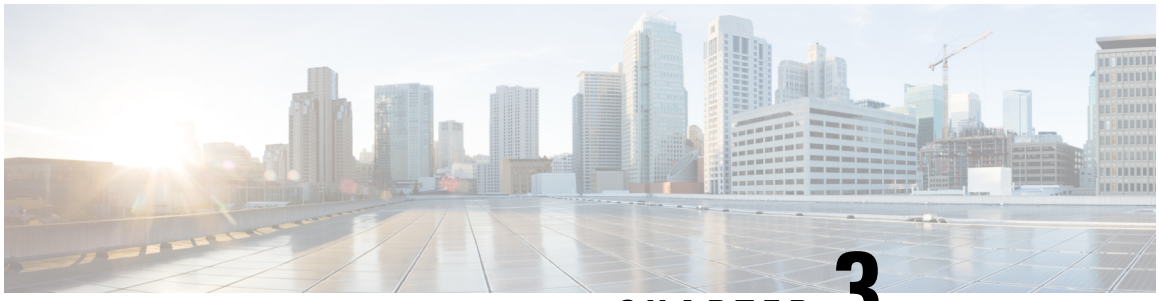
If the ICM-CCE installer installs JRE on the Windows platform, the system retains only the Cisco approved CA certificates in the java certificate store, and removes all the unapproved certificates.

Do not run the installer remotely. Download the installer to a local machine for installation.

- ICM12.6.2.exe—The Unified CCE patch installer. It copies all files into relevant folders, updates the registries, and installs needed third-party software such as JRE, Apache Tomcat, and Microsoft .NET Framework.
- Cisco Unified Intelligent Contact Management Database Administration (ICMDBA) Tool—Used to create new databases, modify or delete existing databases, and perform limited SQL Server configuration tasks.
- Domain Manager—Used to provision Active Directory.
- Web Setup—Used to set up the Call Routers, Loggers, Network Gateways, Network Interface Controllers, and Administration & Data Servers.
- Peripheral Gateway (PG) Setup—Used to set up PGs, the CTI server, and the Outbound Option dialer.
- AdminClientInstaller—Installs the Administration Client on a system that is not running other Unified CCE components.

  The AdminClientInstaller is delivered on the installation media with the ICM-CCE-Installer.

- Administration Client Setup—Used to add, edit, or remove Administration Clients and Administration Client Instances.



CHAPTER 3

# Preinstallation


- Preinstallation Task Flow, on page 11
- Preinstallation Tasks, on page 11


# Preinstallation Task Flow

Before you can install Unified CCE and the associated components, set up the network, create virtual machines, and install and configure third-party software.

**Important** The length of the hostname of any Unified CCE server must not exceed 24 characters.

| Task | See |
|---|---|
| If you are integrating Unified CCE into an existing corporate network, verify Domain Controller health. If you are installing into a new Active Directory domain, install and configure Active Directory and DNS server. | Set up Active Directory, on page 11 |
| Download Open Virtualization Format (OVA) templates and create virtual machines. | Set Up Virtual Machines, on page 12 |
| Install and configure third-party software. | Set Up Third-Party Software, on page 16 |

# Preinstallation Tasks

## Set up Active Directory

Ensure that you have a completed plan for your domain structure and Active Directory implementation before you set up your network.

**Warning** The Unified CCE servers should be in the same domain, and multiple domains are not supported.

For more information, see the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

# Set Up Virtual Machines

## Verify Datastores

Before you install the VMs, verify that the datastore is in place. The type of datastore depends on the type of server on which you deploy the VMs. For example, UCS-B servers use a SAN datastore and UCS-C servers use DAS datastores.

For more information, see the VMware documentation at https://www.vmware.com/support/pubs/.

For more information, see *Virtualization for Unified Contact Center Enterprise* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html.

## Configure HyperFlex M5 Series and M6 Series

Cisco HyperFlex HX-Series System provides a unified view of the storage across all nodes of the HyperFlex HX cluster via the HX Data Controller Platform. For optimal performance, it is recommended that all VMs are mapped to the single unified datastore. This mapping enables the HX Data Platform to optimize storage access based on the workload and other operating parameters.

For more information, see the documentation on Cisco HyperFlex HX Data Platform at https://www.cisco.com/c/en/us/support/hyperconverged-systems/hyperflex-hx-data-platform-software/products-installation-guides-list.html.

For information on installing collaboration software, see the *Cisco Collaboration on Virtual Servers* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.

## Configure RAID for Cisco UCS C240 M5SX and Cisco UCS C240 M6SX

The disk array configuration for the Cisco UCS C240 M5SX and Cisco UCS C240 M6SX is already set up to match the requirements. Verify the settings as follows:

### Procedure

Using Cisco Integrated Management Controller, check that the following settings are configured correctly:

- Virtual Drive Info: RAID 5 with 6 (Physical Disks) * 4 (Virtual Drives or Datastores)
- Stripe Size: 128KB
- Write Policy: Write Back with BBU
- Read Policy: Read Ahead Always

For more information regarding RAID configuration for Cisco UCS C240 M5SX or Cisco UCS C240 M6SX, see the *Installation and Configuration* section of the Cisco Collaboration on Virtual Servers Guide.

## Download Unified CCE OVA Files

The Unified CCE Open Virtualization Format (OVA) files define the basic structure of the corresponding VMs that are created. The structure definition includes the CPU, RAM, disk space, reservation for CPU, and reservation for memory.

### Before you begin

You must have a valid service contract associated with your Cisco.com profile.

### Procedure

**Step 1** Go to the Unified CCE Download Software page on Cisco.com.

**Step 2** Click **Download** to download and save the appropriate OVA file to your local hard drive. When you create VMs, you select the OVA required for the application.

## Create a Virtual Machine from the OVA

To create virtual machines (VMs) from the OVA files, complete the following procedure.

**Note** ECE requires a second virtual hard drive on its VM. The OVA creates one virtual hard drive. Create a second hard drive of an appropriate size for your solution requirements.

### Procedure

**Step 1** Select the host in the vSphere client and click **Deploy OVF Template**.

**Step 2** On the **Select an OVF template** page, browse to the location on your local drive where you stored the OVA. Click **Open** to select the file. Click **Next.**

**Step 3** On the **Select a name and folder** page, enter a name for the virtual machine and then choose the location for the virtual machine.

**Important** The virtual machine name cannot contain spaces or special characters. Enter a maximum of 32 characters. After the VM is created, you cannot rename it.

**Step 4** Click **Next**.

**Step 5** On the **Select a compute resource** page, select the destination compute resource. Click **Next.**

**Step 6** On the **Review details** page, verify the OVF template details.

**Step 7** On the **Configuration** page, select the applicable configuration from the available list. Click **Next**.

**Step 8** On the **Select storage** page, ensure that the virtual disk format is **Thick provision Lazy Zeroed** and then choose a datastore on which you want to deploy the new virtual machine. Click **Next.**

**Note** **Thick provision Eager Zeroed** is also supported, but **Thin provisioned** is not supported.

For each datastore, the following tables describe the RAID group, the ESXi Host, and the virtual machines for the Cisco UCS C240 M4SX, Cisco UCS C240 M5SX, and Cisco UCS C240 M6SX servers.

**RAID configuration for the Cisco UCS C240 M4SX, Cisco UCS C240 M5SX, and Cisco UCS C240 M6SX**

| RAID Group | VM Datastore | ESXi Host | Virtual Machines |
|---|---|---|---|
| VD0 | datastore 1 | A | ESXi operating system<br>Unified CCE Rogger, Side A<br>Unified Communications Manager Publisher<br>Cisco Finesse Primary |
| VD1 | datastore 2 | A | Unified CCE AW-HDS-DDS, Side A |
| VD2 | datastore 3 | A | Unified Communications Manager Subscriber 1<br>Unified CVP OAMP Server<br>Unified CVP Server, Side A |
| VD3 | datastore 4 | A | Unified Intelligence Center Server Publisher<br>Unified CCE PG, Side A |
| VD0 | datastore 1 | B | ESXi operating system<br>Unified CCE Rogger, Side B<br>Unified Communications Manager Subscriber 2<br>Cisco Finesse Secondary |
| VD1 | datastore 2 | B | Unified CCE AW-HDS-DDS, Side B |
| VD2 | datastore 3 | B | Unified Customer Voice Portal Reporting Server (optional)<br>Unified CVP Server, Side B |
| VD3 | datastore 4 | B | Unified Intelligence Center Server Subscriber<br>Unified CCE PG, Side B<br>Enterprise Chat and Email Server (optional) |

**Step 9** On the **Select networks** page, select the destination network:

a) Public network adapter to Public network

b) Private network adapter to Private network

**Note** Certain VMs do not require a private network connection. The OVAs for those VMs do not create a second network adapter.

**Step 10** On the **Ready to complete** page, click **Finish** to create the VM.

**Note** For more information, see *Virtualization for Unified Contact Center Enterprise* at http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html.

# Allocate a Second Virtual Hard Drive

After deploying the OVA files, the second hard drive is no longer automatically created. To create a second hard drive:

### Procedure

**Step 1** Right-click the virtual machine and click **Edit Settings**.

**Step 2** In the **Virtual Hardware** tab, click on **Add New Device**.

**Step 3** You can select the type of device you wish to add. Select **Hard Disk**. The new hard disk appears. Assign the desired disk space to the hard disk.

**Note** Virtual machine templates for Logger, Rogger, AW, and HDS servers do not have a SQL database drive preprovisioned. The following reference table can be used to assign disk space to the virtual machine based on the type:

| Virtual Machine Template | Default Second Disk Size |
|---|---|
| Logger | 500 GB |
| Rogger | 150 GB |
| AW-HDS-DDS | 500 GB |
| AW-HDS | 500 GB |
| HDS-DDS | 500 GB |

You can custom size the SQL database disk space to meet data retention requirements, as calculated by the Database Estimator tool.

**Step 4** On the **Disk Provisioning** section, choose **Thick provision Lazy Zeroed**.

**Step 5** In the **VM Options** > **Advanced Options** section, retain the default options.

**Step 6** Click **OK** to confirm the changes.

The Recent Tasks window at the bottom of the screen displays the progress.

# Mount ISO Files

**Upload ISO image to data store:**

1. Select the host in the vSphere client and click **Configuration**. Then click **Storage** in the left panel.
2. Select the datastore that will hold the ISO file.
3. Right click and select **Browse datastore**.
4. Click the **Upload** icon and select **Upload file**.
5. Browse to the location on your local drive where you saved the ISO file, and upload the ISO to the datastore.

**Mount the ISO image:**

1. Right-click the VM in the vSphere client and select **Edit virtual machine settings**.
2. Click **Hardware** and select **CD|DVD Drive 1**.
3. Check **Connect at power on** (Device status panel upper right).
4. Click the **Datastore ISO File** radio button and then click **Browse**.
5. Navigate to the data store where you uploaded the file.
6. Select the ISO file and click **OK**.

# Unmount ISO File

**Procedure**

**Step 1** Right-click the virtual machine in the vSphere client and select **Edit virtual machine settings**.
**Step 2** Click **Hardware** and select **CD/DVD Drive 1**.
**Step 3** Select **Client Device** and click **OK**.

# Set Up Third-Party Software

## Install Microsoft Windows Server

Complete the following procedure to install Microsoft Windows Server on the virtual machines deployed.

**Note** Deploying VM with Guest Operating System 'Microsoft Windows Server 2019' on ESXi 7.0 using CCE OVA template displays a warning message "The configured guest OS (Microsoft Windows Server 2016 or later (64-bit)) for this virtual machine does not match the guest that is currently running (Microsoft Windows Server 2019 (64-bit)). You should specify the correct guest OS to allow for guest-specific optimization". This warning message is informational only and has no detrimental effect on the system. This warning message is displayed only once and can be dismissed.

**Note** For information about supported editions, 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

**Note** Before installing 12.5(1) ICM on SQL Server 2019, make sure to install ODBC Driver 13 for SQL Server® manually.

### Procedure

**Step 1** Mount the Microsoft Windows Server ISO image to the virtual machine.

Check the **Connect at power on** check box when mounting the ISO.

For more information, see *Mount and Unmount ISO File*.

**Step 2** Power on the VM.

**Step 3** Enter the Language, Time and Currency Format, and Keyboard settings. Click **Next**.

**Step 4** Click **Install Now**.

**Step 5** If prompted, enter the product key for Windows Server and click **Next**.

**Step 6** Select the Desktop Experience option for the Windows Server and click **Next**.

**Step 7** Accept the license terms and click **Next**.

**Step 8** Select **Custom: Install Windows only (advanced)**, select **Drive 0** to install Microsoft Windows Server, and then click **Next**.

The installation begins. After the installation is complete, the system restarts without prompting.

**Step 9** Enter and confirm the password for the administrator account, and then click **Finish**.

**Step 10** Enable Remote Desktop connections as follows:

a) Navigate to **Control Panel** > **System and Security** > **System**.
b) Click **Remote Settings**.
c) Click the **Remote** tab.
d) Select the **Allow remote connections to this computer** radio button. The Remote Desktop Connection dialog displays a notification that the Remote Desktop Firewall exception is enabled. Click **OK**.

**Step 11** Install VMWare tools. See Install Vmware Tools, on page 20

**Step 12** Open the **Network and Sharing Center**, and in the View your basic network info and set up connections section, click **Ethernet**.

**Step 13** In the Ethernet Status window, click **Properties**.

**Step 14** In the **Ethernet Properties** dialog box, configure the network settings and the Domain Name System (DNS) data:

a) Uncheck **Internet Protocol Version 6 (TCP/IPv6)**.
b) Select Internet Protocol Version 4 (TCP/IPv4) and click **Properties**.
c) Select **Use the following IP Address**.
d) Enter the IP address, subnet mask, and default gateway.
e) Select **Use the following DNS Server Address**.
f) Enter the preferred DNS server address, and click **OK**.

**Step 15** Navigate to **Control Panel** > **System and Security** > **System**. Follow the instructions:

a) Click**Change Settings**.
b) In Computer name tab, click **Change**.
c) Change the name of the computer from the name randomly generated during Microsoft Windows Server installation. The name does not contain underscores or spaces.
d) Select **Domain** radio button to change the member from Workgroup to Domain.
e) Enter qualified domain name and click **OK**.
f) In the Windows security dialog, validate the domain credentials and click **OK**.
g) On successful authentication, click **OK**.
h) Reboot the server and sign in with domain credentials.

Restart your system for the change to take effect.

**Step 16** Go to **Settings** > **Update & Security** and run Microsoft Windows Update. Microsoft Windows Server is installed.

---

Edge Chromium (Microsoft Edge) is not installed by default on the Windows server. To install Edge Chromium (Microsoft Edge), see *Microsoft* documentation.

**Note** If you want to install Unified CCE on a multilingual version of Windows Server, refer to Microsoft documentation for details in installing Microsoft Windows Server Multilingual language packs.

If Unified CCE language pack is applied on Chinese Windows OS machine, set the screen resolution to 1600 x 1200.

## Install Microsoft Windows 11 for Administration Client

Download Win 11 OVA and deploy the VM using the OVA. For Windows 11, the SecureBoot and TPM devices are mandatory which must be added after deploying the VM from OVA.

**Note** If the ESXi version is 7.0 U2 and above you must upgrade the VM Hardware version.

### Procedure

**Step 1** Mount the Microsoft Windows 11 ISO image to the VM.

Select the **Connect at power on** check box while mounting the ISO. For more information, see Mount ISO Files and Unmount ISO File.

**Step 2** Power on the VM.

**Step 3** Enter the Language, Time and Currency Format, Keyboard settings and click **Next**.

**Step 4** Click **Install Now**.

**Step 5** Select the **Windows 11 Enterprise** or **Windows 11 Pro** option and click **Next**.

**Step 6** If prompted, enter the product key for Windows 11 and click **Next**.

**Step 7** Accept the license terms and click **Next**.

**Step 8** Select **Custom: Install Windows only (advanced)**, select Drive 0 and click **Next**.

**Step 9** Enter and confirm the password for the administrator account. Click **Next**.

**Step 10** Enable Remote Desktop connections as follows:

a) Navigate to **Control Panel > System and Security > System**.
b) Click **Remote Settings**.
c) Click the **Remote** tab.
d) Select the **Allow remote connections to this computer** option.

The Remote Desktop Connection dialog displays a notification that the Remote Desktop Firewall exception is enabled. Click **OK**.

**Step 11** Install VMWare tools.

**Step 12** Open the **Network and Sharing Center**. In the **View your basic network info and set up connections** section, click **Ethernet**.

**Step 13** In the **Ethernet Status** window, click **Properties**.

**Step 14** In the **Ethernet Properties** dialog box, configure the network settings and the Domain Name System (DNS) data.

a) Clear the **Internet Protocol Version 6 (TCP/IPv6)** option.
b) Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
c) Select **Use the Following IP Address**.
d) Enter the **IP Address**, **Subnet Mask**, and **Default Gateway**.
e) Select **Use the following DNS Server Address**.
f) Entered the preferred DNS server address and click **OK**.

**Step 15** Navigate to **Control Panel > System and Security > System**.

a) Click **Advanced system settings**.
The **System Properties** dialog is displayed.
b) In the **Compute Name** tab, clcik **Change**.
c) Change the **Compute name**. The name must not contain an underscore or space.
d) Select **Domain** from the **Member of** pane.
e) Enter a qualified domain name and click **OK**.
f) In the **Windows security** dialog, validate the domain credentials and click **OK**.
g) On successful authentication, click **OK**.
h) Reboot the machine and sign in with domain credentials.

i) Restart your system for the change to take effect.

**Step 16** Go to **Settings > Update & Security** and run **Microsoft Windows Update**.
Microsoft Windows 11 is installed.

## Set Windows Locale

If the Windows system locale differs from the display language (and therefore also the SQL collation setting), some characters appear incorrectly in the user interface and are saved incorrectly to the database. For example, if the system locale is English and an agent works in Spanish, characters such as the acute *a* do not appear correctly.

If you use a multilingual version of Microsoft Windows Server, complete this procedure to set the Windows locale.

### Procedure

**Step 1** Open **Control Panel** > **Clock, Region and Language**.

**Step 2** In the Region section, click **Change date, time, or number formats**.

**Step 3** Click the **Administrative** tab.

**Step 4** In the Language for non-Unicode programs section, click **Change system locale**.

**Step 5** In the **Region Settings** window, select the language that matches the display language.

**Step 6** Restart the virtual machine.

## Install Vmware Tools

VMware Tools is a suite of utilities that enhance the performance of the virtual machine guest operating system. It also aids virtual machine management.

**Note** The AppInfo feature provided by the VMware tools has to be disabled. For instructions to disable the AppInfo feature, see the VMware documentation.

### Install VMware Tools for Windows

### Procedure

**Step 1** From the vSphere Client, right-click the virtual machine, select **Power**, and click **Power On**.

**Step 2** Click the **Summary** tab.
In the General section, the VMware Tools field indicates whether VMware Tools are:

- installed and current
- installed and not current

- not installed

**Step 3** Click the **Console** tab to make sure that the guest operating system starts successfully. Log in if prompted.

**Step 4** Right-click the virtual machine, select **Guest OS**, and then click **Install/Upgrade VMware Tools**. The **Install/Upgrade VMware Tools** window appears with the option - Interactive Tools Upgrade and Automatic Tools Upgrade.

a) To install/upgrade the VMware tools manually, select the **Interactive Tools Upgrade** option, and click **OK**. Follow the on-screen instructions to install/upgrade the VMware tools, and restart the virtual machine when prompted.

b) To install/upgrade the VMware tools automatically, select the **Automatic Tools Upgrade** option, and click **OK**. This process takes a few minutes to complete, and restart the virtual machine when prompted.

## Initialize and Format Secondary Disk

After the second hard disk is created, allocate memory to the hard disk.

### Procedure

**Step 1** Open the command prompt, and type **`diskmgmt.msc`**.

**Step 2** Right-click **Disk 1**, and click **Online**.

**Step 3** After the disk goes online, right-click the disk, and then click **Initialize Disk**.

**Step 4** Select **Master Boot Record (MBR)** radio button.

**Step 5** After the disk is initialized, right-click the disk, and then click **Convert to Dynamic Disk**.

**Step 6** In the **Convert to Dynamic Disk** window, check the **Disk 1** check box to select it, and then click **OK**.

**Step 7** Right click on the unallocated disk space, and click **New Simple Volume**. The **New Simple Volume** Wizard window appears.

**Step 8** Click **Next** and follow the on-screen instructions to create a simple volume on the disk.

**Step 9** Click **Finish** to complete the process of allocating memory to the hard drive.

## Install Microsoft SQL Server

Install Microsoft SQL Server and store the SQL Server log and temporary files on the same vDisk as the operating system when using **default** (two) vDisk design. If you choose to use more than two virtual disks, then the tempDB cannot be on the same vDisk as the solution database.

For further information about the database placement and performance tuning the SQL installation, see the Microsoft documentation.

**Note** For information about supported editions, 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.

### Before you begin

**Note** Microsoft SQL Server does not contain SQL Server Management Studio in the default toolkit. To rerun the SQL Server setup to install Management Studio, navigate to: **SQL Selection Center** > **Installation** > **Install SQL Server Management Tools**. If your computer has no internet connection, download and install SQL Server Management Studio manually.

VC++ 2017 `build# 14.12.25810` is not compatible with the Cisco Contact Center Enterprise, ensure that it is not installed.

### Procedure

**Step 1** Mount the Microsoft SQL Server ISO image to the virtual machine. For more information, see Mount ISO Files, on page 16.

**Step 2** Select **Installation** in the left pane and then click **New SQL Server stand-alone installation or add features to an existing installation**. Click **OK**.

**Step 3** On the **Product Key** page, enter the product key and then click **Next**.

**Step 4** Accept the **License Terms** and then click **Next**.

**Step 5** Optional: On the **Microsoft Update** page, check the **Use Microsoft Update to check for updates** check box, and then click **Next**.

**Note** If you do not check the **Use Microsoft Update to check for updates** option, click **Next** on the **Product Updates** page.

**Step 6** On the **Install Rules** page, click **Next**.

In this step, the installation program checks to see that your system meets the hardware and software requirements. If there are any issues, warnings or errors appear in the **Status** column. Click the links for more information about the issues.

**Step 7** On the **Feature Selection** page, select only the following, and click **Next**:

- **Database Engine Services**
- **Client Tools Connectivity**
- **Client Tools SDK**
- **SQL Client Connectivity SDK**

**Step 8** On the **Instance Configuration** page, select **Default Instance** and click **Next.**

**Step 9** On the **Server Configuration** page, click the **Services Account** tab.

a) Associate the SQL services with the virtual account.

- For the SQL Server Database Engine, in the Account Name field, select **NT Service\MSSQLSERVER**.

**Note** While you can use the Network or Local Services account instead of the Virtual account, using the Virtual account provides security.

b) For the remaining services, accept the default values.
c) In the **Start Up Type** column, for the **SQL Server Agent service** account, select **Automatic** from the list.
d) Enable **Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service**.

**Note** Unified ICM Installer automatically enables the **Grant Perform Volume Maintenance Task** for the NT service account.If it is not enabled automatically then you must enable **Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service** manually on the SQL server.

**Step 10** On the **Server Configuration** page, click the **Collation** tab.

a) In the Database Engine section, click **Customize**.
b) Select the **Windows Collation designator and sort order** radio button.
c) Select the appropriate collation. Typically, you choose the SQL Server collation that supports the Windows system locale most commonly used by your organization; for example, "Latin1_General" for English.

The database entry is related to the collation that you select. For example, if you set the collation for Latin1_General, but you select Chinese language at sign-in. When you enter field values in Chinese, the application displays the `unsupported character` error, because the database does not support the characters.

**Important** It is critical to select the correct collation setting for the language display on your system. If you do not select the correct collation during installation, you must uninstall and reinstall Microsoft SQL Server.

d) Check the **Binary** check box.
e) Click **OK**, and then click **Next**.

**Step 11** On the **Database Engine Configuration** page:

a) On the Server Configuration tab, click the **Mixed Mode** radio button.
b) Enter the password for the SQL Server system administrator account, and confirm by reentering it.
c) Click **Add Current User** to add the user who is installing the SQL Server as an administrator.
d) On the **TempDB** tab, set the **Initial size** and **Autogrowth** for Rogger, Logger, AW-HDS-DDS, AW-HDS, and HDS-DDS. For information about values for respective components Increase Database and Log File Size for TempDB, on page 25.

For more information about the SQL Server TempDB Database and its use, see the Microsoft SQL Server documentation.

e) On the **MaxDOP** tab, choose the value of MaxDOP as half the value of logical CPU cores detected on the computer which is displayed just above the MaxDOP configuration. For example, if the logical CPU cores are detected as 4, then MaxDOP should be configured as 2.

**Note** SQL Server installation automatically recommends the MaxDOP server configuration based on the number of processors available. This feature is introduced in SQL Server 2019 and later. In SQL Server 2017, you can configure MaxDOP post installation. To configure MaxDOP, do the following:

1. In **Object Explorer**, right-click the database instance and select **Properties**.
2. Select **Advanced**.
3. In the **Max Degree of Parallelism** box, configure the number of processors as recommended above.

f) Click **Next**.

**Step 12** On the **Ready to Install** page, click **Install**.

**Step 13** On the **Complete** page, click **Close**.

**Step 14** Enable Named Pipes and set the sort order as follows:

a) Open the SQL Server Configuration Manager.
b) In the left pane, navigate to **SQL Native Client 11.0 Configuration (32bit)** > **Client Protocols**.
c) In the right pane, confirm that **Named Pipes** is **Enabled**.
d) Right-click **Client Protocols** and select **Properties**.
e) In the **Enabled Protocols** section of the **Client Protocols Properties** window, use the arrow buttons to arrange the protocols in the following order:

1. Named Pipes
2. TCP/IP

f) Check the **Enable Shared Memory Protocol** and then click **OK**.
g) In the left pane, navigate to **SQL Server Network Configuration** > **Protocols for MSSQLSERVER**.
h) In the right pane, right-click **Named Pipes** and select **Enable**.

**Note** By default, Microsoft SQL Server dynamically resizes its memory. The SQL Server reserves the memory based on process demand. The SQL Server frees its memory when other processes request it, and it raises alerts about the memory monitoring tool.

Cisco supports the Microsoft validation to dynamically manage the SQL Server memory. If your solution raises too many memory alerts, you can manually limit SQL Server's memory usage. Set the maximum and minimum limit of the SQL memory using the **maximum memory usage** settings in the **SQL Server Properties** menu.as shown below:

| Component | SQL Server Minimum Memory | SQL Server Maximum Memory |
|---|---|---|
| Logger | 2GB | 4GB |
| Rogger | 2GB | 3GB |
| AWS-HDS | 4GB | 8GB |
| AWS-HDS=DDS | 4GB | 8GB |
| HDS-DDS | 4GB | 8GB |

For more information about the SQL Server memory settings and its use, see the Microsoft SQL Server documentation.

**Step 15** Set the SQL Server's default language to English as follows:

a) Launch SQL Server Management Studio.
b) In the left pane, right-click the server and select **Properties**.
c) Click **Advanced**.
d) In the **Miscellaneous** section, set the **Default Language** to **English**.
e) Click **OK**.

**Important** Set the SQL Server default language to English because Cisco Unified Contact Center Enterprise requires a US date format (MDY). Many European languages use the European date format (DMY) instead. This mismatch causes queries such as `select * from table where date = '2012-04-08 00:00:00'` to return data for the wrong date. Handle localization in the client application, such as Cisco Unified Intelligence Center.

**Step 16** Restart the SQL Server service as follows:

a) Navigate to the **Windows Services** tool.
b) Right-click **SQL Server (MSSQLSERVER)** and click **Stop**.
c) Right-click **SQL Server (MSSQLSERVER)** and click **Start**.

**Step 17** Ensure that the SQL Server Browser is started, as follows:

a) Navigate to the **Windows Services** tool.
b) Navigate to the SQL Server Browser.
c) Right-click to open the **Properties** window.
d) Enable the service, change the startup type to **Automatic**, and click **Apply**.
e) To start the service, click **Start**, and then click **OK**.

### What to do next

**Caution** Do not change the SQL port number. Retain the default port numbers as 1433 for TCP and 1434 for UDP connections. In case you change the port numbers, the applications like CCEAdmin will not work.

## Increase Database and Log File Size for TempDB

To get the benefits of TempDB multiple data files support in CCE components, configure the following values as suggested for respective components.

| CCE Component | vCPU | TempDB Data Files | | | TempDB Transaction Log File | |
|---|---|---|---|---|---|---|
| | | Number of Files | Initial Size | Autogrowth | Initial Size | Autogrowth |
| Rogger | 4 | 4 | 800MB | 100MB | 600MB | 10MB |
| Logger | 4 | 4 | 800MB | 100MB | 600MB | 10MB |
| AW-HDS-DDS | 4 | 4 | 800MB | 100MB | 600MB | 10MB |
| AW-HDS | 8 | 8 | 400MB | 100MB | 600MB | 10MB |
| HDS-DDS | 8 | 8 | 400MB | 100MB | 600MB | 10MB |

## Install Antivirus Software

For details about supported anitvirus softwares, see *Contact Center Enterprise Compatibility Matrix*, see https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html

Use your antivirus vendor's product documentation for installation instructions, and adhere to the following:

- Update antivirus software manually. Do not enable automatic updates.
- To allow required access to installation program files or folders, perform file-blocking exclusions in the antivirus product file-and-folder protection rules. For example, to create the exclusions in McAfee VirusScan:
  1. Open the VirusScan console.
  2. Right-click **Access Protection** and select **Properties**.
  3. In the Anti-virus Standard Protection category, make sure that the rule **Prevent IRC communication** is unchecked in the **Block** column.
- Be aware that in the firewall component of Symantec Endpoint Protection 14.2, the Network Threat Protection feature must be disabled. The feature is enabled by default. When the feature is enabled, both sides of a redundant router come up in stand-alone mode which blocks communication between each side of the router pair. This blocking affects all deployment types.

  If you retain the default (enabled) and start serviceson side A and B of the router, the following Symantec message appears in the system tray: “The client will block traffic from IP address [side A router address] for the next 600 seconds.” The same message is also written to the security login client management. The Symantec Network Threat Protection traffic log indicates that a default firewall rule called “Block_all” was dynamically enabled. The router logs show that both sides of the router came up in stand-alone mode.

  To resolve the issue, disable the Symantec firewall on all Unifed CCE boxes and restart the services.

  If you are using a managed client, perform the following steps:
  1. Launch Symantec Endpoint Protection Manager.
  2. Click **Policies**.
  3. To disable a firewall policy, right-click on it and select **Edit**.
  4. Uncheck **Policy**.
  5. Click **OK**.

  If you are using an unmanaged client, perform the following steps:
  1. Double-click on the **Symantec** icon, in the system tray.
  2. Select **Change Settings**.
  3. Configure the required settings for Network Threat Protection and uncheck **Enable Firewall**.
- The firewall component of Trend Micro Deep Security blocks the communication between each side of the Router/PG. If you retain the default (enabled) setting and start the services on side A and side B, then the system logs a new deny event in the location: **Trend Micro Manager** > **Events** > **Firewall Events**.

  To resolve the issue, disable the Trend Micro firewall policy or add a new firewall exception for that particular policy.

# Set Up Virtual Machines for Installation

## Validate Network Adapter Settings and Power On

**Procedure**

**Step 1** Select the virtual machine (VM) in the vSphere client. Right-click the VM and choose **Edit settings**.

**Step 2** On the Hardware tab, select each network adapter. Make sure that **Connect at power on** in the Device Status group is checked.

**Step 3** Under Network Connection, select the applicable network connection from the **Network label** drop-down list:

- Network adapter 1 = **Public** (visible)
- Network adapter 2 = **Private**

**Note** Certain VMs do not require a private network connection. The OVAs for those VMs do not create a second network adapter.

**Step 4** Close the dialog box.

**Step 5** If you are powering up the VM for the first time, power on the VM and wait for the VM to restart and to apply customization. The restart can take 5–10 minutes.

**Important** Do not press Ctrl-Alt-Delete. If you press Ctrl-Alt-Delete after powering on, the customization does not take effect, which requires completing the customization manually.

## Configure Network Cards

**Procedure**

**Step 1** In the virtual machine, open Network and Sharing Center.

**Step 2** Click **Change adapter settings**.

**Step 3** Rename Ethernet 0 to **public** for the Public network card.

**Step 4** Rename Ethernet 1 to **private** for the Private network card.

**Step 5** Assign an interface metric value for the network adapter:

a) Select the network adapter and right-click **Properties**.
b) In the **Networking** tab, select the appropriate Internet Protocol version and click **Properties**.
c) In the **Internet Protocol Version Properties** dialog box, click **Advanced**.
d) In the **IP Settings** tab, uncheck the **Automatic metric** checkbox and type a low value in the **Interface metric** text box.

**Note** A low value indicates a higher priority. Make sure that the Public Network card should have a lower value compared to the Private Network card.

By default, the value of the Interface Metric property for a network adapter is automatically assigned and is based on the link speed.

e) Click **OK** to save the settings.

Repeat the steps to assign an interface metric value for the internal/private cluster communication network adapter.

## Set Persistent Static Routes

For geographically distributed Central Controller sites, redundant CallRouter, Logger, and Peripheral Gateway components typically have a Private IP WAN connection between Side A and Side B. Windows only allows one default gateway for each VM (which sends the Private Network traffic to the Public Network). So, you add a Static Route to all the VMs running the CallRouter, Logger, and PG applications.

To create a persistent static route with the **route add** command, you need the destination subnet, the subnet mask, the local gateway IP, and the interface number of the local Private Network interface:

`route add <destination subnet> mask <subnet mask> <gateway IP> IF <interface number> -p`

You must launch the DOS prompt as an administrator to run the commands in this procedure.

### Procedure

**Step 1** On each CallRouter, Logger, or PG VM, run `ipconfig /all`.
Record the `IPv4 Address`, `Subnet Mask`, and `Physical Address` (MAC address) for the Private Network interface.

**Step 2** On each of these VMs, run `route print -4`.
Record the `Interface` for the Private Network. You can identify the correct interface by looking for its `Physical Address` (MAC address).

**Step 3** On each of these VMs, run `route add <destination subnet> mask <subnet mask> <gateway IP> IF <interface number> -p` to add a persistent static route for the remote Private Network.

## Configure Private Ethernet Card

### Procedure

**Step 1** Right-click **private** and select **Properties**.

**Step 2** Uncheck **Client for Microsoft Networks**.

**Step 3** Uncheck **File and Printer Sharing for Microsoft Networks**.

**Step 4** Uncheck **Internet Protocol Version 6 (TCP/IPV6)**.

**Step 5** Check **Internet Protocol Version 4 (TCP/IPV4)** and click **Properties**.

a) Remove the IP Address for the Default Gateway.
b) Remove the IP Address for the Preferred DNS server.
c) Remove the IP Address for the Alternate DNS server.

**Step 6** Click the **Advanced** button. Open the DNS tab. Uncheck **Register this connection's addresses in DNS**.

**Step 7** Add an entry for the private IP address.

**Note** This IP address should have an entry in the DNS server. This would be required while adding the Router or a Peripheral Gateway through Websetup and PeripheralGatewaySetup respectively.

A host (A) resource record must be created in the **DNS' Forward Lookup Zones**, and can be of the form hostname followed by a suffix "p" to easily identify it as the private interface.

For example: If the host name is **RoggerA**, make an entry in the DNS as "RoggerAp" for the private IP address.

**Step 8** Optional: Add another entry for the private high IP address.

**Note** This IP address should have an entry in the DNS server. This would be required while adding the Router or a Peripheral Gateway through Websetup and PeripheralGatewaySetup respectively.

A host (A) resource record must be created in the **DNS' Forward Lookup Zones**, and can be of the form hostname followed by a suffix "ph" to easily identify it as the private interface.

For example: If the host name is **RoggerA**, make an entry in the DNS as "RoggerAph" for the private high IP address.

**Step 9** Click **OK** twice. Then, click **Close**.

## Configure Public Ethernet Card

### Procedure

**Step 1** Right-click **Visible** and select **Properties**.

**Step 2** Check **Client for Microsoft Networks**.

**Step 3** Check **File and Printer Sharing for Microsoft Networks**.

**Step 4** Uncheck **Internet Protocol Version 6 (TCP/IPV6)**.

**Step 5** Check **Internet Protocol Version 4 (TCP/IPV4)** and click **Properties**.

**Step 6** Confirm the **Public IP address**, **Subnet mask**, **Default gateway** and **Preferred DNs server**, and click **Advanced**.

**Step 7** On the **Advanced** tab, enter the public IP addresses.

**Step 8** On the DNS tab, in the DNS suffix for this connection field, enter the name of the local DNS zone for the server and check **Register this connection's addresses in DNS**.

**Step 9** Optional: Add another entry for the public IP address.

**Note** This IP address should have an entry in the DNS server. This would be required while adding the Router or a Peripheral Gateway through Websetup and PeripheralGatewaySetup respectively.

A host (A) resource record must be created in the **DNS' Forward Lookup Zones**, and can be of the form hostname followed by a suffix "PuH" to easily identify it as the public interface.

For example: If the host name is **RoggerA**, make an entry in the DNS as "RoggerAPuH" for the public IP address.

**Step 10** If the server requires access to resources in a different trusting or trusted domain or DNS zone, select **Append these DNS suffixes (in order)** and enter the local DNS zone for the server first, and then add the other secondary zones that represent the trusting or trusted domain.

**Step 11** Click **OK** twice. Then, click **Close**.

# Verification of the Downloaded ISO or Minor Release Installer

Perform the following procedure to validate the downloaded ISO or Minor Release Installer signed by Cisco, to ensure that it is authorized.

### Procedure

**Step 1** Install **OpenSSL** on Microsoft Windows.

**Step 2** Add the OpenSSL installation path to **System variables** in the **Environment Variables** of the system.

**Step 3** Add the downloaded ISO Image or Minor Release Installer, ISO Image signature file or Minor Release Installer signature file and the Public key.der file in the same folder for the specific product component.

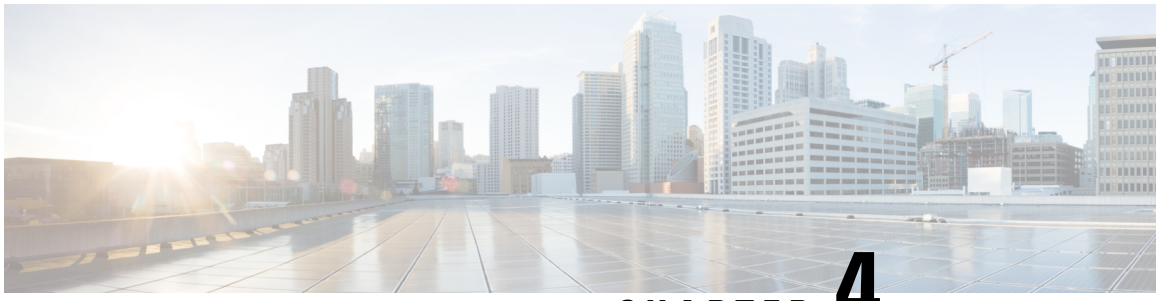
**Step 4** Launch **Command Prompt** on the system.

**Step 5** Run the following CLI (Command Line Interface) command to verify the files:

```
openssl dgst -sha512 -keyform der -verify <PUBLIC key.der> -signature
<ISO Image.iso.signature or Minor Release Installer.exe.signature> <ISO
Image or Minor Release Installer exe>
```

The system displays `Verified OK` on successful verification and `Verification failed` on verification failure.

**Note** If the verification fails do not proceed with the installation, contact Cisco Support for a valid ISO or Minor Release Installer.



CHAPTER 4

# Installation


- Installation Task Flow, on page 31
- Installation Tasks, on page 32


## Installation Task Flow

This section lists the installation tasks for a Unified CCE contact center solution.

Installation procedures for Unified CCE components appear later in this chapter. For the non-Unified CCE components in your solution, follow the links in the table to access the installation guides for those components.

For the Unified CCE components, the sequence you follow can vary according to the distribution of Unified CCE components on virtual machines.

| Task | See |
|---|---|
| Ensure that virtual machines are ready for installation | Set Up Virtual Machines for Installation, on page 27 |
| Install Unified Communications Manager | Installing Cisco Unified Communications Manager |
| Install Unified CCE components (Router, Logger, Administration & Data Servers, peripherals) | Install Unified CCE Software, on page 33 |
| Install Outbound Option | Create Outbound Option Database, on page 38<br>and then see<br>*Outbound Option Guide for Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html |
| Install Finesse | Cisco Finesse Server Installation, on page 63 |
| Install Enterprise Chat and Email | Enterprise Chat and Email Installation Guide (for Unified Contact Center Enterprise) at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html |

| Task | See |
|---|---|
| Install Single Sign-On Identity Service Standalone (4000, 8000, 12000 Agent Deployment)<br>or<br>Install Coresident Deployment (2000 Agent Deployment) | Install Cisco Identity Service Standalone Deployment, on page 75<br>or<br>Install Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS), on page 84 |
| Install Cisco Unified Intelligence Center Standalone (4000, 8000, 12000 Agent Deployment)<br>or<br>Install Coresident Deployment (2000 Agent Deployment) | *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<br>or<br>Install Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS), on page 84 |
| Install Live Data Standalone (4000, 8000, 12000 Agent Deployment)<br>or<br>Install Coresident Deployment (2000 Agent Deployment) | Live Data Standalone Installation, on page 79<br>or<br>Install Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS), on page 84 |
| Install Cisco Unified Customer Voice Portal (Unified CVP) [1] | *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 |
| Install Unified Contact Center Management Portal (Unified CCMP) | *Installation and Configuration Guide for Cisco Unified Contact Center Management Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-management-portal/products-installation-guides-list.html |
| Install Cloud Connect (2000 Agent Deployment) | Install Cloud Connect, on page 89 |

[1] If you are using IP IVR for self-service and queueing, see Getting Started with Cisco Unified IP IVR.

# Installation Tasks

The following section provides instructions about installing Unified CCE components. For instructions about installing non-Unified CCE components in a Unified CCE solution, see the links to component-specific documents in the Installation Task Flow.

**Note** Take a backup of the VM snapshot before installing the Unified CCE software, because uninstallation support is not provided for 12.5(1) .

**Note** Uninstallation is supported for Unified CCE 12.6(x). Uninstalling Unified CCE 12.6(x) brings the component back to the previous version.

# Install Unified CCE Software

### Before you begin

Before installing Unified CCE 12.6(2), you must install Unified CCE 12.5(1). While installing Unified CCE 12.5(1), you can perform an in-line upgrade to Unified CCE 12.6(2).

**Note** Before installing Unified CCE 12.5(1) on SQL Server 2019, make sure to install ODBC Driver 13 for SQL Server® manually.

**Note** During Unified CCE installation on Windows Server 2019 and SQL Server 2019, do not select the SQL Server Security Hardening optional configuration as part of installation. Post the installation of Unified CCE 12.6(2), use the Security Wizard tool to apply SQL Security Hardening.

### Procedure

**Step 1** Mount the Unified CCE Installer ISO image to the virtual machine. For more information, see Mount ISO Files, on page 16.

**Step 2** Open the ICM-CCE-Installer, click **Next**.

**Step 3** Select **Fresh Install** and click **Next**.

**Step 4** To apply Unified ICM Maintenance 12.6(2) Release, click **Browse** and navigate to the Maintenance Release software.

**Note** You can also proceed with the installation of Unified ICM 12.5(1) without selecting Unified ICM 12.6(2) installer in this step. After installing Unified ICM 12.5(1), double-click the Unified ICM 12.6(2) installer, and proceed from step 8.

**Step 5** The installer program proceeds through a series of screens on which you specify information.

**Note** If the ICM-CCE installer installs JRE on the Windows platform, the system retains only the Cisco approved CA certificates in the java certificate store, and removes all the unapproved certificates.

**Step 6** Select **Yes** for the system to restart and complete the installation automatically or select **No** to restart the system manually after installing Unified ICM 12.5(1).

**Note**
- If you have selected Unified ICM 12.6(2) in step 4, you must select **Yes** for the system to restart automatically.
- After installing Unified ICM 12.5(1), you must restart the system manually before launching the Unified ICM 12.6(2) installation wizard and proceeding to step 8.

**Step 7** Log in to your system using domain credentials with administrative privileges.

**Step 8** Wait for the Unified CCE 12.6(2) installation wizard to launch. Click **Next** to proceed.

**Step 9** Select the radio button to accept the license agreement and click **Next**.

**Step 10** Click **Install** to begin the installation.

**Step 11** Select the radio button to restart the system and click **Finish**.

# Set up Organizational Units

## Add a Domain

Use the Domain Manager tool to add a domain.

**Procedure**

**Step 1** Log in with a Domain Administrator privilege.

**Step 2** Open the **Domain Manager** Tool from Unified CCE Tools shortcut on your desktop.

**Step 3** Click **Select**. under **Domains**.

**Step 4** You can add domains through the **Select Domains** dialog box, or you can add a domain manually if the target domain cannot be detected automatically.

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

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

To add a domain manually:

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

## Add Organizational Units

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

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

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

**Procedure**

**Step 1** Log in with a domain administrator privilege and open the **Domain Manager** Tool from Unified CCE Tools shortcut on the desktop.

**Step 2** Choose the domain.

**Step 3** If this OU is the first instance, then perform the following steps to add the Cisco_ICM root:

a) Under Cisco root, click **Add**.

b) Select the OU under which you want to create the Cisco root OU, then click **OK**.

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

**Step 4** Add the facility OU:

a) Select the Cisco Root OU under which you want to create the facility OU.

b) In the right pane, under Facility, click **Add**.

c) Enter the name for the Facility, and click **OK**.

**Step 5** Add the instance OU:

a) Navigate to and select the facility OU under which you want to create the instance OU.

b) In the right pane, under Instance, click **Add**.

c) Enter the instance name and click **OK**.

**Step 6** Click **Close**.

## Add Users to Security Groups

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

**Procedure**

**Step 1** Open the Domain Manager tool and select the Security Group (**Config** or **Setup**) you want to add a user to.

**Step 2** Under Security group, click **Members**.

**Step 3** Under Users, click **Add**.

**Step 4** Select the domain of the user you want to add.

**Step 5** (Optional) In the **Optional Filter** field, choose to further filter by the Name or User Logon Name, apply the search condition, and enter the search value.

**Step 6** Click **Search**.

**Step 7** Select the member you want to add to the Security Group from the search results.

**Step 8** Click **OK**.

# Add Unified CCE Instance

**Procedure**

**Step 1** Open the Unified CCE Web Setup tool from shortcut on your desktop.

**Step 2** Sign in as a domain user with local administrator rights.

**Step 3** Click **Instance Management**, and then click **Add**.

**Step 4** On the **Add Instance** page, from the drop-down list, choose the customer **Facility and Instance**.

**Step 5** Enter an instance number.

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

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

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

# Set Up Unified CCE Central Controller and Administration and Data Server Components

## Create Component Databases

To improve database performance, Unified ICM uses a reduced fill factor from previous releases for the index pages in every table of the Logger, AW, and HDS databases.

### Create Logger Database

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

**Procedure**

**Step 1** From Unified CCE Tools, open the ICMDBA tool, and click **Yes** at any warnings that display.

**Step 2** Navigate to **Server** > **Instances**.

**Step 3** Right-click the instance name and choose **Create** to create the logger database.

**Step 4** In the Select Component dialog box, choose the logger you are working on (Logger A or Logger B). Click **OK**.

**Step 5** At the prompt, “SQL Server is not configured properly. Do you want to configure it now?”, click **Yes**.

**Step 6** On the Configure page, in the SQL Server Configurations pane check **Memory (MB) and Recovery Interval**. Click **OK**.

**Step 7** On the Stop Server page, click **Yes** to stop the services.

**Step 8** In the Select Logger Type dialog box, choose **Enterprise**. Click **OK** to open the Create Database dialog box.

**Step 9** Create the Logger database and log as follows:

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

**Note** Ensure that there is enough free space in the hard disk (at least 20% of database size) to accommodate the log growth.

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

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

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

## Create HDS Database

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

### Procedure

**Step 1** Open the ICMDBA tool, and click **Yes** at any warnings that display.

**Step 2** Navigate to **Servers** > **Instances**.

**Step 3** Right-click the instance name and choose **Create**.

**Step 4** In the Select Component dialog box, choose **Administration & Data Server**. Click **OK**.

**Step 5** At the prompt “SQL Server is not configured properly. Do you want to configure it now?”, click **Yes**.

**Step 6** On the Configure dialog box, click **OK**.

**Step 7** On the Select AW Type dialog box, choose **Enterprise**. Click **OK** to open the Create Database dialog box.

**Step 8** Create the HDS database as follows:

a) From the DB Type drop-down list, choose **HDS**.
b) Click **Add**.
c) On the Add Device dialog box, select **Data**.

d) From the Available Drives list, choose the drive on which you want to install the database.
e) In the Size field, you can leave the default value or enter an appropriate size for your deployment.

**Note** Ensure that there is enough free space in the hard disk (at least 20% of database size) to accommodate the log growth.

**Note** You can use the Database Size Estimator Tool to calculate the appropriate size for your deployment.

f) Click **OK** to return to the Create Database dialog box.
g) Click **Add**.
h) On the Add Device dialog box, select **Log**.
i) From the Available Drives list, choose the drive on which you created the database.
j) In the Size field, you can leave the default value or enter an appropriate size for your deployment.
k) Click **OK** to return to the Create Database dialog box.

**Step 9** On the Create Database dialog box, click **Create** and then click **Start**.

**Step 10** When you see the successful creation message, click **OK** and then click **Close**.

## Create Outbound Option Database

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

After you complete this procedure, see the *Outbound Option Guide for Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html .

### Procedure

**Step 1** Open the ICMDBA tool and click **Yes** to any warnings.

**Step 2** Navigate to **Servers** > **<Logger Server>** > **Instances** > **<Unified CCE instance>** > **LoggerA** or **LoggerB**. Right-click the instance name and select **Database** > **Create**.

**Step 3** On the Stop Server message, click **Yes** to stop the services.

**Step 4** In the Create Database dialog box, click **Add** to open the Add Device dialog box.

**Step 5** Click **Data**, and choose the drive on which you want to create the database, for example, the E drive. In the database size field, you can choose to retain the default value or enter a required value.

**Note** Ensure that there is enough free space in the hard disk (at least 20% of database size) to accommodate the log growth.

**Step 6** Click **OK** to return to the Create Database dialog box.

**Step 7** In the Add Device dialog box, click **Log**. Choose the desired drive. Retain the default value in the log size field and click **OK** to return to the Create Database dialog box.

**Step 8** In the Create Database dialog box, click **Create**, and then click **Start**. When you see the successful creation message, click **OK** and then click **Close**.

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

# Add Components to Unified CCE Instance

## Add Logger Component to Instance

Perform this procedure on the Side A and Side B Loggers; both logger machines must be up and operational.

### Before you begin

If you choose to enable Outbound Option, you can also enable Outbound Option High Availability. Outbound Option High Availability facilitates two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B. Use the ICMDBA tool to create an outbound database on Side A and Side B; then set up the replication by using the Web Setup tool, as described in several of the following steps.

### Procedure

**Step 1** Open the Web Setup tool.

**Step 2** Choose **Component Management > Loggers**. Click **Add**, and then choose the instance.

**Step 3** On the Deployment page, select the Logger (A or B). Click **Duplexed**, and then click **Next**.

**Step 4** On the Central Controller Connectivity page, enter the host names for Sides A and B for these interfaces: **Router Private** and **Logger Private**. Then, click **Next**.

**Step 5** If an external AW-HDS-DDS exists in the deployment, check **Enable Historical/Detail Data Replication**. If no external AW-HDS-DDS exists in the deployment, leave **Enable Historical/Detail Data Replication** unchecked.

**Step 6** On the Additional Options page, click **Display Database Purge Configuration Steps**.

**Step 7** Click the **Enable Outbound Option** check box if you are installing a Unified CCE Logger and choose to deploy Outbound Option.

**Note** If this Logger is being added for a Rogger server, where there are two IP addresses that are configured on the public Network Interface Card (for IP-based prioritization), uncheck "Register this connection's addresses in DNS" for the public ethernet card. In addition, ensure that there is only one A-record entry in the DNS server corresponding to the host name of the server, which maps to the general priority IP address. This is necessary for processes like the campaign manager and replication running as part of the Logger service, to listen on the right interface IP address for client connections.

**Step 8** Click the **Enable High Availability** check box to enable Outbound Option High Availability on the Logger. (An Outbound Option database must exist on Logger Side A and Logger Side B.) Checking this check box enables Outbound Option High Availability two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B. Two-way replication requires that you check this check box on both the Logger Side A and Side B Additional Options page. If you disable two-way replication on one side, you must also disable it on the other side.

You must enable Outbound Option in order to enable Outbound Option High Availability. Similarly, if you want to disable Outbound Option and you have enabled Outbound Option High Availability, you must disable High Availability (uncheck the **Enable High Availability** check box) before you can disable Outbound Option (uncheck the **Enable Outbound Option** check box).

**Note** Disabling HA will not disable outbound option, customer has to explicitly disable outbound when HA is disabled.

**Step 9** If you enable High Availability, enter a valid public server hostname address for **Logger Side A** and **Logger Side B**. Entering a server IP address instead of a server name is not allowed.

**Step 10** If you enable High Availability, enter the **Active Directory Account Name** that the opposite side logger runs under or a security group that includes that account. For example, if you are running Websetup on the logger on Side A, enter the name of the Active Directory account (or security group) that is run on Side B logger.

**Step 11** Select the **Syslog** box to enable the Syslog event feed process (cw2kfeed.exe).

**Note** The event feed is processed and sent to the Syslog collector only if the Syslog collector is configured. For more information about the Syslog event feed process, see the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

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

**Step 13** On the Data Retention page, modify the Database Retention Configuration table:

a) For these tables, set the retention period to 40 days:

- Application_Event
- Event
- Network_Event
- Route_Call_Detail
- Route_Call_Variable
- Termination_Call_Detail
- Termination_Call_Variable

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

**Step 14** Click **Next**.

**Step 15** On the Data Purge page, configure purges for a day of the week and a time when there is low demand on the system.

**Step 16** Accept the default **Automatic Purge at Percent Full**.

**Step 17** Click **Next**.

## Add Router Component to Instance

Perform this procedure for Side A and Side B Routers.

### Procedure

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

**Step 2** Click **Add** to set up the Call Router.

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

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

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

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

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

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

**Step 7** In the **Enable Peripheral Gateways** field, enter the number assigned to the PGs to enable it. Click **Next**.

Use a hyphen to indicate a range and commas to separate values. For example, "2-4, 6, 79-80" enables PG2, PG3, PG4, PG6, PG79, and PG80. Spaces are ignored.

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

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

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

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

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

## Add Administration & Data Server Component to Instance

Follow this procedure for all types of Administration & Data Servers:

- Configuration-Only Administration Server—Supports configuration changes only. Does not support reporting.
- Administration Server and Realtime Data Server (AW)—Supports configuration changes and real-time reporting. Does not support historical reporting.
- Administration Server, Realtime and Historical Data Server, and Detail Data Server (AW-HDS-DDS)—Supports configuration and real-time and historical reporting, including call detail and call variable data.

Not all fields apply to all server types.

**Note** AW Database is created when you add **Administration & Data Server** Component. Data from the **Config_Message_Log table** is replicated from the Logger database to the AW database; you can use the AW database for auditing purposes. When you add the Administration & Data Server component, the retention period for the Config_Message_Log table in the AW database defaults of 90 days. To change the retention period, modify the following registry key: `Cisco Systems, Inc.\ICM\<instancename>\Distributor\RealTimeDistributor\CurrentVersion\Recovery\CurrentVersion\Purge\Retain\System\ConfigMessageLog`.

### Procedure

**Step 1** Open the Web Setup tool.

**Step 2** Select **Component Management > Administration & Data Servers**. Click **Add**.

**Step 3** On the **Deployment** page, configure as follows:

a) Choose the current instance.

b) Choose the deployment type as **Enterprise**.

c) Choose the deployment size. If you choose **Small to Medium**, go to step 4. If you choose **Large**, go to step 5.

**Note** For deployment size definitions and guidelines, see the *Solution Design Guide for Cisco Unified Contact Center Enterprise*.

d) Click **Next**.

**Step 4** On the **Role** page, in the Server Role in a Small to Medium Deployment section, select the radio button for your preferred option.

The three options from which to select are:

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

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

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

**Step 5** On the **Role** page, in the Server Role in a Large Deployment section, select the radio button for your preferred option.

The four options from which to select are:

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

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

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

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

**Step 7** On the **Administration & Data Server Connectivity** page, enter connectivity information between Primary and Secondary Administration and Data servers.

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

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

Next enter the host name or IP address of the Primary and Secondary Administration and Data Server at the site. The Secondary Administration and Data Server field is mandatory. If there is no secondary Administration and Data Server being deployed at the site, then the same host name as that of the primary needs to be provided in this field.

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

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

**Step 9** On the **Database and Options** page, configure as follows:

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

**Step 10** On the **Central Controller Connectivity** page, configure as follows:

a) For **Router Side A**, enter the Router Side A IP address.
b) For **Router Side B**, enter the Router Side B IP address.
c) For **Logger Side A**, enter the Logger Side A IP address.
d) For **Logger Side B**, enter the Logger Side B IP address.
e) Enter the **Central Controller Domain Name**.
f) Based on the Reference Design of your deployment type, distribute your AW-HDS and HDS-DDS VMs on Side A or Side B by selecting **Central Controller Side A Preferred** or **Central Controller Side B Preferred**. For details on the Reference Designs, see the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_5_1/design/guide/ucce_b_soldg-for-unified-cce-12_5.html .
g) Click **Next**.

**Note** The Administration & Data Server can connect to the router with a hostname of maximum 24 characters.

# Set up Peripheral Gateways

To set up all the following types of Peripheral Gateways (PG), complete the procedures in this section:

- Cisco Unified Communications Manager PG (CUCM PG)
- Voice Response Unit PG (VRU PG)
- Media Routing PG (MR PG)
- Unified CCE Gateway PG (UCC Enterprise Gateway PG)

## Configure Peripheral Gateways in PG Explorer

Follow this procedure to complete the first portion of PG configuration. After this procedure, you add a peripheral to the PG; you cannot save the configuration unless there is at least one peripheral in the configuration.

Not all fields apply to all PG types.

### Before you begin

Ensure that the Logger, Router, and Distributor services are running.

### Procedure

**Step 1** From your desktop, double-click the Unified CCE Tools icon, and open Administration Tools folder from Unified CCE Tools icon on the desktop.

**Step 2** Double-click the Configuration Manager icon.

**Step 3** Select **Tools** > **Explorer Tools** > **PG Explorer Tool**.

**Step 4** Click **Retrieve**, then click **Add PG**.

**Step 5** Complete the Logical Controller section as follows:

a) **Logical Controller ID**—Leave blank. This value is generated automatically when the record is saved.
b) **Physical Controller ID**—Leave blank. This value is generated automatically when the record is saved.
c) **Name**—Enter a unique enterprise name for the PG.
d) **Client Type**—Select as follows from the drop-down list:

- For a CUCM PG: CUCM
- For a VRU PG: VRU
- For an MR PG: MediaRouting
- For a UCC Enterprise Gateway PG: UCC Enterprise Gateway

e) **Configuration Parameters**—Leave blank.

f) **Description**—Enter any other information about the PG. Configuration Manager copies this value to the description fields of the logical interface controller, physical interface controller, peripheral, and (if applicable) the routing client records.
g) **Physical Controller Description**—Enter a description for the physical controller.
h) **Primary CTI Address**—Enter the address for the primary CTI server. Make this entry in the form of <IP address or server name where the CTI server is installed>: <Client Connection Port Number>.
i) **Secondary CTI Address**—Enter an address for a secondary CTI server (for duplexed systems).
j) **Reporting Interval**—Select the 15 or 30 Minute reporting interval option (default is 30 Minute). Unified CCE software stores historical information in either half-hour or 15-minute summaries (but not both), based on the reporting interval value that you set. The Router sends these records to the Logger, which in turn writes them to the Central Database.

**Step 6** Do not exit the PG Explorer tool. You add a peripheral to the PG and save the configuration in the next procedure.

## Add Peripherals to Peripheral Gateways

Fields can vary according to PG type.

### Procedure

**Step 1** With the PG record open in the PG Explorer tool, highlight the PG icon in the tree hierarchy in the lower-left corner of the window.

**Step 2** On the Peripheral tab, enter the following:

a) **Name**—Enter a unique enterprise name for this peripheral.
b) **Peripheral Name**—Enter the name of the peripheral as it is known at the site. Unlike the Enterprise Name field, the value of this field does not have to be unique. For example, at each site you can label the peripherals Switch1, Switch2, and so forth.
c) **Client Type**—Select as follows:

- For a CUCM PG: CUCM
  - Configure Agent Desk settings before adding CUCM PG. See Assign Agent Desk Settings
- For a VRU PG: VRU
  - Configure Network VRU before adding VRU PG. See Configure Network VRUs, on page 116
- For an MR PG: MediaRouting
- For a UCC Enterprise Gateway PG: UCC Enterprise Gateway

d) **Location**—Enter the peripheral's location, for example, the name of a city, building, or department.
e) **Abandoned Call Wait Time**—Enter the minimum time (in seconds) an incoming call must be queued before being considered an abandoned call if the caller ends the call.
f) **Configuration Parameters**—As desired, enter a string containing any parameters that must be sent to the device to initialize it. In most cases, you leave this field blank.
g) **Peripheral Service Level Type**—The default type of service level calculation that the peripheral performs for its associated services. Select **Calculated by Call Center**.

h) **Call Control Variable Map**—As desired, enter a string that describes the mappings of the peripheral call control variables to Unified CCE call control variables.

i) **Agent Phone Line Control**—Specify one of the following agent phone line control options:

- **Single Line:** Enables single-line monitoring and reporting (default).
- **All Lines:** Enables multiline monitoring and reporting.

j) **NonACD Line Impact**—Specify one of the following nonACD line impact options:

- **Available Agent Goes Not Ready:** Agent state is set to Not Ready with a system reason code when the agent answers or calls out on a secondary line while in the Available or Not Ready state.
- **Available Agent Stays Available:** Agent state is unchanged when agent is on a call on a secondary line.

k) **Description**—As desired, enter any additional information about the peripheral.

l) **Default Desk Settings**—Select as follows:

- For a CUCM PG: Select the Agent Desk Settings that you created earlier
- For a VRU PG: None
- For an MR PG: None
- For a UCC Enterprise Gateway PG: None

m) **Enable Post Routing**—Check this check box to enable the Unified Communications Manager peripheral to send route requests to the Router. When you check this check box, the Routing Client tab is enabled.

**Step 3** On the Advanced tab, enter the following:

a) **Available Holdoff Delay**—Set this field to zero.

b) **Answered Short Calls Threshold**—Maximum duration, in seconds, for a short call. Any calls with a duration below the threshold are considered short. You can choose to exclude short calls from handle times you calculate.

c) **Network VRU**—The type of network VRU. Select as follows:

- For a CUCM PG: None
- For a VRU PG: Select the corresponding Network VRU that you created earlier.
- For an MR PG: Select the Type 2 Network VRU that you created earlier.
- For a UCC Enterprise Gateway PG: None

d) **Agent Auto-Configuration**— Not supported for Unified CCE. Leave this option disabled.

e) **Internal IPTA Only**—Be sure that you check this check box for the Unified CCE System PG.

f) **Agent Targeting Mode**—Determines how the Router builds the labels. Select **Rule Preferred**.

When this check box is checked, only the local PG can target agents on the PG. The Router uses the skill group IPTA configuration to select agents. When this check box is unchecked, for calls routed between different PGs, the Router picks the agent (which minimizes the benefit of the Unified CCE System PG). Unchecking the check box also requires the creation of more device targets.

**Step 4** On the Agent Distribution tab, enter the following:

a) **Enable Agent Reporting**—Check to allow Unified CCE reporting on agents.

b) **Agent Event Detail**—Enables label text (as opposed to numeric) Not Ready Reason Code reporting.
c) The Agent Distribution Entries section of this tab contains entries for agent Administration & Data Servers available for distributing agent report data for the selected peripheral. Click **New**, then define the values in the Currently Selected site section of this tab as follows:

- **Administration & Data Server site name:** The name of the currently selected site in the agent distribution entries list. For MR PGs, do not specify a name for this field.
- **Agent real time data:** Check to enable the flow of agent real-time data from the peripheral to the Administration & Data Server. Uncheck to disable the flow of agent real-time data.
- **Agent historical data:** Check to enable the flow of agent historical data from the peripheral to the Administration & Data Server. Uncheck to disable the flow of agent historical data.

**Step 5** On the Routing Client tab, enter the following:

a) **Name**—An enterprise name for this routing client. The name must be unique among all routing clients in the enterprise.
b) **Timeout threshold**—The maximum time, in milliseconds, the routing client can wait for a response to a routing request.
c) **Late threshold**—The threshold value, in milliseconds, for classifying responses as late. Any response that exceeds this threshold is considered late even if it does not exceed the Timeout threshold.
d) **Timeout limit**—The maximum time, in seconds, for which the routing client waits for a response. If the routing client receives no responses from the Unified CCE system within this limit, it terminates routing operation.
e) **Default media routing domain**— Retain the default value, which is **None**.
f) **Default call type**—Use this call type for any route request that does not match a defined call type mapping.

The drop-down list contains all configured call types. The Unified CCE uses the default call type for any routing request from the routing client that does not otherwise map to a call type. If you do not define a default call type for the routing client, the Unified CCE uses a general default call type if you define one through the System Information command.

g) **Configuration parameters**—Leave blank.
h) **Dialed Number/Label map**—Indicates whether only specific labels are valid for each dialed number associated with this routing client (when selected) or whether all labels associated with the routing client are valid for any dialed number (when not selected). Leave unchecked.
i) **Client Type**—Select as follows from the drop-down list:

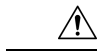
- For a CUCM PG: IPCC/Enterprise Agent
- For a VRU PG: VRU
- For an MR PG: MediaRouting
- For a UCC Enterprise Gateway PG: UCC Enterprise Gateway

j) **Description**—More information about the routing client.
k) **Network routing client**—A name used to associate routing clients across instances.
l) **Network transfer preferred**—If this check box is checked, indicates that network transfer is preferred. When the target of a call is reachable by both a label defined for the requesting routing client and by another label defined for the network routing client that prerouted the call, this option indicates which choice is preferred.

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

**Step 7** Record the Logical Controller ID and Peripheral ID for subsequent use in setting up the PG.

## Configure Peripheral Gateway Setup



**Caution** To ensure that PGs work synchronously, configure the PGs that are collocated on the same physical server in the same order on both the sides. This must be based on the order in which they are installed and not on peripheral identifiers. For information on port utilization, refer to the *Port Utilization Guide for Cisco Unified Contact Center Solutions* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Before you enable secured connection between the components, ensure to complete the security certificate management process.

For more information, see the *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.

### Procedure

**Step 1** Open the **Peripheral Gateway Setup** tool from Unified CCE Tools on the desktop.

**Step 2** Click **Add** in the **Instance Components** section.

**Step 3** Click **Peripheral Gateway**.

**Step 4** Complete the following steps in the Peripheral Gateway Properties dialog box.

a) Choose **Production Mode**. Do not set the Auto Start feature until after the installation is complete.
b) Specify whether the PG is part of a duplexed pair.
c) In the ID field, select from the drop-down list the PG device number as enabled in the Router.
d) If the PG is duplexed, specify whether you are installing Side A or Side B. If the PG is simplex, select Side A.
e) In the **Client Type Selection** section of the window, select the client type:

- For a CUCM PG: CUCM
- For a MediaRouting PG: MediaRouting
- For a VRU PG: VRU
- For a UCC Enterprise Gateway PG: UCC Enterprise Gateway

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

**Step 6** Enter the Logical Controller ID generated while configuring the PG in the **PG Explorer** tool. Click **Add** and select **PIM 1** from the list. Click **OK**.

**Step 7** Configure the PG properties:

a) To put the PIM into service, check the **Enabled** option. Enabling the PIM allows it to communicate with the peripheral when the Peripheral Gateway is running.

b) Enter the peripheral name in the **Peripheral name** field. Usually, the enterprise name from the associated Peripheral record is the most appropriate name to use. When creating peripheral names, use short descriptive names and keep the length to a minimum.

c) Enter the Peripheral ID in the **Peripheral ID** field. This is the ID that you created when you configured the PG in the PG Explorer tool.

d) For CUCM PG:

1. Enter the **Agent extension length**.
2. In the CUCM Parameters section, in the **Service** field, provide the IP address of the CUCM.
3. Enter the credentials of Application User that you created in CUCM.

   For more information about Application User, see Set Up Application User , on page 164.
4. Select the appropriate **Mobile Agent Codec**, and click **OK**.

e) For MR PG:

- To add MR PG for ECE:

1. In the **Application Hostname (1)** field, enter the hostname or the IP address of the ECE services server. If you have installed two services servers for high availability, provide the information for the primary service server on Side A.
2. In the **Application Connection Port (1)** field, enter the port number on the ECE services server that the PIM will use to communicate with the application. The default port is 38001.
3. In the **Application Hostname (2)** and **Application Connection Port (2)** fields, enter the hostname or the IP address of the secondary ECE services server VM and port number on Side B.

   **Note** Set these values only if you have installed two services servers for high availability.

- To add MR PG for Customer Collaboration Platform:

1. In the **Application Hostname (1)** field, enter the hostname or the IP address of the Customer Collaboration Platform.
2. 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 as specified in the **Application Connection Port (1)** field.
3. Leave the **Application Hostname (2)** and **Application Connection Port (2)** fields blank.

- To add MR PG for Digital Routing service:

1. In the **Application Hostname (1)** and **Application Hostname (2)** fields, enter the hostname or the IP address of the Cloud Connect publisher and subscriber, respectively.

   **Note** Ensure to configure the **Application Hostname(1)** field to the network-nearest Cloud Connect. For example, if PIM-A is closer to the Cloud Connect publisher node, you must enter the IP address or hostname of the Cloud Connect publisher node in the **Application Hostname(1)** field and the IP address or hostname of the Cloud Connect subscriber node in the **Application Hostname (2)** field when configuring side "A".

2. In the **Application Connection Port (1)** and **Application Connection Port (2)** fields, retain the default port number, that is 38001, which is the fixed port for the Digital Routing service.

- To add MR PG for Outbound Option:
  1. In the **Application Hostname (1)** field, enter the hostname or the IP address of the BA_IP Dialer.
  2. In the **Application Connection Port (1)** field, enter the connection port for the BA_IP Dialer. Otherwise, accept the default port number (38001) on the application server machine that the PIM uses to communicate with the application.

- To add MR PG for any third-party application:
  1. In the **Application Hostname (1)** field, enter the hostname or the IP address of the multichannel application server machine.
  2. In the **Application Connection Port (1)** field, enter the port number on the application server that the PIM will use to communicate with the application. The default port is 38001.
  3. If two applications interact with the Unified CCE, in the **Application Hostname (2)** field, enter the hostname or the IP address of the second application server machine. If you are using the hostname, the name must be in the hosts file.
  4. For two applications that interact with the Unified CCE, in the **Application Connection Port (2)** field, enter the port number on the second application server machine that is used by the PIM.

The below steps are common for any application server:

1. For **Heartbeat Interval** (seconds), specify how often the PG checks its connection to the call server. Use the default value.
2. For **Reconnect Interval** (seconds), specify how often the PG should try to reestablish a lost connection to the call server. Use the default value.
3. Check the **Enable Secured Connection** checkbox to enable secured connection.

   **Enable Secured Connection** 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.

**Note** In case you are enabling ECDSA certificate, refer to the *How to enable ECDSA for Unified CCE core components* section in the Security Guide for Cisco Unified ICM/Contact Center Enterprise.

For more information, refer to the *Generate CVP ECDSA Certificate with OpenSSL* section in the Configuration Guide for Cisco Unified Customer Voice Portal.

f) For VRU PG:

1. In the **VRU host name** field, enter the name by which the VRU is known to the network.
2. In the **VRU connect port** field, enter the number of the VRU connection port that the PG connects to.

3. In the **Reconnect interval (sec)** field, specify how often, in seconds, the PG tries to re-establish a lost connection to the VRU. The default value is usually appropriate.
4. In the **Heartbeat interval (sec)** field, specify how often, in seconds, the PG checks its connection to the VRU. The default value is usually appropriate.
5. In the **DSCP** field, use the drop-down box to override the default value and set it to the desired DSCP value. The list of DSCP values in the drop-down box are the same as what are used during setup for connection between the Peripheral Gateway (PG) and the CallRouter. On an existing VRU PG system, this registry key does not exist. In that scenario, the PIM code uses CS3 as the default value when the VRU PIM process is activated.
6. Check the **Enable Secured Connection** checkbox to enable secured connection.

