Cisco Unified Contact Center Express Administration and Operations Guide, Release 12.5(1) SU3

First Published: 2023-05-08

Last Modified: 2023-05-08

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)

© 2000–2023 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface xxxi

Change History xxxi

About This Guide xxxi

Audience xxxii

Conventions xxxii

Related Documents xxxiii

Documentation and Support xxxiv

Documentation Feedback xxxiv

CHAPTER 1

Unified CCX Introduction 1

Unified CCX Components 1

Unified CCX Product Family 2

Unified IP IVR 3

Unified Contact Center Express 3

Unified CCX Cluster Architecture 4

Unified CCX Active Server 5

Unified CCX Engine 6

Set Up Unified CCX 7

Provision Telephony and Media Subsystems 7

Configure Unified CCX Subsystems 7

Provision Unified CCX Subsystem 8

Provision Additional Unified CCX Subsystems 8

View License Information 9

Upload Licenses 10

Enable Smart Licensing 10

Configure Transport Settings for Smart Licensing 12

Available Applications 12
Manage Scripts Prompts, Grammars, and Documents 12
Configure Unified CCX Historical Reporting 13
Manage Unified CCX 13

CHAPTER 2 **Unified CCX AdministrationWeb Interface 15**
Access Unified CCX Administration Web Interface 15
Supported Languages 16
Cisco Unified CCX Administration Menu Bar and Menus 16
Cisco Unified CCX Administration Navigation 17
Unified CCX Configuration Web Pages 19
Details for Advanced Configuration 19
Toolbar and Buttons 20
Application and RmCm Wizards 20

CHAPTER 3 **Unified CCX Provision Checklist 21**
Unified CCX 21
Provision Unified CCX 22
Change Licensing Packages 23

CHAPTER 4 **Provision Unified CM for Unified CCX 25**
Configure Unified Communications Manager Information 25
Modify AXL Information 26
Modify Unified Communications Manager Telephony Information 27
Modify RmCm Provider Information 29
Unified Communications Manager for Unified CCX Configuration 30
Invoke Unified Communications Manager Administration 30
Unified Communications Manager Users as Unified CCX Agents 31
Guidelines for Agent Phone Configuration 32
Modify Existing Unified Communications Manager Users 34
Assign Unified Communications Manager Users as Cisco TelePresence Virtual Agents 36
Configure Tool for Auto-Registered Phones Support (TAPS) 37

CHAPTER 5 **Update Unified CM IP Address Change in Unified CCX 41**

Update Unified CM IP Address Change in Unified CCX 41

CHAPTER 6 **Cisco Applications Configuration** 43

About Unified CCX Applications 43

Configure Script Applications 43

Add New Cisco Script Application 44

Configure Busy Application 46

Configure Ring-No-Answer Application 47

Application Triggers 49

Unified CM Telephony Trigger 49

Add Unified CM Telephony Triggers from Application Web Page 49

Add Unified CM Telephony Triggers from Unified CCX 49

HTTP Trigger Provision 50

Add HTTP Trigger from Application Web Page 50

Add HTTP Trigger from HTTP Subsystem 51

Script Management 52

Upload New Scripts 53

Download Script File 54

Refresh Scripts 55

Refresh Scripts Individually 55

Refresh Bulk Scripts 55

Rename Script or Folder 56

Delete Script or Folder 57

Sample Scripts 57

CHAPTER 7 **Telephony and Media Provision** 59

Unified CCX Telephony and Media 59

Media Termination Groups 60

Channels Required to Process Calls 60

Provision Telephony and Media Resources 61

Provision Unified CM Telephony Subsystem 61

Resynchronize Cisco JTAPI Client 62

Resynchronize Unified CM Telephony Data 62

Configure Unified CM Telephony Provider 63

Add New Call Control Group 64
Add Unified CM Telephony Trigger 70
Additional Unified CM Telephony Information 74
Unified CM Telephony Triggers for Unified CCX Queuing 74
Unified CM Telephony Information Resynchronization 75
Cisco Media Subsystem 75
Add CMT Dialog Control Group 76
ASR and TTS in Unified CCX 77
Prepare to Provision ASR/TTS 77
Provision of MRCP ASR Subsystem 78
Provision MRCP ASR Providers 78
Provision MRCP ASR Servers 79
Provision MRCP ASR Dialog Groups 81
MRCP TTS Subsystem 83
Provision MRCP TTS Providers 83
Provision MRCP TTS Servers 84
Provision MRCP TTS Default Genders 86