   This establishes a secured connection between VRU PIM and CVP.

**Note** In case you are enabling ECDSA certificate, refer to the topic *How to enable ECDSA for Unified CCE core components* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_6_1/configuration/guide/ucce_b_security-guide_12_6_1/ucce_b_security-guide_12_6_1_chapter_01000.html#Cisco_Task_in_List_GUI.dita_d28788be-b6ec-4017-922e-0eec9851df53

**Step 8** Click **OK**.

**Step 9** From the **Peripheral Gateway Component Properties** window, click **Next**. The **Device Management Protocol Properties** window appears.

a) Enter the appropriate settings and click **Next**. The **Peripheral Gateway Network Interfaces** window appears.
b) Configure the Private Interface and Public interfaces and click **Next**.

**Note:**

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

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

**Step 10** In the **Check Setup Information window**, verify the setup information and click **Next**.

**Step 11** When the **Setup Complete** window appears, click **Finish** .

**Note** When you add new PG, ensure that the PG ID is provided in the Router configuration. Provide the number that is assigned to the PG in the Enable Peripheral Gateway field in Web Setup

## Install Cisco JTAPI Client on PG

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

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

To install the JTAPI client for CUCM, Release 12.5 and above, see Install Cisco JTAPI Client on PG, on page 52.

#### Before you begin

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

#### Procedure

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

**Step 2** Enter the URL for the Unified Communications Manager Administration utility: http://<*Unified Communications Manager machine name*>/ccmadmin.

**Step 3** Enter the username and password that you created while installing and configuring the Unified Communications Manager.

**Step 4** Choose **Application** > **Plugins**. Click **Find**.

**Step 5** Click the link next to **Download Cisco JTAPI for Windows**.We recommend you to download the 64 bit version. However, if you have already downloaded the 32 bit version, you can proceed to step 7.

Download the JTAPI plugin file.

**Step 6** Choose **Save** and save the plugin file to a location of your choice.

**Step 7** Open the installer.

**Step 8** In the Security Warning box, click **Yes** to install.

**Step 9** Choose **Next** or **Continue** through the remaining Setup screens. Accept the default installation path.

**Step 10** When prompted for the TFTP Server IP address, enter the CUCM IP address.

**Step 11** Click **Finish**.

**Step 12** Reboot the machine.

## Install Cisco JTAPI Client on PG

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

#### Before you begin

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

#### Procedure

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

**Step 2** Enter the URL for the Unified Communications Manager Administration utility: http://<*Unified Communications Manager machine name*>/ccmadmin.

**Step 3** Enter the username and password that you created while installing and configuring the Unified Communications Manager.

**Step 4** Choose **Application** > **Plugins**. Click **Find**.

**Step 5** Click the link next to **Download Cisco JTAPI Client for Windows** 64 bit or **Download Cisco JTAPI Client for Windows** 32 bit.

Download the JTAPI plugin file.

**Step 6** Choose **Save** and save the plugin file to a location of your choice.

**Step 7** Unzip the JTAPI plugin zip file to the default location or a location of your choice.

There are two folders in the unzipped folder `CiscoJTAPIx64` and `CiscoJTAPIx32`.

**Step 8** Run the `install64.bat` file in the `CiscoJTAPIx64` folder or run the `install32.bat` file in the `CiscoJTAPIx32` folder.

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

**Step 9** To accept the default installation path, click Enter and proceed.

Follow the instructions. Click Enter whenever necessary as per the instructions.

**Note** Starting from Cisco Unified Communications Manager (CUCM) 12.5 SU4 and 14.0 (or any other service updates thereafter) on these release trains, only 64-bit version of the JTAPI client is supported on the Agent PG.

The JTAPI client installation completes at the default location. The following message is displayed:

```
Installation Complete.
```

**Step 10** Reboot the machine.

### What to do next

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

# Set up CTI Server

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

## Add CTI Server Component

### Procedure

**Step 1** Open Peripheral Gateway Setup tool from **Unified CCE Tools** on the desktop.

**Step 2** Click **Add** in the Instance Components section.

The ICM Component Selection dialog box opens.

**Step 3** Click **CTI Server**, and click **OK**.

The CTI Server Properties dialog box opens.

## Set CTI Server Properties

### Procedure

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

**Note** During Unified CCE installation on to Windows Server 2019, perform step 1 only after Unified CCE 12.6(2) for Windows Server 2019 and SQL Server 2019 support is installed.

**Step 2** Check the **Duplexed CTI Server** option if you are configuring redundant CTI Server machines.

**Step 3** In the CG Node Properties section, the numeric portion of the CG node **ID** must match the PG node ID (for example, CG 1 and PG 1).

**Step 4** The **ICM system ID** is the Device Management Protocol (DMP) number of the PG associated with the CTI Gateway. Generally this number is the number associated with the CG ID in step 3.

**Step 5** If the CTI Server you add is duplexed, specify which **Side** you are setting up: Side A or Side B. If the CTI Server is simplex, choose Side A.

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

The CTI Server Component Properties dialog box opens.

## Set CTI Server Component Properties

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

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

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

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

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

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

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

### Procedure

**Step 1** Select the appropriate connection type.

a) For *Secured Connection*, check the **Enable Secure-Only Mode** check box.

This option disables the **Non-Secured Connection Port** field.

b) For *Mixed-mode connection*, ensure that the **Enable Secure-Only Mode** check box is unchecked.

This is the default connection mode.

**Step 2** To ensure that an agent is logged in to the client before the client receives events from the CTI Server, check the **Agent Login Required for Client Events** check box. This ensures that the clients are prevented from accessing data for other agents.

**Step 3** Click **Next**.

The CTI Server Network Interface Properties dialog box opens.

**Note** In case your enabling ECDSA certificate, refer to the topic *How to enable ECDSA for Unified CCE core components* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

## Set CTI Server Network Interface Properties

**Procedure**

**Step 1** In the CTI Server Network Interface Properties dialog box, in the **PG public interfaces** section, enter the public network addresses for the PGs associated with the CTI Server.

**Step 2** In the **CG private interfaces** section, enter the private network addresses of the CTI Server.

**Step 3** In the **CG visible interfaces** section, enter the public network addresses of the CTI Server.

**Step 4** Click **Next**.

The Check Setup Information window opens.

## Complete CTI Server Setup

**Procedure**

**Step 1** In the Check Setup Information window, ensure that the settings displayed are as you intended. If you want to modify any settings before proceeding, use the **Back** button.

**Step 2** When the settings are correct, click **Next**.

**Step 3** The final screen displays and asks whether you want to start the Node Manager now.

**Step 4** Click **Finish** to exit setup (and optionally start the Node Manager).

If you choose to start it, the Node Manager automatically starts the other Unified CCE processes on the CTI Server.

# Install Unified CCE Administration Client

## Install Administration Client

Don't install the Administration Client on a system that already has other Unified CCE software installed; the Administration Client must reside on a standalone machine. **AdminClientInstaller** is available in the Unified CCE Installer ISO image and Minor Release installer.

For information on supported operating systems, 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

**Note**

- Unified CCE 12.6(2) installs .Net Framework 4.8.

### Procedure

**Step 1** Mount the Unified CCE Installer ISO image to the virtual machine. For more information, see Mount ISO Files, on page 16.

**Step 2** Launch 12.5 **AdminclientInstaller** from **AdminClientInstaller** folder.

The Administration Client Installer program proceeds through a series of screens on which you specify information.

**Step 3** To apply the Unified ICM 12.6(2) Maintenance Release, click **Browse** and navigate to the Maintenance Release Software. Click **Next**.

**Note** You can also proceed with the installation of Administration Client 12.5(1) without selecting the Unified ICM 12.6(2) installer in this step. After installing Unified ICM 12.5(1), double-click the Unified ICM 12.6(2) installer, and proceed from step 5.

**Step 4** When the installation is complete, reboot the server.

**Step 5** Log in to your system using domain credentials with administrative privileges. The Unified CCE 12.6(2) installation wizard launches. Click **Next** to proceed.

**Step 6** Select the radio button to accept the license agreement and click **Next**.

**Step 7** Click **Install** to begin the installation.

**Step 8** Select the radio button to restart the system and click **Finish**.

## Set Up Administration Client

You can't run the Administration Client Setup tool remotely through a browser. Run the tool on the local machine. You must log in to the local machine with the system Administrator account. Configure Microsoft Chromium Edge as the default browser before launching Administration Client.

### Before you begin

To view the lists and to perform tasks with the Administration Client Setup tool, you must have the following permissions:

- Administrator on the local machine
- Either a domain administrator or a member of at least one Setup security group in the machine domain

### Procedure

**Step 1** Open the Administration Client Setup tool from Unified CCE Tools shortcut on the desktop.

**Step 2** Sign in as a domain user with local Administrator rights.

**Step 3** Click **Instance Management**, and then click **Add**.

**Step 4** On the **Add Instance** page, from the drop-down list, choose the customer facility and instance.

**Step 5** Enter an instance number.

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

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

**Step 7** Select **Component Management** > **Administration Clients**.

**Step 8** Click **Add**.

**Step 9** Select an instance for the Administration Client from the drop-down list.

**Step 10** Click the radio button for your Administration Client type.

**Step 11** Enter the hostname or IP address of the Primary and Secondary Administration & Data Servers. If you have only one Administration & Data Server, specify it for both Primary and and Secondary Administration & Data Servers; both fields are required.

**Step 12** Click **Save**.

# Install Unified CCE Language Pack

The Unified CCE Language pack is used to install the localized version of the help files of the Unified CCE Web Administration tool.

The Unified CCE Language pack also contains the customized version of Configuration Manager tools for east Asian locales like Chinese, Japanese and Korean. The language pack enables localized input to be entered in those Configuration Manager tool sets.

These tool sets include some of the following tools:

- Explorer Tools
- List Tools
- System Information
- Outbound Option related tools

**Note** Unified CCE 12.6(2) has a separate language pack.

# Java Upgrades

During installations and upgrades, Unified CCE installs the base required Java version.

You can apply Java updates to your contact center as follows:

- Apply Java updates for the latest 32-bit Java 8 minor version.

  For the most current Java support information, 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.

  You can download and install the OpenJDK Java updates from the OpenLogic website.

- Modify the Windows CCE_JAVA_HOME environment variable to point to the new OpenJDK Java Runtime Environment (JRE) location if it has changed.

**Note** AppDynamics machine agent that is packaged with Unified ICM and Unified CVP uses a separate copy of OpenJDK. Any vulnerability fix for OpenJDK requires an upgrade of the AppDynamics machine agent. This update is delivered through an engineering special (ES) for Unified ICM and Unified CVP.

# Upgrade OpenJDKUtility

The Cisco Upgrade OpenJDKUtility:

- Upgrades OpenJDK JRE to latest release.
- Supports upgrade for both MSI and Zip file formats.
- Automatically sets the CCE_JAVA_HOME environment variable to updated version so that Unified CCE applications can employ the latest OpenJDK version as the Java runtime.

Before using the tool:

- Download the OpenJDK installer from the OpenLogic OpenJDK website: https://www.openlogic.com/openjdk. (Both msi and zip formats are supported).
- Copy the downloaded file into the Unified CCE component VMs. *For Example* **C:\UpgradeOpenJDKTool**.
- Download the utility from https://software.cisco.com/download/home/284360381/type/284416107/release/12.6(2) and unzip **OpenJdkUpgradeTool.zip** to any local folder. For example: Download and Unzip under **C:\UpgradeOpenJDKTool**.
- Run **openJDKUtility.exe** from unziped folder For all the supported commands and for more details, refer to the *Readme.html* (which is available as part of the *OpenJdkUpgradeTool.zip* ).

  Once the installation is successful, **CCE_JAVA_HOME** is updated and does not trigger the system reboot.

# Upgrade Tomcat Utility

Use the optional Cisco Upgrade Tomcat Utility to:

- Upgrade Tomcat to version 9.0 build releases. (That is, only version 9.0 build releases work with this tool.) You may choose to upgrade to newer builds of Tomcat release 9.0 to keep up with the latest security fixes.

  Tomcat uses the following release numbering scheme: Major.minor.build. For example, you can upgrade from 9.0.22 to 9.0.69. You cannot use this tool for major or minor version upgrades.

Before using the tool:

- Download the Tomcat installer (apache-tomcat-version.exe) from the Tomcat website: http://archive.apache.org/dist/tomcat/tomcat-9/. Copy the installer onto the Unified CCE component VMs. For Example C:\UpgradeTomcatTool.

- Download the utility zip file, extract it, and run the batch file to upgrade Tomcat.

  Download link: https://software.cisco.com/download/home/284360381/type/284416107/release/12.6(2)

- Delete or back up large log files in these directories to reduce upgrade time:

  <ICM install directory>:\icm\tomcat\logs
  <ICM install directory>:\icm\debug.txt

# Install Tomcat

For detailed information on the results from each step, see the ../UpgradeTomcatResults/UpgradeTomcat.log file.

**Note** Stop Unified CCE services on the VM before using the Tomcat Utility.

**Procedure**

**Step 1** From the command line, navigate to the directory where you copied the Upgrade Tomcat Utility.

**Step 2** Enter this command to run the tool: **tomcatutility.bat**.

**Step 3** When prompted, enter the full pathname of the Tomcat installer version you want to use.

For example:

```
c:\tomcatInstaller\apache-tomcat-9.0.69.exe
```

**Step 4** When prompted, enter **yes** to continue with the install.

**Step 5** Repeat these steps for all unified CCE component VMs.

**Note** If the latest installed Tomcat does not work properly, install the previous working version using the Tomcat utility by following the above-mentioned steps.

# Silent Installation

In certain situations, such as when a system administrator wants to install or upgrade software silently on multiple systems simultaneously, a silent installation is performed to run an installation wizard.

## Silent Installation Prerequisites for Unified CCE Release 12.5(1)

Before running a silent installation, complete the following tasks:

- Stop all applications that are running on the system.
- By default, silent installation assumes the following parameter: **Install on Drive C**.

  To override this default, edit the ICMCCSilentsetup.ini file in the ICM-CCE-Installer directory.
- Mount the ISO image to the target machine, and make the following edits on the target machine:

- If you are performing a Technology Refresh upgrade, change the **szInstallType** from **0** to **1**. The default value of **0** is for a Fresh Install.
- If you are performing a Technology Refresh upgrade, provide a path for the **szExportedRegistryPath** parameter where the exported registry from source machine is placed.
- To change the drive on which you are installing the application, change the **szDrive** parameter. Replace C with the drive where you want to install.
- If you do not want to apply SQL Security Hardening, change the line that reads **szSQLSecurity=1** to **szSQLSecurity=0**.

**Note** SQL Security Hardening should not be applied as part of silent installation on Windows Server 2019 and SQL Server 2019 platform. Change the line that reads szSQLSecurity=1 to szSQLSecurity=0. SQL Security Hardening can be applied post installation using Security Wizard tool.

## Perform a Silent Installation for Unified CCE Release 12.5(1)

**Procedure**

**Step 1** Mount the Installation ISO image to the target machine. For more information, see Mount ISO Files, on page 16.

**Step 2** From a command prompt window, navigate to the ICM-CCE-Installer directory.

**Step 3** Enter the command **setup.exe /s**.

Installation starts. Upon successful installation, the server reboots.

**Note** If the installation is not successful, no error message appears in the command prompt window. You must check the installation log file `<SystemDrive>:\temp\ICMInstall.log` to determine the reason why the installation failed.

## Silent Installation Prerequisites for Unified CCE Release 12.6(2)

Before running a silent installation, complete the following tasks:

- Stop all applications that are running on the system.
- The machine on which you create your response file should have a configuration that closely matches the machines on which you will run silent installs. This minimizes the chances of unexpected dialogs being triggered during the installation that could terminate the installation.

  For example, if the response file is created on a machine with Unified CCE services set to Manual and then run on a machine with those services set to Automatic, an additional dialog will open during the install (alerting you that the services have been set from Automatic to Manual). This unexpected dialog

will cause the install to terminate, potentially leaving the system in an invalid state that requires manual recovery.

## Perform a silent installation for Unified CCE Release 12.6(2)

### Procedure

**Step 1** Run setup from a command prompt with two command line arguments to create the response file.

**Example:**

```
"c:\ICM12.6(2).exe" -r -f1 c:\myanswerfilename.iss
```

The -r flag is for recording the response file.

The -f1 flag is the full path and filename for the resulting response file to be created.

**Note** There is no space between the -f1 and the start of the file path. If no -f1 flag is present, the response file is written to a default location (C:\Windows)".

When you have navigated through the setup process (which completes a full installation of the product on the machine recording the response file) the resulting response file can be copied to any additional machine during a silent installation.

**Step 2** Run setup from a command prompt using the same syntax as listed in step 1, with one exception: use **-s** instead of **-r** to indicate the install should run silently using the response file found at -f1filepath.

**Example:**

```
"c:\ICM12.6(2).exe" -s -f1 c:\myanswerfilename.iss -f2 c:\silentinstall.log
```

The -f2 flag creates a log file.

### What to do next

Verify that the silent installation was successful by checking the installer log file to make sure no errors were reported. If your silent installation does not run, check the log file for `ResultCode=-5`. It indicates the installer could not find your response file; recheck your path and file names.

During the creation of the response file, if you chose not to reboot the machine after the installation, ensure that you manually reboot any silently installed system prior to starting the services.

# Set Deployment Type in Unified CCE Administration Configuration

Perform the following steps to set the deployment type.

For more information on deployment types, see the following document:

*Solution Design Guide for Cisco Unified Contact Center Enterprise* at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html

### Procedure

**Step 1** On Administration & Data Server, from the desktop open the **Unified CCE Tools** folder and navigate to: **Administration Tools** > **CCE Web Administration** .

**Step 2** Log in as a *Config* security group member in the format user@domain.

**Step 3** Double-click **Unified CCE Administration**.

**Step 4** Click **Infrastructure Settings** > **Deployment Settings**.

**Step 5** On the **Deployment Type** page, select your deployment from the drop-down menu and click **Next**.

**Step 6** Click **Done**.

### What to do next

Set the principal AW and configure it with the Diagnostic Framework Service domain, username, and password if you have not already.

# Cisco Finesse Server Installation

Cisco Finesse server is installed on a virtual machine (VM). The installation runs from an ISO image and uses an OVA template. For more information, see *Cisco Finesse Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html.

**Note** Configure a DataStore ISO file on the virtual CD/DVD drive of the target VM to install Finesse.

The installation takes about an hour. For most of that time, it can run unattended. Much of the installation requires no action on the part of the person who runs it. When user input is required, use the following keyboard navigation and selection actions. The installation wizard screens do not recognize a mouse or a touchpad.

| To do this | Press this key |
|---|---|
| Move to the next field. | Tab |
| Move to the previous field. | Alt-Tab |
| Select an option. | Spacebar |
| Scroll up or down a list. | Up or Down Arrow keys |
| Go to the previous screen. | Tab to Back and press the Spacebar |
| Get information about a screen. | Tab to Help and press the Spacebar |

## Installation Task Flow

The following table provides an overview of the tasks you perform to install Cisco Finesse. Tasks must be performed in the order they are listed.

| | | |
|---|---|---|
| 1 | Install Finesse on the primary node. | See Install Finesse on Primary Node, on page 64. |
| 2 | Configure the database settings. | See Configure Contact Center Enterprise Administration and Data Server Settings, on page 67. |
| 3 | Configure the CTI server settings. | See Configure Contact Center Enterprise CTI Server Settings, on page 172 |
| 4 | Restart Cisco Finesse Tomcat on the primary node. | See Restart Cisco Finesse Tomcat, on page 71. |
| 5 | Validate configuration | See Validate Configuration, on page 71 |
| 6 | Configure the cluster settings for the secondary node. | See Configure Cluster Settings, on page 72. |
| 7 | Install Finesse on the secondary node. | See Install Finesse on Secondary Node, on page 72. |
| 8 | Ensure replication is functioning between the two nodes. | See Check Replication Status, on page 75. |
| 8 | Install language packs (optional). | See Install language pack. |
| 9 | Install VMware Tools | See Install VMware Tools for VOS, on page 93 |

## Install Finesse on Primary Node

### Procedure

**Step 1** Follow the instructions in the OVA README.txt file to import and deploy the OVA, to edit VM settings, and to power on the VM and edit the BIOS settings in the console. For more information, see the section on *Installation Files*.

**Note** Do not use Thin Provisioning or a VM snapshot when creating a VM to host Cisco Finesse. The use of Thin Provisioning or snapshots can negatively impact the performance of Cisco Finesse operation.

Messages appear while the preinstallation script runs. When the preinstallation script ends, the DVD Found screen opens.

**Step 2** Select **OK** on the Disk Found screen to begin the verification of the media integrity and a brief hardware check.

If the media check passes, select **OK** to open the Product Deployment Selection screen. Continue to Step 3.

If the media check fails, the installation terminates.

**Step 3** The Product Deployment Selection screen states that the Cisco Finesse product suite will be installed. This screen has only one choice: **OK**.

Select **OK** to open the Proceed with Install screen.

**Step 4** The Proceed with Install screen shows the version of the product that is currently installed (if any) and the version of the product for this ISO. For the initial installation, the version currently installed shows NONE.

Select **Yes** on the Proceed with Install screen to open the Platform Installation Wizard screen.

**Step 5** On the Platform Installation Wizard screen, select **Proceed** to open the Basic Install screen.

**Step 6** Select **Continue** on the Basic Install screen to open the Basic Install wizard.

The Basic Install wizard presents a series of screens that present questions and options pertinent to the platform and the setup configuration. Help is available for each wizard screen.

The first Basic Install wizard screen is Timezone Configuration.

**Step 7** On the Timezone Configuration screen:

a) Use the up and down arrows to locate the local time zone that most closely matches your server location. You can also type the initial character of the time zone to move to that item in the list. The Timezone field is based on country and city and is mandatory. Setting it incorrectly can affect system operation.
b) Select **OK** to open the Auto Negotiation Configuration screen.

**Step 8** On the Auto Negotiation Configuration screen, select **Continue** to use automatic negotiation for the settings of the Ethernet network interface card (NIC).

The MTU Configuration screen appears.

**Step 9** In the MTU Configuration screen, select **No** to keep the default setting for Maximum Transmission Units (1500).

**Note** Finesse supports the default setting of 1500 for MTU only. No other value is supported.

Your selection of No opens the Static Network Configuration screen.

**Step 10** On the Static Network Configuration screen, enter static network configuration values as follows, referring to the Configuration Worksheet if necessary:

a) Enter the **Host Name**.
b) Enter the **IP Address**.
c) Enter the **IP Mask**.
d) Enter the **GW Address**.
e) Select **OK** to open the Domain Name System (DNS) Client Configuration screen.

**Step 11** On the DNS Client Configuration screen, select **Yes** to specify the DNS client information.

**Important** DNS client configuration is *mandatory* for Cisco Finesse. Select Yes on this screen. If you select No, after the installation is complete, agents *cannot* sign in to the desktop and you have to reinstall Finesse.

**Step 12** Specify your DNS client information as follows, referring to the Configuration Worksheet if necessary:

a) Enter the **Primary DNS** (mandatory).
b) Enter the **Secondary DNS** (optional).
c) Enter the **Domain** (mandatory).
d) Select **OK** to open the Administrator Login Configuration screen.

**Step 13** On the Administrator Login Configuration screen:

a) Enter the credentials for the administrator.
b) Select **OK** to open the Certificate Information screen.

**Step 14** On the Certificate Information screen:

a) Enter the following data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country.
b) Select **OK** to open the First Node Configuration screen.

**Step 15** On the First Node Configuration screen, select **Yes** to indicate that you are configuring the first node.

Your selection of Yes opens the Network Time Protocol Client Configuration screen.

**Step 16** On the Network Time Protocol Client Configuration screen, enter the IP address, NTP server name, or NTP Server Pool name for at least one external NTP server.

**Step 17** After you complete the NTP configuration, select **OK**. This action opens the Security Configuration screen.

**Step 18** On the Security Configuration screen, enter the Database Access Security password, and then select **OK**.

**Step 19** On the Application User Configuration screen, enter the credentials for the application user.

Select **OK** to open the Platform Configuration Confirmation screen. This screen states that the platform configuration is complete.

**Step 20** On the Platform Configuration Confirmation screen, select **OK**.

The installation begins.

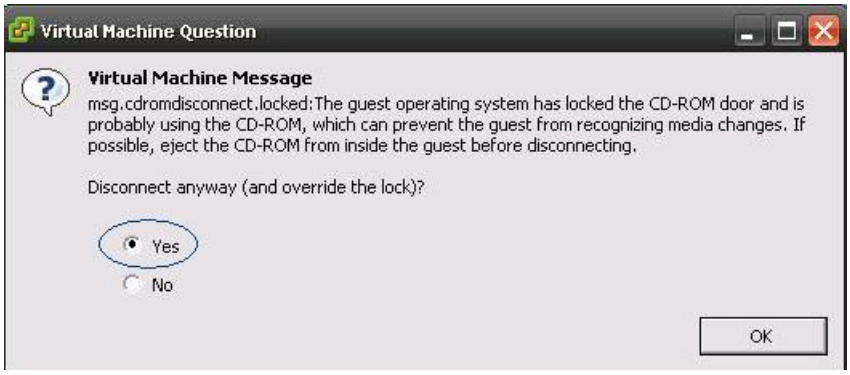
The installation can take up to an hour to complete and can run unattended for most of that time.

During the installation, the monitor shows a series of processes, as follows:

- Formatting progress bars
- Copying File progress bar
- Package Installation progress bars
- Post Install progress bar
- Populate RPM Archive progress bar
- Application Installation progress bars (multiple Component Install screens, security checks)
- An informational screen saying the system will reboot momentarily to continue the installation

  If you see the following virtual machine question, select **Yes**, and then click **OK**:

***Figure 1: Virtual Machine Message***




- A system reboot

Messages stream down your monitor during the reboot. Some of them prompt you to press a key. *Do not* respond to these prompts to press a key.

- Application Pre Install progress bars
- Configure and Setup Network progress bars

**Note** If a Network Connectivity Failure screen appears during the Configure and Setup Network process, click **Review**, and then click **OK** at the Errors screen. Follow the prompts to reenter the information that caused the failure. The installation continues when the connection information is complete.

- Security configuration

A message appears that states the installation of Cisco Finesse has completed successfully.

```
The installation of Cisco Finesse has completed successfully.

Cisco Finesse <version number>
<hostname> login: _
```

### What to do next

Sign in to the Finesse administration console on the primary Finesse server (https://*FQDN of Finesse server:8445*/cfadmin) to configure CTI server, Administration & Database server, and cluster settings.

After you configure these settings, install Finesse on the secondary node.

## Configure Contact Center Enterprise Administration and Data Server Settings

Configure the Contact Center Enterprise Administration & Data Server settings to enable authentication for Cisco Finesse agents and supervisors.

**Note** If you are using HTTPS, the first time you access the administration console, you see a browser security warning. To eliminate browser security warnings each time you sign in, you can trust the self-signed certificate provided with Finesse or obtain and upload a CA certificate.

### Procedure

**Step 1** Sign in to the administration console.

**Step 2** In the Contact Center Enterprise Administration & Data Server Settings area, enter the Administration & Data Server settings as described in the following table. Refer to your configuration worksheet if necessary.

| Field | Description |
|---|---|
| Primary Host/IP Address | The hostname or IP address of the Unified CCE Administration & Data Server. For example, **abcd12-5-aw-a**. |

| Field | Description |
|---|---|
| Backup Host/IP Address | The hostname or IP address of the backup Unified CCE Administration & Data Server. For example, **abcd12-5-aw-b**. |
| Database Port | The port of the Unified CCE Administration & Data Server.<br>The default value is 1433.<br>**Note** Cisco Finesse expects the primary and backup Administration & Data Server ports to be the same, hence the Finesse administration console exposes one port field. You must ensure that the port is the same for the primary and backup Administration & Data Servers. |
| AW Database Name | The name of the AW Database (AWDB). For example, **ucceinstance_awdb**. |
| Domain | The domain name of the AWDB. For example, **cisco.com**. |
| Username | The username required to sign in to the AWDB.<br>**Note** If you specify a domain, this user refers to the Administrator Domain user that the AWDB uses to synchronize with the logger. In which case, the AWDB server must use Windows authentication and the configured username must be a domain user.<br>If you do not specify a domain, this user must be an SQL user. |
| Password | The password required to sign in to the AWDB. |

**Step 3** Click **Save**.

## Contact Center Enterprise CTI Server Settings

Use the Contact Center Enterprise CTI Server Settings gadget to configure the A and B Side CTI servers.

All fields on this tab are populated with default system values or with values an administrator has previously entered. Change values to reflect your environment and preferences.

For configuring secure connection select the Enable SSL encryption check box.

Test the CTI connection for given configuration using the **Test Connection** button.

**Note** After you make any changes to the values on the Contact Center Enterprise CTI Server Settings gadget, you must restart all the nodes of Cisco Finesse Tomcat. To make changes to other settings (such as Contact Center Enterprise Administration & Data Server settings), you can make those changes and then restart Cisco Finesse Tomcat.

If you restart Cisco Finesse Tomcat, agents must sign out and sign in again. As a best practice, make changes to CTI server settings and restart the Cisco Finesse Tomcat Service during hours when agents are not signed in to the Finesse desktop.

The secure encryption and Test Connection functionality is supported only from Unified CCE 12.5.

**Note** Although the B Side Host/IP Address and B Side Port fields are not shown as required, A and B Side CTI servers are mandatory for a production deployment of Unified CCE and Cisco Finesse.

The following table describes the fields on the Contact Center Enterprise CTI Server Settings gadget:

| Field | Explanation |
|---|---|
| A Side Host/IP Address | The hostname or IP address of the A Side CTI server. This field is required.<br>This value is typically the IP address of the Peripheral Gateway (PG). The CTI server runs on the PG. |
| A Side Port | The value of this field must match the port configured during the setup of the A Side CTI server.<br>This field is required and accepts values between 1 and 65535.<br>You can find this value using the Unified CCE Diagnostic Framework Portico tool on the PG box. For more information about Diagnostic Framework Portico, see the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise*.<br>The default value is 42027. |
| Peripheral ID | The ID of the Agent PG Routing Client (PIM).<br>The Agent PG Peripheral ID should be configured to the same value for the A and B Side CTI server.<br>This field is required and accepts values between 1 and 32767.<br>The default value is 5000. |
| B Side Host/IP Address | The hostname or IP address of the B Side CTI server. |

| Field | Explanation |
|---|---|
| B Side Port | The value of this field must match the port configured during the setup of the B Side CTI server.<br>This field accepts values between 1 and 65535. |
| Enable SSL encryption | Check this box to enable secure encryption. |

### Actions on the Contact Center Enterprise CTI Server Settings gadget:

- **Save:** Saves your configuration changes.
- **Revert:** Retrieves the most recently saved server settings.
- **Test Connection:** Tests the CTI connection.

### CTI Test Connection

When you click **Test Connection**:

1. Input validation is done on the request attributes.

   Host/IP Address must not be empty. Port and Peripheral IDs must be within the valid range.

2. Validation is done to check if the provided Host/IP is resolved by Finesse box.
3. Validation is done to check if AW Database is reachable and if a valid path ID is configured for the provided Peripheral ID.
4. Socket connection is established to the provided Host/IP and port. The connection might fail if there is no route to the provided IP. If SSL encryption box is checked, this step also checks for successful TLS handshake. For TLS handshake to be successful, mutual trust has to be established between Finesse and CTI server.

   For information on how to establish trust between Finesse and CTI server, see *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

5. After successful socket connection, a CTI initialization request is sent to check if the provided host is a CTI host.

   If the CTI response is a success for the CTI initialization request and peripheral provided is configured with Unified CCE, it is confirmed to be a CTI host.

6. CTI connection is closed by sending a CTI session close request.

**Note** If **Test Connection** is successful for Side A or B of the CTI cluster and the other side fails, it is a valid configuration as CTI server works in active-passive mode and connects to the active node. Inactive CTI node will refuse connection on the CTI port. However, Administrator has to ensure that the failed side also has a valid entry for CTI host and port field. System cannot verify this due to server restrictions.

If **Test Connection** is successful on Side A and B of the CTI cluster, then there is an error in the system configuration. Verify that the Side A and B of the CTI node have valid entries for port and host.

Test connection API success result does not guarantee peripheral to be online. It only validates if the peripheral provided is configured with Unified CCE.

Test connection API with insecure connection parameter will function as intended for earlier versions of Unified CCE deployments.

## Restart Cisco Finesse Tomcat

After you make changes to the Contact Center Enterprise CTI Server, Contact Center Enterprise Administration & Data Server, or cluster settings, restart Cisco Finesse Tomcat for the changes to take effect.

**Note** After you restart Finesse, it can take approximately 6 minutes for all server-related services to restart. Therefore, you wait 6 minutes before you attempt to access the Finesse administration console.

### Procedure

**Step 1** Access the CLI and run the following command:

**utils service restart Cisco Finesse Tomcat**

**Step 2** You can enter the command **utils service list** to monitor the Cisco Finesse Tomcat Service. After Cisco Finesse Tomcat changes to STARTED, the configured agents can sign in to the desktop.

## Validate Configuration

After starting the Tomcat service, you must test the configuration for the changes you have made.

### Procedure

**Step 1** Log in to the GUI

**Step 2** Click **Test** to test the configuration changes.

Validation errors, if any, in the configuration are displayed.

If there are any errors, you must restart the Tomcat service after you resolve the errors.

## Configure Cluster Settings

Configure the cluster settings for the secondary Finesse node. The secondary Finesse node handles agent requests if the primary server goes down.

### Procedure

**Step 1** If you are not already signed in the primary node, sign in to the administration console of the primary node with the Application User credentials.

**Step 2** In the Cluster Settings area, in the Hostname field, enter the hostname of the secondary Finesse server.

**Step 3** Click **Save**.

## Install Finesse on Secondary Node

Install the same version of Finesse on both the primary and secondary Finesse nodes.

**Note** Configure a Datastore ISO file on the virtual CD/DVD drive of the target VM to install Finesse.

**Note** Finesse administration tasks can only be performed on the primary Finesse server. After you install the secondary server, sign in to the administration console on the primary server to perform administration tasks (such as configuring reason codes or call variable layout).

### Before you begin

- Install Finesse on the primary server. See *Install Finesse on Primary Node*.
- Use the Finesse administration console on the primary Finesse server to configure CTI server, Administration & Database server, and cluster settings.
- Ensure that the DNS server has forward and reverse DNS set up for both the primary and secondary node.

### Procedure

**Step 1** Follow the instructions in the OVA README.txt file to import and deploy the OVA, to edit VM settings, and to power on the VM and edit the BIOS settings in the Console.

Messages appear while the preinstallation script runs. When the preinstallation script ends, the DVD Found screen opens.

**Step 2** Select **Yes** on the DVD Found screen to begin the verification of the media integrity and a brief hardware check.

If the media check passes, select **OK** to open the Product Deployment Selection screen. Continue to Step 3.

If the media check fails, the installation terminates.

**Step 3** The Product Deployment Selection screen states that the Cisco Finesse product suite will be installed. This screen has only one option: **OK**.

Select **OK** to open the Proceed with Install screen.

**Step 4** The Proceed with Install screen shows the version of the product that is currently installed (if any) and the version of the product for this ISO. For the initial installation, the version currently installed shows NONE.

Select **Yes** on the Proceed with Install screen to open the Platform Installation Wizard screen.

**Step 5** On the Platform Installation Wizard screen, select **Proceed** to open the Basic Install screen.

**Step 6** Select **Continue** on the Basic Install screen to open the Basic Install wizard.

The Basic Install wizard presents a series of screens that present questions and options pertinent to the platform and the setup configuration. Help is available for each wizard screen.

The first Basic Install wizard screen is Timezone Configuration.

**Step 7** In the Timezone Configuration screen:

a) Use the up and down arrows to locate the local time zone that most closely matches your server location. You can also type the initial character of the time zone to move to that item in the list. The Timezone field is based on country and city and is mandatory. Setting it incorrectly can affect system operation.
b) Select **OK** to open the Auto Negotiation Configuration screen.

**Step 8** On the Auto Negotiation Configuration screen, select **Continue** to use automatic negotiation for the settings of the Ethernet network interface card (NIC).

The MTU Configuration screen appears.

**Step 9** On the MTU Configuration screen, select **No** to keep the default setting for Maximum Transmission Units (1500).

**Note** Finesse supports the default setting of 1500 for MTU only. No other value is supported.

Your selection of No opens the Static Network Configuration screen.

**Step 10** On the Static Network Configuration screen, enter the static network configuration values as follows, referring to the Configuration Worksheet if necessary:

a) Enter the **Host Name**.
b) Enter the **IP Address**.
c) Enter the **IP Mask**.
d) Enter the **GW Address**.
e) Select **OK** to open the Domain Name System (DNS) Client Configuration screen.

**Step 11** On the **DNS Client Configuration** screen, select **Yes** to specify the DNS client information.

**IMPORTANT:** DNS client configuration is *mandatory* for Cisco Finesse. Select Yes on this screen. If you select No, after the installation is complete, agents **can't** sign in to the desktop and you have to reinstall Finesse.

**Step 12** Specify your DNS client information as follows, referring to the Configuration Worksheet if necessary:

a) Enter the **Primary DNS** (mandatory).
b) Enter the **Secondary DNS** (optional).
c) Enter the **Domain** (mandatory).

d) Select **OK** to open the Administrator Login Configuration screen.

**Step 13** On the Administrator Login Configuration screen:

a) Enter the credentials for the administrator.
b) Select **OK** to open the Certificate Information screen.

**Step 14** On the Certificate Information screen:

a) Enter the following data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country.
b) Select **OK** to open the First Node Configuration screen.

**Step 15** On the First Node Configuration screen, select **No** to indicate that you're configuring the second node.

A warning message appears that indicates you must first configure the server on the first node before you can proceed. If you already configured the first node, select **OK**.

**Step 16** On the Network Connectivity Test Configuration screen, select **No** to proceed with the installation after connectivity is verified.

**Step 17** On the First Node Configuration screen, specify the information about the first node as follows:

a) Enter the **Host Name** of the primary Finesse server.
b) Enter the **IP Address** of the primary Finesse server.
c) Enter the **Security Password** of the primary Finesse server.
d) Confirm the **Security Password**.

**Step 18** Select **OK** to open the Platform Configuration Confirmation screen.

**Step 19** On the Platform Configuration Confirmation screen, select **OK**.

The installation begins.

The installation can take up to an hour to complete and can run unattended for most of that time.

A message appears that states the installation of Cisco Finesse has completed successfully.

```
The installation of Cisco Finesse has completed successfully.

Cisco Finesse <version number>
<hostname> login: _
```

### What to do next

Check the replication status. If all nodes in the cluster show a **replication status of 2**, replication is functioning correctly.

After installation, by default the configuration that controls the reverse-proxy authentication is enabled. When the reverse-proxy authentication is enabled and multiple client-side certificates are configured on the system, it impacts the certificate acceptance pop-ups from clients that are connected directly to the Finesse server without using a reverse-proxy. To prevent these pop-ups from appearing, use the **utils systems reverse-proxy client-auth** command on both the Finesse nodes to disable the reverse-proxy authentication that don't need VPN-less access to Finesse.

**Note** It can take 10–20 minutes to establish replication fully between the two nodes.

To access platform-specific applications like Disaster Recovery System, Cisco Unified Serviceability, and Cisco Unified Operating System Administration, use the following URL, https://*FQDN of Finesse server*:8443.

## Check Replication Status

### Procedure

**Step 1** Access the CLI on the primary Finesse server.

**Step 2** Sign in with the Administrator User credentials that are defined during installation.

**Step 3** Run the following command:

**utils dbreplication runtimestate**

This command returns the replication status on both the primary and secondary Finesse servers.

# Install Cisco Identity Service Standalone Deployment

Follow this sequence of tasks to install the Cisco Identity Service (Cisco IdS) standalone deployment.

| Sequence | Task |
|---|---|
| 1 | Verify that you created a separate virtual machine for the IdS publisher node and the IdS subscriber node. See Set Up Virtual Machines, on page 12. |
| 2 | Install IdS publisher node. See Install Publisher/Primary Node of Cisco Identity Service , on page 75 |
| 3 | Set IdS subscriber node. See Set IdS Subscriber Node, on page 77 |
| 4 | Install IdS subscriber node. See Install Subscriber/Secondary Node of Cisco Identity Service , on page 77 |
| 5 | Upgrade VMware Tools. See Install VMware Tools for VOS, on page 93 |

## Install Publisher/Primary Node of Cisco Identity Service

### Before you begin

DNS Configuration is mandatory for installation of Cisco Identity Service. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

**Note** If the deployment uses host files in addition to DNS, use FQDNs in the host file.

### Procedure

**Step 1** Create a virtual machine for your VOS-based contact center application using the OVA.

**Step 2** Mount the ISO image for the software to the virtual machine.

**Step 3** Select the virtual machine and power it on.

**Step 4** Follow the Install wizard, making selections as follows:

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.
b) In the **Success** screen, select **OK**.
c) In the **Product Deployment Selection** screen, select **Cisco Identity Service** and click **OK**.
d) In the **Proceed with Install** screen, select **Yes**.
e) In the **Platform Installation Wizard** screen, select **Proceed**.
f) In the **Apply Patch** screen, select **No**.
g) In the **Basic Install** screen, select **Continue**.
h) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

**Note** For Live Data servers, use the same timezone for all the nodes.

i) In the **Auto Negotiation Configuration** screen, select **Continue**.
j) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
k) In the **DHCP Configuration** screen, select **No**.
l) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
m) In the **DNS Client Configuration** screen, enter your DNS client configuration. Select **OK**.
n) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
o) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
p) In the **First Node Configuration** screen, select **Yes**.
q) In the **Network Time Protocol Client Configuration** screen, enter a valid NTP server IP address and select **OK**.
r) In the **Security Configuration** screen, enter the security password and select **OK**.
s) In the **SMTP Host Configuration** screen, select **No**.
t) In the **Application User Configuration** screen, enter the application username. Enter, and confirm the application user password. Select **OK**.
u) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

- There is a reboot in the middle of the installation.
- The installation ends at a sign-in prompt.

**Step 5** Unmount the ISO image.

## Set IdS Subscriber Node

You must provide the publisher node the address of the subscriber node. You do this with the **set ids subscriber** command.

### Procedure

**Step 1** Log in to your publisher IdS node.

**Step 2** Run the following command to set the subscriber node:

**set ids subscriber** *name*
**name**
Specifies the hostname or ip address of the IdS subscriber node address.

### What to do next

You can use these Cisco IdS CLI commands only in an IdS standalone deployment. You run these commands on the IdS publisher node.

**Required Minimum Privilege Level:** Ordinary

Use this command to show IdS subscriber node information.

**show ids subscriber**

There are no required parameters.

**Required Minimum Privilege Level:** Advanced

Use this command to unset IdS subscriber node configuration.

**unset ids subscriber**

There are no required parameters.

## Install Subscriber/Secondary Node of Cisco Identity Service

### Before you begin

DNS Configuration is mandatory for installation of Cisco Identity Service. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

**Note** If the deployment uses host files in addition to DNS, use FQDNs in the host file.

Before you install the subscriber/secondary nodes, you must install the publisher/primary nodes and configure the clusters.

### Procedure

**Step 1** Create a virtual machine for your VOS-based contact center application using the OVA.

**Step 2** Mount the ISO image for the software to the virtual machine.

**Step 3** Select the virtual machine and power it on.

**Step 4** Follow the Install wizard, making selections as follows:

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.
b) In the **Success** screen, select **OK**.
c) In the **Product Deployment Selection** screen, select **Cisco Identity Service** and click **OK**.

**Step 5** Follow the Install wizard, making selections as follows:

a) In the **Proceed with Install** screen, select **Yes**.
b) In the **Platform Installation Wizard** screen, select **Proceed**.
c) In the **Apply Patch** screen, select **No**.
d) In the **Basic Install** screen, select **Continue**.
e) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

**Note** For Live Data servers, use the same time zone for all the nodes.

f) In the **Auto Negotiation Configuration** screen, select **Continue**.
g) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
h) In the **DHCP Configuration** screen, select **No**.
i) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
j) In the **DNS Client Configuration** screen, enter your DNS client configuration. Select **OK**.
k) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
l) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
m) In the **First Node Configuration** screen, select **No**.
n) In the warning screen, select **OK**.
o) In the **Network Connectivity Test Configuration** screen, select **No**.
p) In the **First Node Access Configuration** screen, enter the host name and IP address of the first node. Enter and confirm the security password. Select **OK**.
q) In the **SMTP Host Configuration** screen, select **No**.
r) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

- There is a reboot in the middle of the installation.
- The installation ends at a sign-in prompt.

**Step 6** Unmount the ISO image.

# Live Data Standalone Installation

Follow this sequence of tasks to install Live Data Standalone.

| Sequence | Task |
|---|---|
| 1 | For all deployments except the 2000 agent reference design, verify that you created a separate virtual machine for the IdS publisher node and the IdS subscriber node. See Set Up Virtual Machines, on page 12. |
| 2 | Install Live Data Primary Node.<br>See Install Publisher/Primary Node of Live Data , on page 79 |
| 3 | Set Live Data Secondary Node, on page 80 |
| 4 | Install Live Data Secondary Node.<br>See Install Subscriber/Secondary node of Live Data , on page 81 |
| 5 | Upgrade VMware Tools. See Install Vmware Tools, on page 20. |
| 6 | See *Configure Live Data with AW* section in the chapter "Upgrade from a Standalone Deployment to a Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS)." |
| 7 | Configure Live Data Machine Services, on page 82 |
| 8 | Configure Live Data for Unified Intelligence Center Data Sources, on page 83 |
| 9 | Restart Live Data, on page 84 |
| 10 | Set Up Certificates for Live Data, on page 84 |

## Install Publisher/Primary Node of Live Data

### Before you begin

DNS Configuration is mandatory for installation of Live Data. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

**Note** If the deployment uses host files in addition to DNS, use FQDNs in the host file. Live Data and single sign-on (SSO) require FQDNs to work properly.

### Procedure

**Step 1** Create a virtual machine for your VOS-based contact center application using the OVA.

**Step 2** Mount the ISO image for the software to the virtual machine.

**Step 3** Select the virtual machine and power it on.

**Step 4** Follow the Install wizard, making selections as follows:

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.
b) In the **Success** screen, select **OK**.
c) In the **Product Deployment Selection** screen, select **Live Data** and click **OK**.
d) In the **Proceed with Install** screen, select **Yes**.
e) In the **Platform Installation Wizard** screen, select **Proceed**.
f) In the **Apply Patch** screen, select **No**.
g) In the **Basic Install** screen, select **Continue**.
h) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

**Note** For Live Data servers, use the same timezone for all the nodes.

i) In the **Auto Negotiation Configuration** screen, select **Continue**.
j) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
k) In the **DHCP Configuration** screen, select **No**.
l) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
m) In the **DNS Client Configuration** screen, enter your DNS client configuration. Select **OK**.
n) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
o) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
p) In the **First Node Configuration** screen, select **Yes**.
q) In the **Network Time Protocol Client Configuration** screen, enter a valid NTP server IP address and select **OK**.
r) In the **Security Configuration** screen, enter the security password and select **OK**.
s) In the **SMTP Host Configuration** screen, select **No**.
t) In the **Application User Configuration** screen, enter the application username. Enter, and confirm the application user password. Select **OK**.
u) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

- There is a reboot in the middle of the installation.
- The installation ends at a sign-in prompt.

**Step 5** Unmount the ISO image.

## Set Live Data Secondary Node

Use the **set live-data secondary** command to provide the primary node the address of the secondary node.

### Procedure

**Step 1** Log in to your primary Live Data node.

**Step 2** Run the following command to set the secondary node:

**set live-data secondary** *name*
**name**

Specifies the hostname or IP address of the Live Data secondary node.

## Install Subscriber/Secondary node of Live Data

This task is required for installation of the DNS Configuration is mandatory for installation of Live Data. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

### Before you begin

**Note** If the deployment uses host files in addition to DNS, use FQDNs in the host file. Live Data and single sign-on (SSO) require FQDNs to work properly.

Before you install the subscriber or secondary nodes, you must install the publisher or primary nodes and configure the clusters.

### Procedure

**Step 1** Create a virtual machine for your VOS-based contact center application using the OVA.

**Step 2** Mount the ISO image for the software to the virtual machine.

**Step 3** Select the virtual machine and power it on.

**Step 4** Follow the Install wizard, making selections as follows:

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.
b) In the **Success** screen, select **OK**.
c) In the **Product Deployment Selection** screen, select **Live Data** and click **OK**.

**Step 5** Follow the Install wizard, making selections as follows:

a) In the **Proceed with Install** screen, select **Yes**.
b) In the **Platform Installation Wizard** screen, select **Proceed**.
c) In the **Apply Patch** screen, select **No**.
d) In the **Basic Install** screen, select **Continue**.
e) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

**Note** For Live Data servers, use the same timezone for all the nodes.

f) In the **Auto Negotiation Configuration** screen, select **Continue**.
g) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
h) In the **DHCP Configuration** screen, select **No**.
i) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
j) In the **DNS Client Configuration** screen, enter your DNS client configuration. Select **OK**.

k) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
l) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
m) In the **First Node Configuration** screen, select **No**.
n) In the warning screen, select **OK**.
o) In the **Network Connectivity Test Configuration** screen, select **No**.
p) In the **First Node Access Configuration** screen, enter the host name and IP address of the first node. Enter and confirm the security password. Select **OK**.
q) In the **SMTP Host Configuration** screen, select **No**.
r) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

- There is a reboot in the middle of the installation.
- The installation ends at a sign-in prompt.

**Step 6** Unmount the ISO image.

## Configure Live Data Machine Services

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

**Note**

- Whenever you run set live-data machine-services, be sure to also run set live-data cuic-datasource to reconfigure the Live Data data sources for the Unified Intelligence Center. See Configure Live Data for Unified Intelligence Center Data Sources, on page 83.
- If you are using any certificates that are unapproved by Cisco or self-signed certificate, ensure to import the AWDB certificate into the Live Data server before you run set live-data machine-services.

### Procedure

**Step 1** Log in to your Live Data server.

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

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

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

**Note**

- The Router and Peripheral Gateway (PG) TIP and TOS connection information is automatically populated for Unified CCE deployments that support Live Data. To set the deployment type, see Set Deployment Type in Unified CCE Administration Configuration, on page 62. The Live Data server uses this information to establish a connection, and receive reporting data as well as agent and call events as they occur.
- Cisco Unified Communications Manager (CUCM) PG, generic PGs with CUCM peripherals, and Unified CCE Gateway PGs are supported for Live Data.

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

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

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

Verify that the show machine-services display changed hostname.

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

## Configure Live Data for Unified Intelligence Center Data Sources

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

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

**Procedure**

**Step 1** Log in to your Live Data server.

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

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

## Configure Cross Origin Resource Sharing (CORS) for Live Data

Live Data CORS commands allow you to configure CORS and hence allow web applications running on different origins to communicate with Live Data and CUIC.

For Unified Intelligence Centre gadgets (Live Data) to load in Cisco Finesse, ensure to:

- Enable CORS using `utils cuic cors enable` and `utils live-data cors enable` commands.
- Set the Finesse host URL in `utils cuic cors allowed_origin add URLs` and `utils live-data cors allowed_origin add URLs` commands.

**Examples:**

- https://<finesse-FQDN>
- https://<finesse-FQDN>:port

For more information on CUIC CORS CLIs, 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

## Restart Live Data

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

**Procedure**

Access the Live Data CLI and run the following command:

**utils system restart**

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

## Set Up Certificates for Live Data

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

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

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

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

For complete information

# Install Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS)

Follow this sequence of tasks to install the coresident deployment (Cisco Unified Intelligence Center with Live Data and IdS).

| Sequence | Task |
|---|---|
| 1 | Set Deployment Type in Unified CCE Administration Configuration:<br>Set Deployment Type in Unified CCE Administration Configuration, on page 62 |
| 2 | Install Coresident Deployment Primary Node.<br>See Install Publisher/Primary Node of Co-resident Deployment (Cisco Unified Intelligence Center with Live Data and IdS), on page 85 |
| 3 | Install Coresident Deployment Secondary Node.<br>See Install Subscriber/Secondary Node of Co-resident Deployment (Cisco Unified Intelligence Center with Live Data and IdS), on page 87 |
| 4 | Add Coresident (Cisco Unified Intelligence Center with Live Data and IdS) Machine Type to the System Inventory, on page 88 |
| 5 | Upgrade VMware Tools. See Install Vmware Tools, on page 20. |
| 6 | |
| 7 | Configure Live Data Unified Intelligence Center Data Sources, on page 89 |
| 8 | Restart Live Data, on page 89 |
| 9 | Set up certificates for Live Data. See |

**Note** From Cisco Finesse Release 12.5(1) or later, Cisco Unified Intelligence Center supports XML gadgets. Switching to XML based gadgets reduces latency and improves performance.

After Cisco Unified Intelligence Center or Coresident deployment installation, run **utils finesse layout updateCuicGadgetUrl** command to optimize the loading of Cisco Unified Intelligence Center gadgets. This command allows you to change the .jsp references of Cisco Unified Intelligence Center gadgets to .xml with no functional changes.

# Install Publisher/Primary Node of Co-resident Deployment (Cisco Unified Intelligence Center with Live Data and IdS)

### Before you begin

DNS Configuration is mandatory for installation of Coresident deployment (Cisco Unified Intelligence Center with Live Data and IdS). To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

**Note** If the deployment uses host files in addition to DNS, use FQDNs in the host file. Live Data and single sign-on (SSO) require FQDNs to work properly.

### Procedure

**Step 1** Create a virtual machine for your VOS-based contact center application using the OVA.

**Step 2** Mount the ISO image for the software to the virtual machine.

**Step 3** Select the virtual machine and power it on.

**Step 4** Follow the Install wizard, making selections as follows:

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.
b) In the **Success** screen, select **OK**.
c) In the **Product Deployment Selection** screen, for the Progger (Lab only) or 2000 agent reference design, choose **Cisco Unified Intelligence Center with Live Data and IdS**, and then select **OK**. The **Cisco Unified Intelligence Center with Live Data and IdS** option installs Cisco Unified Intelligence Center with Live Data and Cisco Identity Service (IdS) on the same server.
d) In the **Proceed with Install** screen, select **Yes**.
e) In the **Platform Installation Wizard** screen, select **Proceed**.
f) In the **Apply Patch** screen, select **No**.
g) In the **Basic Install** screen, select **Continue**.
h) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

**Note** For Live Data servers, use the same timezone for all the nodes.

i) In the **Auto Negotiation Configuration** screen, select **Continue**.
j) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
k) In the **DHCP Configuration** screen, select **No**.
l) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
m) In the **DNS Client Configuration** screen, enter your DNS client configuration. Select **OK**.
n) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
o) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
p) In the **First Node Configuration** screen, select **Yes**.
q) In the **Network Time Protocol Client Configuration** screen, enter a valid NTP server IP address and select **OK**.
r) In the **Security Configuration** screen, enter the security password and select **OK**.
s) In the **SMTP Host Configuration** screen, select **No**.
t) In the **Application User Configuration** screen, enter the application username. Enter, and confirm the application user password. Select **OK**.
u) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

- There is a reboot in the middle of the installation.
- The installation ends at a sign-in prompt.

**Step 5** Unmount the ISO image.

# Install Subscriber/Secondary Node of Co-resident Deployment (Cisco Unified Intelligence Center with Live Data and IdS)

### Before you begin

DNS Configuration is mandatory for installation of Coresident deployment (Cisco Unified Intelligence Center with Live Data and IdS). To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

**Note** If the deployment uses host files in addition to DNS, use FQDNs in the host file. Live Data and single sign-on (SSO) require FQDNs to work properly.

Before you install the subscriber or secondary nodes, you must install the publisher or primary nodes and configure the clusters.

### Procedure

**Step 1** Create a virtual machine for your VOS-based contact center application using the OVA.

**Step 2** Mount the ISO image for the software to the virtual machine.

**Step 3** Select the virtual machine and power it on.

**Step 4** Follow the Install wizard, making selections as follows:

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.
b) In the **Success** screen, select **OK**.
c) In the **Product Deployment Selection** screen, for the Progger (Lab only) or 2000 agent reference design, choose **Cisco Unified Intelligence Center with Live Data and IdS**, and then select **OK**. The **Cisco Unified Intelligence Center with Live Data and IdS** option installs Cisco Unified Intelligence Center with Live Data and Cisco Identity Service (IdS) on the same server.

**Step 5** Follow the Install wizard, making selections as follows:

a) In the **Proceed with Install** screen, select **Yes**.
b) In the **Platform Installation Wizard** screen, select **Proceed**.
c) In the **Apply Patch** screen, select **No**.
d) In the **Basic Install** screen, select **Continue**.
e) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

**Note** For Live Data servers, use the same timezone for all the nodes.

f) In the **Auto Negotiation Configuration** screen, select **Continue**.
g) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
h) In the **DHCP Configuration** screen, select **No**.
i) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
j) In the **DNS Client Configuration** screen, enter your DNS client configuration. Select **OK**.
k) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.

l) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
m) In the **First Node Configuration** screen, select **No**.
n) In the warning screen, select **OK**.
o) In the **Network Connectivity Test Configuration** screen, select **No**.
p) In the **First Node Access Configuration** screen, enter the host name and IP address of the first node. Enter and confirm the security password. Select **OK**.
q) In the **SMTP Host Configuration** screen, select **No**.
r) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

- There is a reboot in the middle of the installation.
- The installation ends at a sign-in prompt.

**Step 6** Unmount the ISO image.

## Add Coresident (Cisco Unified Intelligence Center with Live Data and IdS) Machine Type to the System Inventory

### Procedure

**Step 1** In Unified CCE Administration, navigate to **System** > **Deployment**.

**Step 2** Add the new machine to the System Inventory:

a) Click **Add**.

The **Add Machine** popup window opens.

b) From the Type drop-down menu, select the following machine type:

CUIC_LD_IdS Publisher, for the coresident Unified Intelligence Center, Live Data, and Identity Service machine available in the 2000 agent reference design.

c) In the **Hostname** field, enter the FQDN, hostname, or IP address of the machine.

The system attempts to convert the value you enter to FQDN.

d) Enter the machine's Administration credentials.
e) Click **Save**.

The machine and its related Subscriber or Secondary machine are added to the System Inventory.

### What to do next

If you remove a component from your deployment, delete it from your System Inventory. If you add the component again, or add more components, add those components to the System Inventory.

## Configure Live Data Unified Intelligence Center Data Sources

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

### Before you begin

- Ensure that AW distributor and Cisco Unified Intelligence Center Publisher are in service.
- Ensure that AW DB connection information is updated on the same node, where you want to configure Live Data CUIC data source.
- Configure Live Data endpoints in the **Machine Service** table.

### Procedure

**Step 1** Log in to your Live Data server.

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

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

## Restart Live Data

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

### Procedure

Access the Live Data CLI and run the following command:

**utils system restart**

# Install Cloud Connect

Follow this sequence of tasks to install the Cloud Connect cluster.

| Sequence | Task |
|---|---|
| 1 | Install Publisher or Primary Node of Cloud Connect.<br>See, Install Publisher or Primary Node of Cloud Connect, on page 90 |
| 2 | Set Cloud Connect Secondary Node.<br>See, Set Subscriber or Secondary Node of Cloud Connect, on page 91 |
| 3 | Install Subscriber or Secondary Node of Cloud Connect.<br>See, Install Subscriber or Secondary Node of Cloud Connect, on page 91 |

| Sequence | Task |
|---|---|
| 4 | Initial Configuration for Cloud Connect |

# Install Publisher or Primary Node of Cloud Connect

### Before you begin

DNS Configuration is mandatory for installation of Cloud Connect deployment. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

**Note** If the deployment uses host files in addition to DNS, use FQDNs in the host file.

### Procedure

**Step 1** Create a virtual machine for your VOS-based contact center application using the OVA.

**Step 2** Mount the ISO image for the software to the virtual machine.

**Step 3** Select the virtual machine and turn on the power.

**Step 4** Follow the Install wizard and select appropriate values:

a) In the Disk Found screen, click **OK** to begin the verification of the media integrity.
b) In the Success screen, select **OK**.
c) In the Product Deployment Selection screen, choose **Cisco Contact Center Cloud Connect**, and then select **OK**.
d) In the Proceed with Install screen, select **Yes**.
e) In the Platform Installation Wizard screen, select **Proceed**.
f) In the Apply Patch screen, select **No**.
g) In the Basic Install screen, select **Continue**.
h) In the Timezone Configuration screen, use the down arrow to set the zone to Central Controller time. Select **OK**.
i) In the Auto Negotiation Configuration screen, select **Continue**.
j) In the MTU Configuration screen, select **No** to keep the default setting for Maximum Transmission Units.
k) In the DHCP Configuration screen, select **No**.
l) In the Static Network Configuration screen, enter static configuration values. Select **OK**.
m) In the DNS Client Configuration screen, enter your DNS client configuration. Select **OK**.
n) In the Administrator Login Configuration screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
o) In the Certificate Information screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
p) In the First Node Configuration screen, select **Yes**.
q) In the Network Time Protocol Client Configuration screen, enter a valid NTP server IP address and select **OK**.
r) In the Security Configuration screen, enter the security password and select **OK**.
s) In the SMTP Host Configuration screen, select **No**.

t) In the Application User Configuration screen, enter the application username. Enter and confirm the application user password. Select **OK**.
u) In the Platform Configuration Confirmation screen, select **OK**. The installation begins and runs unattended.

**Note** During installation, the system is rebooted automatically. On completing installation, a sign-in prompt is displayed.

**Step 5** Unmount the ISO image.

## Set Subscriber or Secondary Node of Cloud Connect

Use the **set cloudconnect subscriber** command to provide the address of the secondary node in the primary node.

### Procedure

**Step 1** Sign in to your primary Cloud Connect node.

**Step 2** Run the following command to set the secondary node:

**set cloudconnect subscriber [name]**

**name** – Specifies the FQDN or IP address of the Cloud Connect subscriber node (maximum 255 characters).

## Install Subscriber or Secondary Node of Cloud Connect

Before you install the subscriber or secondary node, you must install the publisher or primary node and configure the cluster.

### Before you begin

DNS Configuration is mandatory for installation of Cloud Connect deployment. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

**Note** If the deployment uses host files in addition to DNS, use FQDNs in the host file.

### Procedure

**Step 1** Create a virtual machine for your VOS-based contact center application using the OVA.

**Step 2** Mount the ISO image for the software to the virtual machine.

**Step 3** Select the virtual machine and turn on the power.

**Step 4** Follow the Install wizard and select appropriate values:

a) In the Disk Found screen, click **OK** to begin the verification of the media integrity.
b) In the Success screen, select **OK**.

c) In the Product Deployment Selection screen, choose **Cisco Contact Center Cloud Connect**, and then select **OK**.
d) In the Proceed with Install screen, select **Yes**.
e) In the Platform Installation Wizard screen, select **Proceed**.
f) In the Apply Patch screen, select **No**.
g) In the Basic Install screen, select **Continue**.
h) In the Timezone Configuration screen, use the down arrow to set the zone to Central Controller time. Select **OK**.
i) In the Auto Negotiation Configuration screen, select **Continue**.
j) In the MTU Configuration screen, select **No** to keep the default setting for Maximum Transmission Units.
k) In the DHCP Configuration screen, select **No**.
l) In the Static Network Configuration screen, enter static configuration values. Select **OK**.
m) In the DNS Client Configuration screen, enter your DNS client configuration. Select **OK**.
n) In the Administrator Login Configuration screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
o) In the Certificate Information screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
p) In the First Node Configuration screen, select **No**.
q) In the warning screen, select **OK**.
r) In the Network Connectivity Test Configuration screen, select **No**.
s) In the First Node Access Configuration screen, enter the FQDN of the first node. Enter and confirm the security password. Select **OK**.
t) In the SMTP Host Configuration screen, select **No**.
u) In the Platform Configuration Confirmation screen, select **OK**. The installation begins and runs unattended.

**Note** During installation, the system is rebooted automatically. On completing installation, a sign-in prompt is displayed.

**Step 5** Unmount the ISO image.

**Note**
- In case one needs to add a subscriber back to the cluster, you must run the **set command** and re-install the subscriber.
- If a new subscriber needs to be added, we have to remove the existing subscriber node using the **unset command** and then add the new subscriber node using the **set command**. After that we need to install the new subscriber node to form the cluster.

## Initial Configuration for Cloud Connect

Before adding Cloud Connect to the inventory, you will have to install the certificates from both Cloud Connect publisher and subcriber.

For more information, see the section *Certificates for CCE Web Administration* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

**Procedure**

**Step 1** In the Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings**, click **Inventory**.

**Step 2** In the Inventory page, click **New** to add the new machine to the System Inventory.

**Step 3** In the Add Machine dialog box:

a) Select **Cloud Connect Publisher** from the Type list.
b) Enter Hostname or IP Address of the Cloud Connect Publisher Node.
c) Enter Username and Password for your Cloud Connect cluster Administrator.
d) Click **Save**.

**Note** For more information on Cloud Connect installation and onboarding process, see CCE Orchestration section.

**Note** When you configure Cloud Connect Publisher, its Cloud Connect Subscriber is added to the Inventory automatically.

# Install VMware Tools for VOS

To install or upgrade VMware Tools using VOS, perform the following steps:

**Procedure**

**Step 1** Ensure that your virtual machine is powered on.

**Step 2** Right-click the VM menu. Select **Guest** > **Install / Upgrade VMware tools** .

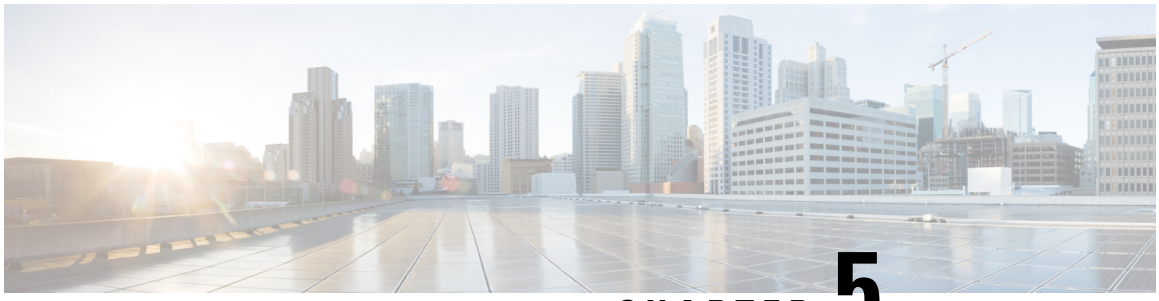
**Step 3** Choose the interactive tools update and press **OK**.

**Step 4** Open the console and log in at the command prompt.

**Step 5** Enter the command **utils vmtools refresh** and confirm.
The server automatically reboots twice.

**Step 6** After reboot, check the **Summary** tab for the VM to verify that the VMware Tools version is current. If it is not current, reboot the VM and check the version again.

The process takes a few minutes. After the process completes, the tools are listed as Running (Current) on the VM's Summary tab in vSphere.



CHAPTER 5

# Initial Configuration


- Initial Configuration Overview, on page 95
- Initial Configuration Task Flow, on page 95
- Initial Configuration Tasks, on page 96


## Initial Configuration Overview

This initial configuration brings the contact center to the point where a complete call flow is possible. The configured system will process information about incoming calls, perform call routing, and enable call handling.

## Initial Configuration Task Flow

| Task | See |
|---|---|
| Set Deployment Type in Unified CCE Administration Configuration | Set Deployment Type in Unified CCE Administration Configuration, on page 62 |
| Configure Cisco Unified Contact Center Enterprise | Configure Cisco Unified Contact Center Enterprise, on page 97 |
| Configure Cisco Unified Intelligence Center | Configure Cisco Unified Intelligence Center, on page 137 |
| Configure Cisco Unified Customer Voice Portal | Configure Cisco Unified Customer Voice Portal, on page 144 |
| Configure Cisco Unified Communications Manager | Configure Cisco Unified Communications Manager, on page 162 |
| Configure Cisco Finesse | Configure Cisco Finesse, on page 172 |

# Initial Configuration Tasks

## Configure Permissions in the Local Machine

In this release,Unified CCE defaults to providing user privileges by memberships to local user groups on local machines. This technique moves authorization out of Active Directory. However, it requires a one-time task on each local machine to grant the required permissions.

**Note** You can use the ADSecurityGroupUpdate registry key to choose between the new default behavior and the previous behavior. For more information, see the chapter on solution security in the Solution Design Guide.

Before using the Configuration Manager tool, configure the required registry and folder permissions for the `UcceConfig` group.

### Configure Registry Permissions

This procedure only applies to all the AW machines. Grant the required registry permissions for the `UcceConfig` group on the local machine.

**Procedure**

**Step 1** Run the `regedit.exe` utility.

**Step 2** Select `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM`.

**Step 3** Right-click and select **Permissions**.

**Step 4** If necessary, add `UcceConfig` in **Group or user names**.

**Step 5** Select `UcceConfig` and check **Allow** for the **Full Control** option.

**Step 6** Click **OK** to save the change.

**Step 7** Repeat the previous steps to grant **Full Control** to the `UcceConfig` group for `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco Systems, Inc.\ICM`.

**Step 8** Repeat the previous steps to grant **Full Control** to the `UcceConfig` group for `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2`.

**Note** If you have configured the Unified CCE Administration Client, open Local security policy and go to **User Rights Assignment**. Right click **Create Global Object**. Go to **properties** and add the local Group `UcceConfig`.

### Configure AW-HDS Database Permissions

Follow this procedure to grant access to the AWDB-HDS database to `UcceConfig` group members.

### Procedure

In SQL Management Studio, do the following:

a) Go to **Security** > **Logins**.
b) Locate `<Machine netbios name>\UcceConfig`. Right-click and select properties.
c) Go to **User Mappings** and select one AWDB database. Ensure that GeoTelAdmin, GeoTelGroup, and public are selected.
d) Repeat step c for the HDS database.

**Note** SQL login account `<Machine netbios name>\UcceConfig` is created during CCE installation on the machine. If there is any change in the machine hostname, the SQL login account has to be deleted and re-created with the new **machine netbios name**.

## Configure Folder Permissions

Grant the required folder permissions to the `UcceConfig` group on the local machine.

### Procedure

**Step 1** In Windows Explorer, select `<ICM install directory>\icm`.
**Step 2** Right-click and select **Properties**.
**Step 3** On the **Security** tab, select `UcceConfig` and check **Allow** for the **Full Control** option.
**Step 4** Click **OK** to save the change.
**Step 5** Repeat the previous steps to grant **Full Control** to the `UcceConfig` group for `<SystemDrive>:\temp`.

### What to do next

To establish secure connection between a client and a server, use one of the following security certificates:

# Configure Cisco Unified Contact Center Enterprise

You can configure individual records, or you can use the Bulk Configuration tool to configure multiple records at one time. Bulk configuration is available for the following:

- Agents
- Call types
- Dialed number plans
- Dialed numbers
- Labels

- Network trunk groups
- Network VRU scripts
- Peripheral targets
- Persons
- Regions
- Region prefixes
- Routes
- Trunks
- Trunk groups
- Scheduled targets
- Services
- Skill groups
- VRU port maps

## Access Configuration Manager tool

You perform all Unified CCE configuration tasks using the Configuration Manager tool, which is installed with the Unified CCE software.

1. From your desktop, double-click the Unified CCE Tools icon, and then select Administration Tools.
2. Double-click the Configuration Manager icon.

## Configure Media Routing Domain

You must establish Media Routing Domains (MRD) for each media type that your Unified CCE System supports. A Voice MRD is installed by default with Unified CCE. You need to create MRDs for other media such as chat, email, and tasks. Additionally, if you are using Cisco Enterprise Chat and Email (ECE), you need to create media classes for ECE chat and email.

If you are configuring Media Routing Domains for ECE, see the *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise* for complete instructions, at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

**Important** If you are configuring a Media Routing Domain for Task Routing with third-party multichannel applications, do not use this procedure. See the *Cisco Unified Contact Center Enterprise Features Guide* for instructions, at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html.

**Procedure**

**Step 1** Start the Configuration Manager and select **Tools** > **List Tools** > **Media Routing Domain List**.

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

The Attributes tab appears.

**Step 3** On the Attributes tab, provide values for the following fields:

**Name**. Enter the enterprise name of the MRD.

**Media Class**. Use the drop-down list to select the media class for the integrated application.

**Max Time in queue**. The default maximum queue time for calls in queue is one hour. To override this default, modify the value of the Max Time In queue field.

The MR domain ID is automatically generated when you save the MRD.

**Step 4** After completing the required fields, click **Save**.

Repeat this procedure to add an MRD for each media class that your system supports.

## Configure Trunk Groups

For the Unified CCE, the *Network Trunk Group* is the placeholder in the Unified CCE database for the trunk group; it performs no other function.

For deployments that:

- Use the Unified CCE System PG, you must create one Network Trunk Group for each Unified CCE System PG peripheral.
- Do not use the Unified CCE System PG, you must create two Network Trunk Groups—one for the Unified Communications Manager and one for the Unified CVP or Unified IP IVR. If you are deploying the Unified CVP, create one Network Trunk Group per CVP Server.

A Unified CCE *Trunk Group* is a collection of trunks associated with a single peripheral and usually used for a common purpose. For the Unified CCE, the trunk groups for VRU peripherals are used primarily as a place holder in the Unified CCE database.

Create a trunk group for each Unified Communications Manager peripheral and a trunk group for each Unified IP IVR application. If you are deploying Unified CVP, you must create two trunk groups for each Unified CVP Server that match the Group Numbers configured in Unified CVP Application Administration. For Unified IP IVR, the trunk group peripheral number in the Unified CCE must match the CTI Port Group ID on Unified IP IVR.

To configure a Network Trunk Group (and the trunk group under it):

**Procedure**

**Step 1** From the Configuration Manager, choose **Configure ICM** > **Peripherals** > **Trunk Group** > **Network Trunk Group Explorer**. The ICM Network Trunk Group Explorer dialog box opens.

**Step 2** Click **Retrieve**.

**Step 3** Click **Add Network Trunk Group**. The Network Trunk Group tab opens.

**Step 4** Add a unique name for the Network Trunk Group and an appropriate description.

**Step 5** Click **Add Trunk Group** to add a trunk group.

**Step 6** Complete these fields:

**Peripheral**. Select the peripheral to which the trunk group is associated.

**Peripheral Number**. Enter the number of the trunk group as understood by the peripheral. This number must be unique among all trunk groups associated with the peripheral. For Unified IP IVR, this number must:

**a.** Match a CTI Port Group ID configured on the Unified IP IVR.

**b.** Be an odd number.

**c.** Be unique for all Unified IP IVRs handled by an Unified CCE System PG.

For example, if a Unified CCE System PG handles four Unified IP IVRs and each Unified IP IVR peripheral has one CTI Port Group, then the CTI Port Group ID for the first Unified IP IVR should be 1, the port group ID for the second Unified IP IVR should be 3, and so on. For the Unified CVP, this number must match a CVP Server Group Number configured on the CVP Server.

**Peripheral Name**. Enter the name of the trunk group as understood by the peripheral. This name must be unique among all trunk groups associated with the peripheral.

**Name**. Enter the enterprise name of the trunk group. The Unified CCE forms a default for this name using the entries from the Peripheral and Peripheral Name fields.

**Extension**. Leave this field blank.

**Trunk Count**. Select **Use Trunk Data**. When you specify **Use Trunk Data**, the system software determines the trunk count dynamically by counting the associated records in the Trunk table.

**Configuration Parameters**. Leave this field blank.

**Description**. Enter an optional description.

**Step 7** To add trunks to the trunk group, click **Add Trunk**.

**Step 8** Add trunks as desired.

**Step 9** Click **Save** and then click **Close**.

**Step 10** Repeat these steps to create all necessary trunk groups.

## Configure Network VRU Bank

The *Network VRU Bank* allows load balancing across multiple VRUs to occur and eliminates the need for complex translation-route configuration.

Configure a Network VRU Bank, only if your deployment uses the Unified CCE System PG.

### Before you begin

Do this after you configure the following:

- Network VRU
- Network Trunk Group

- All other trunk groups

**Procedure**

**Step 1** From the Configuration Manager, choose **Explorer Tools** > **Network VRU Explorer**. The Network VRU Explorer dialog box opens.

**Step 2** Click **Retrieve** and select your Network VRU.

**Step 3** Select the Network VRU Bank tab and click **Add**.

The Select Trunk Group dialog box opens, displaying the all trunk groups configured on all Unified CCE System PG peripherals.

**Step 4** Select the trunk group associated with the translation routing group on your Unified IP IVR. Make the appropriate trunk group selection for each Unified IP IVR in your deployment.

**Step 5** Click **OK**.

**Step 6** Click **Add Label** to add a label for the Network VRU Bank. The label must be the CTI Route Point trigger for the Translation-Routing application on the Unified IP IVR. By default, in the Label tab, the first field shows the selected Network VRU, *not* the Network VRU Bank:

a) Click the drop-down list box to show the available Network VRU banks.
b) Select a Network VRU bank in the drop-down list.
c) Then configure the label for the Network VRU bank.
d) Repeat the steps to configure labels for all of the Network VRU Banks.

If Network VRU Bank labels are available, the Router uses them when it balances the load between the Unified IP IVRs. If the Router cannot find an eligible Network VRU Bank labels, it uses the Network VRU label.

## Configure services

A *service* refers to a type of processing that a caller requires. For example, separate services might be defined for Sales, Support, or Accounts Payable. Services are often associated with a peripheral, and are sometimes referred to as peripheral services. An agent is assigned one or more skills that in turn is associated with services. Routing to a Unified CCE service effectively targets an agent assigned to a Unified CCE skill group associated with the Unified CCE service.

Services on the Unified CCE correspond to CTI Route Points on Unified Communications Manager.

**Note** On Unified CCE systems that interface with Unified CVP systems, you *must* configure two services with Peripheral Numbers of 1 and 2. However, outside of these services the preferred method of defining Unified CCE routable tasks is by defining call types.

For the two Unified CVP services, you do not need to configure Service Members, Routes, Peripheral Targets, or Labels.

### Procedure

**Step 1** From the Configuration Manager menu, choose **Tools** > **Explorer Tools** > **Service Explorer**. The Service Explorer dialog box opens.

**Step 2** Select the peripheral for which you want to create a service and click **Retrieve**.

**Step 3** Click **Add Service**.
The Service Configuration window opens.

**Step 4** On the Service tab, enter the following:

The **Media Routing Domain** associated with the service.

**Peripheral Number**. Enter the number for the service on the peripheral. This field must be unique for all services for the peripheral, but not necessarily across all peripherals. If you are deploying the Unified CVP, enter 1 for the first service and 2 for the second service.

**Peripheral Name**. Enter a name that describes the service.

**Enterprise Name**. Enter an enterprise name for the service. This name must be unique among all the services in the enterprise. If you do not enter a value, this name is autogenerated.

**Config Param**. Not used for the Unified CCE.

**Description**. Enter any additional information about the service.

**Service Level Type**. Indicates how the Unified CCE calculates the service level for the service. You can choose to omit abandoned calls from the calculation, treat them as having exceeded the threshold (negative impact on service level), or treat them as answered calls (positive impact on service level). You can also choose to use the default specified for the peripheral.

**Service Level Threshold**. Enter the time in seconds, for the service level. The Unified CCE tracks the percentage of calls answered within this threshold. If this field is negative, the value of the default for the peripheral is used.

**Step 5** On the Advanced tab, enter the following:

**Peripheral Service Level**. Indicates the type of service level calculation that the peripheral performs for this service. This setting has no effect because the PG does not report a peripheral service level.

**Schedule name**. Identifies an imported schedule associated with the service.

**Extension**. If you are deploying Outbound Option, enter the extension to associate with this service. This corresponds to a CTI Route Point defined in Unified Communications Manager and is associated with the PG User.

**Step 6** On the Service Members tab, select skill groups to associate with this service.

**Step 7** Click **Apply**.

**Step 8** Repeat this procedure to add any other services.

## Configure dialed numbers

The *dialed number* (DN) is the number that the caller dials to start the call and identifies the Unified CCE routing script to run. Set dialed numbers for ring no answer, dialed number plan entries, and for Supervisor/emergency calls.

For Unified Communications Manager to generate a route request to the Unified CCE, the cluster associates the DN with a CTI Route Point for the Unified CCE JTAPI User. Configure the DN in the Unified CCE. After the Unified CCE receives the route request with the DN, that DN is mapped to a Unified CCE Call type, which is then mapped to a Unified CCE routing script.

**Note** You cannot use the DN for a CTI Route Point on a different CTI Route Point in another partition. Ensure that DNs are unique across all CTI Route Points on all partitions.

Unified CCE generates a unique value for the Label Name list after you configure a dialed number.

### Procedure

**Step 1** From the Configuration Manager, choose **Tools > List Tools > Dialed Number/Script Selector List**.

The Dialed Number/Script Selector List dialog box opens.

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

The Attributes tab displays.

**Step 3** In the Attributes tab, enter values in the following fields:

**Routing client**. Choose the enterprise name of the routing client associated with this dialed number. After you select a routing client and save to the database, this field becomes read only.

**Media Routing Domain**. The media routing domain associated with the selected dialed number or script selector.

**Dialed number string**. Enter the string value that the routing client passes to the Unified CCE for this dialed number (for example: 8005551212).

**Name**. Enter the enterprise name for the dialed number. This name must be unique among all dialed numbers in the system. If you do not enter a value, the name is autogenerated.

**Customer**. Use the drop-down list to select the customer (Unified CCE instance) associated with the dialed number.

**Default label**. Choose the name of the default label for this dialed number. The label must have been previously defined for it to be in the selection list. Use the Label List tool in the Configuration Manager to define labels. If the Unified CCE fails to determine a target for the call within the routing client's time-out threshold, then the default label for the dialed number is used.

**Description**. Enter a description for the dialed number.

**Permit application routing**. If you intend to route calls from a parent system to this dialed number, check this dialog box.

**Reserved by IVR**. For VRU dialed numbers, check this box. This setting prevents the CallManager PIM from trying to exert control on the calls arriving on these Route Points.

**Step 4** On the DN Mapping tab, as desired, click **Add** to specify a call type and other dialing information to associate with this dialed number.

**Step 5** Click **Save** to enter the dialed number information.

**Step 6** Repeat this procedure for any additional dialed numbers.

## Configure call types

A *call type* is a category of Unified CCE routable task. Each call type has a schedule that determines which routing script or scripts are active for that call type at any time.

There are two classes of call types:

- Voice (phone calls). Voice call types are categorized by the dialed number (DN), caller-entered digits (CED), and calling line ID (CLID). The CED and CLID can be optional, depending on the call.
- Non-voice (email and text chat). Non-voice call types are categorized by the Script Type Selector, Application String 1, and Application String 2. Application String 1 and Application String 2 can be optional, depending on the application.

To facilitate Unified CCE reporting, it is good practice to create separate call types for VRU applications and queuing applications.

### Procedure

**Step 1** From the Configuration Manager, select **Tools** > **List Tools** > **Call Type List**.

The Call Type List dialog box opens.

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

The Attributes tab appears.

**Step 3** In the Attributes tab, enter values for the following fields:

**Name**. Enter an enterprise name for the call type. This name must be unique among call types in the system.

**Customer**. Choose the customer (Unified CCE Instance) from the drop-down list.

**Service level threshold**. The service level threshold is the target maximum time that a caller spends in a queue before being connected to an agent. When you set up a peripheral, you specify a default service level threshold for all services associated with that peripheral. If you enter a negative number, the service level threshold from the Peripheral table is used.

This field is prepopulated with the default service level threshold for this peripheral and grayed out. If you wish to override this default, check the **Override System Information Default** check box to the right of this field and enter a different value.

You can also set the Service Level in the Configuration Manager with the System Information tool. When the service level is defined with the Call Type tool, this setting overrides a setting made with the System Information tool. If service level is not defined with the Call Type tool, but is defined with the System Information tool, the Unified CCE uses the System Information setting.

**Service level type**. Indicates how the system software calculates the service level for the service. The default is the level specified for the associated peripheral. To set a different level type, check the **Override System Information Default** check box and select the type you want from the selection box.

**Bucket Intervals**. Indicates the Bucket Intervals setting for the call type. Bucket intervals are defined with the Bucket Intervals List tool. If you wish to override the defined default, check the **Override System Information Default** check box and select a different Bucket Intervals setting.

**Description**. Enter an optional description of the call type.

**Step 4** Click **Save** to enter the call type information.

Repeat this procedure to add additional call types.

## Configure Variables

### Configure Expanded Call Context Variables

Expanded Call Context (ECC) variables are variables that you define and enable in the Configuration Manager to store values for a call. You can specify the variable name and data type. The name must begin with the string "user." ECC variables are in addition to the variables the system software defines for each call (PeripheralVariable1 through PeripheralVariable10, CallerEnteredDigits, CallingLineID, and so on).

An ECC variable name can be up to 33 bytes long (1–32 usable characters). Use the following naming convention when creating an ECC variable:

user.<CompanyName>.<VariableDescription>

In this syntax:

- **<CompanyName>** is the name of your company.
- **<VariableDescription>** is a descriptive tag for the variable.

For example:

```
user.Cisco.AcctNum
```

Using this naming convention prevents naming conflicts with any third-party applications that interface with the system software.

**Note** For a large corporation, you can break **<VariableDescription>** down to include the Business Unit, Division, or other organizational entities.

ECC variables follow these size rules:

- An ECC variable can be either a scalar variable or an array element, each with a maximum length of 210 bytes.

**Note** Array types are not supported for an agent request.

- The maximum number of elements in an array is 255.
- The maximum buffer size for each scalar variable = 5 + the maximum variable length. The 5 bytes includes 4 bytes to tag the variable and 1 byte for the null terminator.

- The maximum buffer size for each array = 5 + (1 + the maximum length of an array element) * (the maximum elements in the array). There is a null terminator for each element, and a null terminator for the array as a whole.
- You pass ECC variables in an ECC payload which has a 2000-byte limit. The total sum of all the maximum buffer sizes for each variable and each array in one ECC payload cannot exceed 2000 bytes.

  For example, if you intended to use the following:

  - A scalar ECC variable with a maximum length of 100 bytes
  - A scalar ECC variable with a maximum length of 80 bytes
  - An ECC array with a maximum of 9 elements with each element having a maximum length of 200 bytes

  Totaled the buffer size is: (5+100) + (5+80) + (5 + (1+200)*9) = 2004. Because this size is too large, you must change the length of one of the scalar ECC variables or the length of the array ECC variables.

For Web Callback and Delayed Callback to work properly, an ECC variable (also known as a named variable) must be defined. The Cisco CTI driver supports the use of ECC variables in addition to the standard call variables associated with a call. Before an ECC variable can be used, it must be defined in the Unified CCE ECC variable database table.

### *ECC Variables for Voice MRDs with Collaboration*

ECC variables must be configured in Configuration Manager's Expanded Call Variable List tool (for each integrated application) to route requests using the voice Media Routing Domain.

For Voice MRDs with Collaboration, the ECC variables are:

- user.ewm.activity.id
- user.ewm.customer.name

### *Validate ECC Variable Size for CTI Server*

Before configuring ECC variables, validate the total size of the ECC variables against the following rules and limits:

- Because the total size of the buffer used to store the variables in CTI Server internally is 2500 bytes, the total sum of all the maximum buffer sizes for each scalar variable and arrays must be no greater than 2500.
- The maximum buffer size for each scalar variable = 4 + length of the ECC name + the maximum length of the variable where the 4 bytes includes a 1 byte tag, 1 byte to define the length, and 2 terminating NULL characters.
- The maximum buffer size for each array = (5 + length of the ECC name + the maximum length of array element) * (the maximum number of elements in the array) where the 5 bytes includes a 1 byte tag, 1 byte to define the length, 1 byte for the array index, and 2 terminating NULL characters.
- For example, if you intend to use one scalar ECC variable with a maximum length of 100 bytes named *user.var*, one scalar ECC variable with a maximum length of 80 bytes named *user.vartwo*, and an ECC array named *user.varthree* with a maximum of 9 elements with each element having a maximum length of 200 bytes, the buffer size would be:

(4+8+100) + (4+11+80) + ((5 + 13 + 200)*9)) = 2169

where 8 is the length of *user.var*, 11 is the length of *user.vartwo* and 13 is the length of *user.varthree*.

### *Enable ECC Variables*

**Procedure**

**Step 1** Within the Configuration Manager, double-click **Tools** > **Miscellaneous Tools** > **System Information**.

The System Information window appears.

**Step 2** Select the **Expanded call context enabled** check box.

For additional information, refer to the online Help.

**Step 3** Click **Save** to apply your changes.

### *Define ECC Variables*

**Procedure**

**Step 1** Within the Configuration Manager, double-click **Tools** > **List Tools** > **Expanded Call Variable List**.

The **Expanded Call Variable List** window appears.

**Step 2** Click **Retrieve** to enable adding ECC variables.

**Step 3** Click **Add**.

The **Attributes** property tab appears.

**Step 4** Complete the **Attributes** property tab. See the *List Tools Online Help* for details on the **Attributes** property tab.

**Step 5** Click **Save** to apply your changes.

#### What to do next

If you change the configuration of any ECC variable with the **Expanded Call Variable List** tool, restart the Unified CVP Call Server or VRU PIM to force a renegotiation of the ECC variables.

Before you can use the new ECC variable, you must add it to an ECC payload.

**Note** If your solution only has a Default payload, the solution automatically adds any new ECC variables to the Default payload until it reaches the 2000-byte limit.

### *Define ECC Payloads*

You can create and modify ECC payloads in the **Expanded Call Variable Payload List** tool.

**Note** The tool checks that the ECC payload does not exceed the 2000-byte limit only when you save your changes. The counters on the **Members** tab only show what the current size is with all the selected members. They are only informational and do not enforce the limit. The limit is enforced when you attempt to save the changes.

To define an ECC payload, you create the ECC payload and then add its members.

### Procedure

**Step 1** In the Configuration Manager, open **Tools** > **List Tools** > **Expanded Call Variable Payload List**.

The **ECC Payload List** window appears.

**Step 2** Click **Retrieve** to enable adding ECC payloads.

**Step 3** Click **Add**.

The **Attributes** property tab appears.

**Step 4** Complete the **Attributes** property tab. See the *List Tools Online Help* for details on the **Attributes** property tab.

**Step 5** On the **Members** tab, click **Add**.

A dialog box listing all the existing ECC variables appears.

**Step 6** Select the members for your ECC payload and click **OK**.

Watch that the **ECC Variable Size** counter does not exceed 2000 bytes. For ECC payloads that go to CTI clients, watch that the **CTI Message Size** counter does not exceed 2500 bytes.

**Step 7** Click **Save** to apply your changes.

## Configure User Variables

You can also create global user variables; for example, you can create a user variable called usertemp to serve as a temporary storage area for a string value used by an If node.

After you have defined a user variable, you can then use the Script Editor Formula Editor to access the variable and reference it in expressions, just as you would with a “built-in” variable.

Each user variable must:

- Have a name that begins with **user**.

**Note** This name cannot contain the dot/period (.) character.

- Be associated with an object type, for example, Service. (This enables the system software to maintain an instance of that variable for each object of that type in the system.)
- Be checked as persistent. A persistent variable maintians its value between script invocations. This allows you to set the variable in one script and reference later in another script.

**Note** Because these variables may be persisted, do not use User Variables to store sensitive information belonging to the customer or company. Using these variables to store confidential information could lead to violation of security standards, such as PCI, the Common Criteria, HIPAA, or FIPS 140-2.

A user variable can store a value up to 40 characters long.

*Define User Variables*

**Procedure**

**Step 1** Within the Configuration Manager, select **Tools** > **List Tools** > **User Variable List**.

The User Variable List window appears.

**Step 2** In the User Variable List window, click **Retrieve** to enable Add.

**Step 3** Click **Add**.

The Attributes property tab appears.

**Step 4** Complete the Attributes property tab.

**Note** The **Variable name**, **Object type**, and **Data type** fields are required. All other fields are optional. For additional information refer to the online Help.

**Step 5** Click **Save** to apply your changes.

# Configure Users

## Create Person records

All Unified CCE agents must have a *Person* record. When you create an Agent record, you can associate the record with an existing Person record. If you do not associate the Agent record with an existing Person record, a new Person record is automatically created when you create the agent.

To configure a Person record before configuring an agent, complete the following steps:

**Procedure**

**Step 1** From the Configuration Manager, choose **Peripherals** > **Person** > **Person List**.
The Person List dialog box opens.

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

**Step 3** in the Attributes tab, enter information in the following fields:

**First Name**. Enter the person's first name.

**Last Name**. Enter the person's last name.

**Login Name**. Enter the person's login name.

**Password**. Enter a password for the person.

**Enable Logins**. Check this check box.

**Step 4** Click **Save** and then click **Close**.

**Step 5** Repeat this procedure to add additional Person records.

## Associate agents with peripherals

### Procedure

**Step 1** Select **Tools** > **Explorer Tools** > **Agent Explorer**.
The Agent Explorer dialog box displays.

**Step 2** Select the peripheral you want associated with the agent from the drop-down list and click **Retrieve**.

**Step 3** Click **Add Agent** to display the Agent configuration tab.

**Step 4** In the Agent tab, enter information in the following fields:

**Last Name**. Enter the agent's last name.

**First Name**. Enter the agent's first name.

**Login Name**. Enter the name the agent uses to login. This name must be unique in the enterprise.

**Password**. Enter the agent's password. This password is validated during the agent login process.

**Login Enabled**. Check this check box if you want the enable the agent to login.

**Select Person**. Click this button to select a person to associate with the agent record. You can select a person for a new agent, an existing agent, or a temporary agent.

**Enterprise Name**. Enter an enterprise name for the agent that is unique within the enterprise. The default is a combination of the peripheral name with the agent's first and last name.

**Peripheral Name**. Enter a name for the agent as known to the peripheral.

**Peripheral Number**. Enter the agent's login ID. This number identifies the agent to the peripheral. This number needs to be unique among all agents for the peripheral, but does not need to be unique across all peripherals. Agent IDs can be up to eleven digits long. The first digit in the ID must be 1 through 9. It cannot be 0. Also, this number cannot be the same as the extensions on the Unified Communications Manager cluster for this agent. Finally, the ID can not exceed the extension length specified in the Unified Communications Manager Peripheral Gateway Setup

**Step 5** Click the Advanced tab and enter information in the following fields:

**Desk Setting**. Use the drop-down list to select the desktop settings to be associated with the agent. If you do not make a selection, the Unified CCE applies the default desk settings defined for the peripheral.

**ConfigParam**. Use this field to enter any specific configuration parameters that may be required. Make entries in this field only if instructed to do so by your Cisco support representative.

**Description**. Enter any other information you want about the agent.

**Agent State Trace**. Select to enable the agent's state trace control. When enabled, the Unified CCE records every state transition made by the agent.

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

**Step 7** Repeat this procedure to configure additional agents.

## Assign Agent Desk Settings

Agent Desk Settings associate a set of permissions or characteristics with specific agents. The settings are comparable to Class of Service settings on a PBX or ACD. Desk settings are associated with an agent when you configure the agent. The desk settings are global in scope and you can apply them to any configured agent on any peripheral within a Unified CCE configuration.

Agent Desk Settings provide a profile that specifies parameters such as whether auto-answer is enabled, how long to wait before rerouting a call for Ring No Answer, what DN to use in the rerouting, and whether reason codes are needed for logging out and going not-ready. You must associate each agent with an agent desk setting profile in the Unified CCE configuration. A single agent desk setting profile can be shared by many agents. Changes made to an agent's desk setting profile while the agent is logged in are not activated until the agent logs out and logs in again.

If Agent Desk Settings are not associated with an agent, the agent is assigned the peripheral default settings, which depend on the peripheral to which the agent is assigned.

When you configure Agent Desk Settings, you specify the amount of non-active time after which an agent is automatically logged out, whether wrap up is required following incoming and outbound calls, the amount of time allocated for wrap up, and the method used for assist and emergency calls. You also specify settings for the Ring No Answer feature.

### *Ring No Answer*

The Ring No Answer feature, configured in Agent Desk Settings, ensures that when an agent does not answer a call, the call is taken away from the agent after a specified number of seconds and re-assigned to another agent or requeued.

When a call is routed to an agent but the agent fails to answer the call within a configurable amount of time, the Unified Communications Manager PIM for the agent who did not answer changes that agent's state to not ready (so that the agent does not get more calls) and launches a route request to find another agent. Any call data is preserved and popped onto the next agent's desktop. If no agent is available, the call can be sent back to the Unified IP IVR for queuing treatment again. Again, all call data is preserved. The routing script for this RONA treatment should set the call priority to “high” so that the next available agent is selected for this caller. In the agent desk settings, you can set the RONA timer and the DN used to specify a unique call type and routing script for RONA treatment.

This feature behaves and is configured differently depending on whether you deploy the Unified CVP or Unified IP IVR in the Unified CCE System.

**Note** The Dialed Number for Ring No Answer is peripheral-specific. Therefore, each Unified Communications Manager PG in your deployment must have its own set of Agent Desk Settings configured for it; you cannot use a particular desk setting across peripherals.

### About Ring No Answer with Unified IP IVR

For Unified CCE systems in which you deploy the Unified IP IVR, the Ring No Answer feature ensures that when an agent does not answer a call the following applies:

- The call is taken away from that agent after ringing for a configurable number of seconds and is rerouted to a different agent or placed in queue.
- The state of the agent who did not answer the call is changed to “Not Ready.”

Reroute a call on Ring No Answer works as follows for Unified IP IVR:

1. A routing script connects the call to an agent.
2. If the agent does not answer the phone within the Ring No Answer time set in Agent Desk Settings, the Unified Communications Manager changes the agent's state to “Not Ready” and post routes the call to Unified CCE.
3. The Unified CCE Router runs a routing script using the dialed number specified in the agent desk setting record. The routing script associated with the DN typically looks for another agent and routes the call to that new agent.
4. If no agents are available, the call typically is translation routed or queued to the VRU, or sent to some other queue point. Queuing treatment is restarted.

**Note** Give the call the highest priority in the queue so that the call is routed to the next available agent.

5. Any call data is preserved to be popped onto the agent screen. In addition, a flag is set in the database so that Unified CCE can report on all of the occurrences of Ring No Answer.

### About Ring No Answer with Unified CVP

For Unified CCE systems in which you deploy the Unified CVP, the Unified Communications Manager does not control the Unified CVP and cannot send an unanswered call back to the Unified CVP for re-queuing. You configure the Ring No Answer feature to only make the agent “Not Ready” when they do not answer a call, and use the Unified CVP Router Requery feature to re-queue the call.

As of Release 9.0, the Unified CVP deployment no longer requires that you configure the RNA timer on both sides (Unified CVP and Unified CCE); configure Ring No Answer (RNA) timeout only in Unified CVP. This removes the requirement to manually align the relevant Unified CVP and Unified CCE timer configuration. To configure RNA timeout in Unified CVP, see the **Patterns for RNA timeout on outbound SIP calls** section in the Unified CVP OAMP console.

Reroute a call on Ring No Answer works as follows for Unified CVP:

1. A routing script connects the call to an agent by sending a connect message to the Unified CVP. The script node should have Enable Target Requery enabled. To enable this, edit the node, select **Change** and check the **Enable Target Requery** check box.
2. The agent's phone rings.
3. If the phone is not answered (either via the agent desktop or physically going off-hook) within the Ring No Answer time set in Agent Desk Settings, Unified CCE makes the agent unavailable, but does not actually change the agent state to Not Ready until the call is redirected.

4. When the Unified CVP Ring No Answer timeout expires, the Unified CVP sends an EventReport=No Answer message to the Router instructing it to select another target according to the routing script and send a Connect message to Unified CVP. The target might be another agent or a VRU label to requeue the call.

**Note** Give the call the highest priority in the queue so that the call is routed to the next available agent.

5. Any call data is preserved to be popped onto the second agent screen.

**Note** In addition, a flag is set in the database so that Unified CCE can report on all of the occurrences of Ring No Answer.

6. When the call is redirected from the original agent, the agent's state changes to “Not Ready.”

## *Configure Agent Desk Settings*

### Procedure

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Designate Agent Supervisor

You can identify an agent as a supervisor.

If you define an agent as a supervisor:

- If single sign-on is *disabled* either globally or for the agent you want to designate as a supervisor, the supervisor must have an Active Directory account. If the supervisor does not have an Active Directory account, the designation fails.
- If single sign-on is *enabled* either globally or for the agent you want to designate as a supervisor, you must enter the individual's name in the format that your identity provider requires.

To create an agent who is a supervisor:

### Procedure

**Step 1** In the Configuration Manager menu, select **Tools** > **Explorer Tools** > **Agent Explorer**. The Agent Explorer window appears.

**Step 2** In the **Select filter data** box, select the peripheral with which the agent is to associated and click **Retrieve**. This enables the **Add Agent** button.

**Step 3** Click **Add Agent**.

**Note** You must add the agent supervisor, as both member and supervisor, to the **Member** tab on the agent team list. To get the benefit from the Team layout in Finesse, the agent supervisor must be a member of the team.

**Step 4** In the property tabs on the right side of the window, enter the appropriate property values. Use the Agent Tab to define the agent and designate the agent as a supervisor. Use the Skill Group Membership Tab to map the agent to any skill groups. (See the Configuration Manager online help for more information.)

**Note** An agent team can have only one primary supervisor. There is no upper limit to the number of secondary supervisors for a team. Refer to the online help for instructions on how to assign a primary supervisor.

**Step 5** When finished, click **Save**.

## Create agent teams

You can group individual agents into agent teams that supervisors can manage. Agent teams are assigned to specific peripherals, so you must assign all agents of a given team to the same peripheral. You assign agents individually to agent teams.

When configuring agent teams, be aware of the following rules:

- An agent can be a member of only one agent team.
- An agent team can have only one Primary Supervisor.
- A supervisor can be a supervisor of any number of agent teams.
- A supervisor for an agent team can also be a member of that agent team.
- All agents belonging to an agent team and all supervisors for that agent team must be on the same peripheral.

For more information on team limits, see the appendix on system requirements in the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

### Procedure

**Step 1** From the Configuration Manager, select **Configure ICM** > **Peripherals** > **Agent Team** > **Agent Team List**.

**Step 2** Click **Retrieve** and then **Add** to add a new agent team.

**Step 3** Click the **Attributes** tab and enter values in the following fields:

**Name**. Enter an enterprise name for the agent team that is unique within the enterprise.

**Peripheral**: Enter the name of the agent team peripheral. You can select the name from the drop-down list.

**Supervisor Script Dialed Number**: Select a dialed number for the agent team from the drop-down list. If you have not created a supervisor script, select the default, “none”. When you create the script, return to this screen and enter the dialed number for the script.

**Description**: Enter additional information about the agent team.

**Step 4** Click the **Members** tab and click **Add**.

**Step 5** Choose the agents that you to assign to the team and click **OK**.

**Step 6** Click the **Supervisor** tab and choose the supervisor from the Primary Supervisor drop-down list.

**Step 7** To add a secondary supervisor, click the **Add** button and select a secondary supervisor from the list. Click **OK**.

**Step 8** Click **Save** and then click **Close**.

## Configure Network VRUs

Use the Configuration Manager tool to configure Network VRUs.

After you configure a Network VRU and VRU scripts, you can use the Script Editor to write a routing script to send a call to the VRU and invoke a specific VRU script.

See *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_user_guide_list.html for more information.

### Create Network VRU Target

#### Procedure

**Step 1** Within the Configuration Manager, select **Tools** > **Explorer Tools** > **Network VRU Explorer**.

The Network VRU Explorer window appears.

**Step 2** In the Network VRU Explorer window, click **Retrieve** to enable **Add Network VRU** .

**Step 3** Click **Add Network VRU**.

The Network VRU property tab appears.

**Step 4** Complete the Network VRU property tab.

The Name and Type fields are required. All other fields are optional.

The ECC Payload field provides the name of the ECC payload that has scope for interactions with this network VRU. For additional information refer to the Online Help.

**Step 5** Click **Save** to apply your changes.

### Define Network VRU Label

You must associate all VRU Types (except Type 6) with a Network VRU label.

**Procedure**

**Step 1** In the Network VRU Explorer window, click **Retrieve** and select the Network VRU you want to add the label to.

The Label property tab appears.

**Step 2** Complete the Label property tab.

The **Routing client**, **Label**, and **Label type** fields are required. All other fields are optional. For additional information refer to the online Help.

**Step 3** Click **Save** to apply your changes.

### Set Default Network VRU and Range of Correlation Numbers

For Network VRUs, you must use the System Information dialog to define a range of correlation IDs so the system software can communicate with the VRU about the call.

**Procedure**

**Step 1** Within the Configuration Manager, select **Tools** > **Miscellaneous Tools** > **System Information**.

The System Information window appears.

**Step 2** In the System Information window, select the **Default Network VRU**.

**Step 3** Enter the **Minimum Correlation Number**.

**Step 4** Enter the **Maximum Correlation Number**.

For additional information refer to the online help.

**Step 5** Click **Save** to apply your changes.

## Configure scripts

### Network VRU scripts

*VRU scripts* differ from routing scripts. A configured VRU script runs only when the Unified CCE instructs it to do so from a routing script. A VRU script on the Unified CCE is the configured record for the VRU script that resides on the VRU system. A VRU script runs to collect digits, play hold music, or perform many other common functions.

After you configure the VRU scripts, you can use the Script Editor to write a routing script to send a call to the VRU and invoke a specific VRU script.

For deployments that include the Unified CVP, use the Translation Route to VRU node to send calls to the Network VRU and invoke VRU scripts. Do not use Translation Route to VRU node for deployments that use the Unified CCE System PG. Instead, use any one of Queue to Skill Group or Send to VRU nodes.

### Routing and administrative scripts

A *routing script* processes call routing requests from a routing client. Typically it examines several targets and applies selection rules to find an available qualified agent or a target with the shortest expected delay. You can set up different routing scripts to run for different types of tasks. You can define call types in terms of the telephone number the caller dialed, the number the caller is calling from, and additional digits entered by the caller. For each call type, you can schedule different routing scripts to run on different days or at different times of the day.

An *administrative script* runs periodically to perform a task, such as setting variables.

## Configure Network VRU scripts

### Procedure

**Step 1** From the Configuration Manager, select **Tools > List Tools > Network VRU Script List**.

The Network VRU Script List dialog box opens.

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

**Step 3** On the Attributes tab, enter the configuration information for the VRU script as follows:

**Network VRU**. Specify the Network VRU with which this script should be associated.

**VRU Script Name**. Enter script name; for example, BasicQ.

**Name**. Enter the script file name; for example, BasicQ.aef

**Timeout [seconds]**. Enter 180.

**Configuration param**. Leave blank.

**Customer**. Choose the same Unified CCE customer you chose for call type from the drop-down list.

**Step 4** Check the **Interruptible** check box.

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

## Troubleshoot Network VRU scripts

If a timeout occurs on a VRU script, it is possible that the Router does not notify the VRU PIM that a timeout has occurred. Because the VRU PIM is not informed of the problem, it does not notify the VRU to cancel the script.

At this point, the options for script flow include the following:

- The failure path in the Router script sends the call to a label, the VRU PIM gets a Connect and, if the VRU supports it, generates a Cancel message. This is the most common result.
- Before the Router picks a label, the VRU script completes and the VRU sends a Script Result message to the Router. The Router then sends a Dialogue Failure Event because it is not expecting a Script Result. This is the next most common result.
- The failure path in the Router script tries to run another VRU script. This is not a common result.

Currently, the best resolution to this problem is to use longer time-outs or create shorter VRU scripts. Be aware that the failure exit from the Run VRU Script node is a problem that you may need to resolve.

### *VRU error checking*

A special call variable VruStatus, allows you to check the result of the last VRU node (Send To VRU/Translation Route to VRU/Run VRU Script) that the Unified CCE processed. The following table lists the values for this variable.

| Value | Meaning | Description |
|---|---|---|
| 0 | VRU_SUCCESS | The last VRU node was successful. |
| 1 | VRU_ERROR | The last VRU node failed because of a routing or configuration error. |
| 2 | VRU_TIMEOUT | The last Send To VRU or Translation Route to VRU node failed because the routing client did not respond within 20 seconds or the last Run VRU Script node failed because the timeout limit defined for the script expired. |
| 3 | VRU_ABORTED | The last VRU node did not complete because the caller ended the call or was otherwise lost. (Because this causes the routing script to terminate immediately, this value is never seen.) |
| 4 | VRU_DIALOG_FAILED | The last VRU node failed because communication with the VRU ended unexpectedly. |
| 5 | VRU_SCRIPT_NOT_FOUND | The VRU failed because the referenced VRU script was not found in the Unified CCE configuration. |

## Configure routing and administrative scripts

After you complete your Unified CCE configuration, you can write routing scripts and administrative scripts. You create, maintain, and monitor these scripts using the Script Editor.

| For Information about | See |
|---|---|
| Creating Unified CCE scripts | *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_installation_and_configuration_guides_list.html |
| Designing scripts for Unified CCE using the Script Editor | *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_user_guide_list.html |
| Planning scripts for your Unified CCE reporting needs | *Cisco Unified Contact Center Enterprise Reporting User Guide* at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_user_guide_list.html |
| Creating scripts for Outbound Option | *Outbound Option Guide for Unified Contact Center Enterprise* at http://www.cisco.com/en/US/products/sw/custcosw/ps524/prod_installation_guides_list.html |

# Configure Agent Targeting Rules

The Agent Targeting Rules (ATR) configures call routing by specifying the agent extension range, instead of configuring Device Targets and Labels for every phone/Routing Client. This simplifies the call routing configuration for the Agent PGs. Also, this feature reduces the amount of memory used by the Router because a large number of Device Targets and Labels are replaced by a few rules. ATRs are therefore, the preferred method for installation.

### Before you begin

You must configure the PGs and routing clients before you configure the Agent Targeting Rules.

### Procedure

**Step 1** From the Configuration Manager, choose one of the following:

- **Configure ICM** > **Targets** > **Device Target** > **Agent Targeting Rule**.
- **Tools** > **List Tools** > **Agent Targeting Rule**.

The ICM Agent Targeting Rules dialog box opens.

**Step 2** Click **Retrieve**.

**Step 3** Click **Add**.

**Step 4** Enter a name for the rule.

**Step 5** Select a peripheral where the rule will be associated.

**Step 6** Select the rule type:

- Agent Extension
- Substitute Agent Extension: Enter the agent extension prefix and agent extension length.
- Translation Route: Select a Translation Route.

  For the Translation Route option, you must also configure the Translation Route DAIS as dialed numbers associated with the target agent's peripheral routing client in Unified CCE. You must map the dialed numbers to the route points that are configured in Unified Communications Manager and associated with the JTAPI user. This is necessary to complete the Translation Route Rule.

**Step 7** Select one or more routing clients that can initiate the route request.

**Step 8** Enter the agent's extension range.

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

**Step 10** Test the rule configuration by routing calls from each routing client to each agent extension you defined. If you defined a range, simplify the test by testing the lower and the upper limits of the agent extension, and a sampling of the extensions in between the range limits.

# Configure translation routes

Use the Translation Route wizard to configure the translation routes for the Unified Communications Manager and VRU peripherals. This wizard automates the correct associations with peripheral targets, labels, and routes.

**Note** Run the Translation Route Wizard only if your Unified CCE solution uses Unified CVP.

### Procedure

**Step 1** In the Configuration Manager, select **Tools** > **Wizards** > **Translation Route Wizard**.

The Translation Route Wizard introductory dialog box opens.

**Step 2** Click **Next**.

The Acquire Lock and Select Configuration Task dialog box opens.

**Step 3** Select **Create New**.

**Step 4** Click **Next**.

The Define Translation Route dialog box opens. The graphic on the left of the dialog box shows the entities you are defining while using the Translation Route Wizard.

**Step 5** Enter a long and short name for the translation route and, optionally, a description (the short name is used in forming target names).

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

The Select Configuration dialog box opens.

**Step 7** Choose the single peripheral, single routing client configuration from the drop-down list.

The graphic changes to show the configuration you select.

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

The Select Peripheral Gateway, Peripherals, and Services dialog box opens.

**Step 9** Enter values for the following fields:

**Peripheral Gateway**. Choose the gateway target for the translation route.

**Peripheral**. Choose the single peripheral or the peripheral to route calls to.

**Service/Service Array**. If the translation route is associated with a single peripheral, choose the service associated with the translation route. If the translation route is associated with multiple VRUs, then select a service array.

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

The Select Routing Clients and Dialed Numbers dialog box opens. Use this dialog box to specify the Unified Communications Manager peripheral (or VRU peripheral) as the routing client from which translation routed calls originate. For the Unified CCE the dialed number string is not applicable.

**Step 11** Click **Next**.

The Select Network Trunk Groups for Routing Clients dialog box opens. Choose at least one network trunk group to be used in peripheral targets associated with the translation route.

**Step 12** Choose a routing client, select a network trunk group value for it, and click **Add**.

The Network Trunk Group appears in the list at the bottom of the dialog box.

**Step 13** Click **Next**.

The Configure DAIS dialog box opens.

**Step 14** Use this dialog box to specify the DAIS values that map to route points on the VRU. Do one of the following:

- To enter a specific DAIS value, click **Add DAIS** and enter the value.
- To add a range of DAIS values, typically required by a translation route, click **Add DAIS Range**.

A dialog box prompts you to enter a starting and ending DAIS value. The Translation Route Wizard automatically generates the DAIS values in the range.

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

The Configure Label dialog box appears.

**Step 16** Use this dialog box to define a label that maps to the DAIS/CTI route points. A label consists of a prefix and a suffix. Each DAIS value requires a unique label. Do one of the following:

- Enter prefixes and suffixes individually.
- Use the buttons in this dialog box to set a range of values or to base the prefix or suffix values on the DAIS values.

**Step 17** Click **Next**.

The Wizard Complete dialog box opens.

**Step 18** Click **Create Translation Route** to create the translation route and its associated entities.

First, the Translation Route Wizard displays a success message and then the dialog box appears.

**Step 19** Do one of the following:

- To see details about the translation route you just created, click **Run Report**.
- To return to the beginning of the Translation Route Wizard and perform a new task, select **Start New Task** and click **Finish**.
- To exit the Translation Route Wizard, click **Finish**.

**Note** You can also use the Translation Route Explorer to create a translation route or to modify a translation route that you created with the Translation Route Wizard. Select **Configuration Manager** > **Tools** > **Explorer Tools** > **Translation Route Explorer**.

## Configure Skill Groups or Precision Routing

Skill groups are collections of agents that share a common set of skills. Skill groups are associated with a peripheral and are members of Services. You can associate agents with one or more skill groups.

To configure skill groups, you create skill groups, add the skill groups to services as members, and assign agents to one or more skill groups.

Precision routing offers an 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 precise needs of the caller.

To configure precision routing, you create attributes, assign attributes to agents, create precision queues, and create routing scripts.

## Configure Skill Groups

### *Add skill groups*

You configure skill groups to group agents with similar skills. You can associate agents with one or more skill groups. Skill groups are associated with a specific Unified Communications Manager PIM. You can group skill groups from multiple PIMs into Enterprise Skill Groups. You can direct calls to (routed to) Enterprise Skill Groups to share the load across multiple call centers or Unified Communications Manager installations. You can do reporting on Enterprise Skill Groups.

Agents are assigned one or more skills by associating the agent with the desired skill group.

After you create services and skill groups, you associate one or more skill groups with a service by making them members of that service.

A default skill group is created automatically when you create system PGs. The default skill group acts as a bucket to capture information about calls not routed by Unified CCE. (A call placed directly to an agent extension is an example of such a scenario.) If you deploy multichannel applications in your Unified CCE system, default skill groups are created for each Media Routing Domain that you configure.

**Note** An agent must be assigned to at least one skill group to log in.

#### Procedure

**Step 1** From the Configuration Manager, select **Configure ICM** > **Peripherals** > **Skill Group** > **Skill Group Explorer**.
The Skill Group Explorer dialog box opens.

**Step 2** In the Select filter data section, select the peripheral from the drop-down list:

**Step 3** Click **Retrieve** and then click **Add Skill group** to add a new skill group for the selected peripheral.

**Step 4** Click the **Skill Group** tab and enter values for the following:

**Media Routing Domain**. Use Cisco_Voice for agents that do not use other media. For more information, see the *Enterprise Chat and Email Installation Guide (for Unified Contact Center Enterprise)* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html.

**Peripheral Number**. Enter the skill group number as known by the peripheral. This value must be unique among all skill groups for the peripheral, but does not need to be unique across peripherals.

**Peripheral Name**. Enter the local name for the skill group. This value must be unique among all skill groups for the peripheral, but does not need to be unique across peripherals.

**Name**. The Configuration Manager generates the value for this field. This value is a unique name for the skill group made up of a default value from the peripheral enterprise name and the skill group peripheral name.

**Available Holdoff Delay**. For the Unified CCE peripheral type, set this field to 0.

**Priority**. This field is read-only and defaults to 0.

**Extension**. Leave blank for the Unified CCE peripheral type.

**ICM picks the agent**. Check this check box.

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

**Step 6** Repeat this procedure for any additional skill groups.

*Assign skill groups as service members*

To make a skill group a member of a service, you establish mappings of skill groups to services. Each skill group can be mapped to zero, one, or more services. Each service can have zero, one, or more skill group members.

**Procedure**

**Step 1** From the Configuration Manager, choose **Configure ICM** > **Peripherals** > **Service** > **Service Explorer**. The Service Explorer dialog box opens.

**Step 2** Click **Retrieve**.

**Step 3** Click the service that directs the skill group and then click the **Service Members** tab.

**Step 4** On the Service Members tab, click **Add** to associate a skill group with the service.

**Step 5** Click **OK**.

**Step 6** Click **Save** and then click **Close**.

**Step 7** Repeat this procedure for each skill group you want to associate with a service.

*Assign agents to skill groups*

Agents must be assigned to at least one skill group in order to log in. You can assign agents to the most appropriate skill groups according to their talents and skills to ensure that the most appropriate agent for a request responds to the customer.

**Procedure**

**Step 1** From the Agent Explorer dialog box, choose the **Skill Group Membership** tab.

**Step 2** From the Skill group name list, select the skill groups to which you want this agent assigned.

**Step 3** Click **Add**.
The Add Skill Group Membership box opens, showing the skill groups to which the agent has been assigned.

**Step 4** Click **OK**.

**Step 5** Click **Save** and then click **Close** on the Agent Explorer dialog box.

**Step 6** Repeat this procedure to assign additional agents to skill groups.

**Note** You can remove agents from the Skill Group tab if necessary by selecting the agent and clicking **Remove**, then **Save**.

## Configure Precision Routing

To configure precision routing, use the Unified CCE Web Administration application, which links to various precision routing gadgets. To access the application, click the **CCE Web Administration** shortcut on your desktop, or copy the following URL into your browser: **https://distributor ip/cceadmin**.

For more information on precision routing, see the *Cisco Unified Contact Center Enterprise Features Guide* at https://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_feature_guides_list.html

### Add Attributes

#### Procedure

**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 *mortgage*. |
| **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

### Procedure

**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.

a) Click the attributes you want to add for this agent.
b) Set the attribute value as appropriate for this agent.

## Add Precision Queue

### Procedure

**Step 1** Navigate to **Unified CCE Administration** > **Organization** > **Skills** > **Precision Queues**.

This opens a **List of Precision Queues** window showing all precision queues that are currently configured.

**Step 2** Click **New** to open the **New Precision Queue** window. Complete the fields.

| Name | Required | Description |
|---|---|---|
| **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 *Cisco_Voice*. |

| Name | Required | Description |
|---|---|---|
| **Service Level Type** | yes | Select the service level type used for reporting on your service level agreement.<br><br>Service level type indicates how calls that are abandoned before the service level threshold affect the service level calculation.<br><br>• **Ignore Abandoned Calls** (the default): Select this option if you want to exclude abandoned calls from the service level calculation.<br><br>• **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.<br><br>• **Abandoned Calls have Positive Impact:** Select this option if you consider a call that is abandoned within the service level threshold time as a treated call. With this configuration, abandoned calls have a positive impact on the service level. |
| **Service Level Threshold** | yes | Enter the time in seconds that calls are to be answered based on your service level agreement, from 0 to 2,147,483,647.<br><br>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. |

| Name | Required | Description |
|---|---|---|
| **Agent Order** | yes | Select an option to determine which agents receive calls from this queue.<br>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.<br>• **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.<br>• **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.<br>• **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 | Select the bucket interval whose bounds are to be used to measure the time slot in which calls are answered.<br>The field defaults to the system default.<br>To select a different bucket interval: |

**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.

### Procedure

**Step 1** Click the numbered step link in the **Steps** panel (Step 1, Step 2, and so on).

The step number popup window opens.

**Step 2** Build the first step as follows.

a) Click the **magnifying glass** icon to the right of the Select Attribute field in the Expression 1 panel.
b) Select an attribute from the list.
c) 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.
d) 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.

a) Select **AND** or **OR** to establish the relationship between the first and second attributes.
b) Repeat steps 2b, 2c, and 2d.

**Step 4** Continue to add attributes to Expression 1.

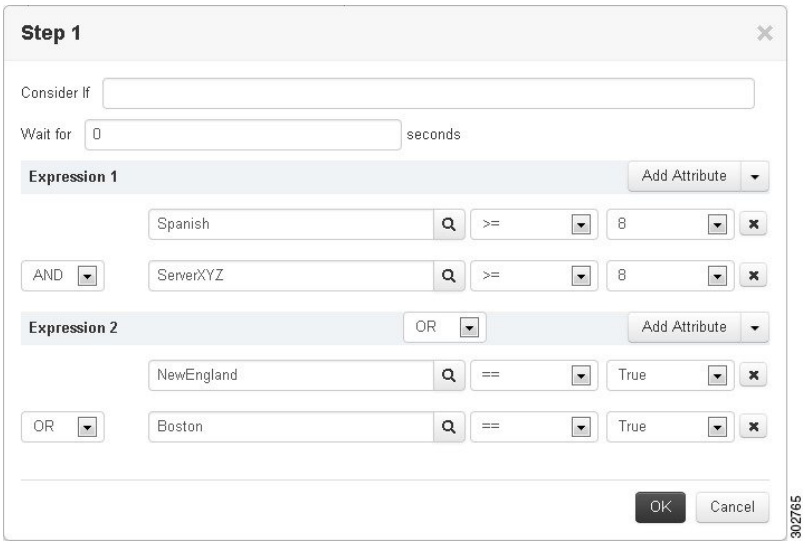
All attributes within an expression must be joined by the same logical operator. They must all be ANDs, or they must all be ORs.

**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 129 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 routes

The *route* is a value returned by a routing script that maps to a target or a peripheral. Those targets include services, skill groups, agents, translation routes, queue points, or CTI route points. The Unified CCE converts a route to a device target to direct to the request destination.

When you create a route, you associate the route with a service.

### Procedure

**Step 1** From the Configuration manager, choose **Tools** > **Explorer Tools** > **Skill Group Explorer**.
The Skill Group Explorer dialog box opens.

**Step 2** Click **Retrieve**.

**Step 3** Choose the skill group for which you are creating the route.

**Step 4** Click **Add Route**.

The Route tab opens.

**Step 5** In the Route tab, enter information in the following fields:

**Skill group priority**. The value 0 indicates a base skill group. This is the default when there is only one skill group and there are no priorities.

**Name**. The enterprise name of the route.

**Description**. Enter an optional description of the route.

**Service Name**: The name for the service.

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

**Caution** When you break the association between a route and a peripheral, the Unified CCE removes the Route ID value from all peripheral targets that reference that route.

# Perform Bulk Configuration

## Access Bulk Configuration Tools

### Procedure

**Step 1** Double-click **Configuration Manager** in the Administration Data Server group or the Administration Client group.

**Step 2** In the Menu selection box, select **Tools** > **Bulk Configuration**.

**Step 3** From the submenu selection list, select **Insert** if you need to insert data or **Edit** if you need to edit.

**Step 4** In the next menu selection list, select the type of table with which you need to work.

## Add New Records

You can add records by inserting multiple blank rows (records) and filling in the data or by importing the data.

You can also edit the data you insert when you insert it.

### *Insert New Records*

To insert a new record:

### Procedure

**Step 1** In the **Bulk Configuration** > **Insert** menu, select the name of the data table to which you want to add records. The appropriate Insert window opens, automatically displaying one new row.

**Step 2** To create additional rows, enter the number of additional rows in the Quantity field and click **Insert**. The additional rows are added in the Insert window.

**Step 3** Enter the data in the rows:

a) If you want to edit individual fields in the new rows, type the information you want in each of the fields and skip to Step 8.

b) If you want to edit a column in multiple rows so that a range of values is entered, continue to Step 4.

**Note** For other ways of entering data into multiple rows, see Edit Range of Data, on page 135

**Step 4** Select the rows in the column you want to modify.

**Step 5** Click **Edit Range**. The Edit Range dialog appears.

**Step 6** Enter a prefix (optional), the start value for the range, and a suffix (optional). The generated values are listed in the dialog.

**Step 7** Click **OK** to close the Edit Range dialog and apply the values to the column you selected.

**Step 8** When you have finished setting fields in the new rows, press **Enter** to apply your changes to the Unified CCE database.

**Note** You can leave empty rows, the system ignores them. No changes are made to the database until you press **Enter**.

## *Import Data*

You can import data from a specified text file into the opened database table. You can import whole records or only columns of data if the data matches (see Step 3 of the following procedure). The process cancels if any error occurs during the import process.

### Procedure

**Step 1** In the Insert or Edit window, click **Import**.

**Step 2** In the Import dialog, click **File**.

**Step 3** In the File Open dialog, select the file containing the data that you want to import and click **Open**.

The Import File Data area displays the first few lines of the opened file.

- When importing data in the Edit mode, the following rules apply:
  - The Bulk Configuration tool reads only those records whose primary key values match those of records in the Edit window.

    If a record does not match the primary key value, the record is considered to be an error and a message box with the primary key value pops up to ask you to correct the problem.
  - If any field in the import record is null, the corresponding field value in the grid window become blank for an edit cell or uses the default value for a drop-down list cell.
  - If any field is missing in the import file, the corresponding field in the Edit window remains unchanged.
  - If there is a larger number of records in the file to be imported than the number of rows in the grid, it is considered an error and a message box pops up asking you to correct it.
  - If there is a duplicated primary key in the file to be imported, it is considered an error and a message box with the duplicated primary key value pops up asking you to correct it.
  - After importing, all records imported (including records marked for deletion in the grid) are marked as “Changed” regardless of whether the value is changed or not.
  - After importing, the records display in index order (ordered by logical keys). If you did not sort before importing, the order appears the same after the import.
- When importing data in the Insert mode, the following rules apply:
  - Only a single import is supported and any existing rows are removed from the grid. When you click **Import**, the following message box pops up if there is any record in the grid:

```
All the existing data will be replaced by the data to be imported.
If you want to retain the current data on the grid please click
the Cancel button then save or export the existing data. Click the
OK button to proceed with the importing.
```

- After importing, all rows are marked as “New” and the ordering is the same as that in the file imported from.
- In the Import Insert mode, the tool reads only those records whose primary key values are not presented. If the primary key field is selected for file to be imported, it is considered an error and a message box with the primary key field name pops up asking you to correct the problem.
- If any field in the import record is null, the corresponding field value in the grid window becomes blank for an edit cell or uses the default value for a drop-down list cell.

**Note** If headers are included in the imported file, the **Add** and **Remove** buttons are not enabled and you can only import the records as a whole. In that case, skip to Step 6.

**Step 4** If the imported data does not contain headers, in the Available Fields list box, select the names of the fields to import that match the data and click **Add**.

**Step 5** To change the order of the columns, select a column and move it within the list by clicking **Up** or **Down**.

**Step 6** Click **OK**. The data is imported into the data table.

## Data File Format

The import and export files used by the Bulk Configuration tool can optionally include a header that identifies the table and columns in the file. The header is followed by one line for each row of data.

The following rules apply to file headers:

- A line beginning with a number sign (#) is a comment and is ignored.
- Blank lines are also ignored.
- The header content is indicated by a line beginning with two underline characters and the word **TABLE** or **COLUMNS**. The following line contains the name of the table or the name of the columns. For example:

```
__TABLE

Call_Type __

COLUMNS

CallTypeID EnterpriseName Description Deleted CustomerDefinitionID
```

- All column names must be on a single line and are separated by Tab characters.

  The following rules apply to the data in the files:

  - One row of table data per line.
  - Column values must be in the same order in all rows. If columns are specified in the header, the columns in the data rows must be in the same order.
  - Column values are separated by a single Tab character.

- Fields intentionally left blank must be represented by two adjacent Tab characters or a Tab character at the end of a line. On import, the default value is used for such a value.
- String values may include spaces.
- An error occurs on import if a line contains too few or too many values.

**Note** A simple way to create the import file with a valid format is to use Excel and save the file as Text (Tab delimited) (*.TXT).

## Select Data

You can select whole records for importing, exporting, setting security, deleting, or undeleting. Or, you can select the same field in multiple records for simultaneous editing.

### *Select Records*

Click in the left-most numbered field in a row to select that row and highlight it. Click in any other field in a row to select the row but not highlight it.

### *Select One Field in Multiple Records*

You can select one edit-control field (when there is no section box in the field) in multiple records in any of the following three ways:

- Click the field where you want to start and, keeping the left mouse button held down, move the cursor to the last field.
- Click the field where you want to start. While holding down the **Shift** key, click the last field.
- Click the field where you want to start. While holding down the **Shift** key, click the down arrow to select.
- Press **Ctrl,** then click on each field you wish to select. This allows you to select a discontinuous group of fields.

## Edit Range of Data

You can edit a range of data in a table column in three ways:

### Procedure

- Apply a single value to a range of edit-control fields
- Apply a single value to a range of selection-box fields
- Apply a range of values to a range of fields

### *Apply a Single Value to a Range of Edit-Control Fields*

An *edit-control field* is one you can edit that does not contain a selection box.

To apply a single value to a range of edit-control fields:

**Procedure**

**Step 1** Make your selection: click the field where you want the range to start and, keeping the left mouse button held down, move the cursor to the last field in the range.

**Step 2** Type the new entry that you want to appear in all the fields.

**Step 3** Click **Enter** or **Tab**. This applies the change to all the records in the range and moves the focus to the next data field.

### *Apply a Single Value to a Range of Selection-Box Fields*

To apply a single value to a range of selection-box fields:

**Procedure**

**Step 1** Select the first field where you want the range to start.

**Step 2** Press the **Shift** key and hold it down for steps 3, 4, and 5.

**Step 3** Click the selection-box down arrow but keep the left mouse button held down and select the fields you want in the range.

**Step 4** Click the last field in the selection to display the selection list. You can also open the selection box by pressing **Alt** + an arrow key.

**Step 5** Click your selection.

**Step 6** Click **Enter** or **Tab** (or any other field). This applies the change to all the records and moves the focus to the next data field.

### *Apply a Range of Values to a Range of Fields in a Column*

To apply a range of values to a range of fields in a column:

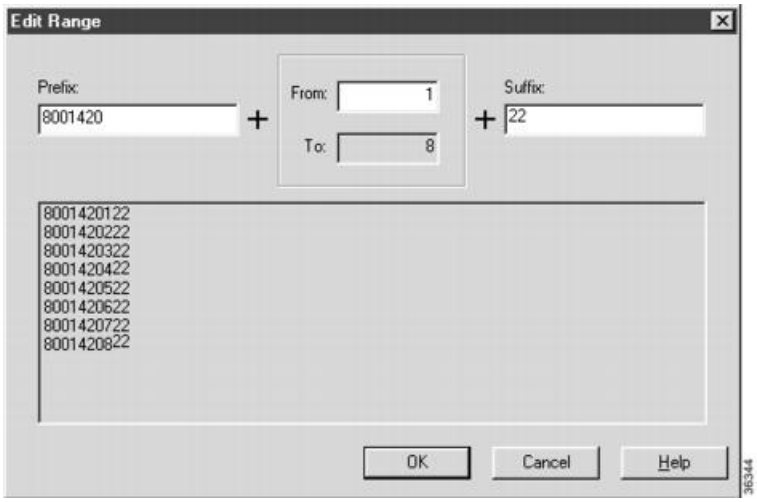
**Procedure**

**Step 1** Select the range of fields in a database column. This enables the **Edit Range** button.

**Note** The **Edit Range** button does not work for selection-box fields.

**Step 2** Click **Edit Range**. The Edit Range dialog displays.

*Figure 2: Edit Range Dialog Box*




**Step 3** In the Edit Range From field, enter the first number of the range.

**Step 4** In the Prefix and Suffix fields, you can optionally enter substrings to appear before or after each value. The Edit Range dialog lists the generated values.

**Note** When entering a numeric range, you may also enter leading zeros to ensure proper alignment (that is, 001 to 999).

**Step 5** Click **OK**. This applies the changes to the fields you selected in the Insert or Edit window.

# Configure Cisco Unified Intelligence Center

## Sign In to Administration Console

Who can sign in to the administration console: The System Application User who is the default Superuser.

To upload the license, you must sign in to the Unified Intelligence Center Administration Console. This is the OAMP interface for Unified Intelligence Center. The first person who signs in to the Administration application must do so using the user ID and password that were defined for the System Application User during the installation. This user is the initial Superuser for Unified Intelligence Center Administration.

### Procedure

**Step 1** Enter this URL: `http://<HOST ADDRESS>/oamp`, where HOST ADDRESS is the IP address or hostname of your Controller node.

**Step 2** Enter the System Application User ID and password that you defined during installation.

# Configure SQL User Account

### Procedure

**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**.

Use these steps to create login accounts for the **Cisco Unified Intelligence Center** reporting data sources and for Finesse connectivity to the AW Database on the **Cisco Finesse Administration** page.

**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** and **Historical database** check boxes.

**b.** In the **Users mapped to this login** area, check the **master** check box. This is required only for an SQL user configured to work with Live Data.

**c.** In the **Database role membership for** area, do the following:

- For CUIC and Finesse users, check the **db_datareader** and check box.
- For Live Data users, check the following check boxes:
  - **db_datareader**
  - **db_datawriter**

**Note** The database role **public** is checked by default. This role is required for CUIC, Finesse, and Live Data users.

**Step 6** Click **OK**.

### What to do next

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

# Configure Data Sources

To integrate Unified Intelligence Center with Unified CCE, you must configure the following two data sources:

- Unified CCE Historical data source—This data source is added by default to support the Unified CCE stock historical reports and Unified CCE User Integration. Complete the Database Host, Database Name, and the Database User ID and Password fields for this data source and ensure that it is online before Unified CCE User Synchronization can occur.
- Unified CCE Realtime data source—This data source is added by default to support the Unified CCE stock real time reports. Complete the Database Host, Database Name, and the Database User ID and Password fields for this data source.

Depending on your environment, the Unified CCE Historical and Realtime data sources can point to the same machine.

You can run a CLI command to point each node to a unique IP Address for the Unified CCE Historical or Realtime data source. The command is `set cuic properties host-to-ip`. For more information about the CLI, see the *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.

To integrate Unified Intelligence Center with Unified CVP, you must add a Unified CVP data source.

A Unified Intelligence Center data source is also installed by default. This data source represents the Unified Intelligence Center database on the node that stores records for reports, dashboards, and users maintained on that node. This data is replicated across all nodes in the cluster. You can edit the description for this data source, but *do not change other fields*. The Unified Intelligence Center data source for each node is configured by default to point to that member.

## Configure Unified CCE Data Sources

### Procedure

**Step 1** From the Unified Intelligence Center Reporting application, click **Data Sources** drawer on the left panel to open the **Data Sources** page.

**Step 2** Select the Unified CCE Historical Data Source.

**Step 3** Click **Edit** to open the **Data Source Create/Edit** page.

**Step 4** Complete the fields for the selected data source. See online help for guidance.

**Note** The name of the database instance is a required field only for Informix databases.

**Step 5** Test the data source connection. Troubleshoot, if required.

**Step 6** Save the data source.

**Step 7** Repeat steps 2 through 6 for the Unified CCE Realtime data source.

## Create Data Source for Cisco Unified CVP Report Data

### Procedure

**Step 1** Log in to the Unified Intelligence Center at `https://<hostname/ IP address of CUIC Publisher>:8444/cuicui`.

**Step 2** Select the **Data Sources** drawer to open the **Data Sources** page.

**Step 3** Click **New** to open **New Data Source** page.

**Step 4** Complete fields on this page as follows:

| Field | Value |
|---|---|
| **Name** | Enter the name of this data source.<br>Report Designers and Report Definition Designers do not have access to the Data Sources page but can see the list of Data Sources when they create custom reports. To benefit those users, give a new Data Source a meaningful name. |
| **Description** | Enter a description for this data source. |
| **Data Source Type** | Choose **Informix**.<br>**Note** Type is disabled in Edit mode. |
| **Host Settings** | |
| **Database Host** | Enter the IP address or hostname for the Unified CVP Reporting server. |
| **Port** | Enter the port number. Typically, the port is 1526. |
| **Database Name** | Enter the name of the reporting database on the Unified CVP reporting server. The database name can be `cvp_data` or `callback`. |
| **Instance** | Specify the instance name of the desired database. By default, this is `cvp`. |
| **Timezone** | Choose the correct time zone for the data stored in the database. In locations that change from Standard Time to Daylight Savings Time, this time zone is updated automatically.<br>**Note** Set CVP datasource timezone configuration to UTC on CUIC. |
| **Authentication Settings** | |
| **Database User ID** | Enter the user ID of the Reporting User who is configured in the Operations Console to access the Unified CVP reporting database.<br>(The cvp_dbuser account is created automatically during Unified CVP Reporting server installation.) |
| **Password and Confirm Password** | Enter and confirm the password for the database user. |
| **Charset** | Choose UTF-8. |
| **Default Permissions** | View or edit the permissions for this datasource for My Group and for the All Users group. |

| Field | Value |
|---|---|
| **Max Pool Size** | Select the maximum pool size.<br>Value ranges from 5-200. The default Max Pool Size value is 100 and is common for both the primary and secondary data source tabs. |

**Step 5** Click **Test Connection**.

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

**Step 6** Click **Save** to close the Add Data Source window.

The new data source appears on the Data Sources list.

## *Cisco Unified Intelligence Center Reporting User Roles*

There are seven User Roles, and a user can be assigned to one, any, or all of them. The roles are:

- Login User
- System Configuration Administrator
- Security Administrator
- Dashboard Designer
- Value List Collection Designer
- Report Designer
- Report Definition Designer

Depending on the size, staff, geographical distribution, and security practices of your call center, you might want to assign multiple user roles to a few people or to distribute user roles to many people.

### Login User

By default, everyone who can sign in to Unified Intelligence Center is a Login User. Login Users have that role and only that role until the Security Administrator assigns additional roles or deactivates (removes) the Login User role.

A Security Administrator or System Application user can remove the login role from any user.

An active login user can:

- Log in to Unified Intelligence Center
- Open the Security drawer, access the User List, and edit his own User Information page; for example, to change his alias or phone number.

### System Configuration Administrator

This user has all the rights of an active Login User and also:

- Has full access to the Data Sources drawer and its functions.
- Has full access to the Scheduler drawer and its functions.

### Security Administrator

This user has all the rights of an active Login User and also has full access to the Security drawer and its functions.

### Dashboard Designer

This user has all the rights of an active Login User and also has full access to the Dashboard drawer.

### Value List Collection Designer

This user has all the rights of an active Login User and also:

- Has full access to the Value Lists drawer.
- Has View (Read) access to the Data Sources drawer.

### Report Designer

This user has all the rights of an active Login User and also:

- Has full access to the Reports drawer.
- Has View (Read) access to the Data Sources and Value Lists drawers.
- Can access the Scheduler drawer to work with the user's own reports.

### Report Definition Designer

This user has all the rights of an active Login User and also:

- Has full access to the Report Definition drawer.
- Has View (Read) access to the Data Sources and Value Lists drawers.

## Download Report Bundles

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

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

- Cisco Unified Intelligence Center Admin Security templates - Templates to report on Cisco Unified Intelligence Server audit trails, permissions, and template ownership.

Additionally, sample custom report templates are available from the Cisco Developer Network (https://developer.cisco.com/web/ccr/documentation).

## Import Report Bundles

**Procedure**

**Step 1** Sign in to Unified Intelligence Center at https://<hostname/ IP address of CUIC Publisher>:8444/cuicui, and click **Reports** in the left pane.

**Step 2** Click **Import Report**.

**Step 3** In the **File Name (XML or ZIP file)** field, click **Browse**.

**Step 4** Browse to and select the report bundle zip file, and click **Open**.

Select a report bundle for the version of software deployed in the contact center.

**Step 5** Select the location where you want to save the file.

**Step 6** Click **Import**.

**Step 7** Choose one:

- If the report or reports do not yet exist, you must provide the data source. From the **Data Source for ValueList** drop-down list, select the data source used. Then click **Import**.

  **Note** You have to select a data source for the value list only if it does not use the same data source as the report definition. For LiveData reports, the Data Source for ReportDefinition is LiveData Streaming and the Data Source for ValueList is UCCE Realtime. For real time reports, the Data Source is UCCE Realtime. For historical reports, the Data Source is UCCE Historical.

- If the report or reports do exist, a message appears asking you if you want to replace the existing report (which overwrites any report definition changes associated to it). Click **Yes**, **Yes to All**, **No**, or **No to All**.

## Configure Unified Intelligence Center Administration

Complete the following procedure to configure Unified Intelligence Center Administration.

**Procedure**

**Step 1** Sign in to the **Cisco Unified Intelligence Center Administration Console** (`https://<hostname>:8443/oamp`).

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

a) For Host Address for the Primary Active Directory Server, enter the IP address of the domain controller.

b) For Port, enter the port number for the domain controller.

c) Complete the **Manager Distinguished Name** fields that are required for the customer.
d) Enter and confirm the password with which the Manager accesses the domain controller.
e) For User Search Base, specify users and the domain name and any sub-domain names .
f) For Attribute for User ID, select the required option.

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

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

**Note** For more details, see the online help.

**Step 3** Configure syslog for all devices.

a) Choose **Device Management** > **Logs and Traces Settings**.
b) For each host address:

- Select the associated servers and click the arrow to expand.
- Select the server name.
- In the **Edit Serviceability Settings** screen **Syslog Settings** pane, configure the Primary and Backup Host. Click **Save**.

**Step 4** Configure SNMP for all devices, if used.

a) Select **Network Management** > **SNMP**.
b) Navigate to SNMP and for each server add the following:

- V1/V2c Community Strings.
- Notification Destination.

# Configure Cisco Unified Customer Voice Portal

## Configure Unified CVP Server

### Set Up FTP Server

**Procedure**

**Step 1** Install the FTP Service on the server.

a) Choose **Start** > **Administrative Tools** > **Server Manager**.

b) Expand **Roles** in the left panel of the Server Manager window.
c) Right-click **Web Server (IIS)** and click **Add Role Services**.
d) Check the **FTP Server** check box, click **Next** and then click **Install**, installation takes a few moments.
e) When the installation is complete, click **Close**.

**Step 2** Enable the FTP Service on the server.

a) Choose **Start** > **Administrative Tools** > **Server Manager**.
b) Expand **Roles** in the left panel of the Server Manager window.
c) Expand **Web Server (IIS)** and then click **Internet Information Services (IIS) Manager**.
d) Expand hostname.
e) Right-click **Sites** and click **Add FTP Site**.
f) Enter a **FTP site name**.
g) Enter **c:\Inetpub\wwwroot** in the **Physical path** of the FTP site name, and click **Next**.
h) Enter the IP address of the CVP Server.
i) Select **No SSL** in SSL Options and then click **Next**.
j) Check the **Anonymous** and **Basic** check boxes.
k) Select **All Users** from the Allow Access To drop-down list.
l) Check the **Read** and **Write** check boxes, and then click **Finish**.

**Step 3** Set the Basic Setting for the FTP Server.

a) Click **Sites** and then click the FTP server that you have created.
b) Click **Basic Settings** in the Actions tab and click **Connect as**.
c) Select **Application user (pass-through authentication)** option and click **OK** twice.

## Configure Unified CVP Reporting Server

### Create Reporting Users

Who can create a user:

- Initially, the System Application User who is the default Superuser.
- Eventually, any Superuser.

Unified CVP reporting users can sign in to Unified Intelligence Center only if they exist in the Administration console as Superusers or if Active Directory (AD) is configured in the Unified Intelligence Center Administration console for their domain:

- Superusers who are added are considered to be IP Multimedia Subsystem (IMS) users.
- Users who are authenticated through Active Directory are considered to be Lightweight Directory Access Protocol (LDAP) users.