CHAPTER 8 **Provision of Unified CCX** 89
RmCm Provider Configuration 89
RmCm Provider Modification 90
Associating Agent Extensions with the RmCm Provider 90
Resource Groups 91
Create Resource Group 91
Modify Resource Group Name 91
Delete Resource Group 92
Skills Configuration 92
Create a Skill 92
Modify a Skill Name 93
Delete a Skill 94
Agent Configuration 95
Implications of Deleting Agents in Unified CM 96
Assign Resource Groups and Skills to One Agent 96
Assign Resource Groups and Skills to Multiple Agents 97

Remove Skills from Agents 98
Contact Service Queue Configuration 99
Create a Contact Service Queue 99
Contact Service Queue Configuration Web Page 102
Modify a Contact Service Queue 104
Delete a Contact Service Queue 105
Resource Pool Selection Criteria: Skills and Groups 105
Resource Skill Selection Criteria within a Contact Service Queue 106
Configure Agent-Based Routing 107
Wrap-Up Data Usage 108
Teams Configuration 108
Assign Supervisor Privilege to a User 109
Create Teams 110
Modify Teams 111
Delete a Team 113

CHAPTER 9 **Provision of Additional Subsystems** 115
About Additional Subsystems 115
Provision of HTTP Subsystem 115
Configure HTTP Triggers 116
Provision of Database Subsystem 117
Database Subsystem Configuration 117
Add New Datasource 117
Datasource Configuration Web Page 118
Poll Database Connectivity 119
Provision eMail Subsystem 120

CHAPTER 10 **Management of Prompts, Grammars, Documents, and Custom Files** 123
Manage Prompt Files 123
Manage Grammar Files 124
Manage Document Files 126
Language Management 127
Create New Language 127
Rename Language 128

Delete Language 128
Upload Zip Files to Language Folder 129
Upload of Prompt Files 130
Record a Prompt 131
Add Spoken-Name Prompts 131
Management of Custom Files 132
Specify Custom Classpath Entries 132
AAR File Management 132
AAR File Creation 134
Upload AAR Files 134
META-INF Directory 135
Directories for Prompts, Grammars, Documents, and Scripts 135
Prompts Directory 135
Grammars Directory 136
Documents Directory 136
Scripts Directory 136
AAR Manifest 136
Attribute Types 137
Main Attributes 138
Per-entry Attributes 139
META-INF Directory Attributes 140

CHAPTER 11 **Unified CCX System Management** 143
Basic Terminology 143
High Availability and Automatic Failover 144
Network Partitions 144
Unified CCX CDS Information Management 145
Manage System Parameters 145
Unified CCX IP Address/hostname Management 146
Prepare System for IP Address/hostname Change 146
IP Address Modification 147
Change IP Address for Server in Single-Node Deployment 148
IP Address Modification in High-Availability (HA) Deployment 149
HostName and Domain Name Modification 154

HostName Modification 154
Verify Proper Function of System after IP Address/hostname Change 159
Domain Name Modification 160
Set Up Certificates 162
Client Requirements 162
Set Up CA Certificate for Firefox Browser 162
Set Up CA Certificate for Chrome and Edge Chromium (Microsoft Edge) Browsers 163
Manage Expired CA Certificates 163
Exit Unified CCX Administration 164

CHAPTER 12 **Unified CCX Reporting** 165
Reporting Administration on Unified CCX 165
Import of Stock Reports 165
Unified CCX Historical Reports 165
Unified CCX Historical Datastore 166
Historical Reporting Configuration 166
Purge of Historical Data 167
Unified CCX to Unified Intelligence Center Synchronization 170
File Restore 170
Unified CCX Real-Time Reports 171
Available Unified CCX Real-Time Reports 171
Open Real-Time Reports 172
Run Reports 173
View Detailed Subreports 174
Print Reports 174
Reset Report Statistics 174
Clear Contact Option for Stuck Calls 175
Set Report Options 175
Set Report Appearance 175
Application Reporting User Interface 176
Reporting Administration on Unified Intelligence Center 204
Start Unified Intelligence Center 205
Administrator Overview 205
Security Overview 206