Both IMS users and LDAP users can log in to Unified Intelligence Center reporting and are restricted to the limited Login User role until the Unified Intelligence Center reporting security administrator gives them additional roles and flags them as active users.

### *Create Superusers*

**Procedure**

**Step 1** Log in to the Cisco Unified Intelligence Center Administration Console `(https://<HOST ADDRESS>/oamp)`.

**Step 2** Navigate to **Admin User Management > Admin User Management** to open the Users page.

**Step 3** Click **Add New** to add and configure a new user or click an existing username to edit the configuration for that user.

This page has three tabs: General, Credentials, and Policy. For information about completing these tabs, see *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/en/US/products/ps9755/prod_maintenance_guides_list.html or the Administration console online help.

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

### *Set Up Active Directory Server for LDAP Users*

Configure the Active Directory tab in the Cisco Unified Intelligence Center Administration console so that Unified CVP reporting users can log in to the Unified Intelligence Center reporting application with the user name and password that is defined in their domain.

**Procedure**

**Step 1** In the Cisco Unified Intelligence Center Administration application, navigate to **Cluster Configuration** > **Reporting Configuration** and select the Active Directory tab.

**Step 2** Complete all fields on this page, referring to the online help for guidance.

**Step 3** Click **Test Connection**.

**Step 4** When the connection is confirmed, click **Save**.

### *Sign In to Cisco Unified Intelligence Center Reporting Interface*

Who can sign in to the Unified Intelligence Center reporting interface:

- Initially, the System Application User who is the default Superuser.
- Eventually, any Unified CVP user who was created in the Administration Console as an IMS superuser or an LDAP user.

Perform the following procedure to sign in to the Unified Intelligence Center reporting interface.

**Procedure**

**Step 1** Sign in to the Cisco Unified Intelligence Center Administration Console (*https://<HOST ADDRESS>/oamp*).

**Step 2** Navigate to **Control Center** > **Device Control**.

**Step 3** Click on the name of the Member node you want to access. This opens the Cisco Unified Intelligence Center login page for that member.

**Step 4** Enter your user ID and password. The Overview page appears.

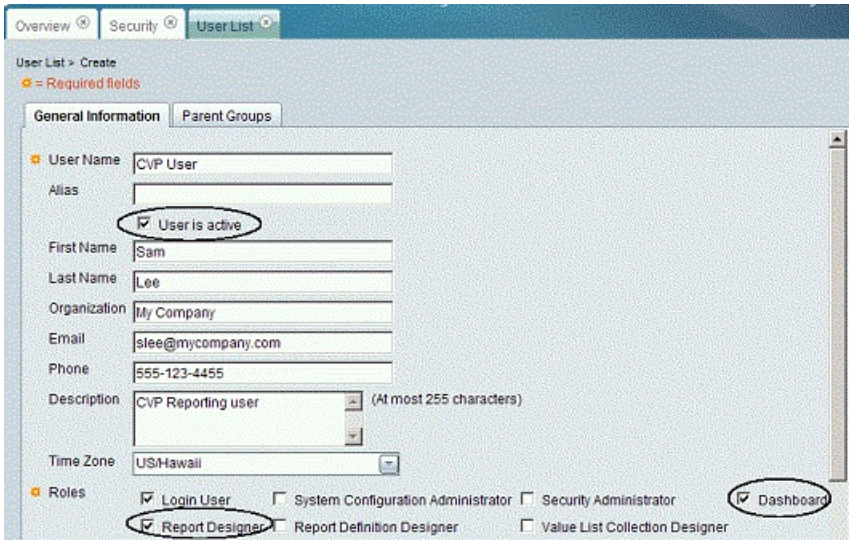
**Step 5**

### *Cisco Unified Customer Voice Protocol Reporting User Role Additions*

Once Unified CVP users log in to Unified Intelligence Center, they are added to the Unified Intelligence Center database and appear on the user list.

New users are initially defined as Login Users: the lowest level user role of Unified Intelligence Center. A Unified Intelligence Center Security Admin user must access the User List page to check a **User is Active** check box and to grant additional user roles to the user.

***Figure 3: User List Page***




## Obtain and Import Report Templates

### *Obtain Cisco Unified CVP Report Templates*

Who can obtain import Unified CVP report templates: any user in your organization.

The Unified CVP reporting template XML files are installed with Unified CVP. Locate them and copy them to a Cisco Unified Intelligence Center client workstation.

Perform the following procedure to obtain import Unified CVP report templates.

#### Procedure

**Step 1** In the Unified CVP server, locate the Unified CVP template files. These are XML files that reside on the reporting server in %CVP_HOME%\CVP_Reporting_Templates. You can also find them in the Installation directory \Downloads and Samples\Reporting Templates.

**Step 2** Choose the files and copy them to the client computer from where you can launch the Unified Intelligence Center Reporting web application.

*Import Unified CVP Report Templates*

**Procedure**

**Step 1** Launch the Unified Intelligence Center web application using the `URL https://<CUCI ADDRESS:8444/cuicui/`.

**Step 2** Enter CUIC Username and Password.

**Step 3** Create a folder to import the reports.

a) Click **Reports**.
b) From the toolbar, click **New** > **Folder**.
c) Enter the folder name and click **Save**.

**Step 4** Import the report templates.

a) Click **Reports** > **New > Import**. You will be redirected to the CUIC legacy interface.
b) Click **Reports** > **Import Report**.
c) In the **File Name (XML or ZIP File)** field, click **Browse** and select the template file to import.
d) In the **Save To** field, expand the Reports tree and select the folder created to import the report template.
e) Click **Import**. CUIC validates the Report Definition ID in the template and successfully imports the template.

**Note** When one or more underlying Report Definitions do not exist in CUIC, you will be prompted to select a data source for the Report Definition and Value Lists. For information on creating Data Sources and Value Lists, see Cisco Unified Intelligence Center Report Customization Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-user-guide-list.html.

# Configure Unified CVP Operations Console

## Enable Unified CVP Operations Console

Complete the following procedure on the Unified CVP OAMP server to enable the Unified CVP Operations Console.

**Procedure**

**Step 1** Go to **Start > Run** and type **services.msc**.

**Step 2** Check that Cisco CVP OPSConsoleServer service is running. If it is not, right-click that service and click **Start**.

**Step 3** Go to **Start > All Programs > Cisco Unified Customer Voice Portal > Operation Console** to open the Unified CVP OPSConsole page.

## Configure Unified CVP Call Server Component

**Note**

- There is one Unified CVP server on Side A and one Unified CVP server on side B for the 500 agent deployment.
- There are two Unified CVP servers on Side A and two Unified CVP server on side B for the 1000 agent deployment.
- There are eight Unified CVP servers on Side A and eight Unified CVP server on side B for the 4000 agent deployment.

### Procedure

**Step 1** On the Unified CVP OAMP server, go to **Start** > **All Programs** > **Cisco Unified Customer Voice Portal**.

**Step 2** Click **Operations Console** and log in.

**Step 3** Navigate to **Device Management > Unified CVP Call Server**.

**Step 4** Click **Add New**.

**Step 5** On the General tab, enter the IP address and the hostname of the Cisco Unified CVP Server. Check **ICM**, **IVR**, and **SIP**. Click **Next**.

**Step 6** Click the **ICM** tab. For each of the Cisco Unified CVP Call Servers, retain the default port of 5000 for the VRU Connection Port.

**Step 7** Click the **SIP** tab:

a) In the Enable outbound proxy field, select **No**.
b) In the Use DNS SRV type query field, select **Yes**.
c) Check **Resolve SRV records locally**.

**Step 8** Click the **Device Pool** tab. Make sure the default device pool is selected.

**Step 9** (Optional) Click the **Infrastructure** tab. In the Configuration Syslog Settings pane, configure these fields as follows:

a) Enter the IP address or the hostname of the syslog server.

**Example:**

Prime server

b) Enter **514** for the port number of the syslog server.
c) Enter the name of the backup server to which the reporting server writes log messages.
d) In the Backup server port number field, enter the port number of the backup syslog server.

**Step 10** Click **Save & Deploy**.

**Step 11** Repeat this procedure for the remaining Unified CVP Servers.

## Configure Unified CVP VXML Server Component

### Procedure

**Step 1** In the Unified CVP Operations console, navigate to **Device Management** > **Unified CVP VXML Server**.

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

**Step 3** On the General tab, enter the IP address and the hostname of the Cisco Unified CVP Server.

**Step 4** Configure the primary and backup CVP Call Servers.

**Step 5** Click the **Configuration** tab. In the **Enable reporting for this CVP VXML Server** field, click **Yes** to optionally enable reporting. If you do not want to enable reporting, click **No**.

**Step 6** Click the **Device Pool** tab. Make sure the default device pool is selected. If prompted to restart the primary and secondary call servers, click No. Do not restart at this time.

**Step 7** Click **Save & Deploy**.

**Step 8** Repeat this procedure for all CVP Servers.

## Configure Unified CVP Media Server

### Procedure

**Step 1** In the CVP Operations Console, navigate to **Device Management > Media Server**.

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

**Step 3** On the **General** tab, configure the following.

a) Enter the IP address and the hostname of the Unified CVP server.
b) Check **FTP Enabled**.
c) Either Check **Anonymous Access** or enter the credentials.
d) Click **Test SignIn** to validate the FTP access.

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

**Step 5** Repeat Step 1 through 4 for all Media Servers.

**Step 6** After you configure all Media Servers, click **Deploy**.

**Step 7** Click **Deployment Status** to make sure that you applied the configuration.

**Step 8** In the CVP Operations Console, navigate to **Device Management > Media Server**.

**Step 9** Change Default Media Server from **None** to any one of the Unified CVP servers. Then click **Set**.

**Step 10** Click **Deploy**.

## Install Unified CVP Licenses

For instructions on installing Unified CVP licences, see the *Smart Licensing* section in *Administration Guide for Cisco Unified Customer Voice Portal* guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.

## Configure Gateways

### Procedure

**Step 1** In the Unified CVP Operations Console, navigate to **Device Management** > **Gateway**.

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

**Step 3** On the General tab, configure as follows:

a) Enter the IP address.
b) Enter the hostname.
c) Choose the Device Type.
d) In the Username and Passwords pane, enter the username, password, and enable password.

**Step 4** Click **Test Sign-in** to verify that a connection with the gateway can be established and that the credentials are correct.

**Step 5** Click **Save**.

**Step 6** Repeat for every gateway.

## Add Unified CCE Devices

### Procedure

**Step 1** Log in to the **Unified CVP Operations Console**.

**Step 2** Choose **Device Management** > **Unified ICM**.

**Step 3** Click **Add New**.

**Step 4** On the General tab, configure as follows:

a) Enter the IP address.
b) Enter the Hostname.
c) Check Enable Serviceability.
d) Enter the Username.
e) Enter the Password.
f) Confirm Password.
g) Accept the default port.

**Step 5** Click **Save**.

**Step 6** Repeat Steps 1 to 5 for all Unified CCE machines.

## Add Unified Communications Manager Devices

### Procedure

**Step 1** Log in to the **CVP Operations Console**.

**Step 2** Choose **Device Management** > **Unified CM**.

**Step 3** Click **Add New**.

**Step 4** On the General tab, configure as follows:

a) Enter the IP address.
b) Enter the Hostname.
c) Check Enable Synchronization.
d) Enter the Username.
e) Enter the Password.
f) Confirm Password.
g) Accept the default port.

**Note** For Small contact center deployment add the NAT IP address of the unified CM.

**Step 5** Click **Save**.

**Step 6** Repeat Steps 1 to 5 for all Unified Communications Manager Devices.

## Add Unified Intelligence Center Devices

### Procedure

**Step 1** Log in to the **CVP Operations Console**.

**Step 2** Navigate to the Cisco Unified Intelligence Center Device. Choose **Device Management** > **Unified IC**.

**Step 3** Click **Add New**.

**Step 4** On the General tab, configure as follows:

a) Enter the IP address.
b) Enter the Hostname.
c) Check Enable Serviceability.
d) Enter the Username.
e) Enter the Password.
f) Confirm Password.
g) Accept the default port.
h) Associate all the existing CVP Reporting Servers.

**Step 5** Click **Save**.

## Transfer Scripts and Media Files

Create the notification destination and deploy to all of the Unified CVP devices.

### Procedure

**Step 1** In the Unified CVP Operations Console, navigate to **Bulk Administration** > **File Transfer** > **Scripts & Media**.

**Step 2** In the Select device type field, select the **Gateway**.

**Step 3** Move all Gateways to **Selected**.

**Step 4** Click **Default Gateway files**.

**Step 5** Click **Transfer** and select **OK** at the popup window.

**Step 6** Click **File Transfer Status** to monitor transfer progress.

## Configure SNMP

For more information about SNMP in Unified CCE, see the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_installation_and_configuration_guides_list.html and *SNMP Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_installation_and_configuration_guides_list.html.

### Procedure

**Step 1** In the Unified CVP Operations Console, navigate to **SNMP** > **V1/V2c** > **Community String** .

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

a) On the **General** tab, name the community string.
b) On the **Devices** tab, select the required device from the list of available devices.
c) Click **Save and Deploy**.

**Step 3** Create the notification destination and deploy to all of the Unified CVP devices.

a) Navigate to **SNMP** > **V1/V2c** > **Notification Destination**.
b) Click **Add New**.
c) Complete the fields.
d) Select the **Devices** tab and assign the SNMP notification destination to a device.
e) Click **Save and Deploy**.

## Configure SIP Server Group

SIP Server Groups are required for Cisco Unified Communications Manager and Gateways.

### Procedure

**Step 1** In the Unified CVP Operations Console, navigate to **System** > **SIP Server Group** .

**Step 2** Create a server group for the Cisco Unified Communications Manager devices:

a) On the General tab, click **Add New**.
b) Fill in the **SRV Domain Name FQDN** field with a value that will also be used in the Cluster FQDN setting in Enterprise Parameters in Communications Manager. For example, cucm.cisco.com.
c) In the **IP Address/Hostname** field, enter an IP address or hostname for the Unified Communications Manager node.
d) Click **Add**.
e) Repeat Steps c and d for each Unified Communications Manager subscriber. Click **Save**.

**Note** Do not put the Publisher node in the server group.

SIP server group for Communications Manager is not required for SCC deployment as there is no direct SIP trunk created from Communications Manager to CVP in SCC model.

The FQDN should match the FQDN configured in the Enterprise Cluster FQDN setting on the Cisco Unified Communications Manager. For example, *cucm.cisco.com*. Adding the cluster subscriber nodes will load balance across all sub nodes.

**Step 3** Create a server group for the gateway devices:

a) On the General tab, click **Add New**.
b) In the **SRV Domain Name FQDN** field, enter the SRV Domain Name FQDN. For example vxmlgw.cisco.com.
c) In the **IP Address/Hostname** field, enter an IP address or hostname for each gateway.
d) Click **Add**.
e) Repeat Steps c and d for each gateway. Click **Save**.

Add all VXML gateways as appropriate for deployment and branches. Adding all VXML gateways to the server group will load balance calls across all the member server group gateways.

**Step 4** Associate these server groups to all Unified CVP Call Servers:

a) On the **Call Server Deployment** tab, move all Unified CVP Call Servers from the **Available** list to the **Selected** list.
b) Click **Save and Deploy**.

**Note** In the small contact center agent deployment, CUBE(SP) does not support FQDN configuration, therefore, you cannot create SIP server group pointing to CUBE(SP) for each sub customer.

**Note**
- In the small contact center agent deployment, CUBE(SP) does not support FQDN configuration, therefore, you cannot create SIP server group pointing to CUBE(SP) for each sub customer.
- In 12000 and 24000 agent deployment model, each CUCM cluster should have one SIP Server group with their subscriber nodes.

## Configure Dialed Number Patterns

Dialed number patterns are required for:

- Agent Device
- Network VRU
- Ringtone
- Error

### Procedure

**Step 1** In the Unified CVP Operations Console, navigate to **System** > **Dialed Number Pattern**.

**Step 2** For each dialed number pattern in the following table:

a) Click **Add New**.
b) In the **Dialed Number Pattern** field, enter the dialed number pattern.
c) In the **Description** field, enter a description for the dialed number pattern.
d) In the **Dialed Number Pattern Types** pane, check the specified dialed number pattern types.
e) Click **Save**.

**Step 3** After you configure all dialed number patterns, click **Deploy**.

**Step 4** Click **Deployment Status** to make sure that you applied the configuration.

| Dialed number pattern | Description | Dialed number pattern types |
|---|---|---|
| 91* | Ringtone | Check **Enable Local Static Route**.<br>Route to SIP Server Group and IP Address/Hostname/Server Group Name are both VXML Gateway (for example, vxmlgw.cisco.com).<br>Check **Enable Send Calls to Originator**. |
| 92* | Error | Check **Enable Local Static Route**.<br>Route to SIP Server Group and IP Address/Hostname/Server Group Name are both VXML Gateway (for example, vxmlgw.cisco.com).<br>Check **Enable Send Calls to Originator**. |
| The agent extension pattern. For example, enter 500* where the range of agent extensions is 5001 to 500999. | Agent Device. | Check **Enable Local Static Route**.<br>Route to SIP Server Group and IP Address/Hostname/Server Group Name are both the Unified Communications Manager gateway.<br>Check **Enable RNA Timeout for Outbound Calls**. The default timeout value is 60 seconds. |
| 777* | Network VRU Label | Check **Enable Local Static Route**.<br>Route to SIP Server Group and IP Address/Hostname/Server Group Name are both VXML Gateway (for example vxmlgw.cisco.com).<br>Check **Enable Send Calls to Originator**. |
| The agent extension pattern for the sub customer in SCC model. For example, enter 500* where the range agent extensions is 5001 to 500999. | Agent Device Label for the sub customer in the SCC model. | Check Enable Local Static Route.<br>In IP Address/Hostname/Server Group field provide the signaling IP address and port of the CVP adjacency in CUBE(SP) in the format:< IP Address>:<Port number><br>For each sub customer a unique port must be configured.<br>Check Enable RNA Timeout for Outbound Calls. The timeout is 15 seconds. |

**Note** In 12000 and 24000 agent deployment model, each CUCM cluster should have separate Dialed number Pattern with their agent extension range.

*Configure Cisco IOS Enterprise Voice Gateway*

Complete the following procedure to configure the Cisco IOS Voice Gateway. Instructions are applicable to both TDM and Cisco UBE Voice gateways, unless otherwise noted.

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

**Procedure**

**Step 1** Configure the network interfaces:

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

**Step 2** Configure global settings:

```
voice service voip
 no ip address trusted authenticate
 allow-connections sip to sip
 signaling forward unconditional
 !If this gateway is being licensed as a Cisco UBE the following lines are also required
 mode border-element
 ip address trusted list
  ipv4 0.0.0.0 0.0.0.0               # Or an explicit Source IP Address Trust List
sip
  rel1xx disable
  header-passing
  options-ping 60
  midcall-signaling passthru
```

**Step 3** Configure voice codec preference:

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

**Step 4** Configure Unified CVP services and settings:

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

# Default CVP http, ivr, rtsp, mrcp and vxml settings
```

```
http client cache memory pool 15000
http client cache memory file 1000
http client cache refresh 864000
no http client connection persistent
http client connection timeout 60
http client connection idle timeout 10
http client response timeout 30
ivr prompt memory 15000
ivr asr-server rtsp://asr-en-us/recognizer
ivr tts-server rtsp://tts-en-us/synthesizer
rtsp client timeout connect 10
rtsp client timeout message 10
mrcp client timeout connect 10
mrcp client timeout message 10
mrcp client rtpsetup enable
vxml tree memory 500
vxml audioerror
vxml version 2.0
```

**Step 5** Configure primary and secondary media servers:

```
#Configure the media servers where
# the primary matches the default media server defined in OAMP.
# the secondary is located on the opposite side of the primary.
ip host mediaserver ###.###.###.### # IP Address for primary media server.
ip host mediaserver-backup ###.###.###.### # IP Address for secondary media server.
```

**Step 6** Configure the dial-peers:

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


# Configure CVP Ringtone
 dial-peer voice 919191 voip
 description CVP SIP ringtone dial-peer
 service ringtone
 incoming called-number 9191T
 voice-class sip rel1xx disable
 dtmf-relay rtp-nte
 codec g711ulaw
 no vad


# Configure CVP Error
 dial-peer voice 929292 voip
 description CVP SIP error dial-peer
 service cvperror
 incoming called-number 9292T
 voice-class sip rel1xx disable
 dtmf-relay rtp-nte
 codec g711ulaw
 no vad



#Configure VXML leg where the incoming called-number matches the Network VRU Label
 dial-peer voice 7777 voip
 description Used for VRU leg
 service bootstrap
 incoming called-number 777T
```

```
 dtmf-relay rtp-nte
 codec g711ulaw
 no vad



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

dial-peer voice 70021 voip
 description Used for Switch leg SIP Direct
 preference 1
 max-conn 225
 destination-pattern xxxx..... # Customer specific destination pattern
 session protocol sipv2
 session target ipv4:###.###.###.### # IP Address for CVP1, SideA
 session transport tcp
 voice-class codec 1
 voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
 dtmf-relay rtp-nte
 no vad


dial-peer voice 70022 voip
 description Used for Switch leg SIP Direct
 preference 1
 max-conn 225
 destination-pattern xxxx..... # Customer specific destination pattern
 session protocol sipv2
 session target ipv4:###.###.###.### # IP Address for CVP2, SideA
 session transport tcp
 voice-class codec 1
 voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
 dtmf-relay rtp-nte
 no vad


dial-peer voice 70023 voip
 description Used for Switch leg SIP Direct
 preference 2
 max-conn 225
 destination-pattern xxxx..... # Customer specific destination pattern
 session protocol sipv2
 session target ipv4:###.###.###.### # IP Address for CVP1, SideB
 session transport tcp
 voice-class codec 1
 voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
 dtmf-relay rtp-nte
 no vad


dial-peer voice 70024 voip
description Used for Switch leg SIP Direct
preference 2
max-conn 225
destination-pattern xxxx..... # Customer specific destination pattern
session protocol sipv2
session target ipv4:###.###.###.### # IP Address for CVP2, SideB
session transport tcp
```

```
voice-class codec 1
voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
dtmf-relay rtp-nte
no vad
```

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

```
# Note: This section is only for reference. You must configure Hardware resources using
Unified Communications Domain Manager.
# Configure the voice-cards share the DSP resources located in Slot0
voice-card 0
dspfarm
dsp services dspfarm
voice-card 1
dspfarm
dsp services dspfarm
voice-card 2
dspfarm
dsp services dspfarm
voice-card 3
dspfarm
dsp services dspfarm
voice-card 4
dspfarm
dsp services dspfarm

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

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

# Configure DSPFarms for Conference, MTP and Transcoder
dspfarm profile 1 conference
codec g711ulaw
codec g711alaw
codec g729r8
maximum sessions 24
associate application SCCP

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

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

**Note** Universal transcoder is only needed for cases where you engage the G.729 caller to G.729 only agent with IVR in middle and performs any supplementary services or use features like whisper announcement or agent greeting. If both the agent and caller are using G.729, transcoding is not required. .

**Step 8** (Optional) Configure the SIP Trunking:

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

# Configure one rai target for each CVP Server
sip-ua
rai target ipv4:###.###.###.### resource-group1 # CVP1A
rai target ipv4:###.###.###.### resource-group1 # CVP2A
rai target ipv4:###.###.###.### resource-group1 # CVP1B
rai target ipv4:###.###.###.### resource-group1 # CVP2B
permit hostname dns:%Requires manual replacement - ServerGroup Name defined in CVP.System.SIP
 Server Groups%
```

**Step 9** Configure Incoming PSTN Sip Trunk Dial Peer

```
dial-peer voice 70000 voip
 description Incoming Call From PSTN SIP Trunk
 incoming called-number xxxx…… # Customer specific incoming called-number pattern
 voice-class sip rel1xx disable
 dtmf-relay rtp-nte h245-signal h245-alphanumeric
 codec g711ulaw
 no vad
```

**Step 10** Configure ASR TTS:

```
#Configure primary server
ip host asr-en-us <ASR server ip>
ip host tts-en-us <TTS server hostname>

voice class uri TTS sip
pattern tts@<TTS server ip>

voice class uri ASR sip
pattern asr@<ASR server hostname>

ivr asr-server sip:asr@<ASR server hostname*>
ivr tts-server sip:tts@<TTS server hostname*>

dial-peer voice 5 voip
description FOR ASR calls
preference1
session protocol sipv2
voice-class sip options-keepalive up-interval 12 down-interval 65 retry
2
session target ipv4:<ASR server IP>
destination uri ASR
dtmf-relay rtp-nte
codec g711ulaw
no vad

dial-peer voice 6 voip
description FOR TTS calls
```

```
preference1
session protocol sipv2
voice-class sip options-keepalive up-interval 12 down-interval 65 retry
2
session target ipv4:<TTS server IP>
destination uri TTS
dtmf-relay rtp-nte
codec g711ulaw
no vad

#Configure backup server
dial-peer voice 7 voip
destination uri ASR
session target ipv4:<ASR backup server IP>
session protocol sipv2
voice-class sip options-keepalive up-interval 12 down-interval 65 retry
2dtmf-relay rtp-nte
codec g711ulaw
preference 2
no vad

dial-peer voice 8 voip
destination uri TTS
session target ipv4:<TTS backup server IP>
session protocol sipv2
voice-class sip options-keepalive up-interval 12 down-interval 65 retry
2dtmf-relay rtp-nte
codec g711ulaw
preference 2
no vad
```

**Step 11** Configure SNMP

```
snmp-server community <string name> ro
```

**Step 12** Configure Back-office

**Note** Example here is for Internal number that is dialed is 82009999 and converting the Internal number to the PSTN number : 2142009999

**Example:**

```
voice translation-rule 2
rule 1 /^8200/ /214200

voice translation-profile Xform
translate called 2
```

**Note** Ensure that you configure dial-peers for each CVP server

```
dial-peer voice 2 voip
description out dial-peer CC pilot dial-peer
translation-profile outgoing Xform
destination-pattern 8200T
session protocol sipv2
session target ipv4:<IP address of CVP Server>
session transport tcp
voice-class codec 1
dtmf-relay rtp-nte
```

# Configure Cisco Unified Communications Manager

## Set Up Device Pool

Complete the following procedure to configure a device pool.

**Procedure**

**Step 1** Choose **System** > **device pool**.

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

**Step 3** Provide an appropriate device pool name in **Device Pool Name**.

**Step 4** Select a corresponding Call manager group in **Cisco Unified Communications Manager group**.

**Step 5** Select appropriate **Date/Time Group** and **Region**.

**Step 6** Select an appropriate Media resource group list in **Media Resource Group List.**

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

## Set Up Unified Communications Manager Groups

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

Before you configure a Unified Communications Manager Group, you must configure the Unified Communications Managers that you want to assign as members to that group.

**Procedure**

**Step 1** Login to the **Cisco Unified Communication Manager Administration** page, choose **System** > **Server**.

**Step 2** Make sure that you configure both the Publisher and Subscriber.

a) Click **Add New**.
b) Select appropriate Server Type Eg: CUCM Voice/Video Select **Next**.
c) Enter the **Host Name/IP Address**.
d) Click **Save**.

**Step 3** Choose **System** > **Cisco Unified CM**.

**Step 4** Click **Find**.

**Step 5** Make sure that you configured both the Publisher and Subscriber.

**Step 6** Choose **System** > **Cisco Unified CM Group**.

**Step 7** Add both Cisco Unified Communications Managers to the Default Unified Communications Manager Group. Select **Default** and from the Available Cisco unified communication managers select both Publisher and Subscriber to Selected Cisco Unified Communications Managers

**Step 8** Click **Save**.

## Set Up CTI Route Point

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

**Procedure**

**Step 1** Choose **Device** > **CTI Route Point**.

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

**Step 3** Use the wildcard string **XXXXX** to represent the digits of the dialed number configured on Unified CCE.

**Note** For example, the preconfigured dialed number in the Unified CCE for an agent phone is 10112.

**Step 4** Select the appropriate device pool.

**Step 5** Click **Save**.

## Set Up Trunk

Complete the following procedure to configure a trunk for the Unified CVP Servers.

**Procedure**

**Step 1** Choose **Device** > **Trunk**.

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

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

**Step 4** In the Device Name field, enter a name for the SIP trunk.

**Step 5** In the Description field, enter a description for the SIP trunk.

a) Enter the SIP Trunk name in the Device Name field.
b) Select the appropriate Device Pool.

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

**Step 7** In the Trunk Configuration window, enter the appropriate settings:

a) Uncheck the **Media Termination Point** Required check box.
b) Enter the **Destination Address**.
c) Select the appropriate SIP Trunk Security Profile
d) From the **SIP Profile** drop-down list, choose **Standard SIP Profile**.
e) From the DTMF Signaling Method drop-down list, choose **RFC 2833**.

**Step 8** Click **Save**.

# Set Up Application User

**Procedure**

**Step 1** Choose **User Management** > **Application User**.

**Step 2** In the Application User Configuration window, click **Add New**.

**Step 3** Enter the User ID that you entered in Set Up Enterprise Parameters , on page 167. Unified CCE defines the user ID as pguser.

**Step 4** Enter a **cisco** in the Password field of your choice.

**Note** If you change this user ID or password in Unified CCE, you must also change the Unified Communications Manager application user configuration.

**Note** To change the JTAPI password on the CUCM configuration page:

**a.** Open the peripheral Gateway Setup in PG Machine.

**b.** Edit the CUCM PG.

**c.** Set the same password for the user as previously set in Step 4.

**Step 5** Add the application user to the Standard CTI Enabled Group and Role:

a) Click **Add to Access Control Group**.
b) Select the **Standard CTI Enabled** group.
c) Select the **Standard CTI Allow Control of Phones supporting Connected Xfer and conf** group.
d) Select the **Standard CTI Allow Control of Phones supporting Rollover Mode** group.
e) Click **Add Selected**.
f) Click **Save**.

**Step 6** Associate the CTI route points and the phones with the application user.

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

# Set Up SIP Options

**Procedure**

**Step 1** Select **Device** > **Device Settings** > **SIP Profile**.

**Step 2** Enter values for the mandatory fields.

**Step 3** Select the **Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"** check box.

**Step 4** Associate this SIP profile on the trunk.

## Set Up Route Pattern

**Procedure**

**Step 1** Choose **Call Routing** > **Route Hunt** > **Route Pattern**.

**Step 2** Add a route pattern for the Unified CVP routing clients as follows:

a) Click **Add New**.
b) In the **Route Pattern** field, enter `7777777777!`
c) In the **Gateway/Route List** field, choose **SIPTRK_to_CVP_1**.
d) Click **Save**.

**Step 3** Add a route pattern for the Cisco Unified Communications Manager routing client.

a) Click **Add New**.
b) In the **Route Pattern** field, enter `8881111!`
c) In the **Gateway/Route List** field, choose **SIPTRK_to_CVP_1**.
d) Click **Save**.

**Note** These route patterns must match the network VRU label defined in Unified CCE.

## Set Up Conference Bridge

**Procedure**

**Step 1** Choose **Media Resources** > **Conference bridge**.

**Step 2** Add a conference bridge for each ingress/VXML combination gateway in the deployment.

**Step 3** In the Conference Bridge name field, enter a unique identifier for the conference bridge name that coincides with the configuration on the gateway.

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

**Step 5** Click **Apply Config**.

## Set Up Media Termination Point

**Procedure**

**Step 1** Choose **Media Resources** > **Media Termination Point**.

**Step 2** Add a media termination point for each ingress/VXML combo gateway in the deployment.

**Step 3** In the Media Termination Point Name field, enter a media termination point name for each ingress/VXML combo gateway in the deployment.

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

**Step 5** Click **Apply Config**.

## Set Up Transcoder

**Procedure**

**Step 1** Choose **Media Resources** > **Transcoder**.

**Step 2** Add a transcoder for each ingress/VXML combo gateway in the deployment.

**Step 3** In the Device Name field, enter a unique identifier for the transcoder that coincides with the configuration on the gateway.

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

**Step 5** Click **Apply Config**.

## Set Up Media Resource Group

Complete the following procedure to configure a media resource group for conference bridge, media termination point, and transcoder.

**Procedure**

**Step 1** Choose **Media Resources** > **Media Resource Group**.

**Step 2** Add a Media Resource Group for Conference Bridges.

**Step 3** Select all the hardware conference bridge resources configured for each ingress/VXML combination gateway in the deployment and add them to the group.

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

**Step 5** Choose **Media Resources** > **Media Resource Group**.

**Step 6** Add a Media Resource Group for Media Termination Point.

**Step 7** Select all the hardware media termination points configured for each ingress/VXML combination gateway in the deployment and add them to the group.

**Step 8** Click **Save**.

**Step 9** Choose **Media Resources** > **Media Resource Group**.

**Step 10** Add a Media Resource Group for Transcoder.

**Step 11** Select all the transcoders configured for each ingress/VXML combination gateway in the deployment and add them to the group.

**Step 12** Click **Save**.

## Set Up and Associate Media Resource Group List

Complete the following procedure to configure and associate a media resource group list. Add the media resource group list to the following devices and device pool.

**Procedure**

**Step 1** Choose **Media Resources** > **Media Resource Group List**.
**Step 2** Add a Media Resource Group list and associate all of the media resource groups.
**Step 3** Click **Save**.
**Step 4** Choose **System** > **Device Pool**.
**Step 5** Click **Default**.
**Step 6** From the Media Resource Group List drop-down list, choose the media resource group added in Step 2.
**Step 7** Click **Save**.
**Step 8** Click **Reset**.
**Step 9** Choose **Device** > **CTI Route Point**.
**Step 10** Click the configured CTI Route Point. For more information, see Set Up CTI Route Point , on page 163.
**Step 11** From the Media Resource Group List drop-down list, choose the media resource group added in Step 2
**Step 12** Click **Save**.
**Step 13** Click **Reset**.
**Step 14** Choose **Device** > **SIP Trunk**.
**Step 15** Click the configured SIP Trunk for. For more information, see Set Up Trunk , on page 163.
**Step 16** From the Media Resource Group List drop-down list, choose the media resource group added in Step 2
**Step 17** Click **Save**.
**Step 18** Click **Reset**.

## Set Up Enterprise Parameters

**Procedure**

**Step 1** Choose **System** > **Enterprise Parameter**.
**Step 2** Configure the Cluster Fully Qualified Domain Name.

**Example:**

ccm.cce.icm

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

## Configure Mobile Agent

Complete the following procedure to configure CTI ports for Unified Mobile Agent.

### Procedure

**Step 1** In Unified Communications Manager Administration, choose **Device** > **Phone**.

**Step 2** Click **Add a New Phone**.

**Step 3** Select **CTI Port** from the **Phone Type** drop-down list.

**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 example naming convention format LCPxxxxFyyyy:

a) LCP identifies the CTI Port as a local device.
b) xxxx is the peripheral ID for the Unified Communications Manager PIM.
c) yyyy is the local CTI Port.

The name LCP5000F0000 would represent CTI Port: 0 in a local CTI Port pool for the Unified Communications Manager PIM with the peripheral ID 5000.

**Step 6** In Description, enter text identifying the local CTI Port pool.

**Step 7** Use the **Device Pool** drop-down list to choose the device pool to which you want network CTIPort pool assigned. (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** When finished, click **Save** and **Close**.

**Step 12** Repeat the preceding steps to configure the network CTI Port pool.

**Step 13** In Device Name, enter a unique name for the local CTI Port pool name; click **OK** when finished.

Use the example naming convention format RCPxxxxFyyyy, where:

a) RCP identifies the CTI Port as a network device.
b) xxxx is the peripheral ID for the Unified Communications Manager PIM.
c) yyyy is the network CTI Port.

The name RCP5000F0000 would represent CTI Port: 0 in a network CTI Port pool for the Unified Communications Manager PIM with the peripheral ID 5000.

**Step 14** In Description, enter text identifying the network CTI Port pool.

**Step 15** Use the **Device Pool** drop-down list to choose the device pool to which you want network CTI Port pool assigned. (The device pool defines sets of common characteristics for devices.)

**Step 16** Click **Save**.

**Step 17** Highlight a record and select **Add a New DN**.

**Step 18** Add a unique directory number for the CTI port you just created.

**Step 19** When finished, click **Save** and **Close**.

## Configure Local Trunk

Complete the following procedure to configure Unified Communications Manager for Local Trunk.

**Procedure**

**Step 1** From Unified Communications Manager Administration choose **System** > **Location info** > **Location**.

**Step 2** Click **Find** to list the locations and add new ones with appropriate bandwidth (8000).

**Step 3** For the branch phones, configure each phone so that it is assigned the branch location for that phone.

a) Choose **Device > Phone**.
b) Click **Find** to list the phones.
c) Select a phone and set the Location field.

**Step 4** Verify that the Cisco AXL Web Service is started and that an Application User is defined and has a role of Standard AXL API Access.

a) Select **Cisco Unified Serviceability** from the **Navigation** drop-down list and click **Go**.
b) Navigate to **Tools** > **Control Center** > **Feature Services** .
c) Start the Cisco AXL Web Service, if it is not started.
d) From Unified Communications Manager Administration, choose **User Management > Application User**. Verify you have a user with the role of Standard AXL API Access, or create a new one and add that user to a group that has the role of Standard AXL API Access.

### Deploy SIP Trunk

Complete the following procedure to deploy the SIP trunk for local trunk:

**Procedure**

**Step 1** Using Unified Communications Manager, create a SIP trunk toward the SIP proxy server and select the Phantom location.

**Step 2** Create a SIP trunk for each ingress gateway and make the location of these ingress TDM-IP gateways the actual branch location.

**Step 3** Create a route pattern pointing the Network VRU Label of the Unified Communications Manager routing client to the SIP trunk toward the SIP proxy.

The SIP proxy should route the Network VRU label of the Unified Communications Manager routing client to the Unified CVP Servers.

**Step 4** For any IP-originated calls, associate the Unified Communications Manager route pattern with the SIP trunk.

**Step 5** Using the Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile > Trunk Specific Configuration > Reroute Incoming Request to new Trunk based on > Call-Info header with the purpose equal to x-cisco-origIP**.

**Step 6** Associate the new SIP profile with the SIP trunk and each ingress gateway.

## Configure Outbound Dialer

Complete the following procedure to configure Unified Communications Manager:

**Procedure**

**Step 1** Log in to the Unified Communications Manager administration page.

**Step 2** Select **Devices** > **Trunk**.

**Step 3** Create a SIP trunk to Outbound gateway.

## Configure A-Law Codec

Complete the following procedure to configure Unified Communications Manager.

**Procedure**

**Step 1** Click the **System**.

**Step 2** Select **Service Parameters**.

**Step 3** Select a Server.

**Step 4** Select the service as **Cisco Call Manager(Active)**.

**Step 5** Under Clusterwide Parameters (system-location and region), ensure the following:

- **G.711 A-law Codec Enabled** is **Enabled**.
- **G7.11 mu-law Codec Enabled** to **Disabled**.

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

## Configure Support for Multiline Agent Control

To enable reporting and control of secondary lines, follow these configuration steps on Unified Communications Manager. This is required for deployments that have agents using phones that require Join Across Line (JAL) to be enabled.

**Note** Use of JAL and DTAL phone features is deprecated. Do not use these features in new deployments.

Multiline Agent Control supports a maximum of four lines per phone, one ACD line and up to three non-ACD lines.

**Note** Unified CCE supports shared lines for ACD lines but does not support for Non ACD lines.

Several agents cannot share a common extension on their phones. However, one agent can have two phones that share a common second line. The agent cannot sign in on both phones at the same time.

### Procedure

**Step 1** Enable the Application User for the agent peripheral with the role of **Standard CTI Allow Control of Phones supporting Connected Xfer and conf** to support phones that require Join Across Line setting.

**Step 2** Configure all agent phones with the following parameters:

- **Busy Trigger: 1**
- **Maximum Number of Calls: 2**

## Configure Caller-Specific Music on Hold

### Upload audio file

Follow this procedure to upload an audio file in an existing node or new node in a Cisco Unified Communications Manager cluster.

If you are uploading to a new node, you must first configure a new and dedicated Music on Hold node that can have only two Cisco Unified Communications Manager services running: Cisco Call Manager, and Cisco IP Voice Media Streaming Application. Additionally, the Cisco IP Voice Media Streaming Application service must be deactivated in all of the other nodes in the Cisco Unified Communications Manager cluster that contains the dedicated Music on Hold node. For more information, see Installing Cisco Unified Communications Manager.

#### Procedure

**Step 1** Log in to the Cisco Unified Communications Manager Administration page.

**Step 2** Click the **Media resources** tab, and then click **MOH Audio File Management**.

**Step 3** In the MOH Audio File Management page, click **Upload File**.

**Step 4** In the Upload File window, click **Browse**, select the audio file that you want to set for Music on Hold, and then click **Open**.

**Step 5** Click **Upload File**.

The audio file is now available for use as a Music on Hold audio source.

#### What to do next

Configure the uploaded audio file so that it can be used as an audio source for Music on Hold.

### Configure audio source

#### Procedure

**Step 1** In the Cisco Unified Communications Manager Administration page, click **Media resources** tab, and then click **Music On Hold Audio Source**.

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

**Step 3** In the MOH Audio Stream Number field, enter a number that you want to assign to the audio file. You cannot choose a number that has already been assigned to another audio file.

**Step 4** In the MOH Audio Source file drop-down menu, choose the audio file that you want to configure as the MoH audio source.

**Step 5** (Optional) The MOH Audio Source Name field automatically populates the name of the audio file that you chose in the previous step. You can edit the name of the audio file that you selected.

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

#### What to do next

Configure the audio source in the Unified CCE routing script.

### Configure Unified CCE routing script

#### Procedure

**Step 1** Log in to the Unified CCE Administrator workstation.

**Step 2** Open the Script Editor.

**Step 3** Open the script in which you want to set the caller specific Music on Hold.

**Step 4** Set the call variable *SIPHeader* with the value `X-cisco-moh-source~mod~<User Hold MoH Audio File number>,<Network Hold MoH Audio File number>.`

**Example:**

For example, X-cisco-moh-source~mod~6,7; where 6 and 7 are the numbers that you assigned to the audio file. In this example, the audio file assigned for number 6 is played when the call is placed on user hold, and the audio file assigned for number 7 is played when the call is placed on network hold.

**Note**

- List the new call variable after a Dialed Number (DN) or CallingLineID node. This ensures that the call is for a particular DN, or from a particular Calling Line ID.
- If only one audio file is specified, the same file is used for both user hold and network hold.
- If the audio stream that you specified is not present in the Cisco Unified Communications Manager cluster, then the default Music on Hold of the device plays.

**Step 5** Click **Save**.

The audio file is now configured as the source audio file that will play for caller specific Music on Hold.

# Configure Cisco Finesse

## Configure Contact Center Enterprise CTI Server Settings

Configure the A Side and B Side CTI servers on the primary Finesse server.

**Procedure**

**Step 1** If you are not already signed in, sign in to the administration console on the primary Finesse server:

https://FQDN of Finesse server/cfadmin

**Step 2** Sign in with the Application User credentials defined during installation.

**Step 3** In the Contact Center Enterprise CTI Server Settings area, enter the CTI server settings as described in the following table. Refer to your configuration worksheet if necessary.

| Field | Description |
|---|---|
| A Side Host/IP Address | Enter the hostname or IP address of the A Side CTI server.<br>This value is typically the IP address of the Peripheral Gateway (PG). The CTI server runs on the PG. |
| A Side Port | Enter the port number of the A Side CTI server. The value of this field must match the port configured during the setup of the A Side CTI server. |
| Peripheral ID | Enter the ID of the Agent PG Routing Client (PIM).<br>The Agent PG Peripheral ID should be configured to the same value for the A Side and B Side CTI servers. |
| B Side Host/IP Address | Enter the hostname or IP address of the B Side CTI server. |
| B Side Port | Enter the port of the B Side CTI server. The value of this field must match the port configured during the setup of the B Side CTI server. |
| Enable SSL encryption | Check this box to enable secure encryption. |

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

## Configure Contact Center Enterprise Administration and Data Server Settings

Configure the Contact Center Enterprise Administration & Data Server settings to enable authentication for Cisco Finesse agents and supervisors.

**Note** If you are using HTTPS, the first time you access the administration console, you see a browser security warning. To eliminate browser security warnings each time you sign in, you can trust the self-signed certificate provided with Finesse or obtain and upload a CA certificate.

**Procedure**

**Step 1** Sign in to the administration console.

**Step 2** In the Contact Center Enterprise Administration & Data Server Settings area, enter the Administration & Data Server settings as described in the following table. Refer to your configuration worksheet if necessary.

| Field | Description |
|---|---|
| Primary Host/IP Address | The hostname or IP address of the Unified CCE Administration & Data Server. For example, **abcd12-5-aw-a**. |
| Backup Host/IP Address | The hostname or IP address of the backup Unified CCE Administration & Data Server. For example, **abcd12-5-aw-b**. |
| Database Port | The port of the Unified CCE Administration & Data Server.<br>The default value is 1433.<br>**Note** Cisco Finesse expects the primary and backup Administration & Data Server ports to be the same, hence the Finesse administration console exposes one port field. You must ensure that the port is the same for the primary and backup Administration & Data Servers. |
| AW Database Name | The name of the AW Database (AWDB). For example, **ucceinstance_awdb**. |
| Domain | The domain name of the AWDB. For example, **cisco.com**. |
| Username | The username required to sign in to the AWDB.<br>**Note** If you specify a domain, this user refers to the Administrator Domain user that the AWDB uses to synchronize with the logger. In which case, the AWDB server must use Windows authentication and the configured username must be a domain user.<br>If you do not specify a domain, this user must be an SQL user. |
| Password | The password required to sign in to the AWDB. |

**Step 3** Click **Save**.

## Configure Cluster Settings

Configure the cluster settings for the secondary Finesse node. The secondary Finesse node handles agent requests if the primary server goes down.

### Procedure

**Step 1** If you are not already signed in the primary node, sign in to the administration console of the primary node with the Application User credentials.

**Step 2** In the Cluster Settings area, in the Hostname field, enter the hostname of the secondary Finesse server.

**Step 3** Click **Save**.

## Restart Cisco Finesse Tomcat

After you make changes to the Contact Center Enterprise CTI Server, Contact Center Enterprise Administration & Data Server, or cluster settings, restart Cisco Finesse Tomcat for the changes to take effect.

**Note** After you restart Finesse, it can take approximately 6 minutes for all server-related services to restart. Therefore, you wait 6 minutes before you attempt to access the Finesse administration console.

### Procedure

**Step 1** Access the CLI and run the following command:

**utils service restart Cisco Finesse Tomcat**

**Step 2** You can enter the command **utils service list** to monitor the Cisco Finesse Tomcat Service. After Cisco Finesse Tomcat changes to STARTED, the configured agents can sign in to the desktop.

## Check Replication Status

### Procedure

**Step 1** Access the CLI on the primary Finesse server.

**Step 2** Sign in with the Administrator User credentials that are defined during installation.

**Step 3** Run the following command:

**utils dbreplication runtimestate**

This command returns the replication status on both the primary and secondary Finesse servers.

## Ensure Agents Have Passwords

Agents who do not have a password defined in Unified CCE Configuration Manager cannot sign in to Finesse.

Agent password is an optional field in Unified CCE, but it is mandatory for Cisco Finesse.

For agents who do not have passwords, you must perform the following steps:

### Procedure

**Step 1** Launch Unified CCE Configuration Manager.

**Step 2** Locate the record for the agent (Agent Explorer > Agent tab).

**Step 3** Enter a password, and save the record.

## Ensure Logout Non-Activity Time for Agents is Configured

The Logout non-activity time specifies how long an agent can remain inactive in the Not Ready state before that agent is signed out of Finesse.

For agents who use the Task Routing interface on Finesse for non-voice tasks, set the Logout non-activity time to blank.

Perform the following steps to configure Logout non-activity time for an agent.

### Procedure

**Step 1** Launch the Unified CCE Configuration Manager.

**Step 2** Launch Agent Desk Settings List (**Tools** > **List Tools**).

**Step 3** Select **Agent Desk Settings List**.

**Step 4** In the Logout non-activity time field, enter the number of seconds of agent inactivity while in the Not Ready state before the system software signs the agent out. You can enter a value between 10 seconds and 7200 seconds.

**Step 5** Click **Save**.

The modified settings are applied to all of the agents who use these agent desktop settings.

## Ensure Agents Can Sign in to Desktop

After the system administrator defines configuration settings and restarts services, agents who have passwords and operational handsets can sign in to the Finesse Agent Desktop.

**Note** Finesse agents can enter either their `AgentID` or `Login name` (in the **Username** field of the desktop login screen) to sign in. Ensure that each agent's `AgentID` and `Login name` are unique across both sets of data. If one agent's `AgentID` matches another agent's `Login name`, neither agent can sign in.

**Note** After you restart Finesse, it takes approximately 6 minutes for all server-related services to restart. Therefore, you should wait 6 minutes before you attempt to sign in to the desktop.

**Note** If you are using HTTPS, the first time you access the agent desktop, you see a browser security warning. To eliminate browser security warnings each time you sign in, you can trust the self-signed certificate provided with Finesse or obtain and upload a CA certificate.

**Procedure**

**Step 1** Enter the following URL in the address bar of your browser:

http://*FQDN of Finesse server*/desktop

**Step 2** If you installed the language pack ES file, you can select the language you want to appear on the desktop from the language selector drop-down list. If you did not install the language pack ES file, the language selector drop-down list does not appear in the user interface.

**Note** If you installed the language pack ES file, you can also select a language by passing the locale as part of the URL (for example, http://*FQDN of Finesse server*/desktop?locale=fr_FR) or by changing your browser preferred language. The default language is English (en_US).

**Step 3** Enter your Username, Password, and Extension, and then click **Sign In**.

If your agent is signed into the Agent Desktop in Single Sign-On Mode or Hybrid Mode, refer to the sections *Sign In to Finesse Desktop Single Sign-On Mode* or *Sign In to Finesse Desktop Hybrid Mode* in the *Cisco Finesse Desktop User Guide for Unified Contact Center Enterprise.*

## Obtain and Upload CA Certificate

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

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

To eliminate browser security warnings each time you sign in, obtain an application and root certificate signed by a Certificate Authority (CA). Use the Certificate Management utility from Cisco Unified Communications Operating System Administration.

To open Cisco Unified Communications Operating System Administration, enter the following URL in your browser:

https://*hostname of primary UCCX server*/cmplatform

Sign in using the username and password for the Application User account created during the installation of Finesse.

**Note** You can find detailed explanations in the Security topics of the *Cisco Unified Communications Operating System Administration Online Help*.

**Procedure**

**Step 1** Generate a CSR.

a) Select **Security** > **Certificate Management** > **Generate CSR**.

b) From the **Certificate Name** drop-down list, select **tomcat**.
c) Click **Generate CSR**.

**Note** To avoid certificate exception warnings, you must access the servers using the Fully Qualified Domain Name (FQDN).

**Step 2** Download the CSR.

a) Select **Security** > **Certificate Management** > **Download CSR**.
b) From the **Certificate Name** drop-down list, select **tomcat**.
c) Click **Download CSR**.

**Step 3** Generate and download a CSR for the secondary Finesse server.

To open Cisco Unified Operating System Administration for the secondary server, enter the following URL in the address bar of your browser:

https://*hostname of secondary UCCX server*/cmplatform

**Step 4** Use the CSRs to obtain the CA root certificate, intermediate certificate, and signed application certificate from the Certificate Authority.

**Note** To set up the certificate chain correctly, you must upload the certificates in the order described in the following steps.

**Step 5** When you receive the certificates, select **Security** > **Certificate Management** > **Upload Certificate**.

**Step 6** Upload the root certificate.

a) From the **Certificate Purpose** drop-down list, select **tomcat-trust**.
b) In the **Upload File** field, click **Browse** and browse to the root certificate file.
c) Click **Upload File**.

**Step 7** Upload the intermediate certificate.

a) From the **Certificate Purpose** drop-down list, select **tomcat-trust**.
b) In the **Upload File** field, click **Browse** and browse to the intermediate certificate file.
c) Click **Upload File**.

**Step 8** Upload the application certificate.

a) From the **Certificate Purpose** drop-down list, select **tomcat**.
b) In the **Upload File** field, click **Browse** and browse to the application certificate file.
c) Click **Upload File**.

**Step 9** After the upload is complete, sign out from the Platform Admin page of Finesse.

**Step 10** Restart Cisco Tomcat on the primary Unified CCX node.

**Step 11** Restart Cisco Finesse Tomcat on the primary Unified CCX node.

**Step 12** Restart Cisco Unified Intelligence Center Reporting Service.

**Step 13** Restart Unified CCX Notification Service.

**Note** It is recommended to delete the self-signed certificates from the clients certificate store. Then close the browser, relaunch, and reauthenticate.

**Step 14** Upload the application certificate to the secondary Unified CCX server.

You do not need to upload the root and intermediate certificates to the secondary Unified CCX server. After you upload these certificates to the primary server, they are replicated to the secondary server.

**Step 15** Restart Cisco Tomcat and Cisco Finesse Tomcat on the secondary Unified CCX node.

## Deploy Certificate in Browsers

### Download CA certificate

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

**Procedure**

**Step 1** On the Windows domain controller, run the CLI command certutil -ca.cert *ca_name*.cer, in which *ca_name* is the name of your certificate.

**Step 2** Save the file. Note where you saved the file so you can retrieve it later.

### Set Up CA Certificate for Firefox Browser

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

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

**Procedure**

**Step 1** From the Firefox browser menu, select **Options**.

**Step 2** Click **Advanced**.

**Step 3** Click the **Certificates** tab.

**Step 4** Click **View Certificates**.

**Step 5** Click **Authorities**.

**Step 6** Click **Import** and browse to the *ca_name*.cer file (in which *ca_name* is the name of your certificate).

**Step 7** Check the **Validate Identical Certificates** check box.

**Step 8** Restart the browser for certificate installation to take effect.

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

**Procedure**

**Step 1** In the browser, go to **Settings**.

**Step 2** In the Chrome browser, select **Advanced Settings** > **Privacy and Security**, click **Manage Certificates**.

**Step 3** In the Microsoft Edge browser, select **Privacy, search, and services**. Under **Security**, click **Manage Certificates**.

**Step 4** Click **Trusted Root Certification Authorities** tab.

**Step 5** Click **Import** and browse to the *ca_name*.cer file.
In the **Trusted Root Certification Authorities** tab, ensure that the new certificate appears in the list.

**Step 6** Restart the browser for the certificate to install.

## Accept Security Certificates

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

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

#### Install certificates on Windows operating system:

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

**Firefox**

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

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

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

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

**Chrome and Edge Chromium (Microsoft Edge)**

1. A page appears that states your connection is not private. To open the Finesse sign in page,

In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.

2. Enter your agent ID or username, password, and extension, and then click **Sign In**.
3. In the **SSL Certificate Not Accepted** dialog box, click the certificate link. A browser tab opens for the certificate that you must accept.
4. On the browser tab,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.

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

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

5. Click on the certificate error that appears in the address bar and then,

   In Chrome, select **Certificate (Invalid)**.

   In Microsoft Edge, select **Certificate (not valid)**.

   The **Certificate** dialog box appears.
6. In the **Details** tab, click **Copy to File**. The **Certificate Export Wizard** appears.
7. Click **Next**.
8. Keep the default selection **DER encoded binary X.509 (.CER)** and click **Next**.
9. Click **Browse** and select the folder in which you want to save the certificate, enter a recognizable file name and click **Save**.
10. Browse to the folder where you have saved the certificate (**.cer** file), right-click on the file, and click **Install Certificate**. The **Certificate Import Wizard** appears.
11. Keep the default selection **Current User** and click **Next**.
12. Select **Place all certificates in the following store** and click **Browse**. The **Select Certificate Store** dialog box appears.
13. Select **Trusted Root Certification Authorities** and click **OK**.
14. Click **Next** and then click **Finish**. A **Security Warning** dialog box appears that asks if you want to install the certificate.
15. Click **Yes**. A **Certificate Import** dialog box that states the import was successful appears.

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

### Install certificates on macOS:

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

**Chrome and Edge Chromium (Microsoft Edge)**

1. A warning page appears which states that your connection is not private. To open the Finesse Console sign in page,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.
2. Click on the certificate error that appears in the address bar and then,

   In Chrome, select **Certificate (Invalid)**.

   In Microsoft Edge, select **Certificate (Not Valid)**.

   A certificate dialog box appears with the certificate details.
3. Drag the **Certificate** icon to the desktop.
4. Double-click the certificate. The **Keychain Access** application opens.
5. In the right pane of Keychains dialog, browse to the certificate, right-click on the certificate, and select **Get Info** from the options that are listed. A dialog appears with more information about the certificate.
6. Expand **Trust**. From the **When using this certificate** drop-down, select **Always Trust**.
7. Close the dialog box that has more information about the certificate. A confirmation dialog box appears.
8. Authenticate the modification of Keychains by providing a password.
9. The certificate is now trusted, and the certificate error does not appear on the address bar.

**Firefox**

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

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

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

## Browser Settings for Firefox

Complete the following steps to ensure Finesse responds as expected when it is not the active window:

**Procedure**

**Step 1** Open Firefox and enter **about:config** in the address bar.
**Step 2** On the warranty page, click **I accept the risk!**.
**Step 3** In the **Search** field, enter `dom.disable_window_flip`.
**Step 4** Double-click **dom.disable_window_flip** to set the value to *false*.
**Step 5** Restart Firefox.

## Browser Settings for Chrome

Ensure that you disable the **Automatic tab discarding** feature in Chrome (version 74 and earlier) to avoid exiting the Finesse desktop tab when the system memory is low.

**Procedure**

**Step 1** Open Chrome and enter **chrome://flags/#automatic-tab-discarding** in the address bar.
**Step 2** Press **Enter**.
**Step 3** Select **Disabled** from the drop-down list.
**Step 4** Click **Relaunch Now**.

## Configure DNS on Clients

**Note** This procedure is required for uncommon environments where non-hierarchical DNS configuration exists. If your environment has hierarchical DNS configuration, you do not need to perform this procedure. This procedure applies to clients that use a Windows operating system. For information about configuring DNS on Mac clients, see your Apple documentation (www.apple.com/mac).

Configuring DNS on client computers allows the clients to resolve the fully-qualified domain name (FQDN) of the active Finesse server during a failover.

**Procedure**

**Step 1** Go to **Control Panel** > **Network and Internet** > **Network and Sharing Center**. (Open the Control Panel, enter Network Connections in the search bar, and then click **View network connections**.)
**Step 2** Click the appropriate network connection.
A dialog box showing the status of the connection appears.

**Step 3** Click **Properties**.

**Step 4** On the Networking tab, select Internet protocol version 4 (TCP/IPv4) or Internet protocol version 6 (TCP/IPv6) if the client is IPV6, and then click **Properties**.

**Step 5** Click **Advanced**.

**Step 6** On the DNS tab, under DNS server addresses, in order of use, click **Add**.

**Step 7** Enter the IP address of the DNS server that was entered during installation and click **Add**.

**Step 8** If a secondary DNS was entered during installation, repeat Step 5 and Step 6 to add its IP address.

## Live Data Reports

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

### Prerequisites for Live Data

Before you add Live Data reports to the desktop, you must meet the following prerequisites:

- You must have the Live Data reports configured and working in Cisco Unified Intelligence Center.
- You must use either HTTP or HTTPS for both Cisco Unified Intelligence Center and Finesse. You cannot use HTTP for one and HTTPS for the other. The default setting for both after a fresh installation is HTTPS. If you want to use HTTP, you must enable it on both Cisco Unified Intelligence Center and Finesse. For information about enabling HTTP for Cisco Unified Intelligence Center, see the *Administration Console User Guide for Cisco Unified Intelligence Center* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.
- Ensure that user integration synchronization is enabled for Cisco Unified Intelligence Center. For more information, see the *Administration Console User Guide for Cisco Unified Intelligence Center* .
- If your deployment uses HTTPS, you must upload security certificates to the Finesse, Cisco Unified Intelligence Center, and Live Data servers depending your deployment:

| On Server | Import Certificates From |
|---|---|
| Finesse | Live Data and Cisco Unified Intelligence Center |
| Live Data | None required |
| Cisco Unified Intelligence Center | Live Data |

Finesse, Cisco Unified Intelligence Center, and Live Data are installed with self-signed certificates. However, if you use the self-signed certificates, agents and supervisors must accept certificates in the Finesse desktop when they sign in before they can use the Live Data gadget. To avoid this requirement, you can provide a CA certificate instead. You can obtain a CA certificate from a third-party certificate vendor or produce one internal to your organization.

### Add Live Data Reports to Finesse

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

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

## *Add Live Data Reports to Default Desktop Layout*

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

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

### Procedure

**Step 1** Sign in to the Finesse administration console (`https://`*`FQDN of Finesse server:Port Number(8445)`*`/cfadmin`), in which FQDN refers to the fully qualified domain name.

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

**Step 3** Remove the comment characters (<!-- and -->) from each report that you want to add to the desktop layout. Make sure you choose the reports that match the method your agents use to access the Finesse desktop (HTTP or HTTPS).

**Step 4** Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

**Step 5** Optionally, change the gadget height.

**Example:**

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

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
        gadgetHeight=400&viewId_1=99E6C8E2100001410000000D80A0006C4&
        filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
        filterId_2=agent.id=CL%20teamName
        </gadget>
```

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

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

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

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

## *Add Live Data Reports to Custom Desktop Layout*

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

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

### Procedure

**Step 1** Sign in to the Finesse administration console.

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

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

**Step 4** Copy the XML code for the report you want to add from the Finesse default layout XML. If your agents use HTTP to access Finesse, copy the XML code for the HTTP report. If they use HTTPS, copy the XML code for the HTTPS report.

**Example:**

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

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

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

**Example:**

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

```
<layout>
  <role>Agent</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
  </page>
  <tabs>
    <tab>
      <id>home</id>
      <label>finesse.container.tabs.agent.homeLabel</label>
      <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
```

```
                gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&
                filterId_1=agent.id=CL%20teamName&
                viewId_2=9AB7848B10000141000001C50A0006C4&
                filterId_2=agent.id=CL%20teamName
      </gadget>
    </tab>
    <tab>
      <id>manageCall</id>
      <label>finesse.container.tabs.agent.manageCallLabel</label>
    </tab>
  </tabs>
</layout>
```

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

**Step 7** Optionally, change the gadget height.

**Example:**

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

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

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

**Step 8** Click **Save**.

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

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

## *Add Live Data Reports to Team Layout*

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

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

### Procedure

**Step 1** Sign in to the Finesse administration console.

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

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

**Step 4** Copy the XML code for the report you want to add from the Finesse default layout XML. If your agents use HTTP to access Finesse, copy the XML code for the HTTP report. If they use HTTPS, copy the XML code for the HTTPS report.

**Example:**

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

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

**Step 5** Click the **Team Resources** tab.

**Step 6** Select the team from the list of teams for which you want to add the report.

**Step 7** In the Resources for <team name> area, click the **Desktop Layout** tab.

**Step 8** Check the **Override System Default** check box.

**Step 9** Paste the XML within the tab tags where you want it to appear.

**Example:**

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

```
<layout>
  <role>Agent</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
  </page>
  <tabs>
    <tab>
      <id>home</id>
      <label>finesse.container.tabs.agent.homeLabel</label>
      <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
              gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&
              filterId_1=agent.id=CL%20teamName&
              viewId_2=9AB7848B10000141000001C50A0006C4&
              filterId_2=agent.id=CL%20teamName
      </gadget>
    </tab>
    <tab>
      <id>manageCall</id>
      <label>finesse.container.tabs.agent.manageCallLabel</label>
    </tab>
  </tabs>
</layout>
```

**Step 10** Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

**Step 11** Optionally, change the gadget height.

**Example:**

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

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

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

**Step 12** Click **Save**.

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

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

### *Modify Live Data Stock Reports for Finesse*

This procedure describes how to modify the Live Data stock reports in Cisco Unified Intelligence Center and add the modified report to the Finesse desktop layout. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.

**Note** To make sure the modified gadget renders in the Finesse desktop, you must give the appropriate permission for that report in Cisco Unified Intelligence Center.

**Procedure**

**Step 1** Sign in to the Finesse administration console.

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

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

**Step 4** Copy the gadget URL for the report you want to modify from the Finesse default layout XML and paste it into a text editor.

**Example:**

If you want to modify the Agent Report for HTTPS, copy the following URL and paste it into a text editor:

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

**Step 5** In Cisco Unified Intelligence Center, in Edit view of the report, select the view for which you want to create a gadget URL and then click **Links**.

The HTML Link field displays the permalink of the customized report.

**Step 6** Copy the permalink of the customized report from the **HTML Link** field, and paste it in a text editor. Then copy the viewId value from this link into the desired view.

**Example:**

Copy the viewId, which is underlined in this example, from the permalink for the report.