User List 206
Create a User 207
User Groups 209
About User Groups 209
Create a User Group 210
Manage User Permissions 211
About Permissions 211
User Roles and Permissions 212
Assigned Group Permissions 213
Assigned User Permissions 214
Run As 214
Audit Trail Logging in Cisco Unified Intelligence Center 215
View Audit Trail Logging in Unified Intelligence Center 215
Audit Trail Report 215
Security Considerations 216

CHAPTER 13 **Unified CCX Outbound Dialer Configuration** 217
Outbound Feature for Unified CCX 217
Outbound Characteristics 217
Unified CCX Requirements 218
Outbound Components 220
Supported Dialers and Dialing Modes for Outbound 220
Unified CCX Outbound Dialing Modes 221
Direct Preview Dialing Mode 221
Progressive Dialing Mode 221
Predictive Dialing Mode 221
Configure Outbound Subsystem in Unified CCX 222
Configure General Outbound Properties 222
Callbacks 225
Outbound Area Code Functionality 225
Configuration Updates 226
CSQ Agent Pool Allocation 226
Configure Application and Trigger for Outbound Campaign 227
Add New Campaign 227

Import Contacts for Campaign 237
Manual Import of Contacts for Campaign 238
Schedule Import of Contacts Using SFTP or HTTPS 240
Enable Campaigns 242
Outbound Subsystem and Time Detection 242
Add Area Codes 243
Call Status Values 244
Contact States Reset at Midnight 244
Call Result Values 245
Reclassification Status Behavior 246
Call Retrieval Priority 247
Failover and System Restarts 248

CHAPTER 14 Cisco Unified Contact Center Express Supervisor and User Options Plug-Ins 249
About User Management 249
About Unified CCX User Capabilities 249
Administrator Privileges 250
Supervisor Privileges 250
Historical Report User Privileges 250
Agent Privileges 251
Unified CCX Supervisor Web Interface 251
Access Unified CCX Supervisor Web Page 251
Unified CCX User Options Web Interface 252
Access Unified CCX User Options Web Page 252
Add Alternative Pronunciations 252
Access Unified CM User Options Page 253

CHAPTER 15 System Menu 255
Access Server Menu 255
Configure Server 255
Server Deletion 256
Cloud Connect 257
Unified CM Configuration 259
System Parameters 259

Single Sign-On (SSO) 265
Custom File Configuration 267
Standalone Cisco Unified Intelligence Center 267
Obtain and Upload SSL Certificates 267
Access Standalone Cisco Unified Intelligence Center Configuration 268
License Information 269
License Management 269
Classic License Management 269
Smart Licensing 271
Smart License Management 272
Configure Transport Settings for Smart Licensing 275
Register with Cisco Smart Software Manager 276
Language Information 277
Logout Menu 278

CHAPTER 16 **Applications Menu** 279
Access Application Management Menu 279
Manage Scripts 279
Prompt Management 280
Grammar Management 281
Document Management 281
AAR Management 281
Calendar Management 282
Calendar Flow 283

CHAPTER 17 **Subsystems Menu** 285
Unified CM Telephony Menu 285
Unified CM Telephony Provider Configuration 286
Unified CM Telephony Call Control Group Configuration 286
Unified CM Telephony Triggers Configuration 286
Synchronize Unified CM Telephony Data 286
Unified CM Telephony Cisco JTAPI Resync 288
Unified CM Telephony Advanced Settings 288
RmCm Menu 289