```
https://<Server Name>:8444/cuic/permalink/PermalinkViewer.htmx?
viewId=5C90012F10000140000000830A4E5B33&linkType=htmlType&viewType=Grid
```

**Step 7** Replace the desired viewId value in the gadget URL with the viewId value from the permalink of the customized report.

**Step 8** Replace my-cuic-server with the FQDN of the Cisco Unified Intelligence Center Server.

**Step 9** Add the customized gadget URL to the desktop layout XML in the Manage Desktop Layout gadget and click **Save**.

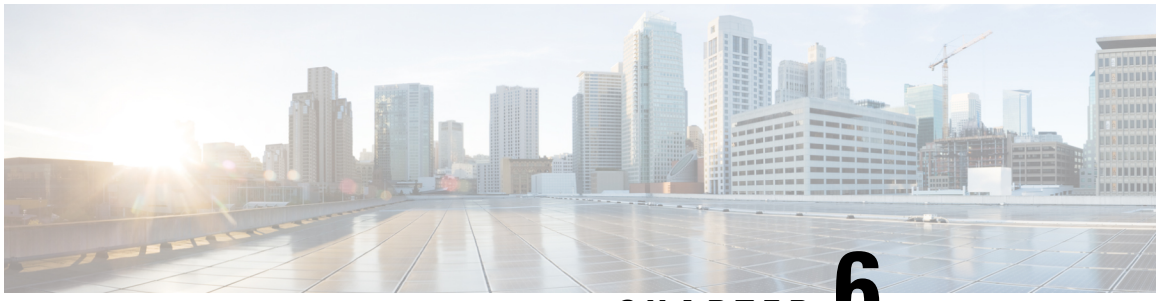
**Note** After you add the gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with a large number of rows, you may want to adjust the gadget height or the screen resolution on the computer used to access the desktop to make the report easier to read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

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

## Initial Configuration Troubleshooting

| If | Then |
|---|---|
| The administration console does not load after a fresh installation. | 1. Clear your browser cache (delete browsing history and cookies).<br>2. If the problem persists, restart the Cisco Finesse Tomcat service or restart the Finesse server. |

| If | Then |
|---|---|
| Agents cannot sign in to the desktop after a fresh installation. | **1.** Verify that a valid domain was configured during installation and that forward and reverse DNS are set up correctly. To check whether DNS was configured during installation, check the install.log for the following:<br>InstallWizard\|USER_ACTION_BTN_PUSH: Screen = DNS Client Configuration, button pushed = No\|<LVL::Info<br>The preceding message indicates that DNS was not configured during the installation. Reinstall Finesse and configure the DNS with a valid domain.<br>**2.** Verify that the agent is configured in Unified CCE.<br>**3.** Verify that the AWDB is configured correctly.<br>**a.** Check the realm.log for the following line:<br>"ERROR com.cisco.ccbu.finesse.realms.ccerealm.CCERealmConfig - Cannot connect to any AWDB! Ensure that at least one AWDB is configured properly and running!"<br>This line indicates that Finesse cannot connect to the AWDB.<br>**b.** Check that the values entered in the Contact Center Enterprise Administration & Data Server Settings gadget are correct.<br>• Verify that the username entered is a Windows domain user.<br>• Verify that the username is not prepended with the domain (for example, domain\username).<br>• Verify that the port configured is open to the Finesse server.<br>**c.** Check that the AWDB is set up correctly and running.<br>• The AWDB SQL server must use Windows authentication.<br>• Verify that the AWDB server is up and that the Distributor service is running.<br>**4.** Restart Cisco Finesse Tomcat on the primary and secondary Finesse servers.<br>**5.** Verify that the agent's device is properly configured in Unified Communications Manager and is active. |



CHAPTER 6

# Upgrade Overview


- Upgrade Overview, on page 193
- Multistage Upgrade Workflow for 2000 Agents Deployment, on page 196
- Multistage Upgrade Workflow for 4000 Agents and above Deployments, on page 209
- Data Migration Considerations, on page 223
- Enable and Disable TDE on a Database, on page 225
- Silent Upgrade, on page 226
- Unified CCE Upgrade Overview, on page 226
- Upgrade Cloud Connect, on page 228


## Upgrade Overview

### Unified CCE Redundant Central Controller Upgrade Flow

The Unified CCE central controller consists of the Logger, Router, and Administration & Data Server. When upgrading the Unified CCE portion of your Cisco Contact Center, the central controller is upgraded before the other Unified CCE components. While one side (Side A or B) of the redundant system is being upgraded, the other side (Side A or B) operates in stand-alone mode.

For redundant systems, the general flow for upgrading the Unified CCE central controller is as follows:

1. Upgrade the Side A Logger and Router along with the Administration & Data Server identified to be upgraded first to verify operations on the upgraded Side A Logger and Router.
2. Bring Side A into service and verify the operation. Side B is brought down as Side A is coming into service along with other non-upgraded Administration & Data Server(s).
3. Upgrade the Side B Logger and Router along with remaining Administration & Data Server(s).
4. Bring Side B into service and verify that duplexed operation begins.

**Note** For better performance, Media Routing PG (MR PG), Dialer, and Agent PG should be on the same VM.

### Update VM Properties

Rather than re-create the VMs in the new version of the OVA, you can manually update the VM properties to match the new OVA. Before you upgrade the Unified CCE or Cloud Connect components, update the properties of each VM to match the appropriate OVA, as follows:

1. Stop the VM.
2. Update the properties of each VM to match the properties of the appropriate OVA. Check the *Virtualization for Unified Contact Center Enterprise* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html for descriptions of each OVA. Save your changes.

   See https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-cloud-connect.html for details on Cloud Connect.
3. Restart the VM.

**Caution** Be careful when you upgrade the virtual machine network adapters. Done incorrectly, this upgrade can compromise the fault tolerance of your Cisco Contact Center.

### SQL Security Hardening

You can optionally apply SQL security hardening when running the installer. If your company employs custom security policies, bypass this option. Most other deployments benefit from SQL security hardening.

**Note** During Unified CCE installation on to Windows Server 2019 and SQL Server 2019, you should not select SQL Server Security Hardening optional configuration as a part of the installation. You can apply the SQL Security Hardening post installation using the Security Wizard tool.

For more information about SQL security hardening, see the *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

### Self-signed Certificate for Unified CCE Web Application

**Note** As part of the upgrade of Unified CCE servers, self-signed certificates employed by Unified CCE web applications such as Unified CCE web administration tool and Websetup, may get regenerated. You must add the new certificates to the trust list on the appropriate end devices.

### Upgrade Tools

During the upgrade process, use the following tools as required:

- ICM-CCE-Installer—The main Unified CCE installer. It copies all files into relevant folders, creates the base registries, and installs needed third-party software such as JRE, Apache Tomcat, and Microsoft .NET Framework.

**Note** Optionally, you can update the JRE installed by the Unified CCE Installer with a later version of the JRE. See Java Upgrades, on page 58.

If the ICM-CCE installer installs JRE on the Windows platform, the system retains only the Cisco approved CA certificates in the java certificate store, and removes all the unapproved certificates.

Optionally, update the Apache Tomcat software. See Install Tomcat, on page 60.

You cannot run the installer remotely. Mount the installer ISO file only to a local machine.

- Cisco Unified Intelligent Contact Management Database Administration (ICMDBA) Tool—Used to create new databases, modify or delete existing databases, and perform limited SQL Server configuration tasks.
- Domain Manager—Used to provision Active Directory.
- Web Setup—Used to set up the Call Routers, Loggers, and Administration & Data Servers.
- Peripheral Gateway Setup—Used to set up PGs, the CTI server, and the Outbound Option dialer.

- ICM12.6.2.exe—The Unified CCE patch installer. It copies all files into relevant folders, updates the registries, and installs needed third-party software such as JRE, Apache Tomcat, and Microsoft .NET Framework.
- AdminClientInstaller—Installs the Administration Client on a system that is not running other Unified CCE components.

  The AdminClientInstaller is delivered on the installation media with the installer.
- Administration Client Setup—Used to add, edit, or remove Administration Clients and Administration Client Instances.

  The Administration Client Setup is delivered on the installation media with the installer.
- Enhanced Database Migration Tool (EDMT)—A wizard application that is used for all upgrades to migrate the HDS, Logger, and BA databases during the upgrade process.

  You can download the EDMT from Cisco.com by clicking **Cisco Enhanced Data Migration Tool Software Releases**.

  The prerequisites for running EDMT are:

  - EDMT requires Microsoft® ODBC Driver 17 for SQL Server® and Visual C++ Redistributable for Visual Studio 2015 (or higher). The latest version of these packages can be downloaded from the Microsoft website. However, a copy of the same is also available in the **Prerequisites** folder of EDMT.

  The EDMT displays status messages during the migration process, including warnings and errors. Warnings are displayed for informational purposes only and do not stop the migration. On the other hand, errors stop the migration process and leave the database in a corrupt state. If an error occurs, restore the database from your backup, fix the error, and run the tool again.

**Note**

- You can select either **SQL Server Authentication** or **Windows Authentication** during database migration. In certain scenarios, for example, where the source and destination machines are in different domains, **SQL Server Authentication** can be used.
- If you are configuring SQL services to run as Virtual account (NT SERVICE) or Network Service account (NT AUTHORITY\NETWORK SERVICE), you must run EDMT as an administrator.
- The installer, not the EDMT, upgrades the AW database for the Administration & Data Server.

- User Migration Tool—A standalone Windows command-line application that is used for all upgrades that involve a change of domain. The tool imports the previously exported user accounts into the target domain during the upgrade.

  You can download the User Migration Tool from Cisco.com by clicking **ICM User Migration Tool Software**.

**Note** User Migration Tool cannot be used for migrating users that are SSO enabled.

- Regutil Tool—Used in Technology Refresh upgrades, exports the Cisco Systems, Inc. registry in the source machine during the preupgrade process. The output of the tool is required on the destination machine when running the Unified CCE Installer during the upgrade process.

  You can download the Regutil Tool from Cisco.com by clicking **Contact Center Enterprise Tools**.

- My Cisco Entitlements (MCE)—You can order software for upgrades in MCE if you have a valid SWSS or Flex contract. It is a secure one-stop platform where you can gain insights into your business, manage your Cisco products and services, and minimize risk.

  You can access MCE from https://www.cisco.com/c/en/us/products/software/my-cisco-entitlements.html .

# Multistage Upgrade Workflow for 2000 Agents Deployment

**Note** The multistage upgrade workflow is applicable for solution deployments with both main site and remote site (if available).

A Unified CCE solution upgrade likely involves a multistage process; components are grouped in several stages for upgrading. At each stage in the upgrade, the upgraded components must interoperate with components that haven't yet been upgraded to ensure the overall operation of the contact center. Therefore, it's important to verify this interoperability during the planning stages of the upgrade.

Before upgrading a production system, perform the upgrade on a lab system that mirrors your production system to identify potential problems safely.

The following table details the required sequence for upgrading Unified CCE 2000 Agent Deployments components, and the minimum component groupings that must occur together within each stage. Follow each stage to completion within each maintenance window. Each maintenance window must accommodate any testing required to ensure system integrity and contact center operation.

You can combine more than one complete stage into a single maintenance window, but you can't break any one stage into multiple maintenance windows.

Upgrade the Unified CCE components as follows:

**Note**

- Upgrade Agent Desktop, CUIC, Live Data, and IdS server along with the Unified CCE Central Controller upgrade.
- After upgrading Finesse, IdS, and CUIC, import the IdS certificates to the Finesse and CUIC servers.
- Run Stage 3 and Stage 4 upgrades in the same maintenance window.

**Note** Components of the same type within a particular stage of the upgrade sequence should be on the same application and operating system version before proceeding to the next stage in upgrade sequence.

| Stage | Component Group | Components | Notes |
|---|---|---|---|
| 1 | Platform Orchestration, Hybrid Features | Cloud Connect | If you have Cloud Connect in your environment, refer the **Update VM Properties** section in Upgrade Overview, on page 193 for Cloud connect upgrade prerequisite to increase the hard disk and RAM before you upgrade the component.<br>Upgrade both the publisher and subscriber. For Cloud Connect upgrade instructions, see the Upgrade Cloud Connect section.<br>If you don't have Cloud Connect in your environment, and you use any Hybrid feature or Orchestration, fresh install Cloud Connect. For fresh install instructions, see the Install Cloud Connect, on page 89 section. |
| 2 | Queuing and self-service | Cisco Unified Customer Voice Portal (CVP) (Operations Console, Reporting Server, Call Server/VXMLServer, Unified Call Studio) | You must upgrade all sites before proceeding to the next stage.<br>For more information, see *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. |

| Stage | Component Group | Components | Notes |
|---|---|---|---|
| 3 | Gateways | • IOS Gateways (If used for ingress access only. If used for Outbound Option Dialer, see Stage 5.)<br>• IOS VXML Gateways<br>• Cisco Virtualized Voice Browser | |

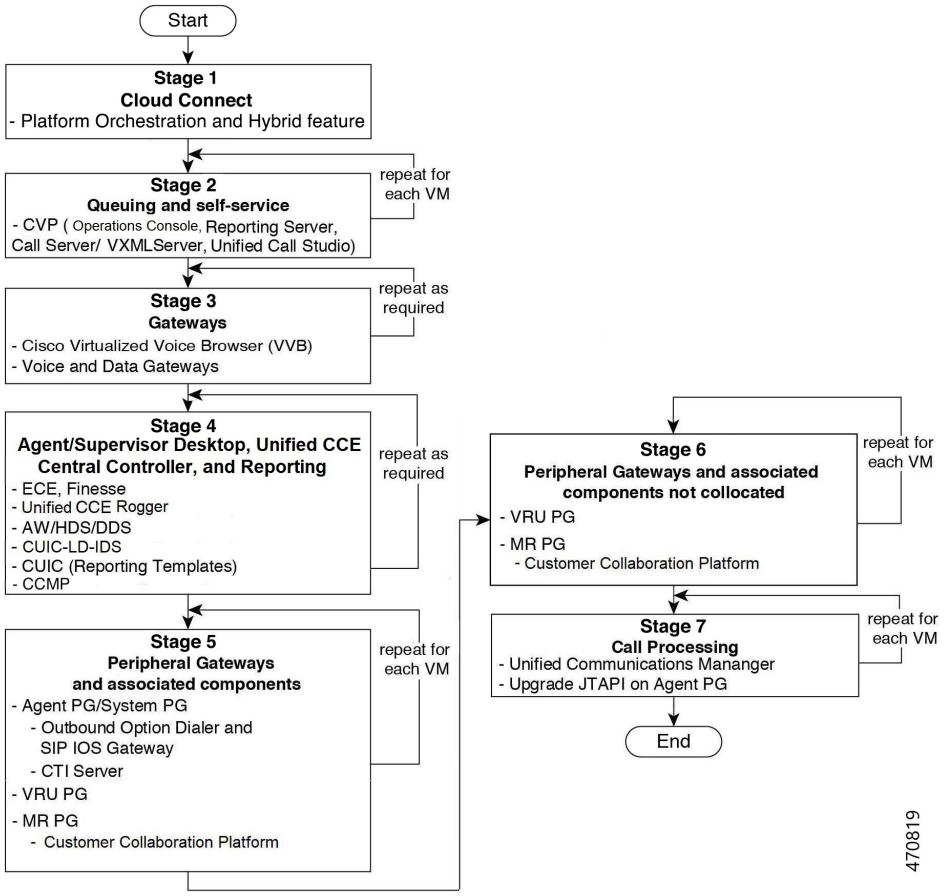
| Stage | Component Group | Components | Notes |
|---|---|---|---|
| 4 | Agent/Supervisor Desktop, Central Controller, and Reporting | • ECE<br>• Cisco Finesse<br>• Unified CCE Rogger<br>• Admin & Data server (AW/HDS/DDS)<br>• CUIC-LD-IDS<br>• CUIC Reporting Templates<br>• CCMP | |

| Stage | Component Group | Components | Notes |
|---|---|---|---|
| | | | • In 12.6(2), the RAM requirement for Live Data VM has changed. Refer to the **Update VM Properties** section in Upgrade Overview, on page 193 to update the Live Data VM properties before you upgrade the component.<br>• After you upgrade AW, import the self-signed certificate of all solution components (if applicable) to all AWs.<br>• If you are using AppDynamics for performance monitoring on 12.6(1), then before upgrading the Distributor node from 12.6(1) to 12.6(2), disable AppDynamics performance monitoring on 12.6(1) and re-enable it after upgrading to 12.6(2). If AppDynamics performance monitoring is not disabled before the Distributor node is upgraded to 12.6(2), then post upgrade, restart the Distributor node.<br>• After you upgrade Finesse to Release 12.6(x) , to load any gadgets to Finesse, you must first import all self-signed certificates (if applicable) to Finesse.<br>After upgrading Finesse to 12.6(2), ensure that both ECDSA and RSA valid certificates are available in the certificate store in PG. If not, you must export the Finesse Tomcat certificates and import them to CTI Gateway (CG) and Peripheral Gateway (PG) systems. For more information, refer to the *Add Certificate for HTTPS Gadget* section in the Cisco Finesse Administration Guide.<br>**Note** After upgrading cuic-ld-ids to 12.6, run the **utils finesse layout updateCuicGadgetUrl** command to update the gadget URL.<br>For more information about Finesse, see *Cisco Finesse Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html.<br>For more information about ECE, see https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html<br>• Cisco IdS 12.6(2) upgrade requires all SSO clients to log out from SSO, before any of the upgraded nodes is brought online. To avoid this requirement, it's recommended that you install 12.6(2) ES02 on the upgraded node and wait for the access token to expire |

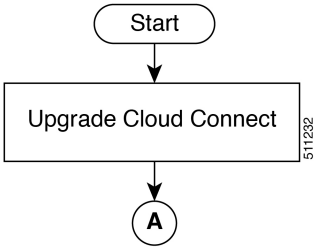
| Stage | Component Group | Components | Notes |
|---|---|---|---|
| | | | before commencing the secondary node upgrade. Without installing the 12.6(2) ES02, graceful shutdown feature will not be available for Cisco IdS 12.6(2) upgrade. You can view the duration of access token expiry in the IdS administration portal under **Settings** > **Security** > **Tokens** > **Access Token Expiry**.<br><br>Deployments using VPN-less access to Finesse desktop should also upgrade the reverse proxy to 12.6(2) before Cisco IdS is upgraded to 12.6(2).<br><br>• After you upgrade Live Data (LD), you must enable CORS on the LD box for Finesse and CUIC. For more information, see *Installation and Upgrade Guide for Cisco Unified Intelligence Center* Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html.<br><br>• After you upgrade LD, you must import the Finesse certificate to LD. |
| 5 | Peripherals | • Agent (Unified Communications Manager) PG<br>• CTI Server<br>• Outbound Option Dialer and SIP IOS Gateway | You can have many PGs located on different virtual machines. You can upgrade each PG virtual machine in its own maintenance window. |
| 6 | Peripherals | • MR PG, VRU PG<br>• CRM connector | You can have many PGs located on different virtual machines. You can upgrade each PG virtual machine in its own maintenance window. |
| 7 | Call Processing | • Cisco Unified Communications Manager (Unified Communications Manager)<br>• JTAPI on Agent (Unified Communications Manager) PG | You must install JTAPI client only when you upgrade to UCM 12.5.<br><br>If you upgrade to CUCM 12.5 on the M4 servers, ensure that you deploy CUCM off-box.<br><br>For more information, refer to *Virtualization for Unified Contact Center Enterprise* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html. |

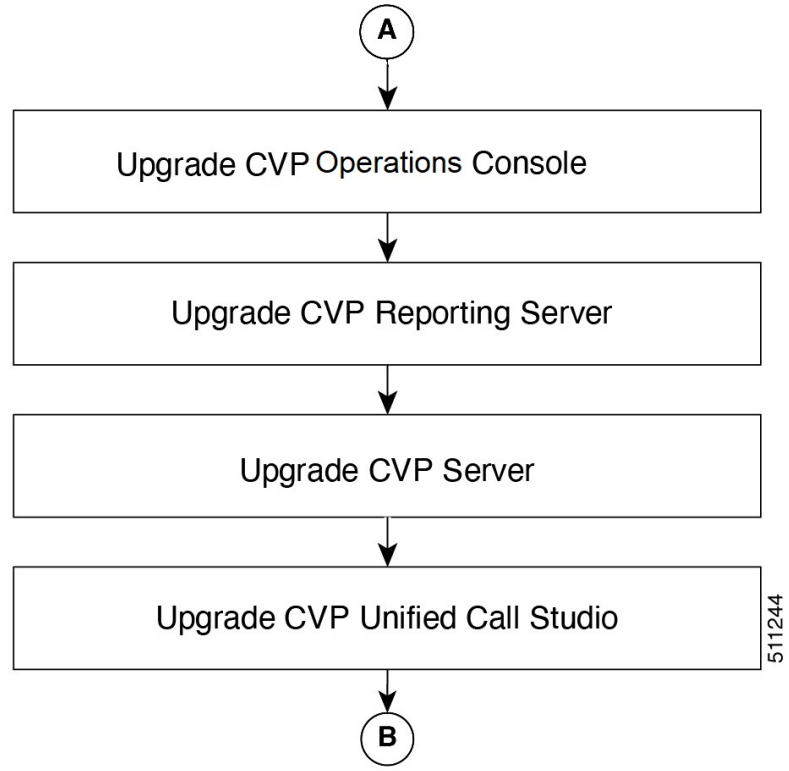
# Upgrade Flowcharts

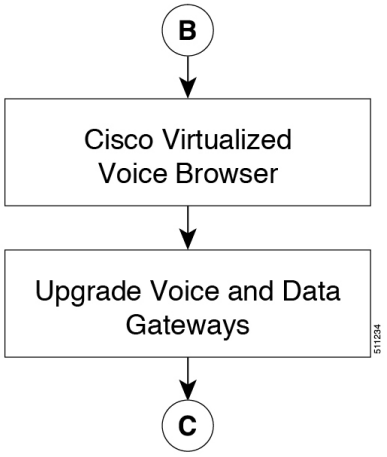
The following diagram illustrates the solution-level upgrade flow for the Unified CCE 2000 Agent Deployment solution upgrade.

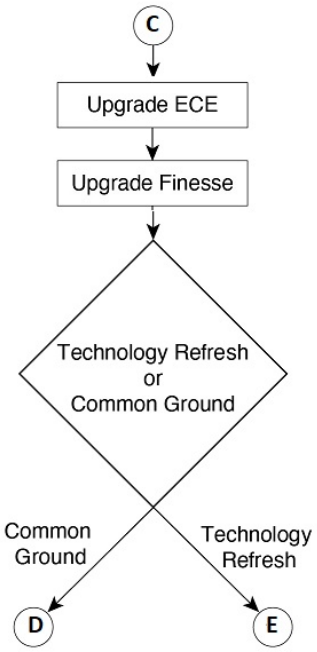


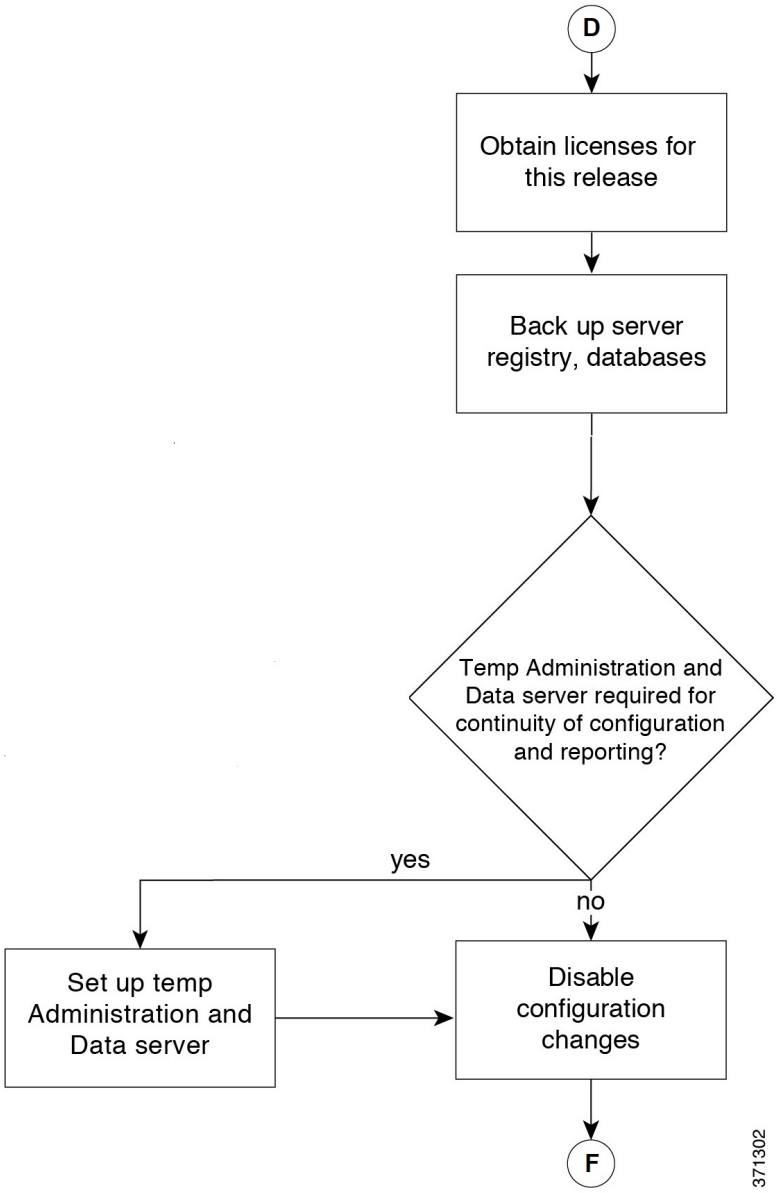

The following diagrams illustrate the stages of the component-level upgrade flows for the Unified CCE 2000 Agent Deployment solution upgrade. Each diagram covers one of the stages. The letter at the end of each flow indicates the start of the next flow that you are required to perform.

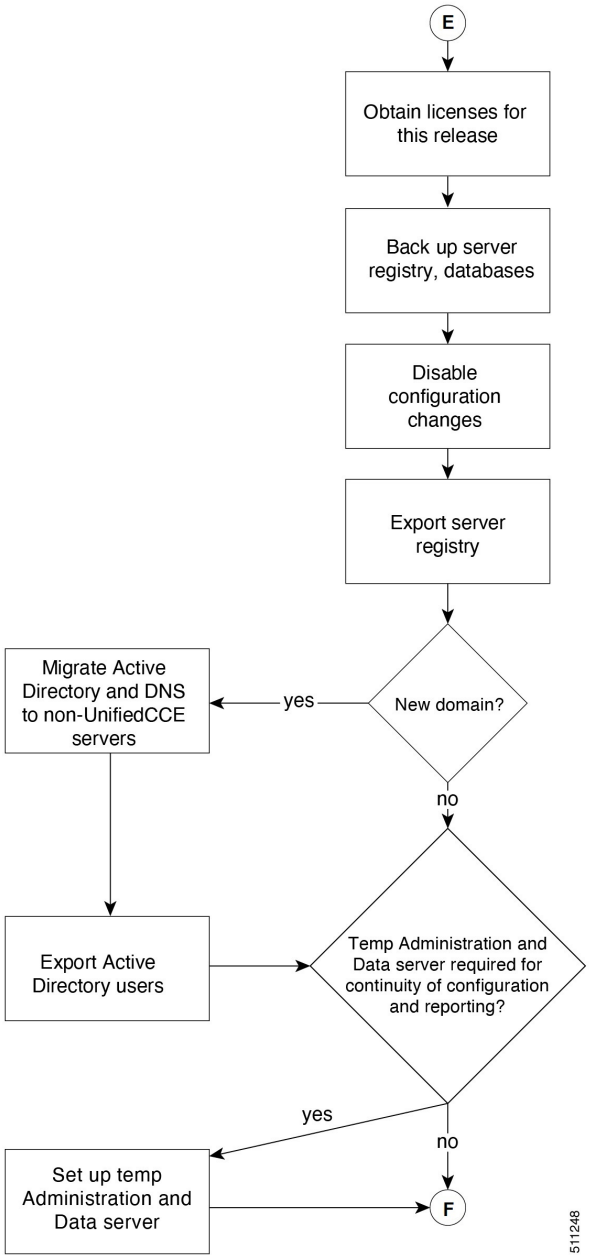


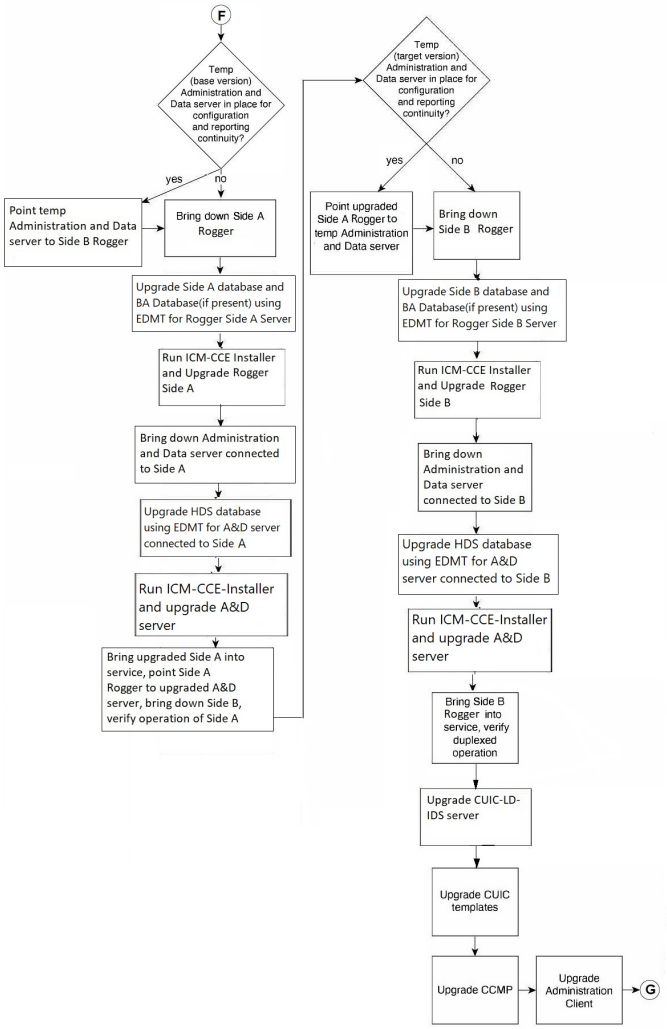

A
Upgrade CVP Operations Console
Upgrade CVP Reporting Server
Upgrade CVP Server
Upgrade CVP Unified Call Studio
511244
B

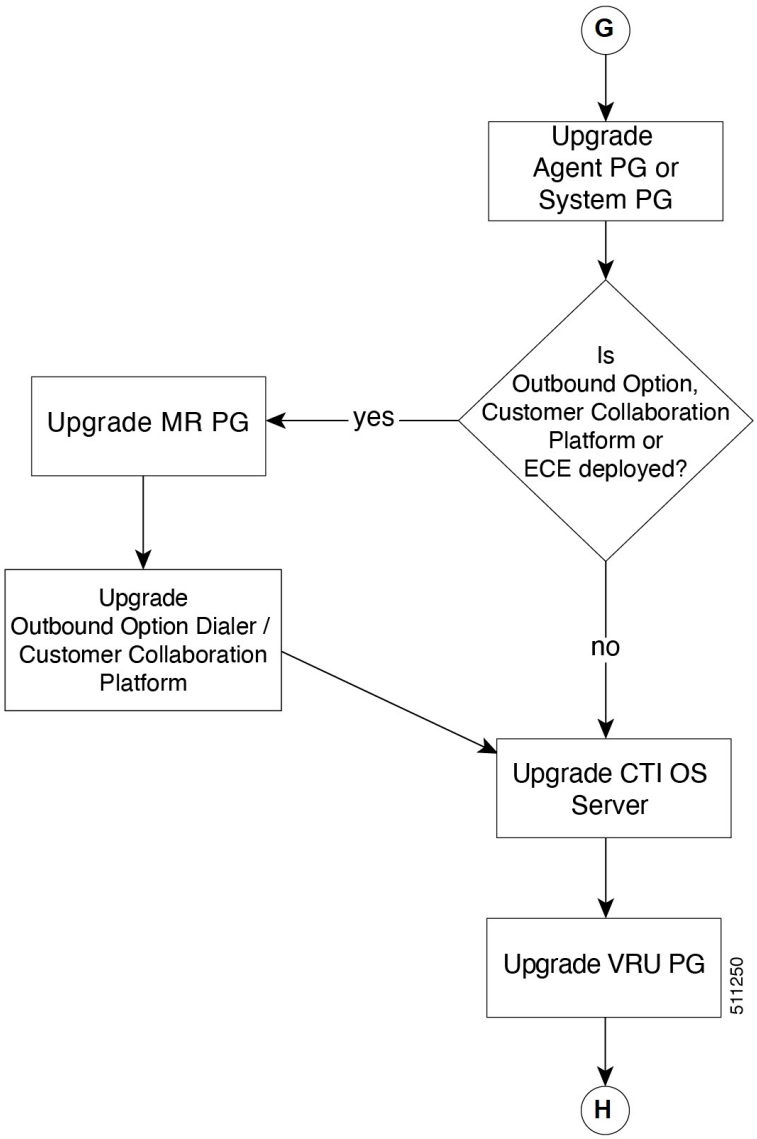

B
Cisco Virtualized Voice Browser
Upgrade Voice and Data Gateways
511234
C

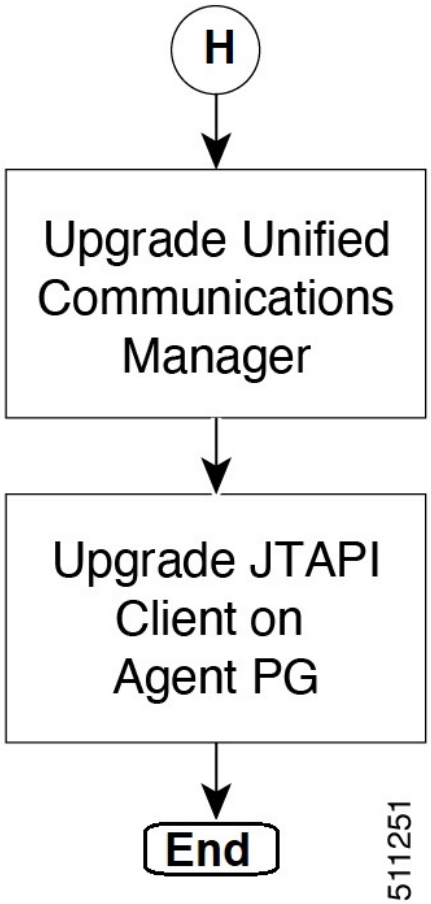

C
Upgrade ECE
Upgrade Finesse
Technology Refresh
or
Common Ground
Common
Ground
Technology
Refresh
D
E


D
Obtain licenses for this release
Back up server registry, databases
Temp Administration and Data server required for continuity of configuration and reporting?
yes
no
Set up temp Administration and Data server
Disable configuration changes
F
371302


E
Obtain licenses for this release
Back up server registry, databases
Disable configuration changes
Export server registry
New domain?
yes
Migrate Active Directory and DNS to non-UnifiedCCE servers
no
Export Active Directory users
Temp Administration and Data server required for continuity of configuration and reporting?
yes
no
Set up temp Administration and Data server
F
511248


F
Temp (base version) Administration and Data server in place for configuration and reporting continuity?
yes
no
Point temp Administration and Data server to Side B Rogger
Bring down Side A Rogger
Upgrade Side A database and BA Database(if present) using EDMT for Rogger Side A Server
Run ICM-CCE Installer and Upgrade Rogger Side A
Bring down Administration and Data server connected to Side A
Upgrade HDS database using EDMT for A&D server connected to Side A
Run ICM-CCE-Installer and upgrade A&D server
Bring upgraded Side A into service, point Side A Rogger to upgraded A&D server, bring down Side B, verify operation of Side A
Temp (target version) Administration and Data server in place for configuration and reporting continuity?
yes
no
Point upgraded Side A Rogger to temp Administration and Data server
Bring down Side B Rogger
Upgrade Side B database and BA Database(if present) using EDMT for Rogger Side B Server
Run ICM-CCE Installer and Upgrade Rogger Side B
Bring down Administration and Data server connected to Side B
Upgrade HDS database using EDMT for A&D server connected to Side B
Run ICM-CCE-Installer and upgrade A&D server
Bring Side B Rogger into service, verify duplexed operation
Upgrade CUIC-LD-IDS server
Upgrade CUIC templates
Upgrade CCMP
Upgrade Administration Client
G


G
Upgrade Agent PG or System PG
Is Outbound Option, Customer Collaboration Platform or ECE deployed?
yes
Upgrade MR PG
Upgrade Outbound Option Dialer / Customer Collaboration Platform
no
Upgrade CTI OS Server
Upgrade VRU PG
H
511250




# Multistage Upgrade Workflow for 4000 Agents and above Deployments

A Unified CCE solution upgrade likely involves a multistage process; components are grouped in several stages for upgrading. At each stage in the upgrade, the upgraded components must interoperate with components that haven't yet been upgraded to ensure the overall operation of the contact center. Therefore, it's important to verify this interoperability during the planning stages of the upgrade.

Before upgrading a production system, perform the upgrade on a lab system that mirrors your production system to identify potential problems safely.

The following table details the required sequence for upgrading Unified CCE solution components, and the minimum component groupings that must occur together within each stage. Follow each stage to completion within each maintenance window. Each maintenance window must accommodate any testing required to ensure system integrity and contact center operation.

You can combine more than one complete stage into a single maintenance window, but you can't break any one stage into multiple maintenance windows.

**Note**

- For coresident configurations, upgrade CUIC/LiveData/IdS server along with the Unified CCE Central Controller upgrade.
- After you upgrade the Standalone Live Data server, upgrade the VMware Tools manually. After upgrading the VMware Tools, check the Check and upgrade VMware Tools before each power on box in **VM Options > VM Edit Settings**.

Upgrade the components that apply to your Unified CCE contact center as follows:

**Note** Components of the same type within a particular stage of the upgrade sequence should be on the same application and operating system version before proceeding to the next stage in upgrade sequence.

**Note** In case of 4K deployment, the Unified CCE components consist of Rogger VM instead of Router and Logger VMs.

| Stage | Component Group | Components | Notes |
|---|---|---|---|
| 1 | Platform Orchestration, Hybrid Features | Cloud Connect | If you have Cloud Connect in your environment, refer the **Update VM Properties** section in Upgrade Overview, on page 193 for Cloud connect upgrade prerequisite to increase the hard disk and RAM before you upgrade the component.<br>Upgrade both the publisher and subscriber. For Cloud Connect upgrade instructions, see the Upgrade Cloud Connect section.<br>If you do not have Cloud Connect in your environment, and you use any Hybrid feature or Orchestration, fresh install Cloud Connect. For fresh install instructions, see the Install Cloud Connect, on page 89 section. |
| 2 | Queuing and self-service[2] | Cisco Unified Customer Voice Portal (CVP) (Operations Console, Reporting Server, Call Server/VXMLServer, Unified Call Studio) | • For more information, see *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. |

| Stage | Component Group | Components | Notes |
|---|---|---|---|
| 3 | Gateways | • IOS Gateways (If used for ingress access only. If used for Outbound Option Dialer, see Stage 8.)<br>• IOS VXML Gateways<br>• Cisco Virtualized Voice Browser | |
| 4 | Identity Service (IdS)/Single Sign-On(SSO) | IdS Server | • Cisco IdS 12.6(2) upgrade requires all SSO clients to log out from SSO, before any of the upgraded nodes is brought online. To avoid this requirement, it's recommended that you install 12.6(2) ES02 on the upgraded node and wait for the access token to expire before commencing the secondary node upgrade. Without installing 12.6(2) ES02, graceful shutdown feature will not be available for Cisco IdS 12.6(2) upgrade. You can view the duration of access token expiry in the IdS administration portal under **Settings** > **Security** > **Tokens** > **Access Token Expiry**.<br>Deployments using VPN-less access to Finesse desktop should also upgrade the reverse proxy to 12.6(2) before Cisco IdS is upgraded to 12.6(2).<br>• SSO is an optional feature and exchanges authentication and authorization details between the IdS component and IdP provider.<br>For more information, see Upgrade Flowcharts, on page 214.<br>• For IdS upgrade, see the procedure as documented in the *Upgrades* section of *Unified Intelligence Center Installation and Upgrade Guide* at:<br>https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html |

| Stage | Component Group | Components | Notes |
|---|---|---|---|
| 5 | Agent and supervisor desktops | Cisco Finesse<br>ECE | • To load any gadget to Finesse, you must first import the certificate to Finesse.<br>**Note** For Finesse VM, you have to increase the RAM before upgrading. See https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html<br>For more information, see *Cisco Finesse Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html.<br>• After upgrading Finesse to 12.6(2), ensure that both ECDSA and RSA valid certificates are available in the certificate store in PG. If not, you must export the Finesse Tomcat certificates and import them to CTI Gateway (CG) and Peripheral Gateway (PG) systems. For more information, refer to the *Add Certificate for HTTPS Gadget* section in the Cisco Finesse Administration Guide.<br>• For more information about ECE, see https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html. |
| 6 | Reporting server | CUIC server | • After you upgrade Cisco Unified Intelligence Center (CUIC), you must:<br>  • Enable CORS on the CUIC server, and add **`cors allowed_origin`** with the Finesse hostname.<br>  • Import LD and Finesse certificates to CUIC.<br>For more information, see *Installation and Upgrade Guide for Cisco Unified Intelligence Center* Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html. |

| Stage | Component Group | Components | Notes |
|---|---|---|---|
| 7 | Central Controller | • Unified CCE Router<br>• Unified CCE Logger<br>• Admin & Data server (AW/HDS/DDS)<br>• Standalone Live Data (if Deployed)<br>• CUIC Reporting Templates<br>• CCMP<br>• Administration Client | • In 12.6(2), the RAM requirement for Live Data VM has changed. Refer to the **Update VM Properties** section in Upgrade Overview, on page 193 to update the Live Data VM properties before you upgrade the component.<br>• After you upgrade AW, import the self-signed certificate of all solution components (if applicable) to all AWs.<br>• If you are using AppDynamics for performance monitoring on 12.6(1), then before upgrading the Distributor node from 12.6(1) to 12.6(2), disable AppDynamics performance monitoring on 12.6(1) and re-enable it after upgrading to 12.6(2). If AppDynamics performance monitoring is not disabled before the Distributor node is upgraded to 12.6(2), then post upgrade, restart the Distributor node.<br>• After you upgrade Live Data (LD), you must enable CORS on the LD box for Finesse and CUIC. For more information, see *Installation and Upgrade Guide for Cisco Unified Intelligence Center* Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html.<br>• After you upgrade LD, you must import the Finesse certificate to LD.<br>• After you upgrade LD, you must run the `set live-data machine-services` and `set live-data cuic-datasource` commands. For more information, see Configure Live Data Machine Services, on page 82 and Configure Live Data for Unified Intelligence Center Data Sources, on page 83. |
| 8 | Peripherals | • Agent (Unified Communications Manager) PG or System PG, plus<br>• CTI Server<br>• CTI OS Server<br>• Outbound Option Dialer and SIP IOS Gateway | You can have many PGs located on different virtual machines. You can upgrade each PG virtual machine in its own maintenance window.<br>**Note** Media Routing PG (MR PG), Dialer, and Agent PG must be upgraded in the same window. |

| Stage | Component Group | Components | Notes |
|---|---|---|---|
| 9 | Peripherals | • MR PG (if not collocated with Agent PG on VM), plus VRU PG (if not collocated with Agent PG on VM)<br>• Unified CCE Gateway PG (if not collocated with Agent PG on VM)<br>• CRM connector | You can have many PGs located on different virtual machines. You can upgrade each PG virtual machine in its own maintenance window.<br>**Note** Media Routing PG (MR PG), Dialer, and Agent PG must be upgraded in the same window. |
| 10 | Agent desktop client software | CTI OS (Agent/Supervisor Desktops) | You can have many desktops located in many different sites. You can upgrade CTI OS desktops in multiple maintenance windows; the later upgrade stages are not dependent on the completion of this stage. |
| 11 | Call Processing | • Cisco Unified Communications Manager (Unified Communications Manager)<br>• JTAPI on Agent (Unified Communications Manager) PG | If you upgrade to CUCM 12.5 on the M4 servers, ensure that you deploy CUCM off-box.<br>For more information, refer to *Virtualization for Unified Contact Center Enterprise* at http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html. |

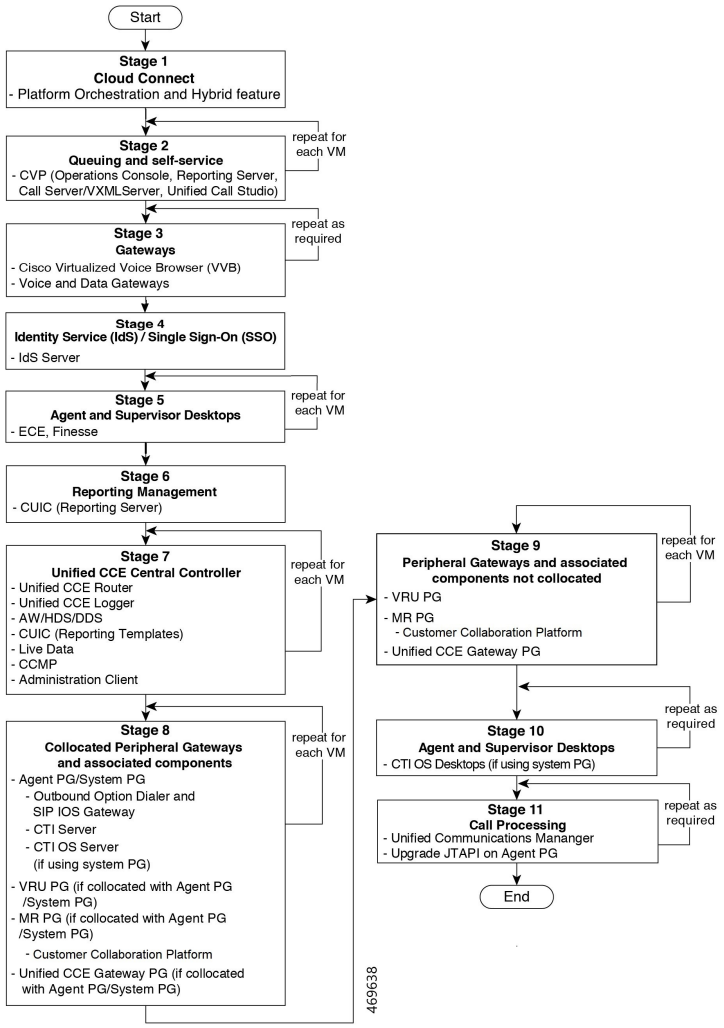
[2] If you are using Unified IP IVR for self-service and queueing, see Getting Started with Cisco Unified IP IVR.

# Upgrade Flowcharts

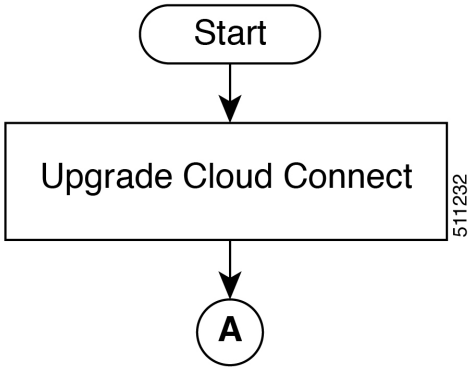
**Note** The multi-stage upgrade flowchart is not applicable for Centralized UCCE 2K deployments that essentially employ a co-resident CUIC/LiveData/IdS server, and have a single Agent PG VM pair.

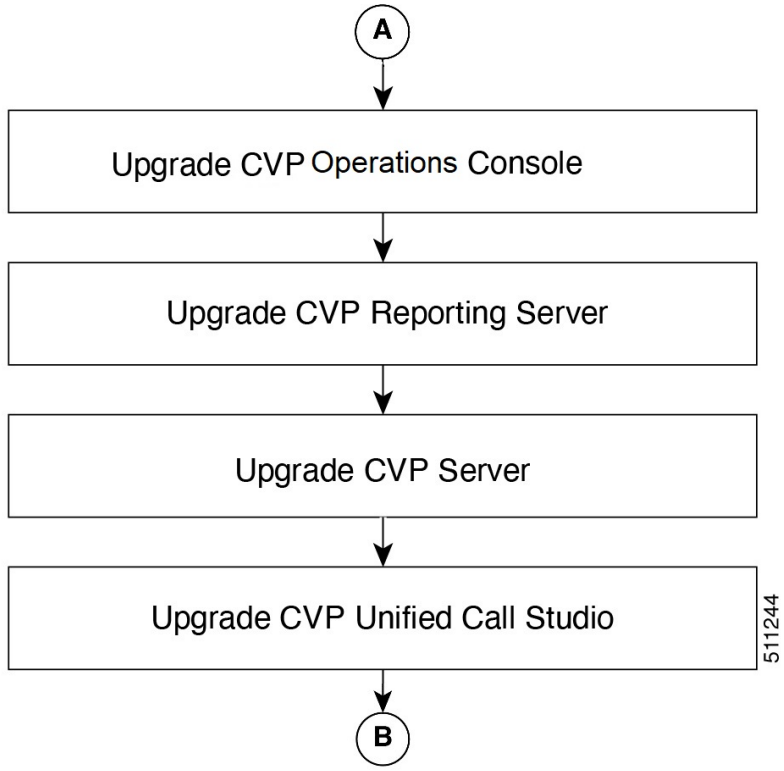
**Note** After upgrading Finesse, IdS, and CUIC, import IdS certificates on Finesse and CUIC servers.

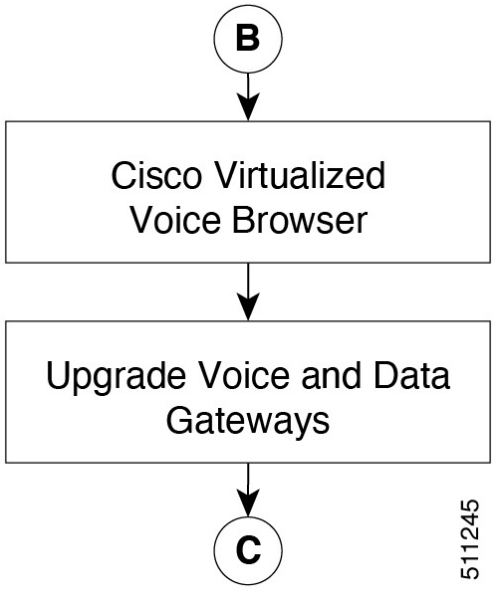
The following diagram illustrates the solution-level upgrade flow for Cisco Contact Center Enterprise solution upgrade.

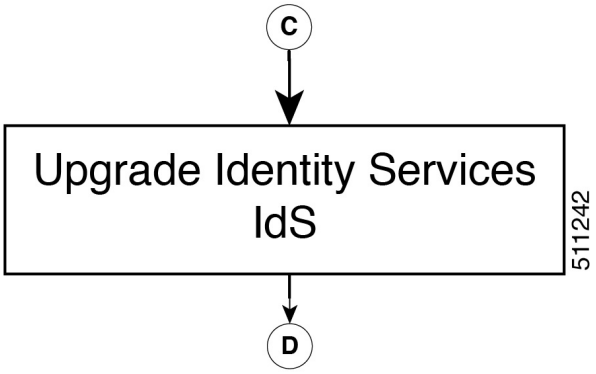


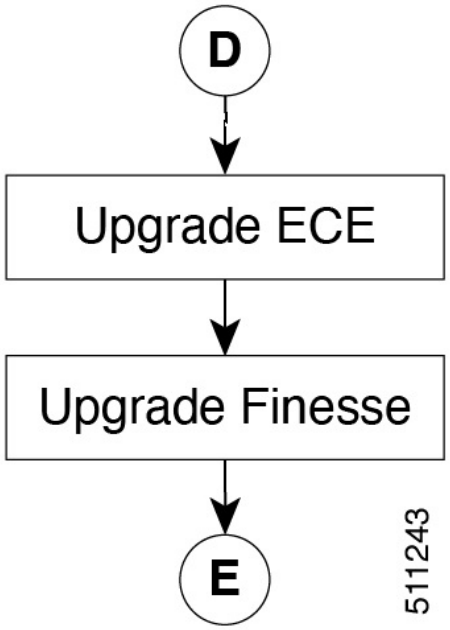

The following diagrams illustrate the stages of the component-level upgrade flows for a Cisco Unified Contact Center Enterprise solution upgrade. Each diagram covers one of the stages. The letter at the end of each flow indicates the start of the next flow that you are required to perform.

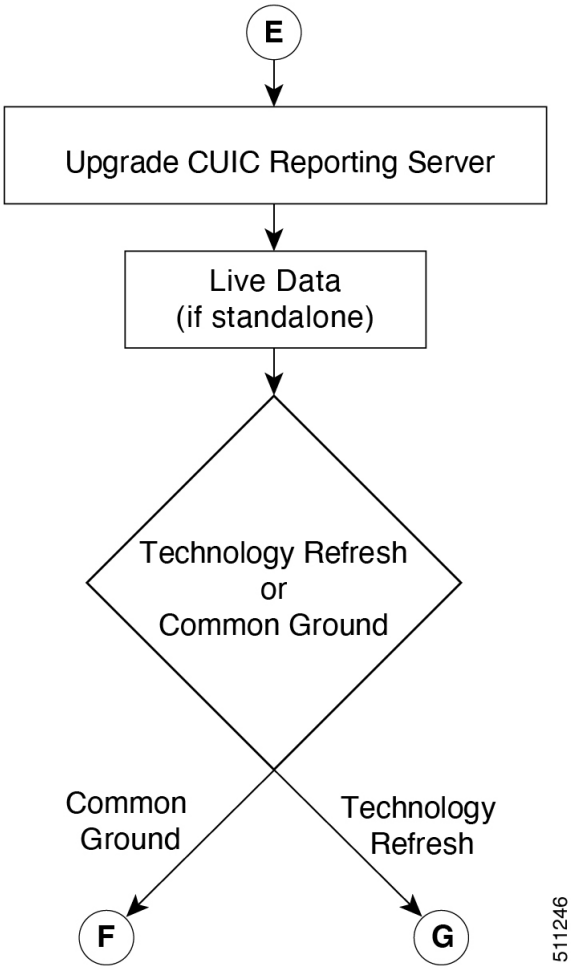


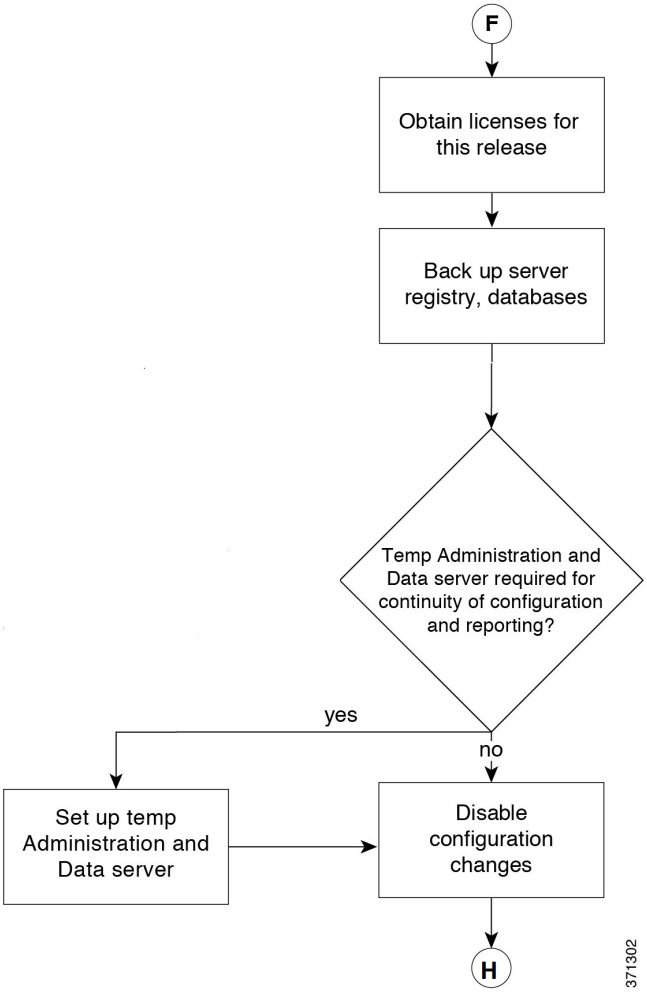

A
Upgrade CVP Operations Console
Upgrade CVP Reporting Server
Upgrade CVP Server
Upgrade CVP Unified Call Studio
511244
B

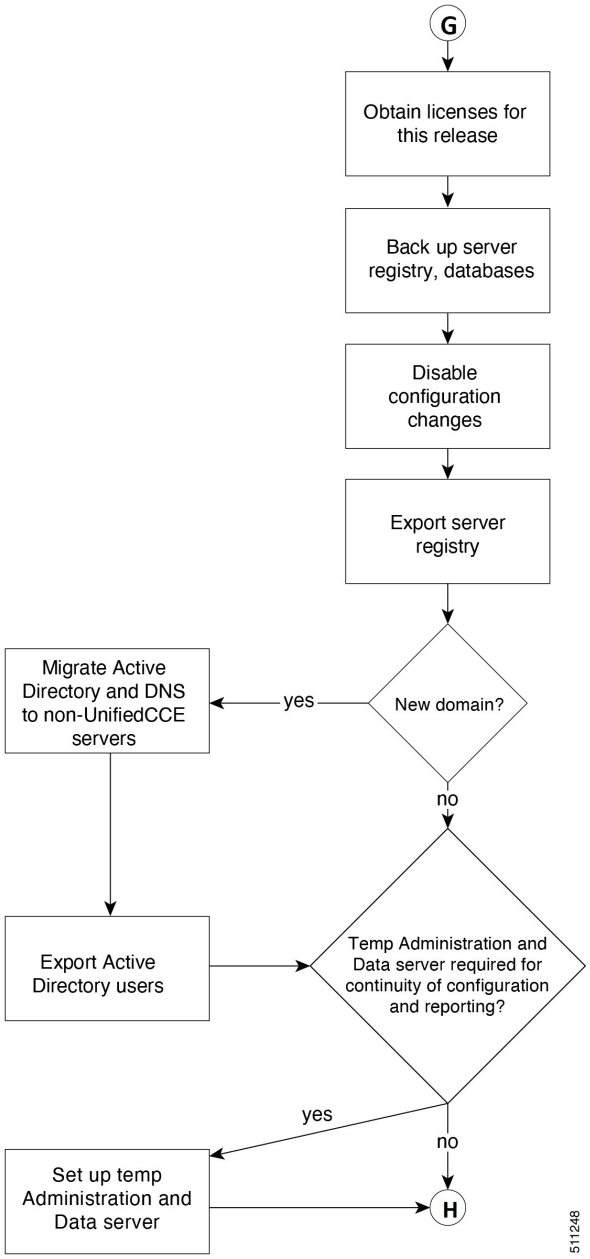

B
Cisco Virtualized Voice Browser
Upgrade Voice and Data Gateways
C
511245

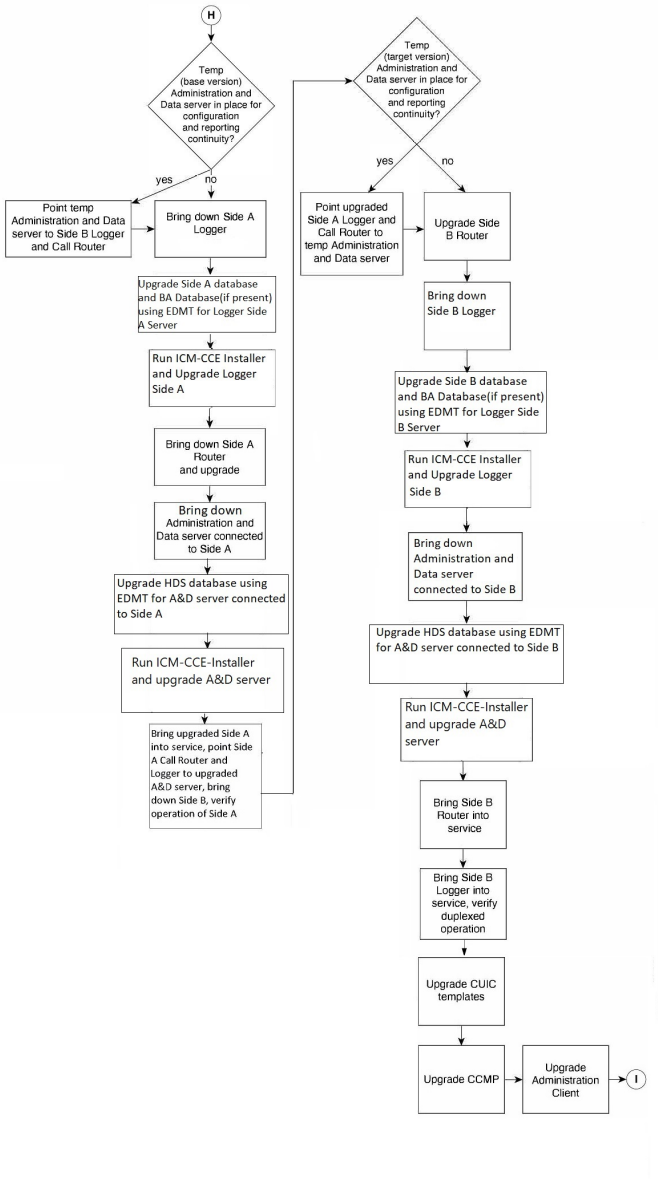

C
Upgrade Identity Services IdS
511242
D

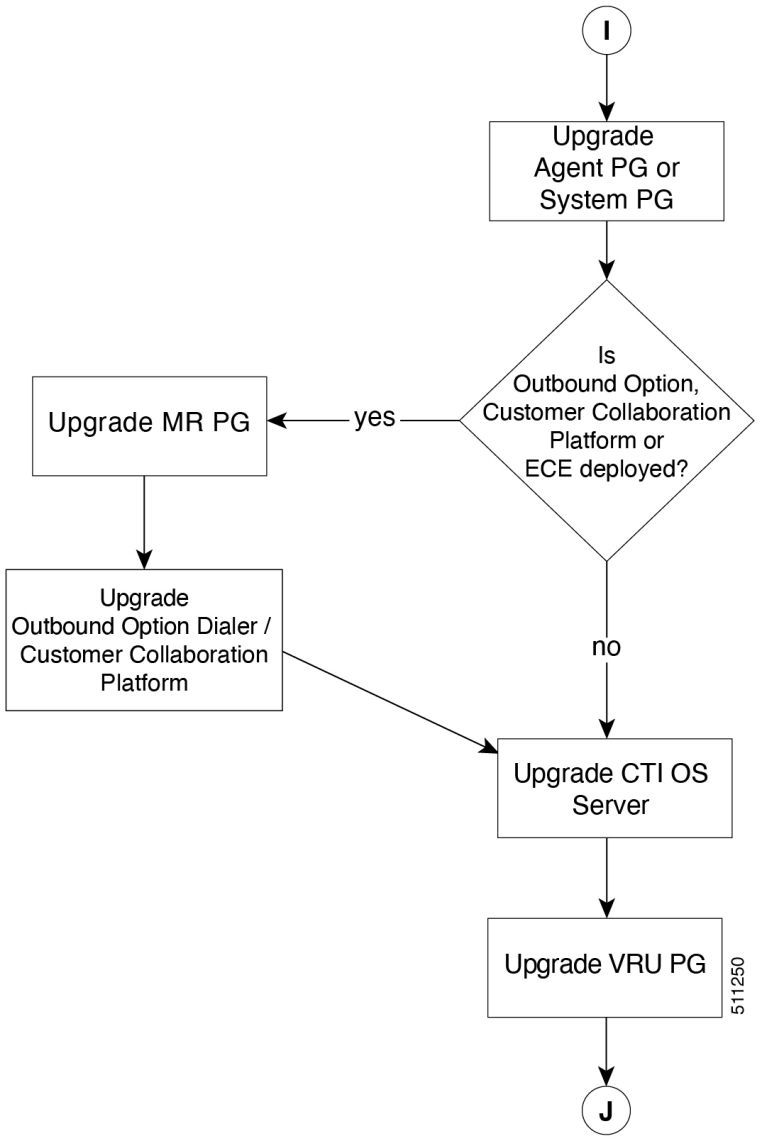

D
Upgrade ECE
Upgrade Finesse
E
511243

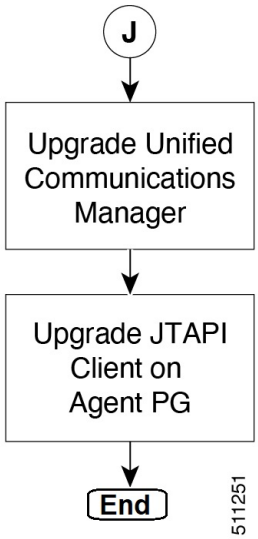

E
Upgrade CUIC Reporting Server
Live Data
(if standalone)
Technology Refresh
or
Common Ground
Common
Ground
Technology
Refresh
F
G
511246


F
Obtain licenses for this release
Back up server registry, databases
Temp Administration and Data server required for continuity of configuration and reporting?
yes
no
Set up temp Administration and Data server
Disable configuration changes
H
371302


G
Obtain licenses for this release
Back up server registry, databases
Disable configuration changes
Export server registry
New domain?
yes
Migrate Active Directory and DNS to non-UnifiedCCE servers
no
Export Active Directory users
Temp Administration and Data server required for continuity of configuration and reporting?
yes
no
Set up temp Administration and Data server
H
511248


H
Temp (base version) Administration and Data server in place for configuration and reporting continuity?
yes
no
Point temp Administration and Data server to Side B Logger and Call Router
Bring down Side A Logger
Upgrade Side A database and BA Database(if present) using EDMT for Logger Side A Server
Run ICM-CCE Installer and Upgrade Logger Side A
Bring down Side A Router and upgrade
Bring down Administration and Data server connected to Side A
Upgrade HDS database using EDMT for A&D server connected to Side A
Run ICM-CCE-Installer and upgrade A&D server
Bring upgraded Side A into service, point Side A Call Router and Logger to upgraded A&D server, bring down Side B, verify operation of Side A
Temp (target version) Administration and Data server in place for configuration and reporting continuity?
yes
no
Point upgraded Side A Logger and Call Router to temp Administration and Data server
Upgrade Side B Router
Bring down Side B Logger
Upgrade Side B database and BA Database(if present) using EDMT for Logger Side B Server
Run ICM-CCE Installer and Upgrade Logger Side B
Bring down Administration and Data server connected to Side B
Upgrade HDS database using EDMT for A&D server connected to Side B
Run ICM-CCE-Installer and upgrade A&D server
Bring Side B Router into service
Bring Side B Logger into service, verify duplexed operation
Upgrade CUIC templates
Upgrade CCMP
Upgrade Administration Client
I


I
Upgrade Agent PG or System PG
Is Outbound Option, Customer Collaboration Platform or ECE deployed?
yes
Upgrade MR PG
Upgrade Outbound Option Dialer / Customer Collaboration Platform
no
Upgrade CTI OS Server
Upgrade VRU PG
J
511250




# Data Migration Considerations

**Note** The EDMT may take a long time to migrate, backup, or restore the data, as the file sizes can be several gigabytes (GB). If the EDMT tool is not responding during data migration or the data migration takes a long time, check the Event logs in the Microsoft Windows Event Viewer tool. The logs may show SQL or BACKUP failure events. These events may occur because of file system errors or hardware errors and failures. Analyze and fix these errors before re-running the EDMT tool.

To reduce data migration time, consider reducing the database size by:

- Removing redundant records, especially call detail records (RCD, RCV, TCD, and TCV tables). However, removing records affects the availability of historical reports; knowledge of the HDS schema is required.
- Purging the Logger database of all data that was already replicated to the HDS (25 GB or less).
- Using more efficient hardware, especially on I/O subsystems:
  - RAID 1 + 0
  - I/O Cache – more is better

Enable the Tempdb log to expand up to 3 GB.

**Note** When you upgrade to Cisco Unified Contact Center Enterprise, Release , the Do Not Call table that existed before the upgrade is not available. Therefore, you must import the Do Not Call table.

### Required Disk Space for Migration

1. Run **EXEC sp_spaceused** command in the SQL Server.
2. Determine the following:
   - DUS (Database Used Size).

     Calculated as:

     Database Used Size (DUS) = (database_size – unallocated space)
   - Required disk space by EDMT for backup of database

     Calculated as:

     Space that is used for backup = 1.2 times of DUS.

**Note** Note: When the backup and restore drive are same, then required disk space by EDMT is equal to restore database size plus space used for backup.

**Note** When the backup and restore has to be done through EDMT, and since the database backup contains encrypted data, this process cannot be performed unless the source certificate that encrypted the database is copied to the destination server.

Follow the procedures outlined in the below Microsoft documentation to restore the certificate on destination server.

- https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/move-a-tde-protected-database-to-another-sql-server?view=sql-server-ver15
- https://www.sqlshack.com/restoring-transparent-data-encryption-tde-enabled-databases-on-a-different-server/
- https://www.databasejournal.com/tips/how-to-move-a-tde-encryption-key-to-another-sql-server-instance.html

If you do not want to move the encrypted backup, then disable TDE on the source database, perform the backup and restore through EDMT, and enable TDE on destination database. To enable and disable TDE on the database, see Enable and Disable TDE on a Database, on page 225.

### Time Guidelines and Migration Performance Values

For a close estimate of time and space requirements, run EDMT against a copy of your production database on hardware that is similar to your production environment, in a lab environment. For customers who do not have the facility, the following sections provide information that is gathered while performance testing in the labs at Cisco Systems, Inc.

- **Typical database migration performance values**: The following table provides high-level guidelines for the time that is taken to upgrade the Loggers and HDSs based on internal upgrade testing with hardware Cisco UCS C240 M4SX. Actual times may vary based on the parameters previously mentioned.

- **Backup and Restore - Technology Refresh only**: The backup speed depends on the speed of the network, and the speed of the disk sub-system. The faster the network, the sooner the network copy.

| Database Used Size (GB) | Backup/Restore Time (hours) | Data Migration Time (minutes) | Total Time (hours) |
|---|---|---|---|
| 500 GB | 1.5-2 hrs | < 2 mins | 2 - 2.5 hrs |

**Note**

- The values in the Database Used Size column are based on the amount of disk space that is used by the source database, and not the size of the disk it resides on.
- The values in the Backup Time and Restore Time columns assumes that the network meets the minimum requirements.

  For more information about the minimum requirements, refer to the *Virtualization for Unified Contact Center Enterprise* at http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html .
- For Technology Refresh upgrades, have the fastest network possible (gigabit through one network switch) between the source and the destination machines. Use of a crossover cable is not supported because it lacks buffer memory and can cause data loss.

# Enable and Disable TDE on a Database

**To enable Transparent Data Encryption (TDE) on a database, perform the following:**

**Note** These steps are to be performed with sysadmin user permission.

1. Create a server certificate data encryption key.

```
USE master
GO
CREATE CERTIFICATE DEKCert WITH SUBJECT = 'DEK Certificate'
GO
```

2. Create a backup of the server certificate data encryption key.

```
BACKUP CERTIFICATE DEKCert TO FILE = '<SystemDrive>:\DEKCert'
WITH PRIVATE KEY ( FILE = '<SystemDrive>:\temp\DEKCertPrivKey' ,
ENCRYPTION BY PASSWORD = 'C1sco123=' )
GO
```

3. Create database encryption key for the database to configure transparent data encryption. In the following query, *ucce_sideA* is the name of the active database.

```
USE ucce_sideA
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_256
ENCRYPTION BY SERVER CERTIFICATE DEKCert
GO
```

4. Enable database encryption. Run the following query where *ucce_sideA* is the name of the active database.

```
ALTER DATABASE ucce_sideA SET ENCRYPTION ON
```

**Note** By setting encryption on, a background task starts encrypting all the data pages and the log file. This can take a considerable amount of time, depending on the size of the database. Database maintenance operations should not be performed when this encryption scan is running.

5. To query the status of the database encryption and its percentage completion, query the new sys.dm_database_encryption_keys.