Skill Configuration 289
Add New Skill 289
Modify Skills 289
Resources Configuration 290
Modify Resource 290
Resource Group Configuration 290
Add New Resource Group 290
Modify Existing Resource Groups 291
Contact Service Queues Configuration 291
Add a CSQ 291
RmCm Provider Configuration 291
Skills Configuration Assignment 292
Add Skills 292
Remove Skills 292
Agent Based Routing Settings Configuration 292
Teams Configuration 292
Assign Supervisor Privilege to a User 292
Create Teams 293
Modify Teams 294
Delete a Team 296
Chat and Email Menu Options 296
Customer Collaboration Platform Configuration 297
Delete Customer Collaboration Platform Configuration 301
Reinject Email Contacts 302
Chat Transcripts 302
Mail Server Configuration 302
Contact Service Queues 305
Predefined Responses 309
Predefined Responses 309
Wrap-Up Reasons 311
Wrap-Up Reasons 311
Email Signatures 312
Email Signature Configuration 312
Channel Parameters 314

Chat Widgets 316
Chat Widgets Page 316
Chat Widget Configuration 316
Chat - Facebook Messenger 321
Teams 323
Outbound Menu 323
General Configuration 323
Campaign Configuration 323
Add New Campaigns 324
Import Contacts 324
Delete Contacts 324
Area Code Management 324
Add New Area Code 324
Configure SIP Gateway 325
SIP Gateway Configuration Web Page 325
Dial Peer Configuration for Outbound 327
Database Menu 328
DataSource 328
New DataSource 328
Add New Database Parameter 329
Driver 329
Add New Database Driver 329
HTTP Menu 330
HTTP Trigger Configuration 330
Add New HTTP Trigger 330
eMail Menu 330
Cisco Media 331
MRCP ASR Menu 331
MRCP ASR Provider 331
MRCP ASR Servers 331
MRCP ASR Dialog Groups 332
MRCP TTS Menu 332
MRCP TTS Providers 332
MRCP TTS Servers 332

MRCP TTS Default Genders 332

CHAPTER 18 **Wizards Menu 333**

Application Wizard 333

RmCm Wizard 334

CHAPTER 19 **Tools Menu 337**

Plug-Ins Menu 337

Real-Time Reporting Tool 338

Install OpenWebStart 339

Real-Time Snapshot Config Menu 339

Create System DSN for Wallboard 341

Wallboard Software in High Availability (HA) Deployment 342

Historical Reporting Menu 343

Database Server Configuration 344

SMTP Configuration 344

Purge Schedule Configuration Option 345

Purge Now Option 345

File Restore Option 345

User Management Menu 346

User View Submenu 346

Name Grammar Generator Configuration 347

Spoken Name Upload Submenu 348

Administrator Capability View Menu 348

Supervisor Capability View 348

Manage Supervisors 349

View Supervisor Details 350

Reporting Capability View Menu 351

Assign Prompts 352

Agent Capability View Menu 353

Password Management 353

CHAPTER 20 **Help Menu 357**

Contents and Index 357

For This Page Menu 358
Unified CCX Documentation Link 358
About Menu 358

CHAPTER 21 Cisco Finesse 359
Introduction 359
Cisco Finesse Administration Console 359
Getting Started 359
Administration Tools 360
Certificate Management 363
Manage System Settings 369
Desktop Chat Server Settings 369
Cloud Connect Server Settings 371
Keyboard Shortcuts 371
Manage Call Variables Layouts 372
Call Variables Layouts 372
Call Variables 373
Configure Call Variables Layouts 374
Add ECC Variables to Call Variables Layout 375
Assign Call Variables Layouts 376
Manipulate Call Variables Layouts with a Workflow 376
Manage Desktop Layout 376
Gadgets and Components 376
Finesse Desktop Layout XML 377
Default Layout XML 378
Update Default Desktop Layout 380
Drag-and-Drop and Resize Gadget or Component 388
Customize Desktop Properties 389
Horizontal Header 391
Customize Title and Logo in the Header 391
alternateHosts Configuration 392
Headless Gadget Configuration 392
Customize Icons in Left Navigation Bar 392
XML Schema Definition 407

Add Webchat and Email to Finesse 411
Enable Advanced Supervisor Capabilities in Finesse 418
Add Team Message in Custom Desktop Layout 421
Add Desktop Chat in Custom Desktop Layout 422
Live Data Gadgets 423
Configure Live Data Reports with Multiple Views 428
Manage Phone Books 429
Phone Books and Contacts 430
Add Phone Book 430
Edit Phone Book 431
Delete Phone Book 431
Import Contacts 431
Export Contacts 432
Add Contact 433
Edit Contact 433
Delete Contact 433
Manage Reasons 434
Not Ready Reason Codes 434
Sign Out Reason Codes 436
Predefined System Reason Codes 439
Manage Reason Code Conflicts During Upgrade 441
Wrap-Up Reasons 441
Manage Team Resources 444
Team Resources 444
Assign Phone Books and Reasons to Team 445
Unassign Phone Books and Reasons from Team 446
Assign Custom Desktop Layout to Team 446
Assign Workflows to Team 449
Unassign Workflows from Team 449
Manage Workflows 449
Workflows and Workflow Actions 449
Add Browser Pop Workflow Action 453
Add HTTP Request Workflow Action 454
Edit Workflow Action 455

Delete Workflow Action 456
Add Workflow 456
Edit Workflow 457
Delete Workflow 457
Manage Connected Agents 457
Connected Agents 457
Manage Security 458
HTTPS Support 459
HSTS 459
Cross-Origin Resource Sharing (CORS) 459
Gadget Source Allowed List 459
Security Enhancements 459
Manage Finesse IP Phone Agent 460
Finesse IP Phone Agent 460
One Button Sign In 460
Finesse IP Phone Service Subscription Options 461
Set Up Application User, Web Access, and HTTPS Server Parameters 462
Configure Finesse IP Phone Service in Unified CM 463
Finesse IP Phone Agent Certificate Management 464
Add Service Parameters for One Button Sign In 467
Subscribe Agent Phones to Manual Subscription Service 468
Set Up Agent Access to the Self Care Portal 469
Cisco Finesse Failover Mechanisms 470
CTI Failover 470
Finesse Desktop Failover 471
Desktop Behavior 472
Finesse IP Phone Agent Failover 474
Guidelines for Optimal Desktop Failover 475
Failover Planning 477
Backup and Restore 478
Additional Language Support 479
Cisco Finesse Agent and Supervisor Desktop 479

CHAPTER 22 **CUIC Cluster Configuration** 481

Cluster Configuration for JVM Using Hazelcast 481
Troubleshooting Cluster Configuration 483

CHAPTER 23 **Extend and Connect** 485
Overview of Extend and Connect 485
Server Configuration 485
Persistent Connection 487
Server Configuration 488
Persistant Connection 490

CHAPTER 24 **VPN-less Access to Finesse Desktop** 493
Prerequisites 494
VPN-less Finesse configurations 494
Populate Network Translation Data 494
Host the Mapping File 496
Add Proxy IP by Using CLI 496
Configure Reverse-Proxy Host Verification 497
Configure Proxy Mapping by Using CLI 498
Configure CORS and Frame-Ancestors 499
Import of Reverse-Proxy Certificates 500
Configure SSO 500
Serviceability 501
Monitor Connected Agents and Supervisors 501
API Modifications to Support Reverse-Proxy Deployments 502
Finesse SystemInfo API 502
Reverse-Proxy selection and configurations 502
Reverse proxy selection criteria 502
Configure Reverse-Proxy 503
Determine Scale and Hardware for Proxy 504
Hardware Recommendations 504
Determine Gadget Compatibility 504
Host Header Configuration 507
Finesse URL 508
Historical and Real Time Gadgets 508

Security Guidelines 509
Caveats 509

CHAPTER 25 **Cisco Unified CCX Serviceability 511**
Cisco Unified CCX Serviceability 511
Access Cisco Unified CCX Serviceability 511
Alarms 512
Alarm Configuration 512
Configure Alarm Settings 512
Alarm Configuration Settings 513
Traces 514
Component Trace Files 515
Configure Trace Parameters 515
Trace Level Options 518
Trace file location 523
Trace File Information 523
Log Profiles Management 523
Create Profile 525
Save as Another Profile 525
Enable Profile 526
Delete Profile 526
Save Current Trace Settings 527
Upload Profile 527
Update Profile 528
Serviceability Tools 528
Access Control Center — Network Services Menu 528
Network Services 529
System Services 529
Admin Services 530
DB Services 530
Finesse Services 530
Manage Network Services 530
Command Line Interface 531
Unified CCX Datastore 531