```
SELECT DB_NAME(e.database_id) AS DatabaseName,
e.database_id,
e.encryption_state,
CASE e.encryption_state
WHEN 0 THEN 'No database encryption key present, no encryption'
WHEN 1 THEN 'Unencrypted'
WHEN 2 THEN 'Encryption in progress'
WHEN 3 THEN 'Encrypted'
WHEN 4 THEN 'Key change in progress'
WHEN 5 THEN 'Decryption in progress'
END AS encryption_state_desc,
c.name,
e.percent_complete
FROM sys.dm_database_encryption_keys AS e
LEFT JOIN master.sys.certificates AS c
ON e.encryptor_thumbprint = c.thumbprint
```

**To disable TDE on a database, perform the following:**

```
USE master;
GO
ALTER DATABASE ucce_sideA SET ENCRYPTION OFF;
GO
-- Remove Encryption Key from Database
USE ucce_sideA;
GO
DROP DATABASE ENCRYPTION KEY;
GO
```

# Silent Upgrade

There are situations when silent upgrade can be used in running an installation wizard. You can run a silent installation while performing a fresh install or an upgrade.

For more information, see Silent Installation, on page 60.

# Unified CCE Upgrade Overview

The supported upgrade paths to Unified CCE 12.6(2) are as follows:

- Unified CCE 12.5(1) to Unified CCE 12.6(2). EDMT is not required during this upgrade process. If Windows and SQL platform upgrade is involved during this upgrade process, see the Technology Refresh Upgrade section for details on using EDMT.

- Unified CCE 12.5(2) to Unified CCE 12.6(2). EDMT is not required during this upgrade process.
- Unified CCE 12.6(1) to Unified CCE 12.6(2). EDMT is not required during this upgrade process.
- Unified CCE 12.0(1) to Unified CCE 12.5(1) with inline upgrade to Unified CCE 12.6(2) using Common Ground or Technology Refresh upgrade. Use EDMT during this upgrade process:
  - In case of Common Ground upgrade, use 12.5(x) EDMT to upgrade from Unified CCE 12.0(1) to Unified CCE 12.5(1).
  - In case of Technology Refresh upgrade, use 12.6(x) EDMT to upgrade from Unified CCE 12.0(1) to Unified CCE 12.5(1).

# Upgrade Prerequisites

### Before you begin

- Make sure that Windows Update is not running in parallel when you begin installation.
- Before you upgrade the Cisco VOS based servers such as the Live Data server, check the **Check and upgrade VMware Tools before each power on** box in the VM's **Options** > **Edit Settings**.

  For more information on VMware Tools upgrade, see the VMware documentation.
- The minimum disk space required to perform the upgrade is 2175 MB.

# Upgrade CCE Minor/Maintenance Release Software

To perform the upgrade from CCE 12.5(x) or CCE 12.6(1) release, do the following:

### Procedure

**Step 1** Log in to your system using domain credentials with administrative privileges.

**Step 2** Launch the CCE 12.6(2) installation wizard. Click **Next** to proceed.

**Step 3** Select the radio button to accept the license agreement and click **Next**.

**Step 4** Click **Install** to begin the installation.

**Step 5** Select the radio button to restart the system and click **Finish**.

# Custom Truststore to Store Component Certificates

Starting Unified CCE 12.6(x), a new custom truststore is created under the Unified ICM Installation directory `<ICM install directory>\ssl\cacerts` to store all the component certificates. With this new custom truststore, you don't need to export and import the certificates each time Java is updated in the system.

After upgrading from Unified CCE 12.5(x) to Unified CCE 12.6(x), you should export the certificates from the Java truststore to the custom truststore under the Unified ICM Installation directory `<ICM install directory>\ssl\cacerts`.

Export the certificate from the Java truststore:

- Run the command at the command prompt: `cd %JAVA_HOME%\bin`.

**Important** Use CCE_JAVA_HOME if upgrading from Unified CCE 12.5(1a) or Unified CCE 12.5(1) with ES55 (mandatory OpenJDK ES).

- Export the certificates of all the components imported into the truststore.

  The command to export the certificates is *keytool -export -keystore <JRE path>\lib\security\cacerts -alias <alias of the component> -file <filepath>.cer*
- Enter the truststore password when prompted.

Import the certificate to the custom truststore:

- Run the command at the command prompt: `cd %CCE_JAVA_HOME%\bin`.
- Import the certificates for all the components that you exported from the Java truststore.

  The command to import certificates is *keytool -import -keystore <ICM install directory>\ssl\cacerts -file <filepath>.cer -alias <alias>*.
- Enter the truststore password when prompted.
- Enter 'yes' when prompted to trust the certificate.

# Upgrade Cloud Connect

Follow the steps to install the ISO file using the Cloud Connect Command line interface (CLI).

You can also install the ISO using the upgrade procedure in the Cisco Unified Operating System Administration web interface. For more information, see *Access Unified OS Administration*.

**Before you begin:**

Before you begin the upgrade from Cloud Connect 12.6(1) to Cloud Connect 12.6(2), check if the **ucos.keymanagement.v02.cop.sgn** is applied on the base version. If not, you must install it; else the upgrade will fail. Restart the Cloud Connect node after installing **ucos.keymanagement.v02.cop.sgn**.

Before you begin the upgrade from Cloud Connect 12.5(1) to Cloud Connect 12.6(2), check if the **ucos.keymanagement.v01.cop.sgn** is applied on the base version. If not, you must install it; else the upgrade will fail. Restart the Cloud Connect node after installing **ucos.keymanagement.v01.cop.sgn**.

Download the ISO file from the software download page for Cloud Connect https://software.cisco.com/download/home/268439622/type/283914286/release/12.6(2) to the SFTP server that can be accessed from the Cloud Connect system.

1. Log in to Cloud Connect CLI and specify the System Administration username and password.
2. Enter the command `utils system upgrade initiate` to initiate the ISO installation.
3. Select **Remote File System** from source list page.
4. Enter the remote path to the directory on the SFTP server where you have downloaded the ISO file.

**Note** If the ISO file is located on a Linux or UNIX server, you must enter a forward slash (/) at the beginning of the directory path. For example, if the ES file is in the patches directory, enter **/patches**. If the ISO file is located on a Windows server, check with your system administrator for the correct directory path.

5. Enter the SFTP server name or IP address and then enter the credentials.

   It is optional for you to enter the SMTP Host Server name.

6. Select the transfer protocol as SFTP. The system displays the list of ISO files available in the SFTP location.

7. Select the number corresponding to the ISO file that you want to install and press **Enter**.

8. Enter the following options when you are prompted `Switch to new version if the upgrade is successful (yes/no).`

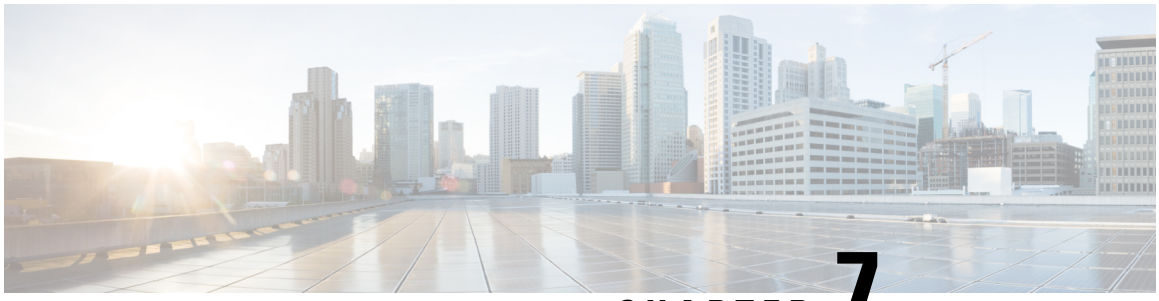
   - Enter **yes** to automatically switch the version.
   - Enter **no** if you need to manually switch the version after all the nodes are upgraded (refer step 10 for more details).

**Note** You must restart the Cloud Connect node after the upgrade.

**Note** Verify if the node is upgraded to Cloud Connect 12.6(2), after you switch the version successfully (where active version is Cloud Connect 12.6(2) and inactive version is Cloud Connect 12.5(1) or Cloud Connect 12.6(1).

9. In cluster setup, first complete the upgrade on the publisher node and perform the upgrade on the subscriber node. After successful upgrades, perform switch version using the command `utils system switch-version` first on the publisher node and later on the subscriber nodes.

**Note** Verify if the nodes are upgraded to Cloud Connect 12.6(2), after you switch the version of the publisher node and subscriber nodes successfully (where active version is Cloud Connect 12.6(2) and inactive version is Cloud Connect 12.5(1) or Cloud Connect 12.6(1).



CHAPTER 7

# Common Ground Upgrade


- Preupgrade Overview, on page 231
- Common Ground Preupgrade Task Flow, on page 232
- Common Ground Preupgrade Tasks, on page 234
- Common Ground Upgrade Task Flow, on page 236
- Common Ground Upgrade Tasks, on page 239


# Preupgrade Overview

The preupgrade process ensures that your systems have the necessary software to support your contact center. These tasks prepare the way for a successful upgrade of your Cisco contact center components to the new release.

**Note** Common Ground Upgrade is not supported if the platform upgrade from Windows Server 2016 and SQL Server 2017 to Windows Server 2019 and SQL Server 2019 is planned as part of upgrade process. Technology Refresh Upgrade is the supported upgrade option for platform upgrade.

### Upgrade Tools

During the preupgrade process, use the following tools as required:

- User Migration Tool—A standalone Windows command-line application that is used for all upgrades that involve a change of domain. The tool exports all existing user accounts (config/setup and supervisors) from the source domain to a **.bin** file. The file is used in the target domain during the upgrade.

  You can download the User Migration Tool from Cisco.com by clicking **ICM User Migration Tool Software**.

- Regutil Tool—Used in Technology Refresh upgrades, exports the Cisco Systems, Inc. registry from the source machine during the preupgrade process. The output of the tool is required on the destination machine when running the Unified CCE Installer during the upgrade process.

  You can download the Regutil Tool from Cisco.com by clicking **Contact Center Enterprise Tools**.

- Domain Manager—Used to provision Active Directory.

  The Domain Manager Tool is delivered with the main installer.

- Upgrade.exe—Used to upgrade the schema of the logger, AW DB, HDS DB, and BA databases to a version compatible with the current Unified CCE Software version. It is typically used when the installer fails to automatically upgrade the schema of the AW database. The other databases are typically upgraded using EDMT and not the installer.

  Perform the following steps to use the tool:

  ```
  <ICM install directory>:\icm\bin>upgrade.exe -s <Server Name> -d
  <Database name> -dt <Database Type> -i <Instance Name>
  ```

  Where

  <Database Type> - can be either " **logger**" or "**hds**" or "**aw**" or "**ba**", depending on the database that requires the schema to be upgraded.

- Enhanced Database Migration Tool (EDMT)—A wizard application that is used for all upgrades to migrate the HDS, Logger, and BA databases during the upgrade process.

  You can download the EDMT from Cisco.com by clicking **Cisco Enhanced Data Migration Tool Software Releases**.

  The prerequisites for running EDMT are:

  - EDMT also requires Microsoft® ODBC Driver 17 for SQL Server® and Visual C++ Redistributable for Visual Studio 2015 (or higher). The latest version of these packages can be downloaded from the Microsoft website. However, a copy of the same is also available in the **Prerequisites** folder of EDMT.

  The EDMT displays status messages during the migration process, including warnings and errors. Warnings are displayed for informational purposes only and do not stop the migration. Errors stop the migration process and leave the database in a corrupt state. If an error occurs, restore the database from your backup, fix the error, and run the tool again.

**Note**

- If you are configuring SQL services to run as Virtual account (NT SERVICE) or Network Service account (NT AUTHORITY\NETWORK SERVICE), you must run EDMT as an administrator.
- The installer, not the EDMT, upgrades the AW database for the Administration & Data Server.

# Common Ground Preupgrade Task Flow

Perform the following Common Ground preupgrade tasks in any order.

**Note** The Common Ground upgrade assumes the host server runs on Windows Server.

| Task | See |
|---|---|
| Review target Release Notes | *Release Notes for Cisco Unified Contact Center Enterprise Solutions* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-release-notes-list.html |
| ESXi Supportability | ESXi Supportability, on page 6 |
| Virtual Machine Snapshot for Unified CCE Component Virtual Machines | Virtual Machine Snapshot for Unified CCE Component Virtual Machines, on page 234 |
| Download the Enhanced Database Migration Tool | Upgrade Overview, on page 193 |
| Notify all stakeholders, including:<br>• Cisco Technical Assistance Center (TAC)<br>• Local Cisco Representatives<br>• Customer Operations and Emergency Management Center<br>• Third-party vendors as applicable | |

# Common Ground Preupgrade Tasks

## Disable Configuration Changes

**Procedure**

**Step 1** To disable configuration changes during the upgrade, set the following registry key to 1 on the Side A Call Router: **HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\Router A\Router\CurrentVersion\Configuration\Global\DBMaintenance**.

**Note** Live data services connect to the new Central controller machines only after you upgrade both sides of Central controller, and enable the configuration changes.

**Step 2** Confirm that configuration changes are disabled by attempting to save a configuration change.

When you try to save the change, a message is displayed confirming the change failure.

## Virtual Machine Snapshot for Unified CCE Component Virtual Machines

Uninstallation of Unified CCE 12.5(1) installed on server machines using the ICM-CCE-Installer ISO is not supported.

To revert to the previous versions that existed before you did a Common Ground in-place upgrade of installations to Unified CCE 12.5(1), perform one of the following tasks:

1. Take a Virtual Machine Snapshot in the powered off state before the upgrade.
2. Clone the Virtual Machine before the upgrade.

Delete these snapshots or clones after the upgrades are successfully completed. Such deletions will prevent performance issues.

Uninstallation and re-installation of other packages like Administration Client and Internet Script Editor (ISE) will continue to be supported.

**Note** Uninstallation and re-installation are supported for Unified CCE 12.6(x).

## VM Hardware Version Upgrade

Perform the following procedure to upgrade the hardware version of the virtual machine (VM).

**Note** The hardware compatibility of the VM must be set to **ESXi 6.7 and later** .

### Before you begin

- Power off the VM.
- Upgrade to the ESXi version compatible with this release. For more information, see https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html.

### Procedure

**Step 1** Launch the vSphere Web Client using the browser.

**Step 2** Log in to the vCenter Server.

**Step 3** Right-click on the VM, and select the menu option **Compatibility** > **Upgrade VM Compatibility**.

**Note** The `Upgrade VM Compatibility` option appears only if the hardware version on the VM is not the latest version supported.

**Step 4** In the **Compatible with** field, select .
This sets the hardware version of the VM to 13.

**Step 5** Click **Ok**.

**Step 6** Power on the VM.

**Note** If the system prompts, upgrade the VMware tools. For more information, see Install Vmware Tools, on page 20.

# Increase the Provisioned Disk Size for Unified Intelligence Center VMs (Standalone and Coresident)

### Procedure

**Step 1** Power off the virtual machine.

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

**Step 3** Click the **Hardware** tab, and select the hard disk to modify.

**Step 4** In the **Disk Provisioning** pane, increase the provisioned size from 146 GB to 200 GB.

**Step 5** Click **OK** to save your changes and close the dialog box.

**Step 6** Start the virtual machine.

# Common Ground Upgrade Task Flow

For the Unified CCE core components, there is a general flow for redundant systems to ensure that Cisco Contact Center operation continues during the entire upgrade process. Sides A and B are brought down, upgraded, tested, and brought back up in a sequence that ensures continuous operation of the Cisco Contact Center.

**Note** For coresident configurations, upgrade CUIC/LiveData/IdS server along with the Unified CCE Central Controller upgrade.

For Common Ground upgrades, perform the following upgrade tasks:

| Task | See |
|---|---|
| **Cloud Connection Components** | |
| Install Cloud Connect | Install Cloud Connect, on page 89<br>If you have Cloud Connect in your environment, refer the **Update VM Properties** section in Upgrade Overview, on page 193 for Cloud connect upgrade prerequisite to increase the hard disk and RAM before you upgrade the component.<br>Upgrade both the publisher and subscriber. For Cloud Connect upgrade instructions, see the Upgrade Cloud Connect section.<br>If you don't have Cloud Connect in your environment, and you use any Hybrid feature or Orchestration, fresh install Cloud Connect. For fresh install instructions, see the Install Cloud Connect, on page 89 section. |
| **Queuing and self-service components** | |
| Upgrade Cisco Unified Customer Voice Portal.[3] | *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 |
| **Infrastructure and media resource components** | |
| Cisco Virtualized Voice Browser | *Installation and Upgrade Guide for Cisco Virtualized Voice Browser* at<br>https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/products-installation-guides-list.html |
| Upgrade voice and data gateways. | Upgrade Voice and Data Gateways, on page 245 |
| **Identity Service/SSO** | |

| Task | See |
|---|---|
| Identity Service (IdS)/Single Sign-On(SSO) | SSO is an optional feature and exchanges authentication and authorization details between an identity provider (IdP) and an identity service (IdS).<br>**Note** Cisco IdS 12.6(2) upgrade requires all SSO clients to log out from SSO, before any of the upgraded nodes is brought online. To avoid this requirement, it's recommended that you install 12.6(2) ES02 on the upgraded node and wait for the access token to expire before commencing the secondary node upgrade. Without installing 12.6(2) ES02, graceful shutdown feature will not be available for Cisco IdS 12.6(2) upgrade. You can view the duration of access token expiry in the IdS administration portal under **Settings** > **Security** > **Tokens** > **Access Token Expiry**.<br>Deployments using VPN-less access to Finesse desktop should also upgrade the reverse proxy to 12.6(2) before Cisco IdS is upgraded to 12.6(2).<br>For more information, see Upgrade Flowcharts, on page 214<br>https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html |
| Upgrade Enterprise Chat and Email (ECE) | For ECE installation or upgrade instructions, see the *Enterprise Chat and Email Installation and Configuration Guide for Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html |
| Upgrade Finesse | For more information, see *Cisco Finesse Installation and Upgrade Guide Cisco Finesse Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html. |
| **Reporting server** | |
| Upgrade Cisco Unified Intelligence Center server. | *Installation and Upgrade Guide for Cisco Unified Intelligence Center* at<br>https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html |
| **Unified CCE Central Controller and Administration & Data Server components** | |
| **Note** To perform upgrade from CCE 12.5(x) to CCE 12.6(2) or from CCE 12.6(1) to CCE 12.6(2), refer Upgrade CCE Minor/Maintenance Release Software, on page 227. | |
| Migrate Side A Logger database, and upgrade the Logger. | Migrate Unified CCE Logger Database and Upgrade Logger, on page 239 |
| Upgrade Side A Call Router. | Upgrade Unified CCE Call Router, on page 241 |
| Upgrade the Administration & Data Server connected to Side A. | Migrate HDS Database and Upgrade Unified CCE Administration & Data Server, on page 241 |
| Bring Side A Logger and Call Router into service, bring down Side B Logger and Call Router. | Bring Upgraded Side A into Service, on page 246 |

| Task | See |
|---|---|
| Migrate Side B Logger database and upgrade the Logger. | Migrate Unified CCE Logger Database and Upgrade Logger, on page 239 |
| Upgrade Side B Call Router. | Upgrade Unified CCE Call Router, on page 241 |
| Bring Side B Call Router into service and verify operation. Bring Side B Logger into service and verify operation. | Verify Operation of Upgraded Side B Call Router and Logger, on page 247 |
| Upgrade the Administration & Data Server connected to Side B. | Migrate HDS Database and Upgrade Unified CCE Administration & Data Server, on page 241 |
| Upgrade Cisco Unified Intelligence Center reporting templates. | Import Reports 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 |
| Upgrade Unified Contact Center Management Portal(Unified CCMP). | *Installation and Configuration Guide for Cisco Unified Contact Center Management Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-management-portal/products-installation-guides-list.html |
| Upgrade Administration Client. | Upgrade Unified CCE Administration Client, on page 280 |
| Database Performance Enhancement. | Database Performance Enhancement, on page 250 |
| Certificates for Unified CCE Web Administration | Certificates for Unified Contact Center Enterprise Web Administration, on page 253 |
| **Unified CCE Peripheral Gateways and associated components** | |
| Upgrade PGs. | Upgrade Peripheral Gateways, on page 243 |
| Upgrade Outbound Option Dialer. | Upgrade Outbound Option Dialer, on page 244 |
| Upgrade Customer Collaboration Platform | *Cisco Customer Collaboration Platform User Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/socialminer/products-installation-guides-list.html. |
| Upgrade CTI OS server. | *Cisco Agent Desktop Installation Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/computer-telephony-integration-option/products-installation-guides-list.html |
| **Desktop client components** | |
| CTI OS Client desktop applications. | *Cisco Agent Desktop Installation Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/agent-desktop/products-installation-guides-list.html<br>**Note** The CTI Toolkit Desktop is only supported for System PG and other TDM PG deployments like Avaya PG. |

| Task | See |
|---|---|
| **Call processing components** | |
| Upgrade Cisco Unified Communications Manager. | *Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/ products-installation-guides-list.html |
| Upgrade (uninstall and reinstall) the JTAPI client on the Cisco Unified Communications Manager PG. | Upgrade Cisco JTAPI Client on PG, on page 250 |

[3] If you are using IP IVR for self-service and queuing, see Getting Started with Cisco Unified IP IVR.

# Common Ground Upgrade Tasks

The following section provides instructions about upgrading the virtual environment and the Unified CCE components. For instructions about upgrading non-Unified CCE components in a Unified CCE solution, for example Finesse and CUIC, see the links to component-specific documents in the Common Ground Upgrade Task Flow, on page 236.

## Migrate Unified CCE Logger Database and Upgrade Logger

To upgrade the Logger, you do the following tasks:

1. Migrate the Logger database.
2. If you use Outbound Option High Availability, do the following:
   - Migrate the Outbound Option database.
   - For the enhancements in Outbound Option High Availability to work effectively, Outbound Option High Availablity must be disabled before the logger upgrade and then enabled after the upgrade. For more information, see Disable Outbound Options High Availability (If Applicable), on page 249.
3. Install the new software.

### Procedure

**Step 1** Using Unified CCE Service Control, stop all Unified CCE services on the server and change to Manual Start.

**Step 2** (Optional) If Outbound Option High Availability is deployed, disable Outbound Options High Availability. For details, see Disable Outbound Options High Availability (If Applicable), on page 249.

**Step 3** Download the EDMT tool from Cisco.com, and ensure pre-requisites for the same have been installed on the Logger system, prior to launching EDMT. These include the ODBC Driver 17 for SQL Server, and Visual C++ Redistributable for Visual Studio 2015.

For more information about EDMT, see Preupgrade Overview, on page 231.

**Step 4** Launch the EDMT and click **Next**.

**Step 5** Select **Common Ground**, and click **Next**.

**Step 6** On the warning message, click **Yes** if you have taken a backup of your database, and no services are currently running.

**Note** If you have not taken the backup of your database, click **No** to exit the installer.

**Step 7** In the Database Connection section, highlight the database that you want to upgrade, and then click **Next**.

**Step 8** Click **Start Migration**. A warning message is displayed asking for confirmation of the data migration.

**Step 9** Click **Yes** to confirm.

**Step 10** Click **OK** to acknowledge the message. After completion of the data migration, a warning message is displayed asking you to select a valid deployment type.

**Note** This message notification is applicable only when EDMT finds the `DeploymentType` as **0(Zero)** in the **Congestion_Control** table during data migration.

**Step 11** Exit the EDMT.

**Step 12** (Optional) If Outbound Option High Availability is deployed, repeat steps 1 through 12 to migrate the BA database.

**Step 13** To upgrade the Logger, launch the ICM-CCE-Installer, and click **Next**.

**Step 14** To apply the Unified ICM 12.6(2) Maintenance Release, click **Browse** and navigate to the Maintenance Release software. Click **Next**. You can also proceed with the installation of Unified ICM 12.5(1) without selecting the Unified ICM 12.6(2) installer in this step. After installing Unified ICM 12.5(1), double-click the Unified ICM 12.6(2) installer, and proceed from step 20.

**Step 15** (Optional) Select **SQL Server Security Hardening** and click **Next**.

**Step 16** Click **OK** on any informational messages that display.

**Step 17** Click **Install**.

**Step 18** Reboot the server when the upgrade completes.

**Step 19** Log in to your system using domain credentials with administrative privileges.

**Step 20** Wait for the Unified CCE 12.6(2) installation wizard to launch. Click **Next** to proceed.

**Step 21** Select the radio button to accept the license agreement and click **Next**.

**Step 22** Click **Install** to begin the installation.

**Step 23** Select the radio button to restart the system and click **Finish**.

**Note** You can upgrade from Unified ICM 12.5(1) to Unified ICM 12.6(2) by double-clicking the Unified ICM 12.6(2) installer, and proceeding from Step 20.

**Step 24** (Optional) If you use Outbound Option High Availability, enable Outbound Option High Availablity in the Web Setup tool. For details, see the *Configure the Logger for Outbound Option* topic in the *Outbound Option Guide for Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html.

# Upgrade Unified CCE Call Router

### Procedure

**Step 1** Launch the ICM-CCE-Installer and click **Next**.

**Step 2** To apply the Unified ICM 12.6(2) Maintenance Release, click **Browse** and navigate to the Maintenance Release software. Click **Next**. You can also proceed with the installation of Unified ICM 12.5(1) without selecting the Unified ICM 12.6(2) installer in this step. After installing Unified ICM 12.5(1), double-click the Unified ICM 12.6(2) installer, and proceed from step 7.

**Step 3** Click **OK** on any informational messages that display.

**Step 4** Click **Install**.

**Step 5** Reboot the server when the upgrade completes.

**Step 6** Log in to your system using domain credentials with administrative privileges.

**Step 7** Wait for the Unified CCE 12.6(2) installation wizard to launch. Click **Next** to proceed.

**Step 8** Select the radio button to accept the license agreement and click **Next**.

**Step 9** Click **Install** to begin the installation.

**Step 10** Select the radio button to restart the system and click **Finish**.

**Note** You can upgrade from Unified ICM 12.5(1) to Unified ICM 12.6(2) by double-clicking the Unified ICM 12.6(2) installer, and proceeding from Step 7.

# Migrate HDS Database and Upgrade Unified CCE Administration & Data Server

The deployment of the Administration & Database Server determines which tools to use for an upgrade:

- For an AW-only deployment, the EDMT is not required; the ICM-CCE-Installer completes the upgrade.
- For any deployment that involves an HDS database, use the EDMT to migrate the HDS database before running the installer.

### Procedure

**Step 1** Using Unified CCE Service Control, stop all Unified CCE services on the Server and change to Manual Start.

**Step 2** For HDS-related deployments. Download the EDMT tool from Cisco.com, and ensure pre-requisites for the same have been installed on the Administration & Database Server system, before launching EDMT. These include the ODBC Driver 17 for SQL Server, and Visual C++ Redistributable for Visual Studio 2015.

For more information about EDMT, see Preupgrade Overview, on page 231.

**Step 3** Launch the EDMT and click **Next**. Select **Common Ground** and click **Next**. Review or change the information that is displayed as required and click **Start Migration**. Click **Yes** on the warning message that displays. Exit the EDMT.

**Note** This message notification is applicable only when EDMT finds the `DeploymentType` as **0 (Zero)** in the **Congestion_Control** table during data migration.

**Step 4** Launch the ICM-CCE-Installer and click **Next**.

**Step 5** To apply the Unified ICM 12.6(2) Maintenance Release, click **Browse** and navigate to the Maintenance Release software. Click **Next**. You can also proceed with the installation of Unified ICM 12.5(1) without selecting the Unified ICM 12.6(2) installer in this step. After installing Unified ICM 12.5(1), double-click the Unified ICM 12.6(2) installer, and proceed from step 11.

**Step 6** (Optional) Select **SQL Server Security Hardening** and click **Next**.

**Step 7** Click **OK** on any informational messages that display.

**Step 8** Click **Install**.

**Step 9** Reboot the server when the upgrade completes.

**Note** The time required to complete a data migration varies in a direct relationship to the database size (the larger the database size, the longer it takes to migrate) and the server hardware performance level.

For more information about configuring permissions in your local machine, see Configure Permissions in the Local Machine, on page 96.

**Step 10** Log in to your system using domain credentials with administrative privileges.

**Step 11** Wait for the Unified CCE 12.6(2) installation wizard to launch. Click **Next** to proceed.

**Step 12** Select the radio button to accept the license agreement and click **Next**.

**Step 13** Click **Install** to begin the installation.

**Step 14** Select the radio button to restart the system and click **Finish**.

**Note** You can upgrade from Unified ICM version 12.5(1) to Unified ICM 12.6(2) by double-clicking the Unified ICM 12.6(2) installer, and proceeding from Step 11.

# Upgrade Unified CCE Administration Client

**Procedure**

**Step 1** Launch the 12.5 AdminClientInstaller and click **Next**.

**Step 2** To apply the Unified ICM 12.6(2) Maintenance Release, click **Browse** and navigate to the Maintenance Release software. Click **Next**. You can also proceed with the installation of Administration Client 12.5(1) without selecting the Unified ICM 12.6(2) installer in this step. After installing Unified ICM 12.5(1), double-click the Unified ICM 12.6(2) installer, and proceed from step 6.

**Step 3** Click **OK** on any informational messages that display.

**Step 4** Click **Install**.

**Step 5** Reboot the server when the upgrade completes.

For more information about configuring permissions in your local machine, see Configure Permissions in the Local Machine, on page 96.

**Step 6** Log in to your system using domain credentials with administrative privileges. The Unified CCE Release 12.6(2) installation wizard to launches. Click **Next** to proceed.

**Step 7** Select the radio button to accept the license agreement and click **Next**.

**Step 8** Click **Install** to begin the installation.

**Step 9** Select the radio button to restart the system and click **Finish**.

# Enable Configuration Changes

**Procedure**

**Step 1** To enable configuration changes during the upgrade, set the following registry key to 0 on the Side A Call Router: **HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\Router A\Router\CurrentVersion\Configuration\Global\DBMaintenance**.

**Step 2** To confirm that configuration changes are enabled, save a configuration change.

Save your changes.

# Upgrade Peripheral Gateways

You can upgrade different Peripheral Gateways (PGs) within a contact center within different maintenance windows. However, upgrade all PGs that reside on the same virtual machine and their redundant PGs (Side A and then the corresponding Side B; or vice-versa) during the same maintenance window.

The following dependencies occur when upgrading the Unified Communications Manager PG:

- If your contact center uses Outbound Option, upgrade any Outbound Option Dialers that are associated with Unified Communications Manager PGs at the same time.
- When you upgrade the Unified Communications Manager application, upgrade the JTAPI client that is associated with the Unified Communications Manager PG at the same time.

When the CTI server that is associated with the PG gets upgraded, the CTI server connection mode is set to the Mixed mode by default. The Mixed mode enables both Secured and Non-Secured mode of connection. For the Secured mode of connection, a new port is selected based on the port selection logic. For more information on Port Utilization, see the *Port Utilization Guide for Cisco Unified Contact Center Solutions*. If the port that is selected by default conflicts with the existing ports, then you need to either release the default port or change the Secured mode port to an available port after the upgrade.

**Procedure**

**Step 1** Launch the ICM-CCE-Installer and click **Next**.

**Step 2** To apply the Unified ICM 12.6(2) Maintenance Release, click **Browse** and navigate to the Maintenance Release software. Click **Next**. You can also proceed with the installation of Unified ICM 12.5(1) without

selecting the Unified ICM 12.6(2) installer in this step. After installing Unified ICM 12.5(1), double-click the Unified ICM 12.6(2) installer, and proceed with the installation.

**Step 3** Click **OK** on any informational messages that display.

**Step 4** Click **Install**.

**Step 5** Reboot the server when the upgrade completes.

# Upgrade Outbound Option Dialer

During the upgrade, information about which contacts were called and which you need call is lost for in-process outbound campaigns. Plan the timing of the upgrade accordingly.

### Procedure

**Step 1** Launch the ICM-CCE-Installer and click **Next**.

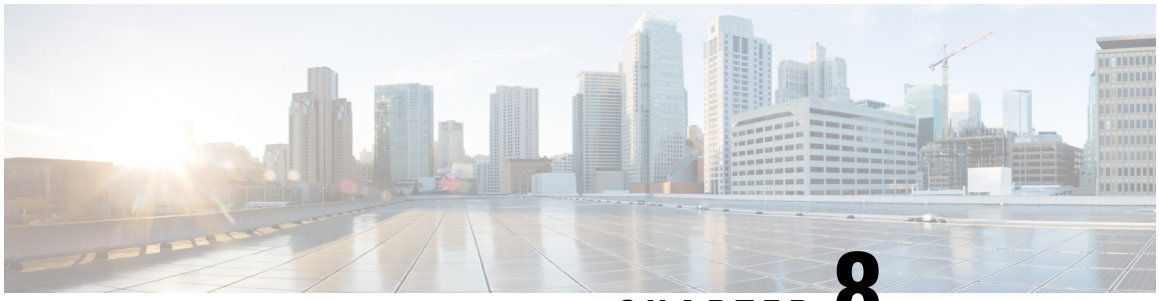
**Step 2** To apply the Unified ICM 12.6(2) Maintenance Release, click **Browse** and navigate to the Maintenance Release software. Click **Next**. You can also proceed with the installation of Unified ICM 12.5(1) without selecting the Unified ICM 12.6(2) installer in this step. After installing Unified ICM 12.5(1), double-click the Unified ICM 12.6(2) installer, and proceed with the installation.

**Step 3** Click **OK** on any informational messages that display.

**Step 4** Click **Install**.

**Step 5** Reboot the server when the upgrade completes.

**Step 6** Use Unified CCE Service Control to set all Unified CCE services to Automatic Start.



CHAPTER 8

# Common Upgrade Tasks


- Upgrade Voice and Data Gateways, on page 245
- Bring Upgraded Side A into Service, on page 246
- Verify Operation of Upgraded Side B Call Router and Logger, on page 247
- Disable Outbound Options High Availability (If Applicable), on page 249
- Upgrade Cisco JTAPI Client on PG, on page 250
- Database Performance Enhancement, on page 250
- Certificates for Unified Contact Center Enterprise Web Administration, on page 253


# Upgrade Voice and Data Gateways

Perform the following procedure on each machine that hosts gateways that are used for TDM ingress, Outbound Option dialer egress, and VXML processing.

### Procedure

**Step 1** For VXML gateways only, perform this step. For all other gateways, proceed to the next step.

Run the `#copy tftp flash <IP Address> <filename>.bin` command to copy the flash from a remote machine to the gateway.

**Step 2** Run the `#sh flash` command to check the version.

**Step 3** Run the following commands in order:

a) `#conf t`
b) `#no boot system flash: <old image>`
c) `#boot system flash: <new image>`
d) `#wr`
e) `#reload`

**Step 4** Run the `#sh version` command to verify that the new version shows in the gateway.

# Bring Upgraded Side A into Service

After the Side A Unified CCE Logger, Call Router, and Administration & Data Server are upgraded, follow this procedure to bring Side A into service.

The logger and distributor services run with existing service logon account and is authorized by service security group in the domain. If you want to run logger and distributor services with local authorization, then you have to modify the service accounts using **Service Account Manager** Tool.

For more information on how to run Service Account Manager tool, see the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

### Before you begin

If the External DBLookUp is configured update the External DBLookUp registry value using the CCEDataProtect Tool. For more information, see **Configure External DBLookUp Registry Value using CCEDataProtect Tool** procedure 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.

**Note** If the external remote database is on SQL Server 2017 version, you have to install the ODBC Driver 17 manually on the server hosting the external database. Download the ODBC Driver 17 from Microsoft.

### Procedure

**Step 1** Use Unified CCE Service Control to stop all Unified CCE services on the side B Call Router and Logger. However, before stopping Side B Router and Logger, also make sure that all non-upgraded Adminitration and Data Servers are stopped and shutdown, before starting the upgraded Side A Logger and Router servers.

**Step 2** Manually start the Unified CCE services on the Side A Call Router and Logger, and the upgraded Administration & Data Server. Verify the following basic operations of the Side A Central Controller categories:

| Category | Operation |
|---|---|
| General | • Setup logs indicate no errors or failure conditions.<br>• AD domain has all users.<br>• Schema upgrade is successful for all databases (no loss of data integrity or loss of data).<br>• All component services start without errors.<br>• Calls are successfully processed. |
| Call Router | • The Rtsvr logs indicate that the upgraded Administration & Data Server has connected successfully. |

| Category | Operation |
|---|---|
| Logger | • Recovery process that is not required, no activity other than process start up.<br>• Users are in correct domain.<br>• Configuration information is passed to Call Router.<br>• Replication process begins when HDS comes online. |
| Administration & Data Server | • The updateAW process logs indicate that the Administration & Data Server is waiting for work.<br>• Replication process begins with no errors.[4] |
| Security | • Specified users are able to use configuration manager. |
| Script Editor | • Previous settings for users are present when application is opened.<br>• Validate All script yields the same results that the preupgrade test yielded.<br>• You can open, edit, delete, or create new scripts. |
| ICMDBA | • Import or Export functionality is present.<br>• Database space allocation and percent used are correct. |

[4] During replication, data from Config_Message_Log table is replicated from Logger database to AW database. A purge mechanism is also introduced for Config_Message_Log table in AW Database. The default retention period is set to 90 days. To change the retention period, modify the following registry key:

```
Cisco Systems,

Inc.\ICM\<instancename>\Distributor\RealTimeDistributor
\CurrentVersion\Recovery\CurrentVersion\Purge\Retain\System\ConfigMessageLog
```

**Step 3** Use Unified CCE Service Control to set the Unified CCE services to Automatic Start on each of the upgraded Unified CCE components.

**Step 4** Verify production system operation while running with the upgraded Side A Call Router and Side A Logger.

# Verify Operation of Upgraded Side B Call Router and Logger

### Before you begin

The logger and distributor services that are run with existing service logon account and is authorized by service security group in the domain. If you want to run logger and distributor services with local authorization, then you have to modify the service accounts using Service Account Manager Tool.

For more information on how to run Service Account Manager tool, see the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

### Procedure

**Step 1** Before bringing Side B into service, manually synchronize Logger B to Logger A using ICMDBA.

**Step 2** Start the Side B Call Router and Logger services.

As each node starts up, it searches for the other server components and attempts to register with them. If you completed the ICM-CCE-Installer and network testing successfully, no major errors should occur.

To verify whether a process is up, use the Diagnostic Framework Portico ListProcess option, available through the Unified CCE Tools shortcut that is created by the installer.

In order to add configuration data, the Central Controller, and Administration & Data Servers must be running.

Verify that the Unified CCE processes have no errors:

| Category | Operation |
|---|---|
| Call Routers | • Router: Running and synchronized with peer.<br>• Rtsvr: Indicates no connectivity to Administration & Data Server currently. |
| Loggers | • Logger: Connected to its respective database and synchronized with peer. MDS is in service.<br>• Replication: No connectivity to Administration & Data Server HDS currently. |

**Step 3** To start the Unified CCE Distributor services, verify that the Unified CCE processes have no errors.

| Category | Operation |
|---|---|
| Call Routers | • Router: Running and synchronized with peer.<br>• CCAgent: In service, and without any errors.<br>• Rtsvr: Feed activated to Administration & Data Server. |
| Loggers | • Logger: Connected to its respective database and synchronized with peer. MDS is in service.<br>• Replication: Connected to the Administration & Data Server. |
| Administration & Data Server | • Updateaw: Displays "Waiting for new work."<br>• Iseman: Listen thread waiting for client connection. (Exists only if Internet Script Editor is configured).<br>• Replication: Replication and recovery client connection initialized. [5] |

[5] **Note** During replication, data from Config_Message_Log table is replicated from Logger database to AW database. A purge mechanism is also introduced for Config_Message_Log table in AW Database. The default retention period is set to 90 days. To change the retention period, modify the following registry key:

```
Cisco Systems, Inc.\ICM\<instancename>\Distributor\RealTimeDistributor
\CurrentVersion\Recovery\CurrentVersion\Purge\Retain\System\ConfigMessageLog
```

**Step 4** Validate the following settings from the system diagram for the Production Environment and make the required changes before you place the systems in production:

a) Clear event logs.
b) Remove any media from drives.
c) Ensure that all services are set to Manual Start. Services are not set to Automatic Start until after the implementation testing in the production environment.

**Step 5** Verify overall system operation.

**Step 6** Enable configuration changes.

a) Set the following registry key to 0 on the Side A and Side B Call Routers of the system: **HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\Router<A/B>\Router\CurrentVersion\Configuration\Global\DBMaintenance**.
b) Verify that configuration changes can be made.

**Step 7** Upgrade any other Administration & Data Servers or HDSs using the steps that are documented in Migrate HDS Database and Upgrade Unified CCE Administration & Data Server, on page 241.

# Disable Outbound Options High Availability (If Applicable)

### Before you begin

If Outbound Options High Availability is enabled, you must disable it on source machines before you perform the upgrade.

Before proceeding with the following steps, ensure that Outbound Options feature is in maintenance mode. There must not be any customer records getting imported to Outbound database. The outbound campaigns must not be active and outbound callflow must not be in progress.

Perform the following steps on Side A:

### Procedure

**Step 1** Launch **Websetup**. Navigate to **Component Management** > **Loggers**.

**Step 2** Edit the **Logger** and navigate to **Additional Options**. Uncheck **Enable High Availability** under **Outbound Option** and click **Next**.

**Step 3** Enable **Stop and then start(cycle) the Logger Service for this instance (if it is running)** checkbox . Click **Next** to complete the setup.

**Step 4** Repeat similar steps (steps 1, 2, and 3) for side B.

### What to do next

You can enable Outbound Options High Availability after the upgrade is successful.

# Upgrade Cisco JTAPI Client on PG

If you upgrade Unified Communications Manager (Unified CM) in the contact center, also upgrade the JTAPI client that resides on the PG. To upgrade the JTAPI client, uninstall the old version of the client, restart the server, and reinstall a new version. You install the JTAPI client using the Unified Communications Manager Administration application.

To install the JTAPI client for the Unified CM release that you have upgraded to, see the Install Cisco JTAPI Client on PG, on page 51 topic.

### Before you begin

Before you perform this procedure, you must:

- Uninstall the old JTAPI client from the Unified Communications Manager PG
- Restart the PG server.

# Database Performance Enhancement

After you perform a Common Ground or a Technology Refresh upgrade, complete the procedures described in this section to enhance the performance of the database. This is a one-time process and must be run only on the Logger and AW-HDS databases during a maintenance window.

- Performance Enhancement of TempDB, on page 250 (You can skip this when performing a Technology Refresh upgrade)
- Performance Enhancement of Logger Database, on page 251
- Performance Enhancement of AW-HDS Database, on page 252

## Performance Enhancement of TempDB

Perform this procedure on Logger, Rogger, AW-HDS-DDS, AW-HDS and HDS-DDS machines to get the benefits of TempDB features for SQL Server. For more information about the SQL Server TempDB Database and its use, see the Microsoft SQL Server documentation for TempDB Database.

**Note** This procedure applies to the Common Ground upgrade process only.

**Note** If the Performance Enhancement of TempDB procedure is already completed on Unified CCE 12.5(1) or 12.6(1), then do not repeat the same procedure upon upgrading to Unified CCE 12.6(2).

**Procedure**

**Step 1** Use **Unified CCE Service Control** to stop the Logger and Distributor services.

**Step 2** Login to **SQL Server Management Studio** and run the following queries on the primary database.

- To modify the existing TempDB Initial size to the recommended value:

```
ALTER DATABASE tempdb MODIFY FILE
   (NAME = 'tempdev', SIZE = 800, FILEGROWTH = 100)
ALTER DATABASE tempdb MODIFY FILE
   (NAME = 'templog', SIZE = 600, FILEGROWTH = 10%)
```

- To add multiple TempDB files:

```
USE [master];
GO
ALTER DATABASE [tempdb] ADD FILE (NAME = N'tempdev2', FILENAME = N'<SQL Server TempDB
path>' , SIZE = 800 , FILEGROWTH = 100);
ALTER DATABASE [tempdb] ADD FILE (NAME = N'tempdev3', FILENAME = N'<SQL Server TempDB
path>' , SIZE = 800 , FILEGROWTH = 100);
ALTER DATABASE [tempdb] ADD FILE (NAME = N'tempdev4', FILENAME = N'<SQL Server TempDB
path>' , SIZE = 800 , FILEGROWTH = 100);
GO
```

**Note**

- For example,

  ```
  <SQL Server TempDB path> = C:\Program Files\Microsoft SQL
  Server\MSSQL12.MSSQLSERVER\MSSQL\DATA\tempdev2.ndf
  ```

- Make sure that you modify the values in the query based on the machines. For more information, see Increase Database and Log File Size for TempDB, on page 25.

**Step 3** Restart the SQL Services.

**Step 4** Start the Logger and Distributor services.

# Performance Enhancement of Logger Database

Perform this procedure on Side A and Side B of the Logger database.

**Procedure**

**Step 1** Use the Unified CCE Service Control to stop the Logger service.

**Step 2** From the command prompt, run the **RunFF.bat** file which is located in the `<ICM install directory>:\icm\bin` directory.

**Step 3** Proceed with the application of fill factor to Unified ICM databases.

**Note:** Based on the size of the database, it takes several minutes to several hours to apply fill factor to the database. For example, it takes anywhere between 2 to 3 hours for a 300-GB HDS. After the process is completed, the log file is stored in `<SystemDrive>:\temp\<DatabaseName>_Result.txt`.

**Step 4** Use the Unified CCE Service Control to start the Logger service.

### Troubleshooting Tips

See the `RunFF.bat/help` file for more information.

# Performance Enhancement of AW-HDS Database

### Procedure

**Step 1** Use the Unified CCE Service Control to stop the Distributor service.

**Step 2** From the command prompt, run the **RunFF.bat** file which is located in the `<ICM install directory>:\icm\bin` directory.

**Step 3** Proceed with the application of fill factor to Unified ICM databases.

**Note:** Based on the size of the database, it takes several minutes to several hours to apply fill factor to the database. For example, it takes between 2 to 3 hours for a 300-GB HDS. After the process is completed, the log file is stored in `<SystemDrive>:\temp\<DatabaseName>_Result.txt`.

**Step 4** Use the Unified CCE Service Control to start the Distributor service.

### Troubleshooting Tips

See the `RunFF.bat/help` file for more information.

## Improve Reporting Performance

To improve the performance of the reporting application, modify the following Windows settings on the database servers (AW-HDS, AW-HDS-DDS, HDS-DDS).

- Increase the Paging File Size to 1.5 times the server's memory.

  To change the Paging File Size, from the Control Panel search for Virtual Memory. In the Virtual Memory dialog box, select **Custom size**. Set both **Initial size** and **Maximum size** to 1.5 times the server memory.

- Set the server's **Power Options** to **High Performance**.

  From the Control Panel, select **Power Options**. By default, the **Balanced** plan is selected. Select **Show additional plans** and select **High performance**.

In SQL Server, disable **Auto Update Statistics** for AW and HDS databases.

In the SQL Server Management Studio, right-click the database name in the Object Explorer and select **Properties**. Select the **Options** page. In the **Automatic** section of the page, set **Auto Create Statistics** and **Auto Update Statistics** to **False**.

## Reduce Reserved Unused Space for HDS and Logger

Enable trace flag 692 on HDS database server to reduce the growth of reserved unused space on the AW-HDS, AW-HDS-DDS, HDS-DDS database servers and Logger database, after you upgrade or migrate to Microsoft SQL 2017 or 2019. For more information about the trace flag 692, see the Microsoft Documentation.

**Procedure**

Run the following command to enable trace flag 692 on HDS database server and Logger database:

```
DBCC TRACEON (692, -1);
GO
```

**Note** An increase in the unused space may lead to unexpected purge trigger in HDS and Logger, trace flag 692 helps in mitigating this unexpected purge issue. After you enable the trace flag, there will be an increase of 10% to 15% CPU for a short duration. If the trace flag needs to be retained, the server startup options has to be updated using the -T(upper case) option. For more information, see https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/database-engine-service-startup-options?view=sql-server-ver15.

## Update User Role

To update the User Role in the database for the existing users, do the following in any one of the AW (distributor) machines:

- Go to the link https://software.cisco.com/download/home/268439622/type and select User Role Update Bulk Tool from the list.
- Download the file UserRoleUpdateScript_1201.zip and extract it.
- Open Windows Powershell and run the script UserRoleUpdate.PS1.

# Certificates for Unified Contact Center Enterprise Web Administration

**Note**

- You must import self-signed certificates of solution components into the AW machines, if you are not using CA-signed certificates.
- Make sure that the certificates in the keystore pertain to the fully qualified domain name (FQDN) of the servers. If you have changed the domain name or hostname, be sure to update the certificates in the keystore.

## CA Certificates

The following table outlines the CA certificate tasks for each component.

| Components | Tasks |
|---|---|
| Unified CCE Components | 1. Generate CSR, on page 255<br>2. Create Trusted CA-Signed Server or Application Certificate , on page 255<br>3. Upload and Bind CA-Signed Certificate, on page 257 |
| Customer Voice Portal (CVP) Call Server/CVP Reporting Server[6] | See *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html |
| Email and Chat | See *Enterprise Chat and Email Installation and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html |
| Cisco Unified Communications Manager (CUCM) | See *Security Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html |
| Cisco Unified Intelligence Center (CUIC) | Obtain and Upload Third-party CA Certificate, on page 264 |
| Cisco Finesse | See *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html<br>Deploy Certificate in Browsers, on page 179 |
| Live Data | Obtain and Upload Third-party CA Certificate, on page 264 |
| Cisco Identity Service (IdS) | 1. From the IdS server, generate and download a Certificate Signing Requests (CSR).<br>2. Obtain Root and Application certificates from the third-party vendor.<br>3. Upload the appropriate certificates to the IdS server.<br>For more information, see https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-configuration-examples-list.html. Ensure to run the instructions in IdS server. |
| Cloud Connect | Obtain and Upload Third-party CA Certificate, on page 264 |
| Virtualized Voice Browser (VVB) | See *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html |

| Components | Tasks |
|---|---|
| Customer Collaboration Platform | See *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html |

[6] CA certificate instructions for CVP Reporting Server are similar to CVP call server.

## Generate CSR

This procedure explains how to generate a Certificate Signing Request (CSR) from Internet Information Services (IIS) Manager.

### Procedure

**Step 1** Log in to Windows and choose **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

**Step 2** In the **Connections** pane, click the server name.
The server **Home** pane appears.

**Step 3** In the **IIS** area, double-click **Server Certificates**.

**Step 4** In the **Actions** pane, click **Create Certificate Request**.

**Step 5** In the **Request Certificate** dialog box, do the following:

a) Specify the required information in the displayed fields and click **Next**.
b) In the **Cryptographic service provider** drop-down list, leave the default setting.
c) From the **Bit length** drop-down list, select 2048.

**Step 6** Specify a file name for the certificate request and click **Finish**.

## Create Trusted CA-Signed Server or Application Certificate

You can create CA-signed certificate in any one of the following ways:

- Create certificate internally. Do the following:
  1. Set up Microsoft Certificate Server for Windows Server, on page 264
  2. Download the CA-signed certificate on each component server. Do the following:
     a. Open the CA server certificate page (*https://<CA-server-address>/certsrv*).
     b. Click **Request a Certificate** and then click **advanced certificate request**. Then do the following:
        1. Copy the Certificate Request content in the **Base-64-encoded certificate request** box.
        2. From the **Certificate Template** drop-down list, choose Web Server.
        3. Click **Submit**.
        4. Choose **Base 64 encoded**.
        5. Click **Download certificate** and save it to the desired destination folder.

c. On the CA server certificate page, click **Download a CA Certificate, Certificate Chain, or CRL**, and then do the following:

1. Select the Encoding method as **Base 64**.
2. Click **Download CA Certificate** and save it to the desired destination folder.

3. Import the Root CA and Intermediate Authority certificates into Windows trust store of every component. For more information on how to import CA certificates into Windows trust store, see *Microsoft* documentation.
4. Import the Root CA and Intermediate Authority certificates into Java keystore of every component. For more information, see Import CA Certificate into AW Machines, on page 256.

- Obtain certificate from a trusted Certificate Authority (CA). Do the following:

1. Send the CSR to a trusted Certificate Authority (CA) for sign-off.
2. Obtain the CA-signed application certificate, Root CA certificate, and Intermediate Authority certificate (if any).
3. Import the Root CA and Intermediate Authority certificates into Windows trust store of every component. For more information on how to import CA certificates into Windows trust store, see *Microsoft* documentation.
4. Import the Root CA and Intermediate Authority certificates into Java keystore of every component. For more information, see Import CA Certificate into AW Machines, on page 256.

## Import CA Certificate into AW Machines

### Procedure

**Step 1** Log in to the AW-HDS-DDS Server.

**Step 2** Run the following command:

```
cd %CCE_JAVA_HOME%\bin
```

**Step 3** Copy the Root or intermediate certificates to a location in AW Machine.

**Step 4** Remove the existing certificate by running the following command:

```
keytool.exe -delete -alias <AW FQDN> -keystore <ICM install directory>\ssl\cacerts
```

**Step 5** Enter the truststore password when prompted.

The default truststore password is **changeit**.

**Note** To change the truststore password, see Change Java Truststore Password, on page 266.

**Step 6** At the AW machine terminal, run the following command:

- `cd %CCE_JAVA_HOME%\bin`
- `keytool.exe -import -file <certificate with fully qualified path> -alias <alias name> <AW FQDN> -keystore <ICM install directory>\ssl\cacerts`

**Step 7** Enter the truststore password when prompted.

**Step 8** Go to Services and restart Apache Tomcat.

**Note** For more information, refer to **Custom Truststore to Store Component Certificate** section.

## Upload and Bind CA-Signed Certificate

### Upload CA-Signed Certificate to IIS Manager

This procedure explains how to upload a CA-Signed certificate to IIS Manager.

#### Before you begin

Ensure that you have the Root certificate, and Intermediate certificate (if any).

#### Procedure

**Step 1** Log in to Windows and choose **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

**Step 2** In the **Connections** pane, click the server name.

**Step 3** In the **IIS** area, double-click **Server Certificates**.

**Step 4** In the **Actions** pane, click **Complete Certificate Request**.

**Step 5** In the **Complete Certificate Request** dialog box, complete the following fields:

a) In the **File name containing the certification authority's response** field, click the **…** button.

b) Browse to the location where signed certificate is stored and then click **Open**.

c) In the **Friendly name** field, enter the FQDN of the server.

**Step 6** Click **OK** to upload the certificate.
If the certificate upload is successful, the certificate appears in the **Server Certificates** pane.

### Bind CA-Signed Certificate to IIS Manager

*Bind CCE Web Applications*

This procedure explains how to bind a CA Signed certificate in the IIS Manager.

#### Procedure

**Step 1** Log in to Windows and choose **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

**Step 2** In the **Connections** pane, choose **<server_name>** > **Sites** > **Default Web Site**.

**Step 3** In the **Actions** pane, click **Bindings...**.

**Step 4** Click the type **https** with port 443, and then click **Edit...**.

**Step 5** From the **SSL certificate** drop-down list, select the uploaded signed Certificate Request.

**Step 6** Click **OK**.

**Step 7** Navigate to **Start** > **Run** > **services.msc** and restart the IIS Admin Service.
If IIS is restarted successfully, certificate error warnings do not appear when the application is launched.

*Bind Diagnostic Framework Service*

This procedure explains how to bind a CA Signed Certificate in the Diagnostic Portico.

**Procedure**

**Step 1** Open the command prompt.

**Step 2** Navigate to the Diagnostic Portico home folder using:

**cd <ICM install directory>:\icm\serviceability\diagnostics\bin**

**Step 3** Remove the current certificate binding to the Diagnostic Portico tool using:

**DiagFwCertMgr /task:UnbindCert**

**Step 4** Open the signed certificate and copy the hash content (without spaces) of the Thumbprint field. Run the following command:

**DiagFwCertMgr /task:BindCertFromStore /certhash:<hash_value>**

If certificate binding is successful, it displays "The certificate binding is VALID" message.

**Step 5** Validate if the certificate binding was successful using:

**DiagFwCertMgr /task:ValidateCertBinding**

**Note** DiagFwCertMgr uses port 7890 by default.

If certificate binding is successful, it displays "The certificate binding is VALID" message.

**Step 6** Restart the **Diagnostic Framework** service by running the following command:

**sc stop "diagfwsvc"**

**sc start "diagfwsvc"**

If Diagnostic Framework restarts successfully, certificate error warnings do not appear when the application is launched.

# Self-signed Certificates

The following table lists components from which self-signed certificates are generated and components into which self-signed certificates are imported.

**Note** To establish a secure communication, run the commands (given in the links below) in the Command Prompt as an Administrator (right click over the **Command Prompt** and select **Run as administrator**).

| Import Self-signed Certificates to Target Server | Generate Self-signed Certificates from Source Component Server | Links |
|---|---|---|
| AW Machines | Unified CCE Components (Router, Logger[7], Rogger[8], PGs, and HDS) | Import Unified CCE Component Certificates, on page 259<br>Import Diagnostic Framework Portico Certificate into AW Machines, on page 260 |
| | Cisco Finesse | Import VOS Components Certificate, on page 261 |
| | Cisco Unified Intelligence Center (CUIC) Publisher and Subscriber | |
| | Cisco Identity Service (IdS) Publisher and Subscriber | |
| | Cloud Connect | |
| | Customer Collaboration Platform | |
| Logger | AW | Import Unified CCE Component Certificates, on page 259 |
| Rogger | | |

[7] Router and Logger are applicable only for 12000 Agent deployments.
[8] Applicable only for 2000 and 4000 Agent deployments.

## Import Unified CCE Component Certificates

This procedure explains how to import self-signed certificates from a source Unified CCE component sever to a target server.

**Important** The certificate CommonName (CN) must match the Fully Qualified Domain Name (FQDN) provided for the Unified CCE components in the Unified CCE Inventory.

### Procedure

**Step 1** Log in to the required Unified CCE component server.

**Step 2** From the browser (*https://<FQDN of the Unified CCE component server>*), download the certificate.

If you want to regenerate RSA a certificate instead of using the existing certificate, run the following commands:

a) From the **Cisco Unified CCE Tools** folder, launch the **SSL Encryption Utility**.
b) Go to the **Certificate Administration** tab and click **Uninstall**.
c) Click **Yes** to confirm uninstallation of certificate.

A message is displayed upon successful uninstallation of the certificate.

d) Click **Install** to generate a new certificate.

**Step 3** Copy the certificate to a location in the target server.

**Step 4** Run the following command at the target server (machine terminal):

- `cd %CCE_JAVA_HOME%\bin`
- `keytool.exe -import -file <certificate with fully qualified path> -alias <alias name> -keystore <ICM install dir>\ssl\cacerts`

**Step 5** Enter the truststore password when prompted.

The default truststore password is **changeit**.

**Note** To change the truststore password, see Change Java Truststore Password, on page 266.

**Step 6** Go to Services and restart Apache Tomcat on target servers.

## Import Diagnostic Framework Portico Certificate into AW Machines

Generate Diagnostic Framework Portico self-signed certificate on each CCE component server and import them into all AW Machines.

### Procedure

**Step 1** Log in to the CCE component server.

**Step 2** From the Unified CCE Tools, open the Diagnostic Framework Portico.

**Step 3** Download the self-signed certificate from the browser.

**Step 4** Copy the certificate to a location in AW Machine.

**Step 5** Run the following command at the AW machine terminal:

- `cd %CCE_JAVA_HOME%\bin`
- `keytool.exe -import -file <certificate with fully qualified path> -alias <alias name> <FQDN of the CCE component Server> -keystore <ICM install dir>\ssl\cacerts`

**Note** The alias name of the CCE component server must be different from the alias name given while creating the CCE component server's self-signed certificate.

**Step 6** Enter the truststore password when prompted.

The default truststore password is **changeit**.

**Note** To change the truststore password, see Change Java Truststore Password, on page 266.

**Step 7** Go to Services and restart Apache Tomcat.

## Import VOS Components Certificate

This procedure explains how to import self-signed certificates from a source VOS component sever to a target server.

**Important** The certificate CommonName (CN) must match the Fully Qualified Domain Name (FQDN) provided for the respective component servers in the CCE Inventory.

### Procedure

**Step 1** Sign in to the **Cisco Unified Operating System Administration** on the source component server using the URL (*https://<FQDN of the Component server>:8443/cmplatform*).

**Step 2** From the **Security** menu, select **Certificate Management**.

**Step 3** Click **Find**.

**Step 4** Do one of the following:

- If the tomcat certificate for your server is not on the list, click **Generate Self-signed**. When the certificate generation is complete, reboot your server.
- If the tomcat certificate for your server is on the list, click the certificate to select it. (Ensure that the certificate you select includes the hostname for the server.)

**Step 5** Download the self-signed certificate that contains hostname of the primary server.

**Step 6** Copy the certificate to a location in the target server.

**Step 7** Run the following command as an administrator at the target server (machine terminal):

- `cd %CCE_JAVA_HOME%\bin`
- `keytool.exe -import -file <certificate with fully qualified path> -alias <alias name> <FQDN of component Server> -keystore <ICM install directory>\ssl\cacerts`

**Step 8** Enter the truststore password when prompted.

The default truststore password is **changeit**.

**Note** To change the truststore password, see Change Java Truststore Password, on page 266.

**Step 9** Go to Services and restart Apache Tomcat.

# Certificates for Live Data

## Certificates and Secure Communications

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

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

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

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

**Note** After the successful upgrade, the CAs that are unapproved by Cisco are removed from the platform trust store. You can add them back, if necessary.

- For information about the list of CAs that Cisco supports, see the Cisco Trusted External Root Bundle at https://www.cisco.com/security/pki.
- For information about adding a certificate, see Insert a new tomcat-trust certificate.

## Self-Signed Certificates and Third-Party CA Certificates

For secure Cisco Finesse, Cisco Unified Intelligence Center, AWDB, and Live Data server-to-server communication, you must set up security certificates (Applicable for both Self-Signed and Third-Party CA Certificates):

- For Cisco Finesse and Cisco Unified Intelligence Center servers to communicate with the Live Data server, you must to import the Live Data certificates and Cisco Unified Intelligence Center certificates into Cisco Finesse, and the Live Data certificates into Cisco Unified Intelligence Center.
- For Live Data servers to communicate with AWDB servers, you must import AWDB certificates into Live Data.
- For Live Data servers to communicate with Cisco Unified Intelligence Center servers, you must import Cisco Unified Intelligence Center servers certificates into Live Data.

| On Server | Import Certificates From |
|---|---|
| Finesse | Live Data and Cisco Unified Intelligence Center |
| Live Data | AW Database<br>Cisco Unified Intelligence Center |
| Cisco Unified Intelligence Center | Live Data |

### Export Self-Signed Live Data Certificates

Live Data installation includes the generation of self-signed certificates. If you choose to work with these self-signed certificates (rather than producing your own CA certificate or obtaining a CA certificate from a third-party certificate vendor), you must first export the certificates from Live Data and Cisco Unified Intelligence Center, as described in this procedure. You must export from both Side A and Side B of the Live Data and Cisco Unified Intelligence Center servers. You must then import the certificates into Finesse, importing both Side A and Side B certificates into each side of the Finesse servers.

As is the case when using other self-signed certificates, agents must accept the Live Data certificates in the Finesse desktop when they sign in before they can use the Live Data gadget.

### Procedure

**Step 1** Sign in to Cisco Unified Operating System Administration on Cisco Unified Intelligence Center (https://*hostname of Cisco Unified Intelligence Center server*/cmplatform).

**Step 2** From the **Security** menu, select **Certificate Management**.

**Step 3** Click **Find**.

**Step 4** Do one of the following:

- If the tomcat certificate for your server is on the list, click the certificate to select it. (Ensure that the certificate you select includes the hostname for the server.)
- If you are using self-signed certificate, do the following:
  **a.** Click **Generate New**.
  **b.** When the certificate generation is complete, restart the Cisco Tomcat service and the Cisco Live Data NGNIX service.
  **c.** Restart this procedure.

**Step 5** Click **Download .pem file** and save the file to your desktop.

Be sure to perform these steps for both Side A and Side B.

**Step 6** After you have downloaded the certificates from Cisco Unified Intelligence Center, sign in to Cisco Unified Operating System Administration on the Live Data server (http://hostname of LiveData server/cmplatform), and repeat steps 2 to 5. This is applicable only for Standalone LiveData.

### What to do next

You must now import the Live Data and Cisco Unified Intelligence Center certificates into the Finesse servers.

## Import Self-Signed Live Data Certificates

To import the certificates into the Finesse servers, use the following procedure.

### Procedure

**Step 1** Sign in to Cisco Unified Operating System Administration on the Finesse server using the following URL:

http://*FQDN of Finesse server*:8443/cmplatform

**Step 2** From the **Security** menu, select **Certificate Management**.

**Step 3** Click **Upload Certificate**.

**Step 4** From the **Certificate Name** drop-down list, select **tomcat-trust**.

**Step 5** Click **Browse** and browse to the location of the Cisco Unified Intelligence Center certificate (with the **.pem** file extension).

**Step 6** Select the file, and click **Upload File**.

**Step 7** After you have uploaded the Cisco Unified Intelligence Center certificate repeat steps 3 to 6 for Live Data certificates.This is applicable only for standalone Live Data.

**Step 8** After you upload both the certificates, restart Cisco Finesse Tomcat on the Finesse server.

#### What to do next

Be sure to perform these steps for both Side A and Side B.

### Obtain and Upload Third-party CA Certificate

You can use a Certification Authority (CA) certificate provided by a third-party vendor to establish an HTTPS connection between the Live Data, Cisco Finesse, Cisco Unified Intelligence Center servers, and Cloud Connect servers.

To use third-party CA certificates:

- From the **Cisco Unified Operating System Administrator** of Live Data, Cisco Finesse, Cisco Unified Intelligence Center, and Cloud Connect servers, generate and download a Certificate Signing Requests (CSR).
- Obtain root and application certificates from the third-party vendor.
- Upload the appropriate certificates to the Live Data, Unified Intelligence Center, Cisco Finesse, and Cloud Connect servers.

Follow the instructions provided in the *Unified CCE Solution: Procedure to Obtain and Upload Third-Party CA certificates (Version 11.x)* technical note at https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-enterprise-1101/200286-Unified-CCE-Solution-Procedure-to-Obtai.html .

## Produce Certificate Internally

### Set up Microsoft Certificate Server for Windows Server

This procedure assumes that your deployment includes a Windows Server Active Directory server. Perform the following steps to add the Active Directory Certificate Services role on the Windows Server domain controller.

#### Before you begin

Before you begin, Microsoft .Net Framework must be installed. See Windows Server documentation for instructions.

#### Procedure

**Step 1** In Windows, open the **Server Manager**.

**Step 2** In the **Quick Start** window, click **Add Roles and Features** .

**Step 3** In the **Set Installation Type** tab, select **Role-based or feature-based installation** , and then click **Next**.

**Step 4** In the **Server Selection** tab, select the destination server then click **Next**.

**Step 5** In the **Server Roles** tab, check the **Active Directory Certificate Services** box, and then click the **Add Features** button in the pop-up window.

**Step 6** In the **Features** and **AD CS** tabs, click **Next** to accept default values.

**Step 7** In the **Role Services** tab, verify that **Certification Authority**, **Certification Authority Web Enrollment**, **Certificate Enrollment Web Service**, and **Certificate Enrollment Policy Web Service** boxes are box is checked, and then click **Next**.

**Step 8** In the **Confirmation** tab, click **Install**.

**Step 9** After the installation is complete, click the **Configure Active Directory Certificate Service on the destination server** link.

**Step 10** Verify that the credentials are correct (for the domain Administrator user), and then click **Next**.

**Step 11** In the **Role Services** tab, check the **Certification Authority**, **Certification Authority Web Enrollment**, **Certificate Enrollment Web Service**, and **Certificate Enrollment Policy Web Service** boxes box, and then click **Next**.

**Step 12** In the **Setup Type** tab, select **Enterprise CA**, and then click **Next**.

**Step 13** In the **CA Type** tab, select **Root CA**, and then click **Next**.

**Step 14** In the **Private Key**, **Cryptography**, **CA Name**, **Validity Period**, and **Certificate Database** tabs, click **Next** to accept default values.

**Step 15** In the following tabs, leave the default values, and click **Next**.

a. **CA for CES**

b. **Authentication Type for CES**

c. **Service Account for CES**

d. **Authentication Type for CEP**

**Step 16** Review the information in the **Confirmation** tab, and then click **Configure**.

### Download CA certificate

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

#### Procedure

**Step 1** On the Windows domain controller, run the CLI command certutil -ca.cert *ca_name*.cer, in which *ca_name* is the name of your certificate.

**Step 2** Save the file. Note where you saved the file so you can retrieve it later.

## Set Up CA Certificate for Firefox Browser

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

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

**Procedure**

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

# Change Java Truststore Password

This procedure explains how to change a truststore password in a Windows machine.

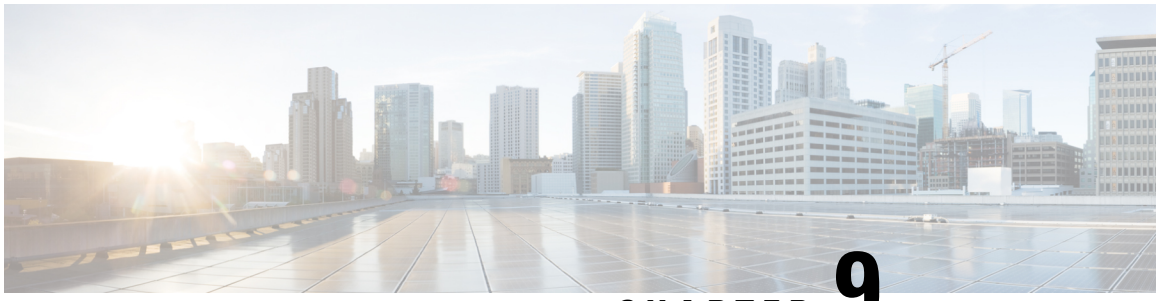
**Procedure**

**Step 1** Log in to the Windows machine.
**Step 2** Run the following command:

```
cd %CCE_JAVA_HOME%\bin
```

**Step 3** Change the truststore password by running the following command:

```
keytool.exe -storepasswd -keystore <ICM install dir>\ssl\cacerts
Enter keystore password:  <old-password>
New keystore password:  <new-password>
Re-enter new keystore password:  <new-password>
```



CHAPTER 9

# Technology Refresh Upgrade


- Preupgrade Overview, on page 267
- Technology Refresh Preupgrade Task flow, on page 268
- Technology Refresh Upgrade Task Flow, on page 269
- Technology Refresh Upgrade Tasks, on page 272


## Preupgrade Overview

The preupgrade process ensures that your systems have the necessary software to support your contact center. These tasks prepare the way for a successful upgrade of your Cisco contact center components to the new release.

**Note** During Unified CCE installation on to Windows Server 2019 and SQL Server 2019, SQL Server Security Hardening optional configuration should not be selected as part of installation. SQL Security Hardening should be applied post Unified CCE installation using Security Wizard tool.

### Preupgrade Tools

During the preupgrade process, use the following tools as required:

- User Migration Tool—A standalone Windows command-line application used for all upgrades that involve a change of domain. The tool exports all existing user accounts (config/setup and supervisors) from the source domain to a `.bin` file. The file is used in the target domain during the upgrade.

  You can download the User Migration Tool from Cisco.com by clicking **ICM User Migration Tool Software**.

- ICM12.6.2.exe—The Unified CCE patch installer. It copies all files into relevant folders, updates the registries, and installs needed third-party software such as JRE, Apache Tomcat, and Microsoft .NET Framework.

- Regutil Tool—Used in Technology Refresh upgrades, the tool exports the Cisco Systems, Inc. registry from the source machine during the preupgrade process. The output of the tool is required on the destination machine when running the Unified CCE Installer during the upgrade process.

  You can download the Regutil Tool from Cisco.com by clicking **Contact Center Enterprise Tools**.

- Cisco Unified Intelligent Contact Management Database Administration (ICMDBA) Tool—Used to create new databases, modify or delete existing databases, and perform limited SQL Server configuration tasks.

  The ICMDBA Tool is delivered with the main installer.

- Domain Manager—Used to provision Active Directory.

  The Domain Manager Tool is delivered with the main installer.

- Upgrade.exe—Used to upgrade the schema of the logger, AW DB, HDS DB, and BA databases to a version compatible with the current Unified CCE software version. It is typically used when the installer fails to automatically upgrade the schema.

  Perform the following steps to use the tool:

  ```
  <ICM install directory>:\icm\bin>upgrade.exe -s <Server Name> -d
  <Database name> -dt <Database Type> -i <Instance Name>
  ```

  Where

  <Database Type> - can be either " **logger**" or "**hds**" or "**aw**" or "**ba**", depending on the database that requires the schema to be upgraded.

# Technology Refresh Preupgrade Task flow

## Disable Configuration Changes

Perform this step on one side only. It is automatically replicated to the other side.

**Procedure**

**Step 1** To disable configuration changes during the upgrade, set the following registry key to 1 on the Side A Call Router: **HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\Router A\Router\CurrentVersion\Configuration\Global\DBMaintenance**.

**Step 2** Confirm that configuration changes are disabled by attempting to save a configuration change.

When you try to save the change, a message is displayed confirming the change failure.

## Export the Server Registry

Export the Cisco registry on each source machine that is involved in a Technology Refresh upgrade.

During the upgrade process, you are prompted for the path to the exported registry file location. Perform the following procedure and note the location of the resulting file for later in the upgrade process.

Each time you run the RegUtil with the export option, if a RegUtil_<hostname>.dat file exists, the utility renames that file to RegUtil_<hostname>.dat.bak<number>.

**Procedure**

**Step 1** Open a command prompt and change the directory to the location where the RegUtil.exe resides.

**Step 2** Run the RegUtil tool to export the Cisco Systems, Inc. registry using the following command: **RegUtil -export [target directory]** , for example, `<ICM install directory>:\icm\bin>RegUtil -export C:\RegUtil`

The target directory must have write access. Therefore, you cannot select the install media on a DVD. The target directory is optional. If it is not specified, the tool outputs the result of the Registry export to the current directory. The output filename is of the format RegUtil_<hostname>.dat, where hostname is the name of the source machine.

# Technology Refresh Upgrade Task Flow

For the Unified CCE core components, there is a general flow for redundant systems; Sides A and B are brought down, upgraded, tested, and brought back up in sequence. That sequence ensures the operation of the Cisco Contact Center during the entire upgrade process.

**Note** For coresident configurations, upgrade CUIC/LiveData/IdS server along with the Unified CCE Central Controller upgrade.

For Technology Refresh upgrades, perform the following upgrade tasks:

| Task | See |
|---|---|
| **Cloud Connection Components** | |
| Install Cloud Connect | Install Cloud Connect, on page 89<br>If you have Cloud Connect in your environment, refer the **Update VM Properties** section in Upgrade Overview, on page 193 for Cloud connect upgrade prerequisite to increase the hard disk and RAM before you upgrade the component.<br>If you don't have Cloud Connect in your environment, and you use any Hybrid feature or Orchestration, fresh install Cloud Connect. For fresh install instructions, see 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 |
| **Queuing and self-service components** | |
| Upgrade Cisco Unified Customer Voice Portal[9] | *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at<br>https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html |
| **Infrastructure and media resource components** | |
| Upgrade voice and data gateways | Upgrade Voice and Data Gateways, on page 245 |

| Task | See |
|---|---|
| **Identity Service/SSO** | |
| Identity Service (IdS) /Single Sign-On(SSO) | SSO is an optional feature and exchanges authentication and authorization details between an identity provider (IdP) and an identity service (IdS).<br>**Note** Cisco IdS 12.6(2) upgrade requires all SSO clients to log out from SSO, before any of the upgraded nodes is brought online. To avoid this requirement, it's recommended that you install 12.6(2) ES02 on the upgraded node and wait for the access token to expire before commencing the secondary node upgrade. Without installing 12.6(2) ES02, graceful shutdown feature will not be available for Cisco IdS 12.6(2) upgrade. You can view the duration of access token expiry in the IdS administration portal under **Settings** > **Security** > **Tokens** > **Access Token Expiry**.<br>Deployments using VPN-less access to Finesse desktop should also upgrade the reverse proxy to 12.6(2) before Cisco IdS is upgraded to 12.6(2).<br>For more information, see Upgrade Flowcharts, on page 214<br>For IdS upgrade, refer to the same steps as documented in the upgrades section of Unified Intelligence Center Installation and Upgrade Guide at:<br>https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html |
| Upgrade Enterprise Chat and Email (ECE) | For ECE installation or upgrade instructions, see the *Enterprise Chat and Email Installation and Configuration Guide for Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html |
| Upgrade Finesse | For more information, see *Cisco Finesse Installation and Upgrade Guide Cisco Finesse Installation and Upgrade Guide* at<br>https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html |
| **Reporting server** | |
| Upgrade Cisco Unified Intelligence Center server | *Installation and Upgrade Guide for Cisco Unified Intelligence Center* at<br>https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html |
| **Unified CCE Central Controller and Administration & Data Server components** | |
| **Note** To perform upgrade from 12.5(x) to 12.6(2) or from 12.6(1) to 12.6(2), refer Upgrade CCE Minor/Maintenance Release Software, on page 227. | |
| Bring down Side A Logger, migrate Logger database, and upgrade Logger | Migrate the Logger Database and Upgrade the Logger, on page 272 |
| Bring down Side A Call Router, and upgrade | Upgrade Unified CCE Call Router, on page 275 |

| Task | See |
|---|---|
| Upgrade Administration & Data Server connected to Side A. | Migrate the HDS Database and Upgrade the Unified CCE Administration & Data Server, on page 276 |
| Bring Side A Logger and Call Router into service, bring down Side B Logger and Call Router | Bring Upgraded Side A into Service, on page 246 |
| Migrate Side B Logger database and upgrade Logger | Migrate the Logger Database and Upgrade the Logger, on page 272 |
| Upgrade Side B Call Router | Upgrade Unified CCE Call Router, on page 275 |
| Bring Side B Call Router into service and verify operation | Verify Operation of Upgraded Side B Call Router and Logger, on page 247 |
| Bring Side B Logger into service and verify operation. | |
| Upgrade Administration & Data Server connected to Side B. | Migrate the HDS Database and Upgrade the Unified CCE Administration & Data Server, on page 276 |
| Upgrade Cisco Unified Intelligence Center reporting templates | *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 |
| Upgrade Cisco Unified Contact Center Management Portal | *Upgrading Dual Sided Unified CCMP* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html |
| Upgrade Administration Client | Upgrade Unified CCE Administration Client, on page 280 |
| Database Performance Enhancement | Database Performance Enhancement, on page 250 |
| **Unified CCE Peripheral Gateways and associated components** | |
| Upgrade PGs | Upgrade Peripheral Gateways, on page 279 |
| Upgrade Customer Collaboration Platform | *Cisco Customer Collaboration Platform User Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/socialminer/products-installation-guides-list.html. |
| Upgrade Outbound Option Dialer | Upgrade Outbound Option Dialer, on page 280 |

| Task | See |
|---|---|
| Upgrade CTI OS server | *CTI OS System Manager Guide for Cisco Unified ICM* at<br>https://www.cisco.com/c/en/us/support/customer-collaboration/computer-telephony-integration-option/products-installation-guides-list.html |
| **Desktop Client components** | |
| Upgrade CTI OS Agent and Supervisor Desktops | *CTI OS System Manager Guide for Cisco Unified ICM* at<br>https://www.cisco.com/c/en/us/support/customer-collaboration/computer-telephony-integration-option/products-installation-guides-list.html |
| **Call Processing components** | |
| Upgrade Cisco Unified Communications Manager | *Upgrade Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-management-portal/tsd-products-support-install-and-upgrade-technotes-list.html |
| (Install) the JTAPI client on the Cisco Unified Communications Manager PG | Upgrade Cisco JTAPI Client on PG, on page 250 |

[9] If you are using Unified IP IVR for self-service and queuing, see Getting Started with Cisco Unified IP IVR.

# Technology Refresh Upgrade Tasks

The following section provides instructions about upgrading Unified CCE components. For instructions about upgrading non-Unified CCE components in a Unified CCE solution, see the links to component-specific documents in the Technology Refresh Upgrade Task Flow, on page 269.

## Migrate the Logger Database and Upgrade the Logger

To upgrade the Logger, do the following tasks:

- Migrate the Logger database.
- If you use Outbound Option High Availability, do the following:
  - Migrate the Outbound Option database.
  - For the enhancements in Outbound Option High Availability to work effectively, Outbound Option High Availability must be disabled before the logger upgrade and then enabled after the upgrade. For more information, see Disable Outbound Options High Availability (If Applicable), on page 249.
- Install the new software.

### Before you begin

- Create a shared folder in any desired location. Ensure that:
  - In the **Properties** window > **Sharing** tab > **Advanced Sharing,** the **Share this folder** check box is checked.
  - In the **Properties** window > **Security** tab > **Advanced Sharing** > **Permission**, the permission level is set as **Full control** for the user group **everyone**.

**Note** If the user group **everyone** is not available, add it using the **Add** button.

### Procedure

**Step 1** Use **Unified CCE Service Control** to stop all Unified CCE services on the Logger.

**Step 2** (Optional) If Outbound Option High Availability is deployed, disable Outbound Options High Availability. For details, see Disable Outbound Options High Availability (If Applicable), on page 249.

**Step 3** Download the EDMT tool from Cisco.com, and ensure prerequisites for the same are installed on the target/destination system, before launching EDMT. These include the ODBC Driver 17 for SQL Server, and Visual C++ Redistributable for Visual Studio 2015.

**Step 4** Run the **EDMT** from the server that will host the destination Logger and click **Next**.

**Step 5** Select **Technology Refresh** and click **Next**.

**Step 6** Under **Source Database Connection**, in the **HostName\IP Address** field, type the Source IP and click **Refresh Database List**.

**Step 7** Select the **Logger Database** name, and click **Next**.

**Step 8** In the **Windows Share Name** field, type the name of the shared folder that you created.

**Step 9** In the **Windows Share Password** field, type the password of the destination machine, and click **Next**.

**Step 10** Review or change the information as required and click **Start Migration**.

**Step 11** Exit the EDMT.

**Step 12** (Optional) If Outbound Option High Availability is deployed, repeat steps 1 through 12 to migrate the BA database.

**Step 13** Launch the ICM-CCE-Installer and click **Next**.

**Step 14** Select **Technology Refresh** and click **Next**.

**Step 15** Click **Browse** and specify the path for the RegUtil file you exported from the source machine during the preupgrade process.

**Step 16** To apply the Unified ICM 12.6(2) Maintenance Release, click **Browse** and navigate to the Maintenance Release software. Click **Next**.

**Note** You can also proceed with the installation of Unified ICM 12.5(1) without selecting the Unified ICM 12.6(2) installer in this step. After installing Unified ICM 12.5(1), double-click the Unified ICM 12.6(2) installer, and proceed from step 22.

**Step 17** (Optional) Select **SQL Server Security Hardening** and click **Next**.

**Note** SQL Security Hardening shouldn't be applied during installation of Windows Server 2019 and SQL Server 2019. SQL Security Hardening can be applied post installation using the Security Wizard tool.

**Step 18** Click **OK** on any informational messages that display.

**Step 19** Click **Install**.

**Step 20** Select **Yes** for the system to restart and complete the installation automatically or select **No** to restart the system manually after installing Unified ICM 12.5(1).

**Note**
- If you have selected Unified ICM 12.6(2) in step 16, you must select **Yes** for the system to restart automatically.
- After installing Unified ICM 12.5(1), you must restart the system manually before launching the Unified ICM 12.6(2) installation wizard and proceeding to step 22.

**Step 21** Log in to your system using domain credentials with administrative privileges.

**Step 22** Wait for the Unified CCE 12.6(2) installation wizard to launch. Click **Next** to proceed.

**Step 23** Select the radio button to accept the license agreement and click **Next**.

**Step 24** Click **Install** to begin the installation.

**Step 25** Select the radio button to restart the system and click **Finish**.

**Step 26** Open the **Web Setup** tool from the desktop shortcut.

**Step 27** Edit the instance as necessary.

**Step 28** (Optional) In case of Cross Domain upgrade, launch **Web Setup**, select instance and click on **Change Domain** to use the new domain for destination Unified CCE.

Edit instance and you might need to change the facility or instance number if required.

**Step 29** (Optional) If you use Outbound Option High Availability, enable Outbound Option High Availability in the Web Setup tool. For details, see the *Configure the Logger for Outbound Option* topic in the *Outbound Option Guide for Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html.

**Step 30** Edit the **Logger** component as necessary.

Edit the **Logger** component. In the **Summary** window, update the service account management section, with a pre-existing domain user that the Logger service would run under.

If there are references to out-of-date network interface names or IP addresses for the public and private networks for the Logger, update this information.

**Note** Ensure that the domain user is created in the new domain to perform the service operation of **Loggers and Administration & Data Servers** component.

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

**Step 31** (Optional) If it's a Cross Domain upgrade, use the User Migration tool to import the users and OU information which you exported from the source machine during the pre-upgrade process. See **User Migration Tool** in Preupgrade Overview, on page 231.

**Step 32** Use Unified CCE Service Control to set all Unified CCE services on the new Logger to Manual Start.

# Upgrade Unified CCE Call Router

To upgrade the Call Router, do the following tasks:

- Import the Cisco registry information.
- Install the new software.
- Set up the new Call Router using the Web Setup tool.

### Procedure

**Step 1** Launch the ICM-CCE-Installer and click **Next**.

**Step 2** Select **Technology Refresh** and click **Next**.

**Step 3** Click **Browse** and specify the path for the RegUtil file you exported from the source machine during the preupgrade process.

**Step 4** To apply the Unified ICM 12.6(2) Maintenance Release, click **Browse** and navigate to the Maintenance Release software. Click **Next**.

**Note** You can also proceed with the installation of Unified ICM 12.5(1) without selecting the Unified ICM 12.6(2) installer in this step. After installing Unified ICM 12.5(1), double-click the Unified ICM 12.6(2) installer, and proceed from step 9.

**Step 5** Click **OK** on any informational messages that display.

**Step 6** Click **Install**.

**Step 7** Select **`Yes`** for the system to restart and complete the installation automatically or select **`No`** to restart the system manually after installing Unified ICM 12.5(1).

**Note**
- If you have selected Unified ICM 12.6(2) in step 4, you must select **`Yes`** for the system to restart automatically.
- After installing Unified ICM 12.5(1), you must restart the system manually before launching the Unified ICM 12.6(2) installation wizard and proceeding to step 9.

**Step 8** Log in to your system using domain credentials with administrative privileges.

**Step 9** Wait for the Unified CCE 12.6(2) installation wizard to launch. Click **Next** to proceed.

**Step 10** Select the radio button to accept the license agreement and click **Next**.

**Step 11** Click **Install** to begin the installation.

**Step 12** Select the radio button to restart the system and click **Finish**.

**Step 13** Open the Web Setup tool from the desktop shortcut.

**Step 14** Edit the instance as necessary.

For a domain change, change the domain of the instance. Additionally, you might need to change the facility or instance number as required.

**Step 15** Edit the Call Router component as necessary.

If there are references to out-of-date network interfce names or IP addresses for the public and private networks for the Router, update this information.

**Step 16** Use Unified CCE Service Control to set all Unified CCE services on the new Call Router to Manual Start.

# Migrate the HDS Database and Upgrade the Unified CCE Administration & Data Server

To upgrade the Administration & Data Server, do the following tasks:

- Migrate the HDS database (if applicable. Non-HDS configurations do not require this action.)
- Import the Cisco registry information.
- Install the new software.
- Set up the new Administration & Data Server through the Web Setup tool.

The Installer upgrades the AW database that is associated with the Administration & Data server. The EDMT does not upgrade the AW database.

### Before you begin

- Create a shared folder in any desired location. Ensure that:
  - In the **Properties** window > **Sharing** tab > **Advanced Sharing,** the **Share this folder** check box is checked.
  - In the **Properties** window > **Security** tab > **Advanced Sharing** > **Permission**, the permission level is set as **Full control** for the user group **everyone**.

**Note** If the user group **everyone** is not available, add it using the **Add** button.

### Procedure

**Step 1** Use **Unified CCE Service Control** to stop all Unified CCE services on the server.

**Step 2** Download the EDMT tool from Cisco.com, and ensure pre-requisites for the same have been installed on the target/destination system, prior to launching EDMT. These include the ODBC Driver 17 for SQL Server, and Visual C++ Redistributable for Visual Studio 2015.

**Step 3** Launch the EDMT tool on the destination server that hosts the **Administration and Data Server with HDS database** and click **Next**. For non-HDS Server configurations, skip to step 11.

**Step 4** Select **Technology Refresh** and click **Next**.

**Step 5** Under **Source Database Connection**, in the **HostName\IP Address** field, type the Source IP, and click **Refresh Database List**.

**Step 6** Under **Destination Database Connection**, in the **SQL Server Port Number** field, enter the destination SQL server port number, and then click **Next**.

**Step 7** Select the **HDS Database** name, and click **Next**.

**Step 8** In the **Windows Share Name** field, type the name of the shared folder that you created.

**Step 9** In the **Windows Share Password** field, type the password of the destination machine, and click **Next**.

**Step 10** Review or change the information as required, highlight the HDS database, and click **Start Migration**.

**Step 11** Exit the **EDMT**.

**Step 12** Launch the ICM-CCE-Installer and click **Next**.

**Step 13** Select **Technology Refresh** and click **Next**.

**Step 14** Click **Browse** and specify the path for the `RegUtil` file you exported from the source machine during the preupgrade process.

**Step 15** To apply the Unified ICM 12.6(2) Maintenance Release, click **Browse** and navigate to the Maintenance Release software. Click **Next**.

**Note** You can also proceed with the installation of Unified ICM 12.5(1) without selecting the Unified ICM 12.6(2) installer in this step. After installing Unified ICM 12.5(1), double-click the Unified ICM 12.6(2) installer, and proceed from step 21.

**Step 16** (Optional) Select **SQL Server Security Hardening** and click **Next**.

**Note** SQL Security Hardening should not be applied during installation of Windows Server 2019 and SQL Server 2019. SQL Security Hardening can be applied post installation using the Security Wizard tool.

**Step 17** Click **OK** on any informational messages that display.

**Step 18** Click **Install**.

**Step 19** Select **`Yes`** for the system to restart and complete the installation automatically or select **`No`** to restart the system manually after installing Unified ICM 12.5(1).

**Note**
- If you have selected Unified ICM 12.6(2) previously, you must select **`Yes`** for the system to restart automatically.
- After installing Unified ICM 12.5(1), you must restart the system manually before launching the Unified ICM 12.6(2) installation wizard.

**Step 20** Log in to your system using domain credentials with administrative privileges.

**Step 21** Wait for the Unified CCE 12.6(2) installation wizard to launch. Click **Next** to proceed.

**Step 22** Select the radio button to accept the license agreement and click **Next**.

**Step 23** Click **Install** to begin the installation.

**Step 24** Select the radio button to restart the system and click **Finish**.

**Step 25** Open the **Web Setup** tool from the desktop shortcut.

**Step 26** Edit the instance as necessary.

**Step 27** (Optional) In case of Cross Domain upgrade, launch **Websetup**, select the instance and click on **Change Domain** in order to use the new domain for destination Unified CCE.

Edit the instance. You might need to change the facility or instance number if required.

**Step 28** Edit the **Administration & Data Server** component as necessary and in the **Summary** window, update the Service Account manager with the domain user to perform the service operation.

If there are references to out-of-date network interface names or IP addresses for the public and private networks for the Logger, update this information.

**Note** Ensure that the domain user is created in the new domain to perform the service operation of **Loggers and Administration & Data Servers** component.

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

For more information about configuring permissions in your local machine, see Configure Permissions in the Local Machine, on page 96.

**Step 29** Use **Unified CCE Service Control** to set all Unified CCE services on the new Administration & Data Server to Manual Start.

**Step 30** Start the Unified CCE services for Logger and Router on both Side A and Side B. Also, start the Distributor service for the all sites. Then, launch the Configuration Manager tool to check if it is working fine.

**Note** The time required to complete a data migration varies in a direct relationship to the database size (the larger the database size, the longer it takes to migrate) and the server hardware performance level.

**Note** If Outbound Options High Availability was disabled on source machines prior to the upgrade, you can enable it on Side A and Side B Destination machines if both the sides have been migrated successfully.

# Synchronizing or Updating Configuration and Historical Data from Production Server to Staged Server During Cut Over

The EDMT tool can also be used to migrate data from a Logger or HDS production server, to the one that has already been staged on version 12.6(x). These two pronged upgrade steps are typically performed to reduce the downtime needed during cut-over to the new version.

While the parallel 12.6(x) systems are staged and tested, the 12.0(1)/12.5(x) production servers continue to process calls. On the day of the cut-over, the data in the 12.6(x) staged servers, can be updated or synchronized with that of the production server, by running the 12.6(x) EDMT tool, for each of the Logger and HDS database.

**Note** Stop the Logger, AW-HDS, and Apache Tomcat services on 12.6(x) staged systems, before running EDMT tool while changing over to synchronize.

# Upgrade Peripheral Gateways

You can upgrade different Peripheral Gateways (PG) within a contact center at different times within different maintenance windows. However, upgrade all PGs that reside on the same virtual machine and redundant PGs (Side A and corresponding Side B) during the same maintenance window.

The following dependencies occur when upgrading the Unified Communications Manager PG:

- If your contact center uses the CTI OS component, upgrade the CTI OS server at the same time as the associated Unified Communications Manager PG.
- If your contact center uses Outbound Option, upgrade any Outbound Option Dialers associated with Unified Communications Manager PGs at the same time.
- If the Unified Communications Manager application is upgraded, upgrade the JTAPI client associated with the Unified Communications Manager PG at the same time.

### Procedure

**Step 1** Use Unified CCE Service Control to stop all Unified CCE and CTI OS (if applicable when upgrading the Unified Communications Manager PG) services on the PG server. Change the services to Manual Start.

**Step 2** Launch the ICM-CCE-Installer and click **Next**.

**Step 3** To apply the Unified ICM 12.6(2) Maintenance Release, click **Browse** and navigate to the Maintenance Release software. Click **Next**. You can also proceed with the installation of Unified ICM 12.5(1) without selecting the Unified ICM 12.6(2) installer in this step. After installing Unified ICM 12.5(1), double-click the Unified ICM 12.6(2) installer, and proceed with installation.

**Step 4** Select **Technology Refresh** and click **Next**.

**Step 5** Click **Browse** and specify the path for the RegUtil file you exported from the source machine during the preupgrade process.

The registry information for the Unified Communications Manager PG also contains information for the CTI OS server (if applicable).

**Step 6** Click **OK** on any informational messages that display.

**Step 7** Click **Install**.

**Step 8** Reboot the system after the upgrade completes.

**Step 9** After reboot, open the Peripheral Gateway Setup tool from the desktop shortcut and make any necessary changes. See the "Install" section of this document for specific information.

If there are references to out-of-date network interface names or IP addresses for the public and private networks for the Logger, update this information.

**Step 10** Open the Peripheral Gateway Setup tool from the Installer dialog box or desktop shortcut and edit the Dialer as required.

**Step 11** Use Unified CCE Service Control to set all Unified CCE services to Automatic Start.

# Upgrade Outbound Option Dialer

To upgrade the Outbound Option Dialer, import the Cisco registry information, install the new software, and set up the new Dialer using the PG Setup tool.

### Before you begin

You must have previously migrated the Outbound Option database during the Logger upgrade.

### Procedure

**Step 1** Launch the ICM-CCE-Installer and click **Next**.

**Step 2** To apply the Unified ICM 12.6(2) Maintenance Release, click **Browse** and navigate to the Maintenance Release software. Click **Next**. You can also proceed with the installation of Unified ICM 12.5(1) without selecting the Unified ICM 12.6(2) installer in this step. After installing Unified ICM 12.5(1), double-click the Unified ICM 12.6(2) installer, and proceed with installation.

**Step 3** Select **Technology Refresh** and click **Next**.

**Step 4** Click **Browse** and specify the path for the RegUtil file you exported from the source machine during the preupgrade process.

**Step 5** Click **OK** on any informational messages that display.

**Step 6** Click **Install**.

**Step 7** Reboot the system after the upgrade completes.

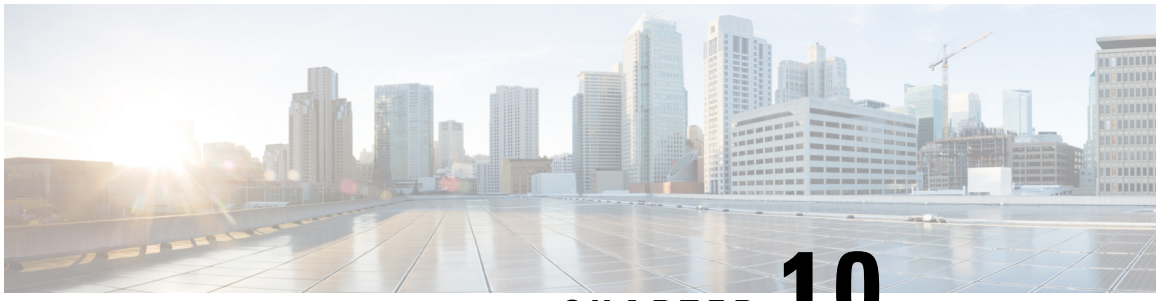
**Step 8** Open the Peripheral Gateway Setup tool from the Installer dialog box or desktop shortcut and edit the Dialer as required.

**Step 9** Use Unified CCE Service Control to set all Unified CCE services to Automatic Start.

# Upgrade Unified CCE Administration Client

There's no support for Administration Clients to be upgraded via Technology Refresh upgrade. Either perform an in-place common ground upgrade of Administration Clients, and make edits as necessary using the Administration Client setup, or perform a fresh installation of Administration Client on a new system.

**Note** To upgrade the Operating System from Windows 10 to Windows 11, you must follow the Unified CCE Virtualisation to get the Latest OVA configuration details. Modify the VM specifications for Windows 11. For Windows 11, the SecureBoot and TPM devices are mandatory which must be added before upgrading the OS from Windows 10 to Windows 11.



CHAPTER 10

# Upgrade from a Standalone Deployment to a Coresident Deployment


- Set Deployment Type in Unified CCE Administration Configuration, on page 281
- Install Publisher/Primary Nodes of VOS-Based Contact Center Applications, on page 282
- Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 283
- Set Up the System Inventory, on page 285
- Configure Live Data with AW, on page 285
- Configure Live Data Unified Intelligence Center Data Sources, on page 286
- Restart Live Data, on page 286


## Set Deployment Type in Unified CCE Administration Configuration

Ensure that the deployment type has been set to **UCCE: 2000 Agents Rogger** via CCE Web Administration tool.

Perform the following steps to set the deployment:

### Procedure

**Step 1** On **Administration & Data Server** open the Unified CCE Tools folder.

**Step 2** Go to **Administration Tools** > **CCE Web Administration.**

**Step 3** Log in as a **Config security group** member in the **user@domain**.

**Step 4** Double-click **Unified CCE Administration**.

**Step 5** Go to **Infrastructure Settings** > **Deployment Settings**.

**Step 6** On the **Deployment Type** page, select **UCCE: 2000 Agents Rogger deployment** from the drop-down list and then click **Next**.

**Note** Whenever you change the deployment type, you need to restart the Apache Tomcat on Logger and AWs.

### What to do next

Set the principal AW and configure it with the Diagnostic Framework Service domain, username, and password if you have not already.

# Install Publisher/Primary Nodes of VOS-Based Contact Center Applications

### Before you begin

DNS Configuration is mandatory for installation of Cisco Unified Communications Manager, Cisco Unified Intelligence Center, Cisco Finesse and Cisco Identity Service (IdS). To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

### Procedure

**Step 1** Create a virtual machine for your VOS-based contact center application using the OVA.

**Step 2** Mount the ISO image for the software to the virtual machine.

**Step 3** Select the virtual machine, power it on, and open the console.

**Step 4** Follow the Install wizard, making selections as follows:

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.

b) In the **Success** screen, select **OK**.

c) In the **Product Deployment Selection** screen:

- For the Progger (Lab only) or 2000 agent reference design, choose the coresident deployment option **Cisco Unified Intelligence Center with Live Data and IdS**, and then select **OK**. The **Cisco Unified Intelligence Center with Live Data and IdS** option installs Cisco Unified Intelligence Center with Live Data and Cisco Identity Service (IdS) on the same server.
- For all other deployments, select one of the standalone install options. For example, select **Cisco Unified Intelligence Center**, **Live Data**, or **Cisco Identity Service (IdS)**. Then select **OK**.

d) In the **Proceed with Install** screen, select **Yes**.

e) In the **Platform Installation Wizard** screen, select **Proceed**.

f) In the **Apply Patch** screen, select **No**.

g) In the **Basic Install** screen, select **Continue**.

h) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

**Note** For Live Data servers, use the same timezone for all the nodes.

i) In the **Auto Negotiation Configuration** screen, select **Continue**.

j) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.

k) In the **DHCP Configuration** screen, select **No**.

l) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.

m) In the **DNS Client Configuration** screen, click **Yes** to enable DNS client.

n) Enter your DNS client configuration. Select **OK**.
o) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
p) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
q) In the **First Node Configuration** screen, select **Yes**.
r) In the **Network Time Protocol Client Configuration** screen, enter a valid NTP server IP address and select **OK**.
s) In the **Security Configuration** screen, enter the security password and select **OK**.
t) In the **SMTP Host Configuration** screen, select **No**.
u) In the **Application User Configuration** screen, enter the application username. Enter, and confirm the application user password. Select **OK**.
v) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

- There is a reboot in the middle of the installation.
- The installation ends at a sign-in prompt.

**Step 5** Unmount the ISO image.

# Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications

**Note** This task is required for installation of the subscriber/secondary nodes of the three VOS-based contact center applications: Cisco Finesse, Cisco Unified Communications Manager, and Cisco Unified Intelligence Center.

### Before you begin

DNS Configuration is mandatory for installation of Cisco Unified Communications Manager, Cisco Unified Intelligence Center, and Cisco Finesse. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

Before you install the subscriber/secondary nodes, you must install the publisher/primary nodes and configure the clusters.

### Procedure

**Step 1** Create a virtual machine for your VOS-based contact center application using the OVA.
**Step 2** Mount the ISO image for the software to the virtual machine.
**Step 3** Select the virtual machine and power it on, and open the console.
**Step 4** Follow the Install wizard, making selections as follows:

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.
b) In the **Success** screen, select **OK**.
c) In the **Product Deployment Selection** screen:

- For the Progger (Lab only) or 2000 agent reference design, choose the coresident deployment option **Cisco Unified Intelligence Center with Live Data and IdS**, and then select **OK**. The **Cisco Unified Intelligence Center with Live Data and IdS** option installs Cisco Unified Intelligence Center, Live Data, and Cisco Identity Service (IdS) on the same server.
- For all other deployments, select one of the standalone install options. For example, select **Cisco Unified Intelligence Center**, **Live Data**, or **Cisco Identity Service (IdS)**. Then select **OK**.

**Step 5** Follow the Install wizard, making selections as follows:

a) In the **Proceed with Install** screen, select **Yes**.
b) In the **Platform Installation Wizard** screen, select **Proceed**.
c) In the **Apply Patch** screen, select **No**.
d) In the **Basic Install** screen, select **Continue**.
e) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

**Note** For Live Data servers, use the same timezone for all the nodes.

f) In the **Auto Negotiation Configuration** screen, select **Continue**.
g) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
h) In the **DHCP Configuration** screen, select **No**.
i) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
j) In the **DNS Client Configuration** screen, click **Yes** to enable DNS client.
k) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
l) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
m) In the **First Node Configuration** screen, select **No**.
n) In the warning screen, select **OK**.
o) In the **Network Connectivity Test Configuration** screen, select **No**.
p) In the **First Node Access Configuration** screen, enter the host name and IP address of the first node. Enter and confirm the security password. Select **OK**.
q) In the **SMTP Host Configuration** screen, select **No**.
r) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

- There is a reboot in the middle of the installation.
- The installation ends at a sign-in prompt.

**Step 6** Unmount the ISO image.

# Set Up the System Inventory

### Procedure

**Step 1** In Unified CCE Administration, navigate to **Infrastructure Settings** > **Inventory** .

**Step 2** Add the new machine to the System Inventory:

a) Click **New**.

The **Add Machine** popup window opens.

b) From the Type drop-down menu, select the following machine type:

CUIC_LD_IdS Publisher, for the coresident Unified Intelligence Center, Live Data, and Identity Service machine available in the 2000 agent reference design.

c) In the **Address** field, enter the FQDN or IP address of the machine.

d) Enter the machine's Administration credentials.

e) Click **Save**.

The machine and its related Subscriber or Secondary machine are added to the System Inventory.

# Configure Live Data with AW

This command tells Live Data how to access the primary AW DB and the secondary AW DB. The command also automatically tests the connection from Live Data to the primary or secondary AW, checks to see if the configured user has appropriate AW DB access, and reports the results.

You can use the optional skip-test parameter if you do not want the test performed. When you include the skip-test parameter, no checking is done to see if the configured user has appropriate AW DB access, and no results are reported.

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

### Before you begin

Before you can configure Live Data, you must first configure a SQL user (with special permissions) to work with Live Data, as described in Configure SQL User Account, on page 138.

The SQL administrative user with read and write permissions must then run the following SQL queries for the SQL user configured to work with Live Data.

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

**Procedure**

**Step 1** Log in to your Live Data server.

**Step 2** Run the following command to configure Live Data with the primary AW DB. The command automatically tests the connection from Live Data, checks the user permission, and displays results.

(The skip-test parameter is optional; include it only if you do not want the test performed).

**set live-data aw-access primary** *addr port db user* [*skip-test*]

**Step 3** Run the following command to configure Live Data with the secondary AW DB. The command automatically tests the connection from Live Data, checks the user permission, and displays results.

(The skip-test parameter is optional; include it only if you do not want the test performed).

(The skip-test parameter is optional; include it only if you do not want the test performed).

**show live-data aw-access** [*skip-test*]

# Configure Live Data Unified Intelligence Center Data Sources

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

**Procedure**

**Step 1** Log in to your Live Data server.

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

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

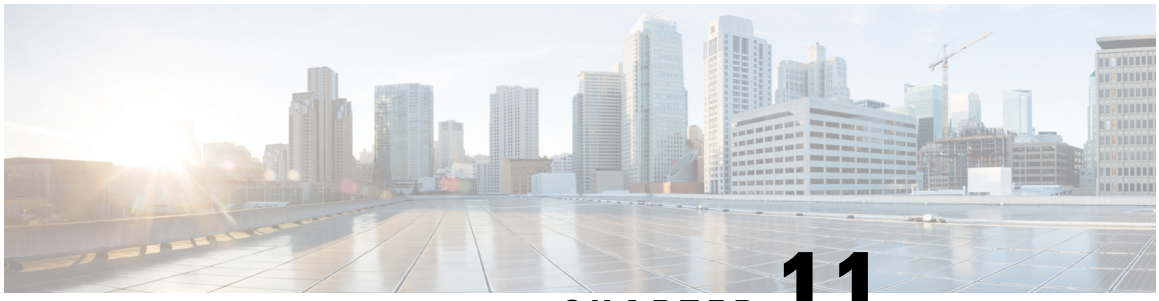
# Restart Live Data

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

**Procedure**

Access the Live Data CLI and run the following command:

**utils system restart**



CHAPTER 11

# Uninstallation


- Uninstallation of Unified ICM/CCE base version 12.5(1), on page 287
- Prerequisite for Uninstallation of CCE 12.6(2) Maintenance Release, on page 287


## Uninstallation of Unified ICM/CCE base version 12.5(1)

Uninstallation of Unified ICM/CCE base of 12.5(1) is not supported for Unified CCE components that are deployed on Windows Server using the ICM-CCE-Installer. However, support for uninstallation and re-installation of client installer packages like Administration Client and Internet Script Editor continues.

**Note** The option to roll back to previous versions is only available with minor and maintenance releases.

## Prerequisite for Uninstallation of CCE 12.6(2) Maintenance Release

If you have enabled the optional feature Outbound Option High Availability, you must disable it before you uninstall Unified ICM 12.6(2). From Unified CCE Web Setup, choose **Component Management** > **Loggers**. Select a logger that is enabled for High Availability, and click **Next** until the **Additional Options** page appears. Uncheck the **Enable High Availability** check box. Perform this action for each logger enabled for Outbound Option High Availability.

If you are planning to roll back to previous version of CCE Release 12.6(2), do the following:

1. Export the certificates of all the components imported into the truststore. To export the certificate, use the command:

   ```
   keytool -export -keystore <ICM install Dir>\ssl\cacerts -alias <alias of the component>
    -file <filepath>.cer
   ```

2. Enter the truststore password when prompted.

After the roll back, do the following:

1. Import the certificates exported in step 1 above, into the JRE keystore. To import the certificate, use the command:

```
keytool -import -keystore <Oracle/OpenJDK JRE path>\lib\security\cacerts -file
<filepath>.cer -alias <alias>
```

2. Enter the keystore password when prompted.
3. Enter **yes** when prompted to trust the certificate.

**Note** You don't need to reimport the certificates if you are rolling back to CCE 12.5(1a) or 12.6(1). Also, if you have already installed ES55 (mandatory OpenJDK ES), you don't need to reimport the certificate when you roll back to CCE 12.5(1).

# Uninstall Unified CCE 12.6(2)

### Procedure

**Step 1** Log in to your system as a user with administrative privileges.

**Step 2** Choose **Control Panel** > **Programs and Features** > **Cisco ICM Maintenance Release ICM 12.6(2)** > **Uninstall**.
The **InstallShield Wizard** launches.

**Step 3** On the confirmation window, click **Yes**.

**Step 4** (Optional) On the **Installation Messages** window, click **Next**.

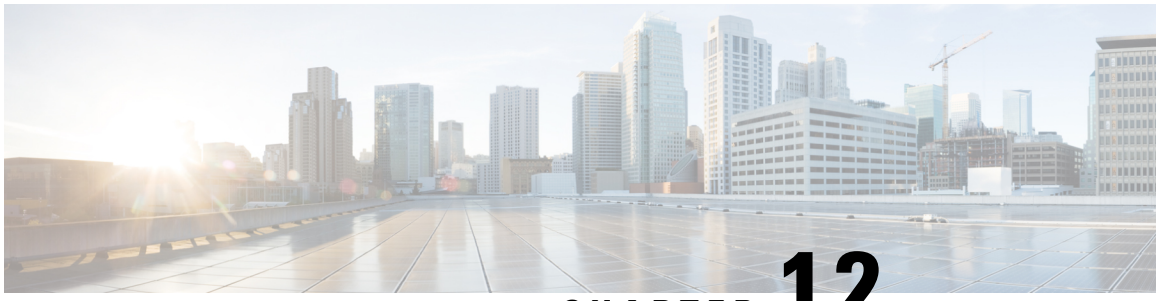
Post Installation Window specifies if any service is set to manual. A pop-up window displays a notification that some services were automatically changed to manual as part of the uninstallation. Make sure that both A and B sides of your system operate properly after uninstalling Unified CCE 12.6(2). Then, set the Unified ICM services that were changed during the uninstallation back to their original setting (Automatic).

**Step 5** At the prompt, restart the machine.

The Unified CCE 12.6(2) application is uninstalled from your machine.

**Note** Before you uninstall, ensure to set *ECDSA enabled* registry to false, and re-boot the box. Once the re-boot is complete, check the registry and set it to "false".

The ECDSA registry path is `HKLM\SOFTWARE\WOW6432Node\Cisco Systems, Inc.\ICM\Cisco SSL Configuration`



CHAPTER 12

# Testing


- Testing Overview, on page 289
- Testing Tasks, on page 289


# Testing Overview

System testing is a part of the installation, upgrade, and ongoing maintenance of a Unified CCE solution. Testing requirements and processes vary from customer to customer. Therefore, specific steps for running the tests are not included in this document.

For installations, testing must ensure all aspects of contact center operation before going live.

For upgrades, at the beginning of each maintenance window, consider running preupgrade tests to establish a benchmark. The benchmark is used when you run the postupgrade tests. Postupgrade tests are necessary for each maintenance window to ensure continued contact center operation throughout the entire upgrade process, which can span multiple maintenance windows.

If you require assistance with Unified CCE solution testing, work with your Cisco representative.

Contact centers need established tests plans and processes for all aspects of contact center operation. Have the plans, tools, and processes in place to test your contact center.

# Testing Tasks

## Verify Upgrade to Cisco Unified Customer Voice Portal

After upgrading Unified CVP, verify the following:

**Procedure**

**Step 1** Verify that error messages did not display during the upgrade process.

**Step 2** Check the upgrade logs for error messages.

**Step 3** Ensure that the Unified CVP Operations, Administration, Monitoring and Provisioning (OAMP) Web interface is available for use.

**Step 4** Use the diagnostic page at http://<CVPHOST>:8000/cvp/diag to verify the status of the Unified CVP system.

**Step 5** Use the Operations Console (**System** > **Control Center**, Device Pool tab) to verify that the upgraded Unified CVP Call Servers, Unified CVP VXML Server and Unified CVP Reporting Server show a status of "Up".

**Step 6** Use the Operations Console (**Device Management** > **Unified CVP Call Server**, General tab for selected Call Server) to verify that the Device Version reflects the correct upgraded version.

**Step 7** Verify that the appropriate voice prompt is heard when the call is made.

**Step 8** Ensure that the Unified CVP license is properly installed.

# Verify IOS Gateway Upgrade

After upgrading IOS gateways, verify the following:

**Procedure**

**Step 1** At the Cisco IOS exec level, run the following CLI commands:

- To check that the upgraded IOS target image is running:

  **show version**

- To verify that the boot system is configured to boot the correct image:

  **show running-config**

- To verify that configuration done previously is not lost:

  **show running-config**

- To verify that the ISDN connection status is at MULTIFRAME_ESTABLISHED:

  **show isdn status**

- To verify that configured interfaces are in up/up state:

  **show ip interface brief**

- To verify manually placed incoming calls:

  **show isdn history**

- To verify IP routing from branch site to a data center:

  **ping** or **traceroute**

- To verify IP routing from one branch site to another branch site:

  **ping** or **traceroute**

**Step 2** Ensure that the following devices are configured and registered correctly: Gatekeeper, trunks, and CTI Route Point.

**Step 3** Ensure that all MGCP end points (FXS, FXO, PRI, T1 CAS and BRI) are properly registered with Unified Communications Manager.

**Step 4** Manually spot check calls as appropriate from the PSTN vis SIP Gateways.

**Step 5** Verify that a PSTN user who places an inbound call from the PSTN to a Unified IP Phone in a Unified Communications Manager cluster through gateways and puts the call on hold can hear Music-on-Hold (MOH) and can also finally resume the call.

# Verify Upgrade to Cisco IOS-Based Transcoders and Conference Bridges

After upgrading Cisco IOS-based transcoders and conference bridges, verify the following:

**Procedure**

**Step 1** Check if the complete configuration before the upgrade still exists.

**Step 2** Check if all DSPs are registered and are functioning as usual.

**Step 3** Check if there are no error messages in the buffer log or console.

**Step 4** Check if no dump file is created in the flash memory.

**Step 5** To verify that the configuration is not lost, type the “show running-config” command.

**Step 6** To verify that the interfaces are in up state, type the “show ip interface brief” command.

**Step 7** Verify IOS Transcoding is working with G711 codec configure for one device while G729 codec is configured on another device.

# Verify Upgrade to Cisco Unified CCE Router and Logger

After upgrading the Cisco Unified CCE Router and Logger, verify the following:

**Procedure**

**Step 1** Verify basic operations such as the following:

- Setup logs indicate no errors or failure conditions (icmsetup.txt and ICMInstall.txt, located in the \Temp directory of the disk on which the application was installed).
- All components can “ping” public and private IP addresses as applicable.
- Schema upgrade is successful for all databases and there is no loss of data integrity or data.
- All component services start correctly without generating errors.
- Firewalls and other security measures do not block the ability to access Microsoft SQL Server and to run third-party software components, like VNC or PCAnywhere.
- Ccagent is in service and connected to any Peripheral Gateways located in Side A.
- Recovery process not required, no activity other than process start-up.
- Configuration information is passed to the Router by the Logger. Replication process begins when the Historical Database Server comes online.
- Replication process begins with no errors. (Use the Windows Event Viewer to view Windows Event logs).
- The Router is in a synchronized state. (Use the Diagnostic Framework Portico, under **ListProcesses**, verify that the status of ccagent and mdsproc is "InSvc".)

- Database space allocation and % used are reported correctly. (Use the dumplog utility to view the hlgr and rcv processes on the Logger server. The trace messages display the percentage of available free space and the log space of the database at 30-second intervals. Verify this using Microsoft SQL Management Studio to view the Logger database properties.)

**Step 2** Use the Windows Event Viewer on each server to check that no exceptions, errors, or unexpected events have occurred. Select **Administrative Tools** > **Event Viewer**, then expand **Windows Logs** and review the Application and System logs.

**Step 3** Verify that configuration changes can be made and are passed to the Logger and AW databases.

**Step 4** Ensure that basic calls and call functionality such as transfers, conferences, call treatment and queuing are working properly.

# Verify Upgrade to Cisco Real Time Administration Workstation, Historical Database Server

After upgrading the Real Time AW/HDS software, verify the following:

### Procedure

**Step 1** Use the Windows Event Viewer on each server to check that no exceptions, errors, or unexpected events have occurred. Select **Administrative Tools** > **Event Viewer**, then expand **Windows Logs** and review the Application and System logs.

**Step 2** After Side A Central Controller components have been upgraded, verify basic operations such as the following:

- Setup logs indicate no errors or failure conditions (icmsetup.txt and ICMInstall.txt located in the \Temp directory of the disk on which the application was installed).
- All components can “ping” public and private IP addresses as applicable.
- Schema upgrade is successful for all databases and there is no loss of data integrity or data.
- All component services start correctly without generating errors.
- All general activities such as the ability to access SQL server and to run third-party software components like VNC or PCAnywhere, etc. are not stopped by any security application.
- Rtsvr, the process that provides real time data from the Router to the AW database, is connected to the primary Administrative Workstation. (Open the Configuration Manager tool on Administration & Data server. If the tool opens without any errors, the feed is active. Additionally, use the Dumplog utility to view the uaw process. The uaw trace message shows "Waiting for new work…".)
- Configuration information is passed to the router by the Logger. Replication process begins when the Historical Database Server comes online.
- Real Time Administrative Workstation indicates that it is ready.
- Replication process begins with no errors. (use the Windows Event Viewer to view Windows Event logs).
- Authorized users are able to use the Configuration Manager on the Real Time Administrative Workstation.
- Authorized users are able to log into Cisco Unified Intelligence Center and can access both public and private reports and that all previously existing reports are still available.
- Previous settings for users are still valid when any application is opened.
- The “Validate All” script yields the same results after the upgrade as prior to the upgrade.

**Note** All existing scripts can be opened and edited and new scripts can be created.

- Database space allocation and % used are reported correctly. (Use the dumplog utility to view the hlgr and rcv processes on the Logger server. The trace messages display the percentage of available free space and the log space of the database at 30 second intervals. Verify this using Microsoft SQL Management Studio to view the Logger database properties.)
- Diagnostic Framework Portico can acquire logs, capture registry information, and schedule collection of logs.
- Verify that configuration changes are possible.

# Verify Upgrade to Peripheral Gateways

After upgrading the peripheral gateways, verify the following:

**Procedure**

**Step 1** Use the Windows Event Viewer on each server to check that no exceptions, errors, or unexpected events have occurred. Select **Administrative Tools** > **Event Viewer**, then expand **Windows Logs** and review the Application and System logs.

**Step 2** Ensure that real time and historical data is sent to the Router and AW database.

**Step 3** Ensure that basic calls and call functionality (such as transfers, conferences, call treatment and queuing) are working properly.

**Step 4** Ensure that the peripheral is running properly on the upgraded gateway by verifying call flows, CTI desktops, Outbound Option, and other applications.

# Verify Redundancy

After you upgrade both sides of all redundant components, verify the following:

**Procedure**

**Step 1** Stop each active component.

**Step 2** Ensure that the backup component assumes an active state and that the system operation switches to the backup component with no loss of functionality.

# Verify Upgrade to Cisco Unified Communications Manager

After upgrading Unified Communications Manager, verify the following:

### Procedure

**Step 1** Verify that no error messages have occurred during the upgrade process.

**Step 2** Check the upgrade log file for any errors.

**Step 3** Start all first node and subsequent node servers.

**Step 4** Verify that there is no replication failure between the first node and subsequent node servers.

**Step 5** Verify that SIP and SCCP IP Phones are registered with Unified Communications Manager.

**Step 6** Ensure that the following devices are configured correctly: gatekeeper, trunks, and CTI route points.

**Step 7** Ensure that the media resources (conference bridges, MTP and transcoders) are configured correctly by checking their status.

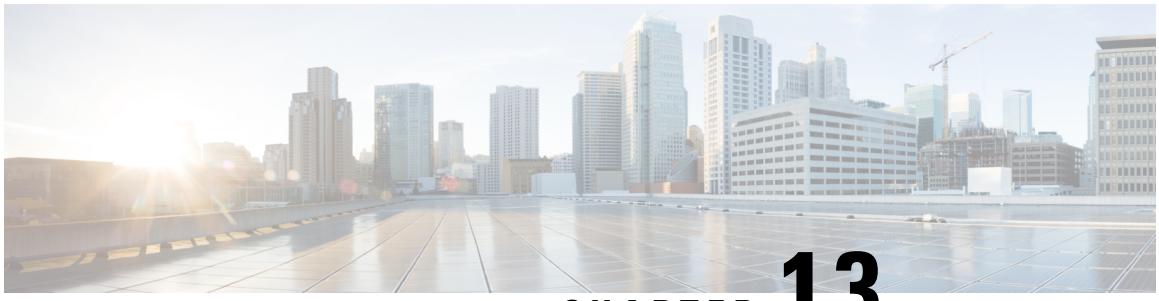
**Step 8** Verify if the end users are able to connect to their CTI managers.

**Step 9** Check if the license usage is correct as reported in the License Unit Report.

**Step 10** Check if services on all servers in the cluster are up.

**Step 11** Perform the Unified Communications Manager first node and subsequent node process verification using the following Real Time Monitoring Tool feature verification process:

a) Verify if Multiple Route Patterns and Route Lists are configured and working properly.
b) Verify if Extension Mobility is configured and working properly.
c) Verify if Unified IP Phone Services are configured and working properly.



CHAPTER 13

# CCE Orchestration


- Overview, on page 295
- Orchestration in CCE Deployment, on page 296
- Configure SSH public key on Windows nodes, on page 333
- Self-Signed Certificate, on page 334
- Things to Know, on page 335


# Overview

The Orchestration feature provides partners and administrators an option to automatically download software updates and simplify the installation and rollback processes. The Orchestration framework is built within the Cloud Connect server that connects to the Cisco hosted cloud software repository. This framework provides the ability to check and download new software updates as and when they are available and notify the administrators via email about the new updates along with the release notes. Orchestration currently supports installation and rollback of Cisco Engineering Specials (ES), Service Updates (SU), Minor Releases (MR), and Microsoft Patches.

## Email Notification

The Cloud Connect server checks for new software updates daily at a predefined time. When the new software updates are available, an email notification is sent. This email notification consists of available software updates details along with the release notes and is triggered to the administrators who have subscribed for it.

Email notifications are also sent to provide updates on the success and failure of any upgrade, rollback, or switch forward procedure. These notifications include details such as:

- Specific nodes on which the upgrade, rollback, or switch forward is initiated.
- Cloud Connect server name from where the procedure is triggered.
- Time (Cloud Connect server time) at which the procedure is started.
- Details about build versions of the respective nodes. For example, for an upgrade procedure, it shows both the version from which it is upgraded (FromVersion) and the version to which it is upgraded (ToVersion).
- Status of the procedure for respective nodes to indicate whether the procedure is successful or has failed; the subject line of the email indicates the overall status: success, failure, or partial success.

Cloud Connect server downloads the available software from Cisco software repository every day at the configured time. Email notification is triggered from Cloud Connect server to subscribed users with software download failure details. Also, Cisco software artifactory will trigger an email notification with entitlement or compliance failure details to the email address mapped to CCO ID that is used to generate the Artifactory API key.

**Note**

- If the option "All nodes" is selected during the upgrade, an email notification is sent about the success or failure at each stage of upgrade.
- The name of the deployment is shown in the subject line of the email, depending on the configuration in the inventory file.
- For patch install or rollback, email notifications are not sent to indicate whether the procedure is successful or if it is a failure.

# Orchestration in CCE Deployment

The Orchestration feature is part of the Cloud Connect node that is configured in the CCE deployment.

To access this feature, Cloud Connect must be added to the inventory in the Unified CCE Administration console.

For more information, see *Initial Configuration for Cloud Connect* section in the *Cisco Unified Contact CenterEnterprise Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-maintenance-guides-list.html.

## System Requirements

Cloud Connect 12.5(x) is obsolete. Cloud Connect 12.6(x) is required.

### VOS Component Upgrade

Refer below for the minimum software version required to enable this feature for the following components:

- Finesse
- CUIC/LD/IDS/Co-resident
- VVB

Apply the ES **ucos.orchestration.enable-12.5.1.cop.sgn** on the above-mentioned components with 12.5(1) version to on-board and orchestrate VOS nodes from Cloud Connect server.

**Note** The ES **ucos.orchestration.enable-12.5.1.cop.sgn** must be applied on both the publisher and subscriber target nodes. This Mandatory ES is not required for onboarding the above-mentioned components with 12.6(x) version. After you install this ES on target VOS node, you will not be able to run commands in the same session. You must restart the session on target nodes to use the Orchestration CLI commands.

**Note**

- Before you begin the VOS node upgrade from 12.6(1) to 12.6(2), check if the **ucos.keymanagement.v02.cop.sgn** is applied on the base version. If not, you must install it; else the upgrade will fail. Restart the VOS node after installing **ucos.keymanagement.v02.cop.sgn**.
- Before you begin the VOS node upgrade from 12.5(1) to 12.6(2), check if the **ucos.keymanagement.v01.cop.sgn** is applied on the base version. If not, you must install it; else the upgrade will fail. Restart the VOS node after installing **ucos.keymanagement.v01.cop.sgn**

### Windows Component Upgrade

Manually install mandatory ES23 on Unified CVP 12.5 (1) and ES66 on Unified ICM 12.5 (1) to onboard and orchestrate Windows nodes from Cloud Connect server.

**Note** For 12.5(1) Windows and VOS nodes, ES is required to onboard and orchestrate from Cloud Connect server. Mandatory ES is not required for onboarding target Windows and VOS components with 12.6(x) version.

# Orchestration Support using Cloud Connect Server

Cloud Connect 12.6(x) supports orchestration in the following scenarios:

- Unified CCE 12.5(x) ES, Unified CCE 12.6(x) ES and Windows Updates can be orchestrated from Cloud Connect 12.6(x)
- Unified CCE 12.5(x) to Unified CCE 12.6(x), software upgrade can be orchestrated from Cloud Connect 12.6(x)

See System Requirements, on page 296 for minimum software requirement to enable orchestration for the above supported model.

# Parallel Running of CLI

Parallel running of same or different CLIs on Cloud Connect server is disabled for Orchestration. However, parallel running of CLIs is allowed for the following commands:

- set cloudconnect orchestration config
- show cloudconnect orchestration config
- utils image-repository show
- utils deployment compatibility-check
- utils deployment show in-progress
- utils system inventory export
- utils system inventory import
- utils deployment show progress-HA

- email configuration-related commands, see Configure Email Notification.
- utils set software-download time
- utils set software-download bandwidth

# Orchestration Deployment Task Flow

| |
|---|
| CLI to configure artifactory URL and API key, on page 301 |
| Generate the Artifactory API Key, on page 299 |
| CLI to configure proxy for orchestration, on page 300 |
| Onboard VOS Nodes to Orchestration Control Node, on page 305 |
| Onboard Windows nodes to orchestration control node, on page 306 |
| Add Deployment Type and Deployment Name, on page 308 |
| Validate Onboarded Nodes for Orchestration, on page 308 |
| Configure Email Notification, on page 309 |
| Configure Windows Server for Updates (Optional), on page 311 |

# Administration Task Flow

| |
|---|
| Check Installed Software Version and Patches, on page 311 |
| Install or Rollback Patch or Upgrade Cloud Connect Server , on page 312 |
| List Available Patches for Specific Node or Group of Nodes, on page 313 |
| Install Patch to Specific Node or Group of Nodes, on page 313 |
| Roll Back Patch from Specific Node or Group of Nodes, on page 314 |
| Install Windows Updates to Specific Node or Group of Nodes, on page 315 |
| Roll Back Windows Update from Specific Node or Group of Nodes, on page 317 |
| Enable or Disable Compatibility Enforcement, on page 318 |
| Initiate maintenance mode for a specific node(s), on page 319 |
| List Available Upgrade Options , on page 320 |
| Upgrade a Specific Node or Group of Nodes or All Nodes , on page 320 |
| Perform Switch Forward on Specific VOS Node or Group of Nodes , on page 322 |
| Roll Back Upgrade from Specific Node or Group of Nodes, on page 322 |
| Check Last Known Orchestration Operation Status on Remote Node, on page 324 |
| Check Status, on page 323 |
| Start Unified ICM Services, on page 324 |

# Maintenance Task Flow

| |
|---|
| CLI to configure software download schedule, on page 325 |
| CLI to configure the bandwidth for Orchestration software download, on page 325 |
| Enforce software download from Cisco hosted software artifactory, on page 327 |
| Update VOS Nodes Onboarded to Orchestration Control Node, on page 327 |
| Remove VOS Nodes from Orchestration Control Node, on page 327 |
| Update Windows Nodes Onboarded to Orchestration Control Node, on page 328 |
| Validate Updated Nodes Onboarded for Orchestration, on page 328 |
| Configure Email Configuration, on page 328 |
| Delete Configuration for Email Notification, on page 329 |
| Unsubscribe Email Notification, on page 330 |
| Export and Import of Nodes Managed by Orchestration Control Node, on page 330 |
| Export Current Patch Level Details, on page 331 |
| Serviceability, on page 332 |
| Enable and View Windows Open SSH Logs, on page 333 |

# Deployment Tasks

## Generate the Artifactory API Key

To generate the Artifactory API Key, follow the steps below:

**Note** It is mandatory for the CCO ID used to generate API keys to have necessary software upgrade entitlements. The CCO ID used by the partner or customer should have a valid SWSS (service contract) or Flex subscription in order to have the necessary entitlement.

- Login to https://devhub-download.cisco.com/console/ using your CCO Username and Password.
- Navigate to '**Manage Download Key** page.
- Click Generate Key option to Generate the API key. Option to **View** and **Revoke** Key is available in **Manage Download Key** page.
- Click on the Copy option to copy the API key to the clipboard.

**Note** You must log into https://devhub-download.cisco.com/console once every six months to extend the validity of the API key.

**Note** Cisco recommends not to use the same Artifactory API key generated by a single CCO ID across multiple deployments. For multiple deployments such as test, pre-production, production, and so on, generate the Artifactory API key for each deployment using different CCO IDs. Artifactory API key generated by a single CCO ID can be used in both publisher and subscriber of Cloud Connect in a single deployment.

## CLI to configure proxy for orchestration

You can enable proxy configuration for orchestration to check and fetch updates from the Cisco-hosted cloud artifactory.

To configure the proxy for orchestration, run the **set cloudconnect orchestration config** command. To view the proxy configured for orchestration, run the **show cloudconnect orchestration config** command.

***Table 1: Set Command Table***

| **Command** | **set cloudconnect orchestration config** |
|---|---|
| **Description** | This command enables the proxy configuration for orchestration to check and fetch updates from the Cisco-hosted cloud artifactory. |
| **Expected Inputs** | In the *Proxy Configured* prompt, enter **Yes** to enable the proxy or **No** to turn-off the proxy.<br>If you choose to enable the proxy, you will be prompted to enter the Proxy Host and Proxy Port details.<br>**Note**<br>• Proxy Host should be the proxy server FQDN or IP address.<br>• Proxy is turned off by default.<br>• Orchestration supports only HTTPS proxy. |
| **Expected Outcome** | This CLI enables or turns-off the proxy for orchestration based on user input. |

**Note** You can run this command only from the publisher node of the Cloud Connect server. The proxy configuration replicates automatically from the publisher node to the subscriber node when the **set cloudconnect orchestration config** command is run successfully on the publisher node.

***Table 2: Show Command Table***

| **Command** | **show cloudconnect orchestration config** |
|---|---|
| **Description** | This command displays the proxy configuration for orchestration to check and fetch updates from the Cisco-hosted cloud artifactory. |
| **Expected Inputs** | NA |

| | |
|---|---|
| **Expected Outcome** | Proxy Host and Proxy Port details will be displayed if proxy is enabled. |

## CLI to configure artifactory URL and API key

Cisco hosts all the software artifacts in a cloud-based artifactory. The Cloud Connect server uses this artifactory to download and notify new updates.

Configure the Cloud Connect server with Cisco-hosted software Artifactory URL, Repository Name, and API Key. Run the command **utils image-repository set**. Refer to the **Set Command** table.

To view the configured Artifactory URL, Repository Name, and API Key in the Cloud Connect server, run the command **utils image-repository show**. Refer to the **Show Command** table.

**Note** You can run the **utils image-repository set** command only in the publisher node of the Cloud Connect server. The replication of image repository configuration occurs automatically from the publisher node to the subscriber node when you run this command with successful results on the publisher node.

**Note** Before running the command **utils image-repository set** on the CLI, access the link https://software.cisco.com/download/eula and accept the End User License Agreement (EULA)

*Table 3: Set Command Table*

| | |
|---|---|
| **Command** | **utils image-repository set** |

| Description | |
|---|---|

| | |
|---|---|
| | This command allows you to configure the Cisco hosted software Artifactory URL, Artifactory Repository Name, and API Key. For information on API Key, refer to the Generate the Artifactory API Key section. This command validates the below:<br>• If the Cisco.com ID used to generate the API key has entitlement to download the Cisco Contact Center software.<br>• If the EULA is signed by the Cisco.com ID that generates the API key.<br>• If the Cisco.com ID that generates the API key has the customer company's full address that is updated in the Cisco.com profile and validated by Cisco.<br>• If the Cloud Connect server is deployed in embargoed countries where software download is restricted.<br>• If the user has valid authentication token that is associated with the API key.<br>If the user doesn't have a valid authentication token associated with the API key, then the user has to sign in to https://devhub-download.cisco.com/console/ to extend the validity of the API key.<br>If compliance validation fails, the Cisco.com ID user must perform the below-mentioned actions:<br>• For EULA compliance failure, confirm that you have read and agreed to be bound by the terms of Cisco EULA. Access the link https://software.cisco.com/download/eula to view and accept the agreement.<br>• For customer company's address verification failure, access the link https://rpfa.cloudapps.cisco.com/rpfa/profile/profile_management.do to update the address.<br>• For Entitlement failure, where Cisco service contract information indicates that you're not authorized to download the Contact Center software, perform one or more of the following actions:<br>  • Identify the product name and MDFID of the Contact Center product for which the entitlement failed. To find the product name and corresponding MDFID of the product, check the CLI log for the keyword **Entitlement check failed for MDFID**. Refer to the Serviceability section for the command to retrieve the CLI log.<br>  • The service contract or subscription containing coverage for the product may not be associated to the Cisco.com user ID. To associate the relevant service contract to the Cisco user ID, use the **Cisco Profile Manager**, and select **Add Access** to request access to the contract (which can now be done using the Serial Number of the product). |

| | |
|---|---|
| | • If your software is covered by a Smart License subscription, go to Cisco Software Central to request access to your company's Smart Account in the **Administration** section.<br><br>Contact your Cisco representative, partner, or reseller to ensure that the product is covered by a service contract or subscription that is associated with your Cisco.com user ID. Use the Partner Locator link to locate your nearest partner.<br><br>For assistance, contact your Cisco Accounts Manager or Partner.<br><br>To expedite your request, include the following information:<br>• User ID (Cisco.com ID used to generate the API key)<br>• Contact Name<br>• Company Name<br>• Contract Number<br>• Product ID or MDFID, Product Name, and Release<br><br>• You can obtain access to U.S. export-restricted software by completing the K9 agreement form.<br><br>**Note** Upon successful configuration of artifactory details, artifacts are downloaded locally to the Cloud Connect server periodically at the configured time. During artifact download, the compliance validation is done. The Cisco.com ID user performs the above-mentioned actions for any compliance failure during artifact download. |
| **Expected Inputs** | User should input Artifactory URL, Artifactory Repository Name, and API Key.<br><br>The Cisco-hosted software Artifactory URL is https://devhub-download.cisco.com/binaries and Artifactory Repository Name is `ent-platform-release-external`.<br><br>**Note** Cisco recommends not to use the same Artifactory API key generated by a single CCO ID across multiple deployments. For multiple deployments such as test, pre-production, production, and so on, generate the Artifactory API key for each deployment using different CCO IDs. Artifactory API key generated by a single CCO ID can be used in both publisher and subscriber of Cloud Connect in a single deployment.<br><br>CLI provides an option to the customer to choose between using export-restricted and unrestricted software, based on the entitlement associated with the Cisco.com ID. For example, VVB has export-restricted and unrestricted software. |

| | |
|---|---|
| **Expected Outcome** | This CLI validates the entitlement associated with the Cisco.com ID and connection to the Cisco-hosted software artifactory using the given configuration. Based on successful validation, the artifactory details are configured in the Cloud Connect server. |

**Note** Use the command **utils image-repository set** to change export-restricted or unrestricted software in the deployment. Use the CLI **utils initiate software-download** to enforce the cleanup and download the restricted vs unrestricted software.

**Note** On the successful configuration of artifactory details, artifacts are downloaded locally to the Cloud Connect server at the scheduled or default time. Orchestration operations such as patch install, rollback, or upgrade can be performed only after the artifacts are downloaded. If you need to download the artifacts immediately after the configuration, use the **utils initiate software-download** CLI. Usage of orchestration-related CLI is blocked during download, and this duration depends on the number of artifacts to be downloaded.

**Note** Before you configure the bandwidth using the **utils set software-download bandwidth** command, make sure the software is downloaded locally for the first time after the artifactory is successfully configured using the **utils image-repository set** command. To download the artifacts immediately after the configuration, use the **utils initiate software-download** command.

***Table 4: Show Command Table***

| **Command** | **utils image-repository show** |
|---|---|
| **Description** | This command displays the configured Cisco-hosted software Artifactory URL, Repository Name, and the API Key (the mix of hash and last 4 characters of key) in the Cloud Connect server. |
| **Expected Inputs** | NA |
| **Expected Outcome** | Displays the configured Artifactory URL, Repository Name, and the API Key. |

## Onboard VOS Nodes to Orchestration Control Node

The onboarding process helps to establish a password-less connection between the Cloud Connect node and the VOS nodes.

**Prerequisites**:

- Ensure that the Cloud Connect server and target nodes maintain the minimum software versions that are required as outlined in System Requirements.
- If you are using self-signed certificates, import the self-signed Tomcat certificate of the Cloud Connect server into the VOS nodes which you have to onboard. Ensure to import both Cloud Connect publisher

and subscriber node certificates on all VOS publisher and subscriber nodes. For details, see Self-Signed Certificate, on page 334.

To onboard Finesse, CUIC, VVB, IDS, LD to a Cloud Connect server, run the **utils system onboard initiate** command from the publisher node of the respective VOS cluster that you wish to onboard. The publisher node of the Cloud Connect server must be up and running when onboarding is initiated from VOS node. When the onboarding is initiated from VOS node, FQDN of the Cloud Connect server must be used.

| **Command** | **utils system onboard initiate** |
|---|---|
| **Description** | This command is used to onboard a VOS node such as Finesse, CUIC, VVB, etc., to a Cloud Connect server. |
| **Expected Inputs** | When run, the command prompts for:<br>• Cloud Connect server FQDN<br>• Cloud Connect application username<br>• Password |
| **Expected Outcome** | The nodes are onboarded to the Cloud Connect server orchestration inventory. A message is displayed indicating the status. |

**Note** If the system (cluster) onboards to the Cloud Connect server with partial error, check the reason for the error and correct it. Then, run the **utils system onboard update** command instead of running the **utils system onboard initiate** command.

**Note** Onboarding is allowed only when all the publisher and subscriber nodes in the Cloud Connect server are reachable.

**Note** If the Cloud Connect server is corrupted and redeployed by doing fresh install, the administrator has to run **utils system onboard remove** from the VOS node and then run **utils system onboard initiate** to onboard the VOS nodes again.

## Onboard Windows nodes to orchestration control node

The onboarding process helps to establish a password-less connection between the Cloud Connect node and the Windows nodes. To onboard the Windows-based nodes to orchestration control node, perform the following steps:

### Procedure

**Step 1** Configure SSH public key on the Windows nodes by following the steps in the section Configure SSH public key on Windows nodes, on page 333.

**Step 2** From the cloud connect server, run the **utils system inventory export** command to download the inventory to an SFTP server. For details, see Export and Import of Nodes Managed by Orchestration Control Node, on page 330.

**Step 3** Edit the inventory file to include the Windows components. Refer to the default template section in the inventory file.

**Note**
- The syntax, alignment, and indentation must be exactly the same as mentioned in the inventory file.
- Ensure the CRLF line endings are of UNIX-Style. Use a Linux-based or a Mac OS-based editor to create the Windows inventory file.

The following fields in the inventory file are mandatory.

| Field | Description |
|---|---|
| **ProductName** | The **ProductName** mentioned in the inventory file must be in uppercase and cannot be changed. For example, CVPREPORTING, CVPSERVER, CVPOAMP, DISTRIBUTOR, LOGGER, PG, ROGGER or ROUTER. |
| **Pair under product** | This is a user-defined pair name. |
| **Hostname** | This can be a valid IP, or hostname, or FQDN name of the target node. |
| **Side of the deployment** | It can either be A or B. |
| **User configured on host** | This is the username for which the SSH keys are configured in Step 1.<br>**Note** The user must have either domain admin or local administrator privilege.<br>**Note** User name can be in User Principal Name (UPN) format or Domain username (domain\username) format for domain administrator or local administrator user name.<br>Example:<br>UPN format : administrator@stooges.icm<br>Domain Administrator: stooges\administrator<br>Local Administrator: administrator |

**Step 4** Import the inventory back from the SFTP server by running the command **utils system inventory import** on the Cloud Connect publisher node. For details, see Export and Import of Nodes Managed by Orchestration Control Node, on page 330.

## Add Deployment Type and Deployment Name

An administrator can edit the inventory file to add the details of the deployment.

### Procedure

**Step 1** Download the inventory to an SFTP server by running the utils system inventory export command. For details, see Export and Import of Nodes Managed by Orchestration Control Node, on page 330.

**Step 2** Edit the following strings in the inventory file, if required.

- **deploymentType**: This field is used for compatibility check during an upgrade or rollback or switch forward procedure. The supported deployment types are:
  - UCCE-2000-Agents
  - UCCE-4000-Agents
  - PCCE-2000-Agents
  - PCCE-4000-Agents

  **Note** Orchestration is not supported for 12000, 24000 and 36000 agent deployment models.

  Ensure that the values entered in this field conform to the above format. The deployment type is case sensitive.

- **deploymentName**: Provide a unique name for the deployment.

  This name appears in the subject line of the email notification. If it is not configured, the subject line of the email notification contains only the type of procedure and the overall status.

**Note** The administrator can update or edit the default values, if required, based on their deployment type and preferred deployment name.

**Step 3** Import the inventory back from the SFTP server by running the utils system inventory import command on the Cloud Connect publisher node. For details, see Export and Import of Nodes Managed by Orchestration Control Node, on page 330.

## Validate Onboarded Nodes for Orchestration

To validate the onboarding of VOS and Windows nodes, and to check whether the Orchestration feature is ready to be used, run the **utils deployment test-connection** command.

| Command | utils deployment test-connection |
|---|---|

| | |
|---|---|
| **Description** | This command is used to validate whether password-less SSH connection is successful between the onboarded nodes and the Cloud Connect server. You can test the connection to all nodes on the deployment or to a specific group or individual nodes. |
| **Expected Inputs** | NA |
| **Expected Outcome** | Shows whether the inventory is accurate and the Cloud Connect node is able to connect to the managed hosts. |

## Configure Email Notification

If an email notification is configured, the Cloud Connect server checks the Cisco-hosted artifact repository periodically at scheduled times and sends email notifications along with the release notes when new software updates are available. Administrators can decide when to apply a patch or perform an upgrade. Email notifications are not triggered if no new software updates are available.

**Note** The SMTP server referred to in this section is the mail server that is used within the customer organization for their internal email communication.

Perform the following procedures in the same sequence as given here.

| | |
|---|---|
| 1 | Set up Email Notification, on page 309 |
| 2 | Validate Email Configuration, on page 310 |
| 3 | Subscribe to Email Notification, on page 310 |
| 4 | Configure Email Notification, on page 309 |

### Set up Email Notification

Configure the email notification by running the following set of commands:

- Set the IP address or hostname of the SMTP server by running the **set smtp-host** command.

| **Command** | **set smtp-host** |
|---|---|
| **Description** | This command is used to set the IP address or hostname of the SMTP server. |
| **Expected Inputs** | SMTP server IP Address/HostName |
| **Expected Outcome** | The SMTP address is updated. |

- Set the email address from which emails are triggered by running the **set smtp-from-email** command.

| **Command** | **set smtp-from-email** |
|---|---|
| **Description** | This command is used to set the email address from which the emails are triggered. This email address is not monitored and therefore not used for replying to any emails. |
| **Expected Inputs** | When run, this command takes an input for a complete email address. |

| | |
|---|---|
| **Expected Outcome** | Configures the email address from which email notifications are triggered. |

- Enable or disable SMTP authentication by running the **set smtp-use-auth** command.

| | |
|---|---|
| **Command** | **set smtp-use-auth** |
| **Description** | This command is used to enable or disable SMTP authentication. By default, this is disabled. |
| **Expected Inputs** | The command takes an input for the values Enable or Disable. |
| **Expected Outcome** | SMTP authentication type is updated. |

- Set the username to be used for SMTP server connection by running the **set smtp-user** command. This is an optional configuration that needs to be set only when the SMTP authentication is enabled.

| | |
|---|---|
| **Command** | **set smtp-user** |
| **Description** | This command is used to set the username to be used for SMTP server connection. |
| **Expected Inputs** | The command takes an input for the username to be used for SMTP authentication. |
| **Expected Outcome** | Configures the SMTP username. |

- Set the password for SMTP server connection by running the **set smtp-pswd** command. This is an optional configuration that needs to be set only when the SMTP authentication is enabled.

| | |
|---|---|
| **Command** | **set smtp-pswd** |
| **Description** | This command is used to set the password for SMTP server connection. The password is stored in an encrypted format. To change the password, run this command again. |
| **Expected Inputs** | The command prompts for a password for the SMTP connection. |
| **Expected Outcome** | Configures the SMTP password. |

### Validate Email Configuration

Validate the configuration by running the **utils smtp test-connection** command.

| | |
|---|---|
| **Command** | **utils smtp test-connection** |
| **Description** | This command is used to establish a connection to the SMTP server using the given configuration. |
| **Expected Inputs** | NA |
| **Expected Outcome** | Shows whether SMTP connection is successful or not. |

### Subscribe to Email Notification

Subscribe to email notifications by running the **utils smtp subscribe** command. Specify the email addresses to which the email notifications must be sent.

| Command | utils smtp subscribe |
|---|---|
| Description | This command is used to specify the email addresses that subscribe to the email notifications. For example:<br>`utils smtp subscribe <emailaddress1,emailaddress2,.....emailaddressesN>` |
| Expected Inputs | Comma-separated list of valid email addresses. |
| Expected Outcome | Email addresses provided are subscribed for notification. |

## Configure Windows Server for Updates (Optional)

Microsoft Windows update configuration needs to be done on the target Windows node. Microsoft Windows updates can be downloaded in one of following ways on the target Windows node:

- by directly connecting to the Microsoft server;
- from the Windows update server configured. To deploy or configure Windows server update services, refer to https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/deploy-windows-server-update-services.

# Administration Tasks

**Note** Before upgrade or rollback of nodes managed by Orchestration, make sure to take backup as suggested by respective component documentation. Backup has to be done manually.

**Note** In case the upgrade or rollback on VOS node fails, then the respective VOS node restart is mandatory before attempting the next upgrade or rollback on the same node. If the administrator does not restart, the next attempt to upgrade or rollback might fail.

## Check Installed Software Version and Patches

To check the currently installed software version and patches on a node or group of nodes or all nodes in either Windows or VOS systems, run the **utils deployment show status** command.

| Command | utils deployment show status |
|---|---|
| Description | This command is used to check the currently installed software version and patches for the selected Windows or VOS node individually or group of nodes or for all nodes in the inventory by selecting the option 'All Nodes in the inventory'. |
| Expected Inputs | Select the node or group of nodes or all nodes from the inventory. |

| | |
|---|---|
| **Expected Outcome** | Displays information about the installed software version and the patches for the selected node or group of nodes or all nodes from the inventory. If there is no patch installed, a message "No patch installed" is displayed to indicate that along with software version. |

## Install or Rollback Patch or Upgrade Cloud Connect Server

To install a patch or to roll back a previously installed patch on Cloud Connect server or to upgrade Cloud Connect Server to next available version, run the **utils system upgrade initiate** command. The **Local Repository** option in this command lists the patches and upgrade options available from Cisco artifactory for patch install or rollback or upgrade on Cloud Connect server. This command can be run separately on the Cloud Connect publisher and subscriber nodes.

**Note** The Cloud Connect publisher should be upgraded before upgrading the subscriber. The switch version on publisher should be done first before doing switch version on subscriber, use **utils system switch version** command to switch between versions.

**Note** The **Local Repository** option is also available on the Cisco Unified OS Administration web page of Cloud Connect server. Select this option to install a patch or to roll back a previously installed patch on Cloud Connect server or to upgrade Cloud Connect Server to next available version.

| **Command** | **utils system upgrade initiate** |
|---|---|
| **Description** | This command is used to initiate the patch install or to roll back the previously installed patch on Cloud Connect server or to upgrade Cloud Connect Server to the next available version. The patches and upgrade options available for patch install or rollback or upgrade are listed from Cisco artifactory. |
| **Expected Inputs** | Select the **Local Repository** option to list the patches and upgrade options available for patch install or rollback or upgrade.<br>Select the patch to install or roll back or upgrade option to upgrade Cloud Connect server. |
| **Expected Outcome** | The selected patch for install or rollback is installed on Cloud Connect server or selected upgrade option is used to upgrade the Cloud Connect server. |

**Note** The **Local Repository** option is used only after the Cisco Artifactory is successfully configured on Cloud Connect server. See CLI to configure artifactory URL and API key, on page 301 for configuring Cisco artifactory.

**Note** Optionally, to receive email notification about the status of the patch installation or rollback or upgrade for Cloud Connect server, provide the SMTP host server details when prompted by the CLI.

**Note** Patch install or roll back or upgrade on Cloud Connect server initiated using **utils system upgrade initiate** command can be canceled using **utils system upgrade cancel** command. The **utils system upgrade status** command can be used to check the status.

## List Available Patches for Specific Node or Group of Nodes

To get a list of available patches for a specific node or group of nodes in the inventory, run the **utils patch-manager list** command.

| **Command** | **utils patch-manager list** |
|---|---|
| **Description** | This command is used to get a list of patches available for installation for a specific node or group of nodes based on the selected option. |
| **Expected Inputs** | Select a node or group of nodes based on the inventory. |
| **Expected Outcome** | Displays information about available patches for the selected node or group of nodes. |

## Install Patch to Specific Node or Group of Nodes

To install patch to a specific node or group of nodes, run the **utils patch-manager install** command.

| **Command** | **utils patch-manager install** |
|---|---|
| **Description** | This command is used to install patches on a specific node or group of nodes onboarded to the Cloud Connect inventory. |

| | |
|---|---|
| **Expected Inputs** | From the list of Windows/VOS nodes displayed, select the node or group of Windows/VOS nodes on which the patch needs to be installed. Once you select the nodes, only the nodes for which patches are available will be displayed. For example, if you select 3 nodes and Windows/VOS patches are available for only 1 of them, you are asked to proceed with only one node. Confirm to proceed. You are also asked to confirm whether the target node needs to be rebooted after installing the patch.<br><br>Selection of components such as Finesse, CVP Call Server, IdS, and PG with software version 12.6(x) will provide the options "With maintenance mode" and "Without maintenance mode"..<br><br>If you select a group of nodes with some nodes on 12.6(x) and some nodes below 12.6(x), then "With maintenance mode" or "Without maintenance mode" option will not be available. In this case if "With maintenance mode" option is required, then the individual node with 12.6(x) can be selected separately.<br><br>If you select "With maintenance mode" option, the maintenance mode is initiated for the selected node to failover active traffic gracefully or shutdown the services gracefully without interrupting the active traffic or causing outage for new traffic before installing the patch and automatically rebooting. If you select, "Without maintenance mode" option, you are initially asked to confirm to proceed.<br><br>Next, you are asked to provide confirmation on rebooting the node after installing the patch. |
| **Expected Outcome** | The selected patch is installed on the selected node or group of nodes. |

**Note** To start Unified ICM services, post the successful completion of patch install with reboot on Unified ICM nodes. See Start Unified ICM Services.

**Note** You can check the status of the patch install which is currently in-progress. For more information, see Check Status, on page 323.

**Note** Maintenance mode for IDS co-resident in 2000 Agents Deployment model is not supported

## Roll Back Patch from Specific Node or Group of Nodes

To roll back a previously installed patch on a specific node or a group of nodes, run the **utils patch-manager rollback** command.

| | |
|---|---|
| **Command** | **utils patch-manager rollback** |

| | |
|---|---|
| **Description** | This command is used to roll back previously installed patches on a specific node or group of nodes.<br><br>In case of Windows-based nodes, the latest applied patch is allowed to roll back. In case of VOS-based nodes, the latest applied ES is rolled back. |
| **Expected Inputs** | From the list of Windows/VOS nodes displayed, select the node or group of Windows/VOS nodes on which the patch needs to be rolled back. Once you select the nodes, only the nodes for which Windows/VOS patch rollback is available will be displayed. For example, if you select 3 nodes and Windows/VOS patch rollback is available for only 1 of them, you are asked to proceed with only one node. There is also a message displayed indicating that the machine would restart after the patch is rolled back. Confirm to proceed.<br><br>Selection of components such as Finesse, CVP Call Server, IdS, and PG with software version 12.6(x) will provide the options "With maintenance mode" and "Without maintenance mode".<br><br>If you select a group of nodes with some nodes on 12.6(x) and some nodes below 12.6(x), then "With maintenance mode" or "Without maintenance mode" option will not be available. In this case if "With maintenance mode" option is required, then the individual node with 12.6(x) can be selected separately.<br><br>If you select "With maintenance mode" option, the maintenance mode is initiated for the selected node to failover active traffic gracefully or shutdown the services gracefully without interrupting the active traffic or causing outage for new traffic before rollback and automatically rebooting. If you select, "Without maintenance mode" option, you are initially asked to confirm to proceed.<br><br>Next, you are asked to provide confirmation on rebooting the node after rollback. |
| **Expected Outcome** | The previously installed patch is rolled back on the selected node or group of nodes. |

**Note** To start Unified ICM services, post the successful completion of patch roll back with reboot on Unified ICM nodes. See Start Unified ICM Services

**Note** You can check the status of patch rollback which is currently in-progress. For more information, see Check Status, on page 323.

## Install Windows Updates to Specific Node or Group of Nodes

To install Windows updates to a node or group of nodes or all Windows nodes, run the **utils patch-manager ms-patches install** command.

**Note** Before running this command, refer to the recommended guidelines in the *Microsoft Security Updates* section of the *SecurityGuide for CiscoUnified 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.

Microsoft Windows updates are NOT hosted on Cisco-hosted Software Artifactory. You must configure the target Windows node to fetch the Microsoft Windows updates, either by directly connecting to the Microsoft Server via Internet or from the Windows Update Server. For more details, refer to the Configure Windows Server for Updates (Optional) section. The **utils patch-manager ms-patches install** command will not list the available Windows updates for the administrator to choose for the target node. Instead, it will check the available updates for the below listed Windows update categories and install all the available updates:

- Application
- Connectors
- DefinitionUpdates
- DeveloperKits
- FeaturePacks
- Guidance
- ServicePacks
- Tools
- UpdateRollups
- CriticalUpdates
- SecurityUpdates
- Updates

The administrator can control the installation of Windows updates using Windows Update Server, instead of directly connecting to the Microsoft Server via Internet. Ansible log, generated during the running of **utils patch-manager ms-patches install** CLI, captures the details of the Windows updates, along with the Knowledge Base (KB) number of the updates that were installed on the target node. Refer to the Serviceability section for the command to retrieve the Ansible log.

| **Command** | **utils patch-manager ms-patches install** |
|---|---|
| **Description** | This command is used to install the latest Windows updates to a node or a group of Windows nodes or all Windows nodes. |

| | |
|---|---|
| **Expected Inputs** | From the list of Windows nodes displayed, select the node or group of Windows nodes or all Windows nodes to which the updates need to be applied. You can also select all the Windows nodes in the inventory. Once you select the nodes, only the nodes for which Windows updates are available will be displayed. For example, if you select 3 nodes and Windows updates are available for only 1 of them, you are asked to proceed with only one node. Confirm to proceed. You are asked to confirm whether the target nodes needs to be rebooted after installing the updates.<br><br>Selection of components such as CVP Call Server and PG with software version 12.6(x) will provide the options "With maintenance mode" and "Without maintenance mode".<br><br>If you select a group of nodes with some nodes on 12.6(x) and some nodes below 12.6(x), then "With maintenance mode" or "Without maintenance mode" option will not be available. In this case if "With maintenance mode" option is required, then the individual node with 12.6(x) can be selected separately.<br><br>If you select "With maintenance mode" option, the maintenance mode is initiated for the selected node to failover active traffic gracefully or shutdown the services gracefully without interrupting the active traffic or causing outage for new traffic before installing the update and automatically rebooting. If you select, "Without maintenance mode" option, you are initially asked to confirm to proceed.<br><br>Next, you are asked to provide confirmation on rebooting the node after installing the patch. |
| **Expected Outcome** | The selected Windows updates are installed on the selected node or group of nodes or all Windows nodes. |

## Roll Back Windows Update from Specific Node or Group of Nodes

To roll back Windows update from a specific node or group of nodes or all Windows nodes, run the **utils patch-manager ms-patches rollback** command.

**Note**

- Before running this command, refer to the recommended guidelines in the *Microsoft Security Updates* section of the *SecurityGuide for CiscoUnified 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
- Listing of Windows updates available for rollback is not supported.

| | |
|---|---|
| **Command** | **utils patch-manager ms-patches rollback** |
| **Description** | This command is used to roll back a specific Windows update from a specific node or group of nodes or all Windows nodes. |

| | |
|---|---|
| **Expected Inputs** | Select the node or group of Windows nodes or all Windows nodes on which the rollback needs to be performed. You can also select all the Windows nodes in the inventory for rollback. Provide the Knowledge Base (KB) number you want to rollback. You are asked to confirm whether the target nodes need to be rebooted after rollback.<br><br>Selection of components such as CVP Call Server and PG with software version 12.6(x) will provide the options "With maintenance mode" and "Without maintenance mode".<br><br>If you select a group of nodes with some nodes on 12.6(x) and some nodes below 12.6(x), then "With maintenance mode" or "Without maintenance mode" option will not be available. In this case if "With maintenance mode" option is required, then the individual node with 12.6(x) can be selected separately.<br><br>If you select "With maintenance mode" option, the maintenance mode is initiated for the selected node to failover active traffic gracefully or shutdown the services gracefully without interrupting the active traffic or causing outage for new traffic after rollback and automatically rebooting. If you select, "Without maintenance mode" option, you are initially asked to confirm to proceed.<br><br>Next, you are asked to provide confirmation on rebooting the node after rollback. |
| **Expected Outcome** | The selected Windows updates are rolled back. |

## Enable or Disable Compatibility Enforcement

You can enable or disable compatibility enforcement. When the compatibility enforcement is enabled, it ensures that the upgrade, rollback, or switch forward is as per the compatibility matrix published by Cisco for reference design-based deployment. To enable or disable compatibility enforcement, run the **utils deployment compatibility-check** command.

**Note** By default, the compatibility enforcement is enabled.

When the compatibility enforcement is disabled, the Orchestration framework does not enforce upgrade, rollback, or switch forward as per the compatibility matrix published by Cisco.

| **Command** | **utils deployment compatibility-check** |
|---|---|
| **Description** | This command is used to enable or disable compatibility enforcement. |
| **Expected Inputs** | User confirmation to proceed with enabling or disabling compatibility enforcement. |
| **Expected Outcome** | Message about the success or failure of enabling or disabling compatibility enforcement. |

**Note** You can run this command only from the publisher node of the Cloud Connect server. The compatibility configuration replicates automatically from the publisher node to the subscriber node when the **utils deployment compatibility-check** command is run with successful results on the publisher node.

## Initiate maintenance mode for a specific node(s)

Initiating maintenance mode allows the components to failover gracefully or shutdown the services gracefully (depending on the selected components) without interrupting the active traffic or causing outage to new traffic. This ensures that the system can be taken down for maintenance activity such as installing new software updates, restarting services etc. Currently, maintenance mode is supported for PG, CVP server, IdS, and Finesse.

**Note** Ensure that not all CVP servers are put into maintenance mode at same time, so that incoming call traffic can be distributed.

To initiate maintenance mode for a specific node in the inventory, run the **utils system maintenance initiate** command.

| **Command** | **utils system maintenance initiate** |
|---|---|
| **Description** | This command is used to initiate maintenance mode for a specific node based on the selected option. Currently, the initiate maintenance command is available for Finesse, CVP Call Server, IdS, and PG components. |
| **Expected Inputs** | When run, this command prompts you to select a node based on the inventory. |
| **Expected Outcome** | Information about success or failure of the initiate maintenance command for a selected node is displayed. |

**Note** The **utils system maintenance initiate** is applicable for target nodes on CCE 12.6(1) and above.

**Note** If either the Publisher or Subcriber or the active/inactive node is already in maintenance mode in any of the components, the other server cannot be initiated for maintenance.

**Note** You can check the status of system maintenance initiate which is currently in-progress. For more information, see Check Status, on page 323.

**Note** Maintenance mode for IDS co-resident in 2000 Agents Deployment model is not supported

## List Available Upgrade Options

To get a list of available upgrade options for VOS and Windows nodes individually or for group of nodes or for all nodes in the inventory, run the **utils upgrade-manager list** command.

| **Command** | **utils upgrade-manager list** |
|---|---|
| **Description** | This command is used to get a list of upgrade options available for the selected VOS or Windows node or group of nodes or all nodes in the inventory by selecting the option "All nodes in the inventory".. |
| **Expected Inputs** | Select a node or group of nodes or all nodes based on the inventory. |
| **Expected Outcome** | Displays information about available upgrade options for selected VOS or Windows nodes or group of nodes or all nodes in the inventory.<br>If the selected node or group of nodes or all nodes are already running the latest software version, a message is displayed to indicate that. |

## Upgrade a Specific Node or Group of Nodes or All Nodes

To perform software version upgrades on VOS or Windows nodes or All nodes in the deployment (VOS and Windows nodes together), run the **utils upgrade-manager upgrade** command from the Cloud Connect server. It is recommended to run this command during a maintenance window as the procedure involves system restart that will cause service outage.

For the selected VOS or Windows component for upgrade, a compatibility check is performed in the background based on the configured deployment type to ensure that all the associated components are onboarded. If the components are onboarded and the required dependent components are either in same target upgrade version or backward compatible version, the upgrade procedure begins. However, if the components are not onboarded, you have to onboard them first or if the versions are not compatible, upgrade them to the required version. For example, if you select to upgrade the Rogger nodes to 12.6(1) version, the inter-component compatibility check is run for the Rogger dependent components such as Finesse, CVP, VVB, CUIC. These must already be in 12.6(1) version and PG must be backward compatible version, that is, 12.5(1) .

**Note** The sub-components sequence dependencies are not validated as part of the upgrade compatibility. Refer to the upgrade guides of the respective components for the correct sequence. For example, in case of CVP, we have sub-components such as Operations Console, Unified CVP Reporting Server and Unified CVP Server. These must be upgraded in the required sequence.

For VOS node/cluster, switch forward is optional at the end of upgrade. If administrators opt for switch forward, the target node is restarted and the active/inactive partition is switched. If they decide not to switch forward, the upgraded version remains in the inactive partition of the target node. Switch forward for these nodes can be performed later. For details, see Perform Switch Forward on Specific VOS Node or Group of Nodes , on page 322.

For VOS cluster, the upgrade or the switch forward procedure is performed first on the publisher and then on the subscriber nodes. If switch forward is performed immediately after an upgrade, the overall procedure takes a significant amount of time; hence plan the maintenance window accordingly.

For selecting "All nodes" option during upgrade, make sure that all the VOS and Windows nodes onboarded are on the same software version. Stage-wise upgrade is performed for the solution components as per the *CCE Installation and Upgrade guide*. In case of any component upgrade failure during the process, the upgrade does not proceed to the next stage. The administrator has to upgrade individual components by selecting the respective individual VOS or Windows nodes.

| **Command** | **utils upgrade-manager upgrade** |
|---|---|
| **Description** | This command is used to upgrade VOS or Windows nodes or group of nodes or All nodes in the deployment (VOS and Windows nodes together) in the inventory. |
| **Expected Inputs** | Select the Windows or VOS node or group of nodes or all nodes in the deployment (VOS and Windows nodes together) that you want to upgrade.<br>From the list of upgrade options available for the selected node or group of nodes or all nodes, select the appropriate option and confirm. A compatibility check is then run in the background.<br>To select "All nodes" upgrade option, make sure that all the VOS and Windows nodes onboarded and the components are on the same software version.<br>Once the upgrade procedure begins, you can see the progress details for each of the machines. You can also see the elapsed time since the procedure started. |
| **Expected Outcome** | The selected node or group of nodes or all nodes is upgraded. |

**Note**

- For faster upgrades, the Cloud Connect server downloads locally all the new software updates from the Cisco hosted repository at a predefined time.
- To start the Unified ICM services, post the successful completion of upgrade with reboot on Unified ICM nodes. See Start Unified ICM Services.
- Upgrade of all nodes to CCE 12.6(2) will be supported for the following scenarios:
  - All CCE components are on 12.6(1)
  - All CCE components are on 12.5(1)
  - All ICM and VOS components are on 12.5(2) and all CVP components are on 12.5(1)

**Note** You can check the status of upgrade which is currently in-progress. For more information, see Check Status, on page 323.

## Perform Switch Forward on Specific VOS Node or Group of Nodes

Administrators can perform switch forward on target VOS nodes independently. When the active partition is on lower version and the inactive partition is on higher version, run the **utils upgrade-manager switch-forward** command to perform a switch forward. It is recommended to run this command during a maintenance window as the procedure involves system restart that will cause service outage.

| **Command** | **utils upgrade-manager switch-forward** |
|---|---|
| **Description** | This command is used to switch forward on target VOS node/cluster from Cloud Connect server. |
| **Expected Inputs** | Select the VOS node/cluster on which you want to perform the switch forward. You will see the details of the current active/inactive versions. Confirm to proceed with the switch forward.<br>A compatibility check is then run in the background.<br>• If there are components whose versions are not compatible or the components are not onboarded as per the compatibility requirements, a list of those components is displayed. Upgrade or switch forward the listed components to the required software versions and re-run this command.<br>• If the versions of the associated components are compatible with the node's inactive version, then the switch forward procedure continues.<br>Once the switch-forward procedure begins, you can see the progress details for each of the machines. You can also see the elapsed time since the procedure started. |
| **Expected Outcome** | The system restarts and the current version of the system is on a higher version. |

**Note** You can check the status of switch forward which is currently in-progress. For more information, see Check Status, on page 323.

## Roll Back Upgrade from Specific Node or Group of Nodes

To roll back an upgrade on VOS or Windows nodes, run the **utils upgrade-manager rollback** command from the Cloud Connect server. It is recommended to run this command during a maintenance window as the procedure involves system restart that will cause service outage.

For the selected VOS or Windows component for rollback, a compatibility check is performed in the background to ensure that all the associated components are onboarded and the versions are compatible. If the components are onboarded and the versions are compatible with each other, the rollback procedure begins. However, if the components are not onboarded, you have to onboard them first or if the versions are not compatible, roll them back to the required version.

For VOS nodes/cluster, the rollback (switch backward) must be initiated from an active higher version to an inactive lower version of the node. Also, the publisher node of the managed cluster must be rolled back before the subscriber node of the cluster.

| Command | utils upgrade-manager rollback |
|---|---|
| **Description** | This command is used to roll back an upgrade on VOS or Windows nodes. |
| **Expected Inputs** | Select the Windows node or VOS node/cluster on which you want to perform the rollback. The rollback option is listed for the selected node or group of nodes. Select the appropriate option and confirm. A compatibility check is then run in the background.<br>• If there are components whose versions are not compatible or if the components are not onboarded as per the compatibility requirements, a list of these components is displayed. Roll back the listed components to the required software versions and then re-run this command.<br>• If the versions of the associated components are compatible with the selected node's rollback version, then the rollback procedure begins.<br>Once the rollback procedure begins, you can see the progress details for each of the machines. You can also see the elapsed time since the procedure started. |
| **Expected Outcome** | The selected node or group of nodes is rolled back. |

**Note** To start Unified ICM services, post the successful completion of roll back upgrade with reboot on Unified ICM nodes. See Start Unified ICM Services.

**Note** You can check the status of rollback which is currently in-progress. For more information, see Check Status, on page 323.

## Check Status

To check the current status of patch manager install, patch manager rollback, upgrade manager upgrade, upgrade manager rollback, switch-forward, or system maintenance initiate, run the **utils deployment show in-progress** command. You can run this command if connectivity to CLI is lost after initiating any of above procedures.

| Command | utils deployment show in-progress |
|---|---|
| **Description** | This command is used to check the current status of any patch manager install, patch manager rollback, upgrade manager upgrade, upgrade manager rollback, switch-forward or system maintenance initiate. It also shows the subsequent progress, if applicable, for each node on which the procedure is initiated.<br>If there is no procedure in progress, this command gives the last successful/failed procedure status. |

| | |
|---|---|
| **Expected Inputs** | NA |
| **Expected Outcome** | Shows the current status of the patch manager install, patch manager rollback, upgrade manager upgrade, upgrade manager rollback, switch-forwardor system maintenance initiate for each node.<br>If there is no patch manager install, patch manager rollback, upgrade manager upgrade, upgrade manager rollback, switch-forward, or system maintenance initiate, then you see the status of the previous upgrade, rollback, or maintenance. |

## Check Last Known Orchestration Operation Status on Remote Node

To check the last known orchestration operation status (last completed state or last known state when the operation is in progress or when the remote node is not reachable ) on the remote node, run the **utils deployment show progress-HA** command. This command is applicable for patch manager install, patch manager rollback, upgrade manager upgrade, upgrade manager rollback, ms patch install, ms patch rollback, switch-forward, system maintenance initiate, and Unified ICM services start.

This command can be used only in Cloud Connect High Availability setup

| **Command** | **utils deployment show progress-HA** |
|---|---|
| **Description** | This command is used to check the last known operation status run on remote node. This will only display the snapshot of the last known operation status and will not display the continuous status changes for the operation that is currently in progress. This command can be used to check the last known operation status on the remote node when the Cloud Connect node is not reachable. |
| **Expected Inputs** | NA |
| **Expected Outcome** | The snapshot of the last known operation status is displayed. |

**Note** Last known orchestration operation status will not be synchronized to remote node, in case of communication loss to remote node after initiating the orchestration operation and operation being completed before re-establishing the communication.

## Start Unified ICM Services

To start Unified ICM services from Cloud Connect server, run the **utils system icm-services start** command.

| **Command** | **utils system icm-services start** |
|---|---|
| **Description** | This command is used to start the Unified ICM services from Cloud Connect server. This CLI will present the user with a list of Unified ICM hosts configured in the inventory, and the admin can select individual or group of Unified ICM hosts. |

| | |
|---|---|
| **Expected Inputs** | User should choose individual or group of Unified ICM hosts from the list.<br>User should give confirmation yes/no to proceed with start of Unified ICM services |
| **Expected Outcome** | As part of CLI output, there are two kinds of messages which displays success as shown below:<br>• When the Unified ICM services are started successfully from stop state, the message "**Services started**" is displayed.<br>• When the Unified ICM services are already up and running, the message "**Services running**" is displayed. |

# Maintenance Tasks

## CLI to configure software download schedule

To change the default schedule for the software download from the Cisco-hosted software artifactory or to change the previously configured software download schedule, run the **utils set software-download time** command.

| **Command** | **utils set software-download time** |
|---|---|
| **Description** | This command changes the default or the previously configured schedule for the software download from the Cisco-hosted software artifactory. |
| **Expected inputs** | Displays the currently configured software download time and prompts you to enter the new time (HH:MM in 24-hours format). |
| **Expected outcome** | Displays the success or failure message for the software download time configuration. |

**Note**

- Cisco recommends that you change the default software download schedule based on your preference.
- Make sure that you configure the time for software download on the publisher and subscriber separately.
- Cisco recommends to set different software download time in Cloud Connect publisher and subscriber, preferably 1 hour apart. For example, if Cloud Connect publisher is set with the download time 3:00 AM, then set Cloud Connect subscriber with the download time 4:00 AM. Avoid using 1:00 AM and 5:00 AM for the software download as this time conflicts with other automatic orchestration operation.
- Default software download time is 2:00 AM Cloud Connect server time.

## CLI to configure the bandwidth for Orchestration software download

To configure the bandwidth that the Orchestration feature uses to download the software from Cisco hosted software artifactory to Cloud Connect server, run the **utils set software-download bandwidth** command.

**Note** Before you configure the bandwidth using the **utils set software-download bandwidth** command, make sure the software is downloaded locally for the first time after the artifactory is successfully configured using the **utils image-repository set** command. To download the artifacts immediately after the configuration, use the **utils initiate software-download** command.

| **Command** | **utils set software-download bandwidth** |
|---|---|
| **Description** | This command configures the bandwidth that the Orchestration feature uses to download software. |
| **Expected inputs** | When run, this command prompts for the following:<br>• Your confirmation with yes or no for turn-on or turn-off the bandwidth configuration.<br>• Enter a valid bandwidth value if you have chosen to turn-on the bandwidth configuration.<br>**Note** • Make sure to suffix the bandwidth value with M for Mbps, K for Kbps and None for Bytes per second. |
| **Expected outcome** | Following are the outcomes:<br>• Displays the success or failure message when you turn-on or turn-off the bandwidth configuration.<br>• If you have turned-on the bandwidth configuration and entered a valid value, this CLI validates and configures the entered bandwidth value. |

**Note**
- Make sure that you configure the bandwidth for software download, on the publisher and subscriber separately.
- Software download bandwidth control is disabled by default. The maximum available bandwidth is used during software download. This might have an impact on the features supported by Cloud Connect only during software download.
- Cisco recommends minimum10-Mbps bandwidth for optimal software download. If you configure the bandwidth to a value that is lesser than 10-Mbps, the duration of the software download increases and the orchestration operations cannot be performed during the software download duration. If you configure the bandwidth to a value that is greater than the maximum available bandwidth, the software download uses only the maximum available bandwidth.
- Proxy configured for orchestration might have an impact on the maximum available bandwidth for software download. Check the proxy configuration and ensure the configured bandwidth will be available for the software download when proxy is used for orchestration.

## Enforce software download from Cisco hosted software artifactory

To initiate software download from Cisco hosted software artifactory to cloud connect server, run the **utils initiate software-download** command.

| **Command** | **utils initiate software-download** |
|---|---|
| **Description** | This command initiates the software download from Cisco hosted software artifactory to Cloud Connect server. |
| **Expected inputs** | User confirmation with yes or no to proceed with software download. |
| **Expected outcome** | Displays the CLI message about the success or failure for the software download initiated. |

**Note**

- Software download must be planned during off-peak hours as it consumes network bandwidth and resources. The duration of the download depends on the number of software that needs to be downloaded.
- Periodic software download happens everyday at 2 AM or at the time configured by admin. Use this CLI to initiate software download before the next scheduled download.
- Software download needs to be initiated in the publisher and the subscriber separately. While software download is in progress on the publisher, you can run the orchestration operation from the subscriber, or vice-versa.
- This CLI only initiates the software download and the download starts after prerequisites are met.

## Update VOS Nodes Onboarded to Orchestration Control Node

To update VOS based nodes that have been onboarded, run the **utils system onboard update** command from the publisher node in the VOS node/cluster that you want to update.

| **Command** | **utils system onboard update** |
|---|---|
| **Description** | This command is used to update a node/cluster on a Cloud Connect node. |
| **Expected Inputs** | When run, this command prompts for:<br>• Cloud Connect server FQDN<br>• Cloud Connect application username and password |
| **Expected Outcome** | The existing node/cluster is updated in the Cloud Connect node inventory. |

## Remove VOS Nodes from Orchestration Control Node

To remove any existing VOS-based node or cluster, run the **utils system onboard remove** command from the publisher node in the VOS node/cluster that you want to remove.

| **Command** | **utils system onboard remove** |
|---|---|

| | |
|---|---|
| **Description** | This command is used to remove a node/cluster from a Cloud Connect node. |
| **Expected Inputs** | When run, this command prompts for:<br>• Cloud Connect server FQDN<br>• Cloud Connect application username and password |
| **Expected Outcome** | The node/cluster is successfully removed from the Cloud Connect node inventory. |

## Update Windows Nodes Onboarded to Orchestration Control Node

The update procedure is similar to the onboarding procedure described in Onboard Windows nodes to orchestration control node, on page 306.

**Note** If SSH connection is already established, skip Step 1 in the above procedure.

## Validate Updated Nodes Onboarded for Orchestration

The procedure to validate updated nodes that have been onboarded is the same as described in Validate Onboarded Nodes for Orchestration, on page 308.

## Configure Email Configuration

You can check your email configuration details by running the respective commands as described below:

- Get the IP address and hostname of the SMTP server by running the **show smtp-host** command.

| | |
|---|---|
| **Command** | **show smtp-host** |
| **Description** | This command is used to get the IP address or hostname of the SMTP server. |
| **Expected Inputs** | NA |
| **Expected Outcome** | Shows the configured IP address or host name of the SMTP server. |

- Get the email address from which the emails are triggered by running the **show smtp-from-email** command.

| | |
|---|---|
| **Command** | **show smtp-from-email** |
| **Description** | This command is used to get the email address from which the emails are triggered. This email address is not monitored and therefore not used for replying to any emails. |
| **Expected Inputs** | NA |
| **Expected Outcome** | Shows the email address from which the emails are triggered. |

- See if SMTP authentication is enabled or not by running the **show smtp-use-auth** command.

| Command | show smtp-use-auth |
|---|---|
| Description | This command is used to know if SMTP authentication is enabled or not. |
| Expected Inputs | NA |
| Expected Outcome | SMTP authentication : <enable/disable> |

- Get the username for SMTP server connection by running the **show smtp-user** command.

| Command | show smtp-user |
|---|---|
| Description | This command is used to show the user name to be used for SMTP server connection. |
| Expected Inputs | NA |
| Expected Outcome | Shows the SMTP username. |

- See if the SMTP password is set or not by running the **show smtp-pswd** command.

| Command | show smtp-pswd |
|---|---|
| Description | This command is used to know if the SMTP password is set or not. To reset the password, run the **set smtp-pswd** command. |
| Expected Inputs | NA |
| Expected Outcome | Shows whether the SMTP password is set or not. |

- See the email addresses subscribed for notification by running the **utils smtp show subscriptions** command.

| Command | utils smtp show subscriptions |
|---|---|
| Description | This command is used to get a list of all the email addresses subscribed for email notification. |
| Expected Inputs | NA |
| Expected Outcome | Shows the email addresses that are subscribed for email notification.<br>If there is no email address subscribed, a message is displayed indicating it. |

## Delete Configuration for Email Notification

To remove the configuration for email notifications, run the **utils smtp remove-config** command.

| Command | utils smtp remove-config |
|---|---|
| Description | This command is used to remove the SMTP configuration from the control node. Email notification will no longer be sent to the subscribed email addresses. This command removes only the SMTP configuration, not the subscribed email addresses. |

| | |
|---|---|
| **Expected Inputs** | NA |
| **Expected Outcome** | SMTP configuration is deleted. |

## Unsubscribe Email Notification

To unsubscribe from email notifications, run the **utils smtp unsubscribe** command.

| **Command** | **utils smtp unsubscribe** |
|---|---|
| **Description** | This command is used to remove one or more email addresses from the existing list of subscribers for email notification.<br>**Note** You can get a list of subscribed email addresses using the **utils smtp show subscriptions** command. |
| **Expected Inputs** | Provide a comma-separated list of the email addresses to unsubscribe. For example:<br>**utils smtp unsubscribe <emailaddress1,emailaddress2,.....emailaddressesN>**<br>You can also remove all the subscribed email addresses from the subscription list at once. To do that, run **utils smtp unsubscribe all** and confirm. |
| **Expected Outcome** | Removes the email addresses you provided as the input from the subscription list. |

## Export and Import of Nodes Managed by Orchestration Control Node

To export inventory to an SFTP server, run the **utils system inventory export** command.

| **Command** | **utils system inventory export** |
|---|---|
| **Description** | This command is used to export inventory to an SFTP server location. The inventory file can then be viewed and edited as required. |
| **Expected Inputs** | When run, this command prompts for:<br>• SFTP Server: IP address of the SFTP remote server<br>• SFTP User<br>• SFTP User's Password<br>• SFTP Directory: Location of the remote server directory where the inventory needs to be exported<br>**Note** Provide the location only; the filename is *inventory.conf* by default. |
| **Expected Outcome** | Inventory is exported to the SFTP server location. |

To import inventory to Cloud Connect server, run the **utils system inventory import** command.

| Command | utils system inventory import |
|---|---|
| Description | This command is used to import inventory to Cloud Connect server. |
| Expected Inputs | When run, this command prompts for:<br>• SFTP Server: IP address of the SFTP remote server<br>• SFTP User<br>• SFTP User's Password<br>• SFTP Directory: Location of the remote server directory from where the inventory needs to be imported<br>**Note** • Provide the location only. The filename is *inventory.conf* by default.<br>• During inventory import, the *inventory.conf* filename should have the side information added for each node. For example, side: "A" /side: "B". During inventory import, the cluster information cannot be blank. It should have valid host details or a default value {}. For example, "ROGGER":{} |
| Expected Outcome | Inventory is imported to Cloud Connect server. |

**Note** For information on adding deployment type and deployment name in the inventory file, see Add Deployment Type and Deployment Name, on page 308.

## Export Current Patch Level Details

Available patches for nodes in the deployment can be obtained in either of the following ways:

- Email Notification
- Using the **utils patch-manager list** command.

Current patch levels can be exported in text file format using the **utils patch-manager export status** command.

| Command | utils patch-manager export status |
|---|---|
| Description | This command is used to export the patch level details of a node or a group of nodes in a text file format. |
| Expected Inputs | Select the node(s) and enter the SFTP server details. |
| Expected Outcome | A text file with the current patch levels of the selected nodes is exported to the provided location. A success message is displayed along with the location where the file is saved. |

# Serviceability

### Audit Logs

Audit trial for administrative operation that is initiated from Orchestration CLI on Cloud Connect is captured in Orchestration Audit logs. Audit trial captures the user, action and date/time details of the CLI operation.

- **file get activelog orchestration-audit/audit.log***

### CLI Logs

Run the following command on the Cloud Connect node to retrieve CLI logs:

- **file get activelog platform/log/cli*.log**

### Ansible Logs

Run the following commands on the Cloud Connect node to retrieve ansible-related logs:

- Current transaction logs: **file get activelog ansible/ansible.log**
- Historical logs: **file get activelog ansible/ansible_history.log**

### Operation Status HA Synchronization Logs

Run the following command on the Cloud Connect node to retrieve synchronization-related logs:

- **file get activelog ansible/sync_ansible_log_to_remote_cc.log**

### Email Notification-related Logs

Run the following commands on the Cloud Connect node to retrieve email-related logs:

- Current transaction logs:**file get activelog ansible/ansible_email_cron.log**

### Software Download Logs

Run the following commands on the Cloud Connect node to retrieve software download-related logs:

- Current transaction logs:**file get activelog ansible/software_download_ansible.log**
- Historical logs:**file get activelog ansible/software_download_ansible_history.log**
- Process logs:**file get activelog ansible/software_download_process.log**

**Note** Software is downloaded separately on Cloud Connect publisher and subscriber.

### Orchestration Logs in RTMT

You can also view the below-mentioned logs using the Real-Time Monitoring Tool (RTMT):

- Audit logs by selecting 'Orchestration Audit' as the Cloud Connect service
- Ansible logs by selecting 'Ansible Controller' as the Cloud Connect service

To download RTMT from Cloud Connect, access https://FQDN:8443/plugins/CcmServRtmtPlugin.exe.

For more information, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide* at:https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

For logs on individual components, refer to the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

## Enable and View Windows Open SSH Logs

To enable and view open SSH logs, do the following:

- Make sure the sshd_config file *%programdata%\ssh\sshd_config* has the value as 'LogLevel DEBUG' and uncomment the line.
- Restart the service (select service name **OpenSSH SSH Server**).
- In the Windows Event Viewer, select option **`Show Analytic and Debug Logs`** from **View** on the top menu bar.
- Select **`Debug`** channel from OpenSSH folder.
- On the right hand side, under Actions from Debug channel, select **`Enable log`**.

To turn on file-based logging, do the following:

- In the sshd_config file *%programdata%\ssh\sshd_config*, set the value as "SyslogFacility LOCAL0" and uncomment the line.
- Restart the service (select service name **OpenSSH SSH Server**).
- The file based logs are collected at location *%programdata%\ssh\logs*.

# Configure SSH public key on Windows nodes

This section describes how to establish password-less Secure Shell (SSH) connection between Cloud Connect server and Windows node (CVP and ICM) using an SSH public key. The Windows node can be in a Workgroup or Domain.

**Note** If the Windows node (CVP and ICM) version is 12.5, install 12.5 mandatory ES before performing this procedure. Mandatory ES is not applicable for 12.6(x) target nodes. See System Requirements, on page 296 for details.

1. Navigate to *%Users%\<logonUser>\.ssh* and create *authorized_keys* file, if it doesn't exist.

**Note**

- The *authorized_keys* extension type is **File** and you should not modify it.
- The user must have either domain admin or local administrator privilege.

2. Open the browser and enter the following Cloud Connect publisher URL: **https://<CloudConnectIP>:8445/inventory/controlnode/key**
3. Provide your Cloud Connect application admin credentials. Upon successful authentication, a REST API response fetches the Cloud Connect Public SSH Key.
4. Copy the public key value that appears between quotes in the API response into the *authorized_keys* file in *%Users%\<logonUser>\.ssh*.
5. Repeat steps 2, 3, and 4 to fetch the Cloud Connect subscriber public key (if Cloud Connect is HA setup).

**Note** You must copy the Cloud Connect publisher and subscriber public keys into a single *authorized_keys* file. The publisher and subscriber entries should be in separate lines and should not use any extra space, comma, or any special characters at the end of the line.

6. Restart the following OpenSSH services:
   - OpenSSH SSH Server
   - OpenSSH Authentication Agent

**Note** For more information on Windows security hardening, see the *Windows Server Hardening* section in the Security Guide for Cisco Unified ICM/Contact Center Enterprise.

# Self-Signed Certificate

You must import the self-signed certificates of both Cloud Connect publisher and subscriber nodes to the VOS publisher and subscriber nodes.

## Get Tomcat Certificate from Cloud Connect Server

**Procedure**

**Step 1** Login to the Cloud Connect server using: `https://<cloud connect hostname>:8443/cmplatform`.

**Step 2** Navigate to **Security** > **Certificate Management**.

**Step 3** Click **Find**.

**Step 4** Click on the Tomcat certificate of the Cloud Connect server.

**Step 5** Download the *.PEM file* and save the file.

# Import Cloud Connect Server Tomcat Certificate to VOS Nodes

**Procedure**

**Step 1** Login to the VOS node server using: `https://<VOS node hostname>:8443/cmplatform`.

**Step 2** Navigate to **Security** > **Certificate Management**.

**Step 3** Click on Upload Certificate/Certificate Chain.

**Step 4** Select 'tomcat-trust' from the drop-down list in the **Certificate Purpose** field.

**Step 5** Click **Browse** to upload the Cloud Connect server *.PEM file*.

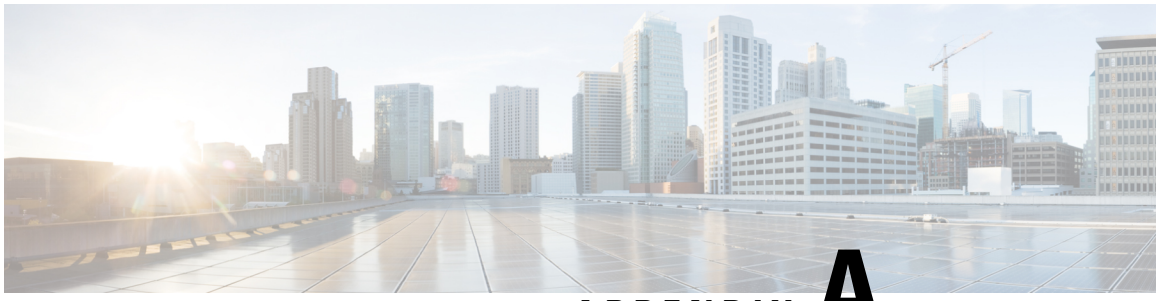
**Step 6** Click **Upload**.

**Step 7** Restart the specific VOS node by running the **utils system restart** command.

# Things to Know

- Orchestration is not supported for CTIOS, Customer Collaboration Platform (CCP), ECE, CCDM, CCMP, and non-Contact Center Cisco products such as UCM, Unity Connection, CUBE gateways, CUSP, IM&P etc. Patches and upgrade operations for these components can be performed in a traditional manner.
- Orchestration is supported only for upgrades and patch install and not for tech refresh or fresh install.
- If any activity is blocked with a message `previous orchestration or upgrade operation is still in progress` even if there is no active operation, then restart Cloud Connect server.
- If one component ES has a dependency on another component ES, then they have to be taken into consideration by the administrator before initiating the patch installation from Cloud Connect server. The administrator should read the release notes that is notified through an email to understand the dependency. The Orchestration framework does not track this aspect automatically. For example, if an ES of Finesse has a dependency on an ES of Live Data and has to be installed in a specific order, then the administrator must consider this before initiating the patch installation from Cloud Connect server.
- Within Upgrade commands 'All Nodes' option for the Roll Back and Switch version commands are not available.
- Only Microsoft Exchange Server is supported for email notification; Office 365 and Gmail are not supported as of now.
- Email notifications are triggered about the available software upgrade from the publisher node of Cloud Connect server. If the publisher node is down at the trigger time, then the Admin will not receive any notification.
- All nodes option in *utils upgrade-manager list* CLI uses an internal cache, which is updated every day at 5 AM. The latest version of components that are upgraded before the cache update scheduled time will not be listed in All nodes option. The latest version of components can be listed by selecting the individual VOS or Windows or group of nodes option in the *utils upgrade-manager list* CLI. The cache update can be enforced by running the *utils system inventory import* CLI.
- For Packaged CCE deployment, only multistage upgrade is supported from Orchestration.

- For Packaged CCE deployment, CVPOAMP is not supported.



APPENDIX A

# CLI Commands during Installation and Upgrade


- Live Data CLI Commands, on page 337
- Transport Layer Security CLI Commands, on page 350
- Cloud Connect CLI Command, on page 351


# Live Data CLI Commands

## Supported Character Set for Live Data Installation CLI Commands

When working with the CLI (and not exclusively for Live Data), you can use plain alphanumeric characters [0-9] [A-Z] [a-z] and the following additional characters:

- ". " (dot)
- "!" (exclamation mark)
- "@" (at sign)
- "#" (number sign)
- "$" (dollar)
- "%" (percent)
- "^" (caret)
- "*" (star)
- "_" (underscore)
- "+" (plus sign)
- "=" (equal sign)
- "~" (tilde)
- ":" (colon)
- "(" and ")" (open and close parentheses)
- "{" and "}" (open and close brackets)

- "[" and "]" (open and close square brackets)

Spaces are used as input separators. Most special characters carry specific meaning to the Cisco Voice Operating System (VOS) command console (for example, "\", "|", and so on). Characters above standard ASCII are mostly ignored.

# Privilege Levels for Live Data Commands

The Live Data CLI commands support the following privilege levels:

- Ordinary
- Advanced

Each Live Data command has a required privilege level related to the sensitivity of data it exposes or its ability to severely affect the operation of the application. The privilege level for each command is the minimum level required; a user with a higher privilege level also has access to the command.

The Cisco Voice Operating System (VOS) also supports a higher privilege level for the administrative user; this user is configured at installation. When the administrative user creates other users (with the set account name command), the administrative user sets each newly created user's privilege level. (For more information about the set account command, see the *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. )

# Live Data AW DB Access

The Live Data AW DB access commands allow you to configure and display CCE AW DB (real-time distributor) access for the Contact Center Enterprise Live Data Product Deployment Selection. By default, the set and show commands also test the connection from Live Data to the primary or secondary AW database, check to see if the configured user has appropriate AW DB access, and report the results.

## set live-data aw-access

**Required Minimum Privilege Level:** Advanced

Use this command to set the access information to the primary or secondary CCE AW. The command also automatically tests the connection from Live Data to the primary or secondary AW, checks to see if the configured user has appropriate AW DB access, and reports the results.

You can use the optional skip-test parameter if you do not want the test performed. No checking is done to see if the configured user has appropriate AW DB access, and no results are reported.

**Command Syntax**

**set live-data aw-access {primary | secondary}** *addr port db user* [*skip-test*]

**addr**

Specifies the FQDN of the primary or secondary CCE AW (maximum 255 characters).

**port**

Specifies the listening port of the database server (range 1 through 65535).

**db**

Specifies the database name (maximum 128 characters).

**user**

Specifies the login user (maximum128 characters).

**skip-test**

Skips the testing of the connection from Live Data to the primary or secondary AW. No checking is done to see if the configured user has appropriate AW DB access, and no results are reported. The skip-test parameter is optional.

**Command Default** When you run this command, it prompts you to specify the login password (maximum 128 characters) to use for authentication with AW database access.

## unset live-data aw-access

**Required Minimum Privilege Level:** Advanced

Use this command to unset the access information to the primary or secondary CCE AW DB.

**Command Syntax**
**unset live-data aw-access {primary | secondary}**

There is a single, required parameter with two possible values.

## show live-data aw-access

**Required Minimum Privilege Level:** Ordinary

Use this command to display the primary and secondary CCE AW DB access information and test the connection from Live Data to each AW DB, check to see if the configured user (on each node) has appropriate AW DB access, and report the results.

You can use the optional skip-test parameter if you do not want the test performed. No checking is done to see if the configured user (on each node) has appropriate AW DB access, and no results are reported.

**Command Syntax**
**show live-data aw-access** [*skip-test*]

Shows the configured primary and secondary CCE AW DB access information. There are no required parameters.

**skip-test**

Skips the testing of the connection from Live Data to the primary or secondary AW. No checking is done to see if the configured user (on each node) has appropriate AW DB access, and no results are reported. The skip-test parameter is optional.

# Live Data Cluster Configuration

Use the following commands to set, unset, or show Live Data cluster configuration information.

## set live-data secondary

**Required Minimum Privilege Level:** Advanced

Use this command to register the Live Data secondary node.

**Command Syntax**
**set live-data secondary** *name*
**name**

Specifies the FQDN of the Live Data secondary node.

## unset live-data secondary

**Required Minimum Privilege Level:** Advanced

Use this command to unset Live Data secondary node configuration.

**unset live-data secondary**

There are no required parameters.

## show live-data secondary

**Required Minimum Privilege Level:** Ordinary

Use this command to show Live Data secondary node configuration information.

**show live-data secondary**

There are no required parameters.

# Live Data Reporting Configuration

## set live-data reporting-interval

**Required Minimum Privilege Level:** Advanced

Use this command to set the Live Data reporting interval in minutes. The reporting interval is the duration of time for which values are aggregated and reported for the **To Interval** fields.

**Command Syntax**
**set live-data reporting-interval** *reporting-interval-in-minutes*
**reporting-interval-in-minutes**

Specifies the reporting interval in minutes. The valid values are 5, 10, 15, 30, and 60 minutes.

When you set the Live Data reporting interval, restart the publisher and then the subscriber. Restart the inactive node and then the active node by using the **utils system restart** command. (For more information about the command, refer to the *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.)

If you restart only the publisher and not the subscriber, the new reporting interval takes effect only on the publisher; likewise, if you restart the subscriber but not the publisher, only the subscriber uses the newly set reporting interval.

When the publisher and the subscriber restart, use the show live-data reporting-interval command to validate the new interval.

## show live-data reporting-interval

**Required Minimum Privilege Level:** Ordinary

Use this command to show the configured and current reporting interval for both the Live Data publisher and subscriber.

**Command Syntax**
**show live-data reporting-interval**

## unset live-data reporting-interval

**Required Minimum Privilege Level:** Advanced

Use this command to reset the Live Data reporting interval to the default value (which is five minutes).

**Command Syntax**
**unset live-data reporting-interval**

When you reset the Live Data reporting interval, restart the publisher and then the subscriber. Restart the inactive node and then the active node by using the **utils system restart** command. (For more information about the command, refer to the *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.)

If you restart only the publisher and not the subscriber, the reset interval takes effect only on the publisher; likewise, if you restart the subscriber but not the publisher, only the subscriber uses the reset reporting interval.

When the publisher and the subscriber restart, use the show live-data reporting-interval command to validate the new interval.

# Live Data Services Registration

## set live-data cuic-datasource

**Required Minimum Privilege Level:** Advanced

Use this command to create or update the Live Data data source in Cisco Unified Intelligence Center.

You can run the command from either the Side A or Side B (not both) Live Data node; and you must run it once for each of the Cisco Unified Intelligence Center Publisher nodes. The AW Distributor and Cisco Unified Intelligence Center Publisher must be in service.

You can use this command after you:

- Set the AW DB connection information on the same node where you want to run this command.
- Configure Live Data endpoints in the Machine Service table.

**Note** You must run this command when there is a change in machine service inventory table. The changes can occur when,

- Recreating the node in Unified CCE Inventory
- Restoring AW database using EDMT
- Running the **set livedata machine-services** CLI command (for 4K and above)

**Command Syntax**
**set live-data cuic-datasource** *cuic-addr cuic-port cuic-user*
**cuic-addr**

Specifies the Cisco Unified Intelligence Center publisher node's fully qualified domain name (FQDN). This node must be in service.

**cuic-port**

Specifies the Cisco Unified Intelligence Center REST API port, which must be 8444.

**cuic-user**

Specifies the user name to use for authentication with Cisco Unified Intelligence Center. By default, Cisco Unified Intelligence Center requires that you specify `CUIC` as the domain with the user name (for example, `CUIC\administrator`).

This user must have system configuration administrative privileges.

**Command Default** When you run this command, it prompts you to specify the password to use for authentication with Cisco Unified Intelligence Center.

## show live-data cuic-datasource

**Required Minimum Privilege Level:** Ordinary

Use this command to list the Live Data data source configuration in Cisco Unified Intelligence Center.

You can use this command after you:

- Set the AW DB connection information on the same node where you want to run this command.
- Configure Live Data endpoints in the Machine Service table.

**Command Syntax**
**show live-data cuic-datasource** *cuic-addr cuic-port cuic-user*
**cuic-addr**

Specifies the Cisco Unified Intelligence Center publisher node's fully qualified domain name (FQDN).

**cuic-port**

Specifies the Cisco Unified Intelligence Center REST API port, which must be 8444.

**cuic-user**

Specifies the user name to use for authentication with Cisco Unified Intelligence Center. By default, Cisco Unified Intelligence Center requires that you specify `CUIC` as the domain with the user name (for example, `CUIC\administrator`).

**Command Default** When you run this command, it prompts you to specify the password to use for authentication with Cisco Unified Intelligence Center.

## unset live-data cuic-datasource

**Required Minimum Privilege Level:** Advanced

Use this command to delete the existing Live Data data source. Ensure that there are no existing reports or report templates that reference the Live Data data source before you run the command; otherwise, the command fails.

After you run this command successfully, you can no longer generate Live Data reports.

You can use this command after you:

- Set the AW DB connection information on the same node where you want to run this command.
- Configure Live Data endpoints in the Machine Service table.

**Command Syntax**
**unset live-data cuic-datasource** *cuic-addr cuic-port cuic-user*
**cuic-addr**

Specifies the Cisco Unified Intelligence Center publisher node's fully qualified domain name (FQDN).

**cuic-port**

Specifies the Cisco Unified Intelligence Center REST API port, which must be 8444.

**cuic-user**

Specifies the user name to use for authentication with Cisco Unified Intelligence Center. By default, Cisco Unified Intelligence Center requires that you specify `CUIC` as the domain with the user name (for example, `CUIC\administrator`).

This user must have system configuration administrative privileges.

**Command Default** When you run this command, it prompts you to specify the password to use for authentication with Cisco Unified Intelligence Center.

## set live-data machine-services

**Note** This command is not valid for coresident deployments. If you have a coresident deployment, use the System Inventory in the Unified CCE Administration tool.

**Required Minimum Privilege Level:** Advanced

Use this command to set or update the Machine Service table with the latest information from Live Data services (publisher and subscriber).

**Note** You must run the **set live-data cuic-datasource** CLI command after running the **set live-data machine-services** command.

**Command Syntax**
**set live-data machine-services** *awdb-user*
**awdb-user**

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

**Command Default** When you run this command, it prompts you to specify the login password to use for authentication with AW database access.

It also prompts you to specify the password of the logged in user for the current CLI session.

## show live-data machine-services

**Required Minimum Privilege Level:** Ordinary

Use this command to display Live Data entries in the Machine Services table.

**Command Syntax**
**show live-data machine-services** [*awdb-user*]
**awdb-user**

Use the `user@domain` format to specify the AW database domain user with at least read-access permission.

**Command Default** When you run this command, it prompts you to specify the login password to use for authentication with AW database access.

## set live-data network-buffer

**Required Minimum Privilege Level:** Advanced

Use this command to set the network buffer size for the Live Data VM.

**Note** During peak load on Live Data, the VMXNET3 adapter is reset due to which the Live Data service is disconnected from other components. To avoid this disconnection, use the `set live-data network-buffer` command to increase the buffer size for the Live Data VM. The recommended value for both receive (rx) and transmit (tx) buffers is 4096 bytes, which is also the maximum allowed value. For more information about handling high traffic bursts, refer to the VMware KB article at https://kb.vmware.com/s/article/2039495.

**Command Syntax**
**set live-data network-buffer** [*options*] [*size*]

OPTIONS:

*[tx]* sets the custom network-buffer tx size.

*[rx]* sets the custom network-buffer rx size.

SIZE:

*[size]* sets the buffer size in bytes.

## show live-data network-buffer

**Required Minimum Privilege Level:** Ordinary

Use this command to view the network buffer size for the Live Data VM.

**Command Syntax**
**show live-data network-buffer** [*options*]

OPTIONS:

*[tx]* shows the custom network-buffer tx size.

*[rx]* shows the custom network-buffer rx size.

## unset live-data network-buffer

**Required Minimum Privilege Level:** Advanced

Use this command to reset to the default network buffer size for the Live Data VM.

**Command Syntax**
**unset live-data network-buffer** [*options*]

OPTIONS:

*[tx]* resets the custom network-buffer tx size to the default value of 512 bytes.

*[rx]* resets the custom network-buffer rx size to the default value of 1024 bytes.

## show live-data appd-monitoring status

**Required Minimum Privilege Level:** Ordinary

Use this command to view the AppDynamics monitoring status for the Live Data worker process. The Live Data worker process is a real-time event processing system in Live Data. The default value is false.

**Note** This command is applicable only if the AppDynamics instrumentation is enabled for the Live Data VM.

**Command Syntax**
**show live-data appd-monitoring status**

There are no required parameters.

## set live-data appd-monitoring enable

**Required Minimum Privilege Level:** Advanced

Use this command to enable the AppDynamics instrumentation for the Live Data worker process.

**Note** This command is applicable only if the AppDynamics instrumentation is enabled for the Live Data VM.

The AppDynamics instrumentation is disabled by default because it has a performance overhead on the worker process, if enabled. For example, the worker process may have an increased latency in Live Data reporting during peak load.

**Command Syntax**
**set live-data appd-monitoring enable**

There are no required parameters.

## set live-data appd-monitoring disable

**Required Minimum Privilege Level:** Advanced

Use this command to disable the AppDynamics instrumentation for the Live Data worker process.

**Note** This command is applicable only if the AppDynamics instrumentation is enabled for the Live Data VM.

**Command Syntax**
**set live-data appd-monitoring disable**

There are no required parameters.

# Live Data CORS Configuration

Live Data CORS commands allow you to configure CORS and hence allow web applications running on different origins to communicate with Live Data.

**Note** Ensure that the CORS update commands are run on all the live data nodes in the cluster.

After you make changes to the CORS status, allowed origins, allowed headers, or exposed headers, restart the Cisco Web Proxy Service.

## utils live-data cors status

**Required Minimum Privilege Level: Ordinary**

Use this command to query the Live Data CORS status.

**Command Syntax**
**utils live-data cors status**

There are no required parameters.

## utils live-data cors enable

**Required Minimum Privilege Level: Advanced**

Use this command to enable CORS in Live Data.

**Command Syntax**
**utils live-data cors enable**

There are no required parameters.

**Note** For Unified Intelligence Centre gadgets (Live Data) to load in Cisco Finesse, ensure to:

- Enable CORS using `utils cuic cors enable` and `utils live-data cors enable` commands.
- Set the Finesse host URL in `utils cuic cors allowed_origin add URLs` and `utils live-data cors allowed_origin add URLs` commands.

  **Examples:**

  - https://<finesse-FQDN>
  - https://<finesse-FQDN>:port

## utils live-data cors disable

**Required Minimum Privilege Level: Advanced**

Use this command to disable CORS in Live Data.

**Command Syntax**
**utils live-data cors disable**

There are no required parameters.

## utils live-data cors allowed_origin list

**Required Minimum Privilege Level: Ordinary**

Use this command to display the list of allowed URLS that can make CORS request to Live Data.

**Command Syntax**
**utils live-data cors allowed_origin list**

There are no required parameters.

## utils live-data cors allowed_origin add

**Required Minimum Privilege Level: Advanced**

Use this command to add the given list of URLs to the allowed origin list.

**Command Syntax**
**utils live-data cors allowed_origin add** *URLs*

**URLs**

Comma separated list of URLs (without spaces) that has to be added to the allowed origins list. The URL should be of the format: **http[s]://<hostname>[:port]**

## utils live-data cors allowed_origin delete

**Required Minimum Privilege Level: Advanced**

Use this command to delete a particular URL entry or all the URL entries from the allowed origins list.

**Command Syntax**
**utils live-data cors allowed_origin delete**

There are no required parameters. This command will prompt for a choice to delete a particular entry or all URL entries from allowed origins list.

**Example**

Utils live-data cors allowed_origin delete

1. https://cisco.com

2. https://google.com

a: all

q: quit

## utils live-data cors allowed_headers list

**Required Minimum Privilege Level: Ordinary**

Use this command to display the list of allowed headers that the client can use to make CORS request to Live Data.

**Command Syntax**
**utils live-data cors allowed_headers list**

There are no required parameters.

## utils live-data cors allowed_headers add

**Required Minimum Privilege Level: Advanced**

Use this command to add the given list of headers to the allowed header list.

**Command Syntax**
**utils live-data cors allowed_headers add** *headers*

**headers**

Comma separated list of headers (without spaces) that has to be added to the allowed headers list.

## utils live-data cors allowed_headers delete

**Required Minimum Privilege Level: Advanced**

Use this command to delete a particular header entry or all the header entries from the allowed headers list. The header names are case-insensitive and any duplicate header name will be ignored.

**Command Syntax**
**utils live-data cors allowed_headers delete**

There are no required parameters. This command will prompt for a choice to delete a particular entry or all the header entries from the allowed headers list.

**Example**

Utils live-data cors allowed_headers delete

1. Header1

2. Header2

a: all

q: quit

## utils live-data cors exposed_headers list

**Required Minimum Privilege Level: Oridnary**

This command displays the list of exposed headers that the client can expect from Live Data when it makes CORS request to Live Data .

**Command Syntax**
**utils live-data cors exposed_headers list**

There are no required parameters.

## utils live-data cors exposed_headers add headers

**Required Minimum Privilege Level: Oridnary**

This command adds given list of headers to the exposed header list.

**Command Syntax**
**utils live-data cors exposed_headers add** *headers*

headers

Comma separated list of headers that has to be added to the exposed headers list.

## utils live-data cors exposed_headers delete

**Required Minimum Privilege Level: Oridnary**

This command deletes a particular header entry or all the header entries from the exposed headers list. The header names are case-insensitive, any duplicate header name will be ignored.

**Command Syntax**
**utils live-data cors exposed_headers delete**

There are no required parameters. This command will prompt for a choice to delete a particular entry or all header entries from exposed headers list.

**Example**

Utils live-data cors exposed_headers delete.

1. Header1
2. Header2

   a: all

   q: quit

# Transport Layer Security CLI Commands

**Note** These CLI commands are only for VOS systems. They are not available for VMs running Windows Server.

# TLS Server Minimum Version

## set tls server min-version

Use this command to set the current TLS minimum version for inbound connections.

**Command Syntax**

**set tls server min-version 1.2**
**1.2**

Specifies the TLS server minimum version 1.2 for inbound connections.

## show tls server min-version

Use this command to display the current TLS minimum version for inbound connections.

**Command Syntax**
**show tls server min-version**

# TLS Client Minimum Version

## set tls client min-version

Use this command to set the current TLS minimum version for outbound connections.

**Command Syntax**

**set tls client min-version 1.2**
**1.2**

Specifies the TLS client minimum version 1.2 for outbound connections.

## show tls client min-version

Use this command to display the current TLS minimum version for outbound connections.

**Command Syntax**
**show tls client min-version**

# Cloud Connect CLI Command

## set cloudconnect subscriber

**Required Minimum Privilege Level:** Advanced

**Command Default** Use this command to configure the cloud connect subscriber node in the cluster. The command verifies if the hostname is valid or not. Ensure to run this command only from publisher node.

**Command Syntax**
**set cloudconnect subscriber** *[ name ]*
**name**

Specifies the FQDN or IP address of the Cloud Connect subscriber node (maximum 255 characters).

When you run this command, it configures the Cloud Connect subscriber node in the cluster.

## show cloudconnect subscriber

**Required Minimum Privilege Level:** Ordinary

**Command Default** Use this command to display the Cloud Connect subscriber node details.

**Command Syntax**
**show cloudconnect subscriber**

When you run this command, it displays the Cloud Connect subscriber node details.

# unset cloudconnect subscriber

**Required Minimum Privilege Level:** Advanced

**Command Default**

Use this command to remove the Cloud Connect subscriber node configuration from the cluster. Ensure to run this commend only from publisher node.

**Command Syntax**
**unset cloudconnect subscriber**

When you run this command, it remove the Cloud Connect subscriber node configuration from the cluster.

# set cloudconnect cherrypoint config

**Required Minimum Privilege Level:** Advanced

**Command Default**

Run this command to update the Cloud Connect Cherry point connector configuration details.

**Note** When you run this command, you are prompted to enter new configuration details. The current configuration details are displayed within *[ ]*. You can enter the new configuration details or retain the existing configuration.

**Note** User input for Web URL Prefix must be a valid http or https URL. The default value is https://nps.bz . For users upgrading Cloud Connect, if the Web URL prefix does not have a valid http or https URL prefix, they must reconfigure Cloud Connect Cherry point to provide a valid URL for Web URL prefix.

When reconfiguring the Web URL prefix, ensure all the inputs are re-entered again.

**Note** **Voice PIN Prefix**, **SIP URI Domain** are no more applicable and the user will not be prompted for the same and will not be shown in the CLI command output.

**Command Syntax**
**set cloudconnect cherrypoint config**

When you run this command, the current Cloud Connect Cherry point connector configuration is fetched and is displayed. You are prompted to enter new configuration details. The current configuration details are displayed within *[ ]*. You can enter the new configuration details or retain the existing configuration.

Example:

```
admin:set cloudconnect cherrypoint config
Fetching existing configuration...
Enter the Config details to be saved:
Desktop User (with Read Only Privileges): readonlyusername
Desktop User API Key []: apikey-ABCD1234EFGH5789!dummy
System User (with Read and Write Privileges): reawriteusername
System User API Key []: apikey-JKMLN012345OPQRST6789!dummy
Web URL Prefix: https://nps.bz
Deployment ID: CCE_Deployment_Bangalore_Site
```

```
Proxy Enabled(true/false) [false]: true
Proxy Host: proxyhost.domain.com
Proxy Port [0]: 5678
The config details updated successfully.
```

# show cloudconnect cherrypoint config

**Required Minimum Privilege Level:** Advanced

**Command Default** Use this command to display the Cherry point connector configuration details.

**Command Syntax**
**show cloudconnect cherrypoint config**

When you run this command, the Cherry point connector configuration details are displayed.

# utils cloudconnect cherrypoint test-connectivity

**Required Minimum Privilege Level:** Advanced

**Command Default** Use this command to test the connectivity to Cloud Cheery server.

**Command Syntax**
**utils cloudconnect cherrypoint test-connectivity**

When you run this command, the connectivity to Cloud Cheery server is checked.

# set cloudconnect digitalrouting config

**Required Minimum Privilege Level:** Advanced

Use this command to update the digitalrouting service configuration details.

**Command Syntax**
**set cloudconnect digitalrouting config**

**Command Default** When you run this command, the current digitalrouting service configuration details is fetched and is displayed. You are prompted to enter new configuration details. The current configuration details are displayed within *[ ]*. You can enter the new configuration details or retain the existing configuration. Depending on the config API response, either the success or the error response is displayed.

Example:

```
admin:set cloudconnect digitalrouting config
Fetching existing configuration...
Enter the Config details to be saved:
MR Server SSL Enabled [false]: true
The config details updated successfully.
```

# show cloudconnect digitalrouting config

**Command Default** **Required Minimum Privilege Level:** Advanced

Use this command to display the digital routing configuration details.

**Command Syntax**
**show cloudconnect digitalrouting config**

When you run this command, the DigitalRouting configuration details are displayed.

# show cloudconnect digitalrouting status

**Command Default**

**Required Minimum Privilege Level:** Advanced

Use this command to display status for cluster nodes and components in digitalrouting.

**Command Syntax**
**show cloudconnect digitalrouting status**

When you run this command, the cluster nodes and the component status details are displayed.

# utils cloudconnect reinit services

**Required Minimum Privilege Level:** Advanced

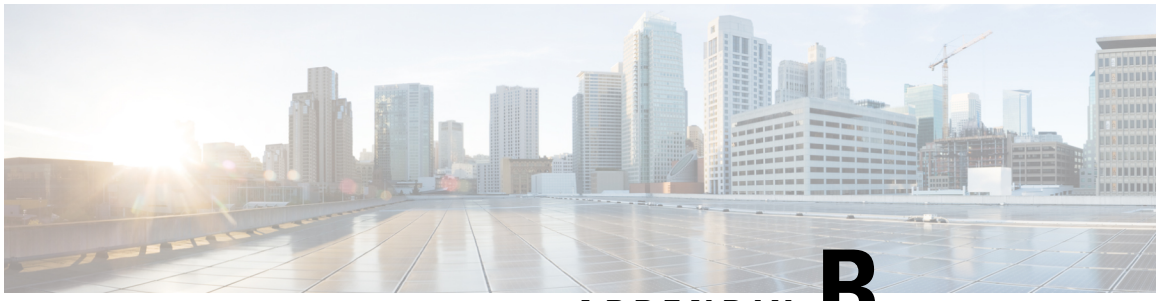
**Command Default**

Use this command to reinitialize Cloud Connect services.

**Command Syntax**
**utils cloudconnect reinit services**

This command stops all the Micro services(Containers) that are running on Cloud Connect, removes the services, and recreates them with new configuration.

**Note** The changes to the timezone take effect on the Cloud Connect services only after you run this command successfully.



APPENDIX B

# Migrate from Co-resident Deployment to Standalone Deployment


- Upgrade from Co-resident to Standalone Deployments, on page 355
- Upgrading Live Data for 24k Deployment Type, on page 356


## Upgrade from Co-resident to Standalone Deployments

If your solution exceeds the configuration limits of 2000 Agent Reference Design, use a Reference Design with higher limits and replace the co-resident deployment of CUIC with a standalone deployment of CUIC, Live Data, and IdS. A standalone deployment allows higher capacity and increased reporting end users. You cannot convert the existing co-resident server to a standalone server.

**Note** You can export the CUIC reports from the co-resident deployment and import them into the new standalone CUIC.

For a new standalone deployment, you must perform fresh install of the following servers, using the method outlined below:

| Sequence | Task |
|---|---|
| 1 | Set up the System Inventory for Standalone Deployment, on page 356 |
| 2 | Install Cisco Unified Intelligence Center Standalone (4000, 8000, 12000 Agent Deployment). See *Installation and Upgrade Guide for Cisco Unified Intelligence Center* at http://www.cisco.com/en/US/products/ps9755/prod_installation_guides_list.html. |
| 3 | Install Live Data. See Live Data Standalone Installation, on page 79. |
| 4 | Install the Identity Service. See Install Cisco Identity Service Standalone Deployment, on page 75 . |

# Set up the System Inventory for Standalone Deployment

### Procedure

**Step 1** In Unified CCE Administration, navigate to **System** > **Deployment**.

**Step 2** Add the new machine to the System Inventory:

a) Select the coresident machine to remove. Cick **Delete**.

b) Click **New**. The **Add Machine** popup window opens.

The **Add Machine** popup window opens.

c) From the **Type** drop-down menu, select the following machine type:

Unified Intelligence Center Publisher.

d) In the **Hostname** field, enter the FQDN, hostname, or IP address of the machine.

The system attempts to convert the value you enter to FQDN.

e) Enter the machine's Administration credentials.

f) Click **Save**.

The machine and its related Subscriber or Secondary machine are added to the System Inventory.

### What to do next

If you remove a component from your deployment, delete it from your System Inventory. If you add the component again, or add more components, add those components to the System Inventory.

# Upgrading Live Data for 24k Deployment Type

After installing Cisco Unified CCE, follow this procedure to upgrade the Live Data server in VM.

### Procedure

**Step 1** In the Virtual Machine:

a) Click the **Edit virtual machine settings** option in **VM Hardware** on the ESXi/ESX host.

b) Increase the CPU cores to 12 and CPU reservation to 24000MHz.

c) Increase the Memory is 36GB and Memory reservation to 36864MB.

For details about how to edit the VM Hardware settings, see the VMware hardware documentation.

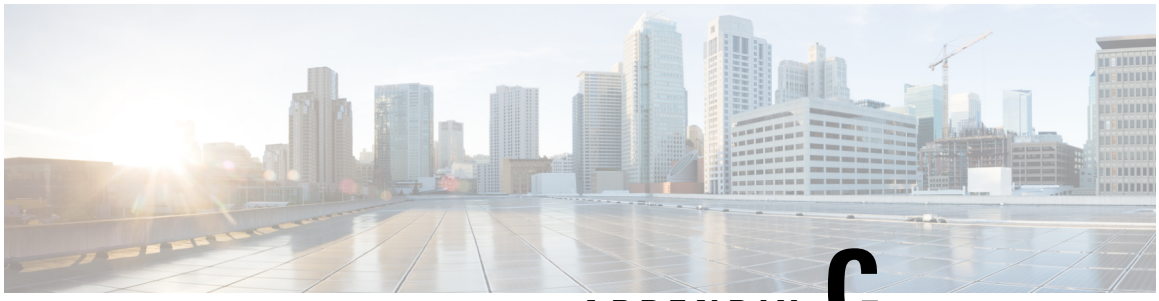
**Step 2** Upgrade live data.

**Note** The System Memory and CPU should be increased before upgrade. If the upgrade is applied before increasing the system memory, use the CLI command in step 3 to set the memory profile parameters correctly.

**Step 3** Run the **set live-data memory profile** CLI command to set the parameters correctly.

**Note** This CLI command updates the memory parameters only if the total RAM on the VM is at least 36 GB. If the RAM is lesser than 36 GB, the CLI resets the memory parameters to default values.

Migrate from Co-resident Deployment to Standalone Deployment



APPENDIX C

# IPv6 Configuration


- Configure NAT64 for IPv6-Enabled Deployment, on page 359
- Set Up IPv6 for VOS-Based Contact Center Applications, on page 361

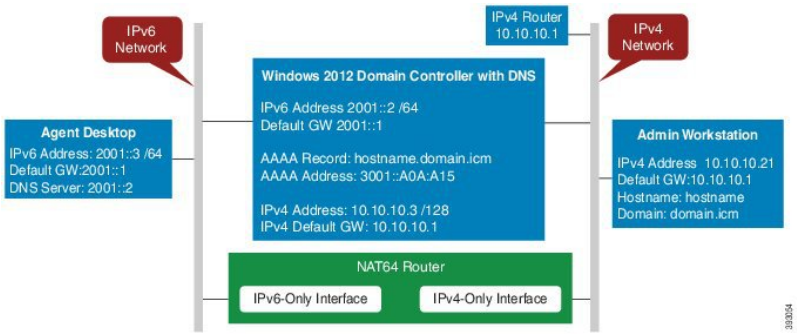

## Configure NAT64 for IPv6-Enabled Deployment

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

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

For more information on *Contact Center Enterprise Compatibility Matrix*, see https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

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




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

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

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

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

# Configure DNS for IPv6

To meet the requirement that Unified CCE Administration be accessed by FQDN, a Forward lookup AAAA record for the AW must be created in DNS.

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

**Procedure**

**Step 1** In Windows, navigate to **Administrative Tools > DNS**. This opens the DNS Manager.

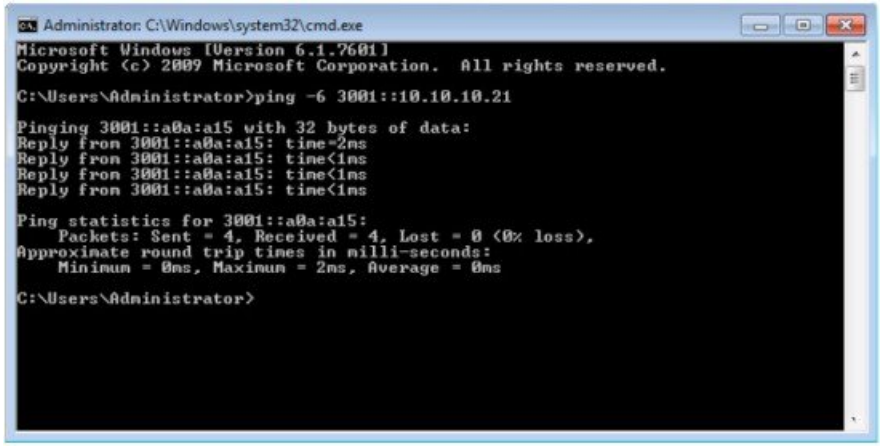
**Step 2** In the Forward lookup zone, navigate to your deployment's domain name.

**Step 3** Right-click the domain name and select **New Host (A or AAAA)**.

**Step 4** In the New Host dialog box, enter the computer name and IP address of the AW. Click **Add Host**.

## Determine IPv6 Translation of IPv4 Address for DNS Entry

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




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

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

# Set Up IPv6 for VOS-Based Contact Center Applications

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

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

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

See the *Solution Design Guide for Cisco 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 more information about IPv6 support in Unified CCE.

## Set Up IPv6 Using Cisco Unified Operating System Administration

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

### Procedure

**Step 1** Sign into Cisco Unified Operating System Administration on the Publisher/Primary node:.

- Unified Communications Manager and Unified Intelligence Center: `https://<host or IP address of the Publisher or Primary node>/cmplatform`
- Finesse: `https://FQDN of the Primary node:8443/cmplatform`

**Step 2** Navigate to **Settings** > **IP** > **Ethernet IPv6**.

**Step 3** Check the **Enable IPv6** check box.

**Step 4** Enter values for **IPv6Address**, **Prefix Length**, and **Default Gateway**.

**Step 5** Check the **Update with Reboot** check box.

**Step 6** Click **Save**.
The server restarts.

**Step 7** Repeat this procedure on the subscriber/secondary node.

# Set Up IPv6 for VOS-Based Applications Using the CLI

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

### Procedure

**Step 1** Access the CLI on the VOS server.

**Step 2** To enable or disable IPv6, enter:
**set network ipv6 service {enable | disable}**

**Step 3** Set the IPv6 address and prefix length:
**set network ipv6 static_address** *addr mask*

**Example:**

```
set network ipv6 static_address 2001:db8:2::a 64
```

**Step 4** Set the default gateway:
**set network ipv6 gateway** *addr*

**Step 5** Restart the system for the changes to take effect.
**utils system restart**

**Step 6** To display the IPv6 settings, enter:
**show network ipv6 settings**