Network Outage 532
Datastore Replication Status 532
Reset Replication Between Nodes 533
Datastores 534
Update Parameters 535
Configure Performance Monitoring of Unified CCX Servers 536

CHAPTER 26 **Real-Time Monitoring** 539
Installation and Configuration 539
Performance Monitoring 539
Performance Objects 539
Performance Counters 540
Performance Objects and Counters for Unified CCX 540
Critical Services 540
Tools 541
Alerts 541
Unified CCX Alerts 541
Cisco Identity Service Alerts 545
Syslog and Alert 546
Syslog Support for Critical Cisco Finesse Log Messages 547
Traces and Logs 549
Cloud Connect Serviceability 549
CUCM Telephony Data Monitoring 549
Triggers Page 550
Call Control Groups page 550
CTI Ports Page 551
Summary Page 551
Cisco Unified Analysis Manager 552
Unified Analysis Manager for Unified CCX 552

CHAPTER 27 **Backup and Restore** 553
Important Considerations 553
SFTP Requirements 554
Master and Local Agents 554

Primary Agent Duties 554
Local Agent Duties 555
Backup Tasks 555
Manage Backup Devices 555
Manage Backup Schedules 556
Perform Manual Backup 556
Check Backup Status 557
Restore Scenarios 557
Restore SA or HA Setup (Without Rebuild) 558
Restore SA Setup (with Rebuild) 559
Restore Only First Node in HA Setup (with Rebuild) 560
Restore Second Node in HA Setup (with Rebuild) 561
Restore Both Nodes in HA Setup (with Rebuild) 562
Trace Files 563
Command Line Interface 563
Alarms 564

APPENDIX A **Command Line Interface** 565
Command Line Interface Basics 565
Start CLI Session 565
Get Help with Commands 566
Exit Command with Ctrl-C Key Sequence 567
End CLI Session 567
Additional CLI Commands 567
Show Commands 568
show uccx version 568
show uccx jtapi_client version 569
show uccx components 569
show uccx subcomponents 570
show uccx license 570
show uccx trace levels 571
show uccx provider ip axl 572
show uccx provider ip jtapi 573
show uccx provider ip rmcm 573

show uccx trace file size 573
show uccx trace file count 574
show uccx livedata connections 574
show tls server cert_type 575
show tls server min-version 575
show tls client min-version 576
show uccx tech dbserver all 576
show uccx tech dbserver log diagnostic 577
show uccx tech dbserver status 577
show uccx dbcontents 578
show uccx dbtable schema 578
show uccx dbschema 579
show uccx dbtable list 579
show uccx dbserver disk 580
show uccx dbserver sessions all 581
show uccx dbserver session 582
show uccx dbserver sessions list 584
show uccx dbserver user list 584
show uccx dbserver user waiting 585
show uccx tech dbserver log message 586
show uccx dbtable contents 587
show vmtools version 587
show uccx asr sessions 588
show uccx tts sessions 588
show webapp session timeout 589
show cli session timeout 589
Set Commands 590
set uccx trace defaults 590
set uccx trace file size component size 590
set uccx trace file count component no-of-files 591
set uccx trace enable 591
set uccx trace disable 592
set password user security 593
set tls server cert_type 593

set tls server min-version 595
set tls client min-version 595
set uccx provider ip axl 596
set uccx provider ip jtapi 596
set uccx provider ip rmcm 597
set uccx appadmin administrator 598
set authmode 598
set uccx asr count clear 599
set uccx tts count clear 599
set webapp session maxlimit 600
set webapp session timeout 601
run Commands 602
run uccx hrdataexport 602
run uccx sql database_name sql_query 603
run uccx sp database_name sp_name 604
Utils Commands 605
utils remote_account 605
utils reset_application_ui_administrator_name 605
utils reset_application_ui_administrator_password 606
utils service 606
utils system upgrade 609
utils system switch-version 609
utils uccx database dbserver integrity 610
utils uccx list license 611
utils uccx delete license licenseName 611
utils uccx jtapi_client update 612
utils uccx prepend custom_classpath 613
utils uccx switch-version db-check 613
utils uccx switch-version db-recover 614
utils uccx syncusers 614
utils uccx synctocuic 615
utils uccx icd clid status 615
utils uccx icd clid enable 616
utils uccx icd clid disable 616

utils uccx icd clid header 617
utils uccx icd clid prefix 617
utils uccx security_filter enable 617
utils uccx security_filter disable 618
utils uccx security_filter status 618
utils uccx dbreplication dump configfiles 619
utils uccx database healthcheck 619
utils uccx database dbperf start 620
utils uccx database dbperf stop 620
utils ids sync-security-config 621
utils uccx healthcheck 621
utils cloudconnect start 626
utils cloudconnect stop 626
utils fips 627
utils fips enable 627
utils fips status 628
utils fips disable 629
Enhanced Security Mode 630
File Commands 630
file uccx view 630
file uccx list custom_file 631
file uccx list prompt_file 632
file uccx get 633
file uccx tail 633
file uccx dump 634
file uccx delete 635
High Availability Commands 635
show uccx dbreplication tables 635
show uccx dbreplication servers 636
utils uccx modify remote_IPAddress 637
utils uccx modify remote_hostname 638
utils uccx database forcedatasync 638
utils uccx setuppubrestore 639
utils uccx dbreplication setup 639

utils uccx dbreplication status 640
utils uccx dbreplication templatestatus 641
utils uccx dbreplication repair 641
utils uccx dbreplication start 642
utils uccx dbreplication stop 642
utils uccx dbreplication reset 643
utils uccx dbreplication teardown 643
Cisco Finesse Commands 644
utils reset_3rdpartygadget_password 644
Finesse Log Configuration 644
Toaster Notifications 648
Finesse IPPA Inactivity Timeout 649
Supported Content Security Policy Directives 649
Finesse System Commands 651
Desktop Properties 651
WebProxy Service 657
Service Properties 661
Cross-Origin Resource Sharing (CORS) 663
Gadget Source Allowed List 665
Log Collection Schedule 667
View Property 668
Update Property 668
ConnectedUsersInfo 669
Cisco Unified Intelligence Center Commands 669
show cuic component-status 669
show cuic properties 670
show cuic tech 671
set cuic properties 672
unset cuic properties 673
set cuic syslog 674
utils cuic purge 674
utils cuic user make-admin [user-name] 675
utils cuic cluster show 676
utils cuic cluster mode 676

utils cuic cluster refresh 676
utils cuic cors 676
utils cuic logging 678
utils cuic logging config set 679
utils cuic logging config show 679
utils cuic logging config clear 679
utils cuic logging list 679
utils cuic logging reset 680
utils cuic logging update 680
utils cuic session list 680
utils cuic session delete 681
Specific License Reservation Commands 681
license smart reservation enable 681
license smart reservation request 682
license smart reservation install 682
license smart reservation return 684
license smart reservation return-authorization 685
license smart hostname enable 686
license smart hostname disable 686
license smart reservation cancel 687
license smart reservation disable 687

APPENDIX B **Unified CCX License Packages** 689
Application Availability by License Package 689
Trigger Availability by License Package 689
Subsystem Availability by License Package 689
Unified CCX Services Availability by License Package 690
Unified CCX Component Availability by License Package 690

APPENDIX C **Bubble Chat Experience** 693
Bubble Chat Experience 693

APPENDIX D **Reverse-Proxy Configuration** 695
Introduction 695

Prerequisites 695
Components Used 696
Background Information 696
Validating unauthenticated static resources 697
Brute Force Attack Prevention 697
Caching CORS Headers 698
Reverse-Proxy Configuration 698
Install OpenResty as a Reverse-Proxy in DMZ 698
Install OpenResty 699
Configure OpenResty Nginx 699
Configure OpenResty Nginx Cache 700
Use Self-Signed Certificates—Test Deployments 701
Use CA-Signed Certificate—Production Deployments 702
Create Custom Diffie-Hellman Parameter 703
Enable OCSP Stapling 703
Modify the Common OpenResty Nginx Configuration 704
Configure Reverse Proxy Port 705
Configure mutual TLS authentication between reverse-proxy and components 706
Clear Cache 707
Standard Guidelines 707
Configure the Mapping File 707
Use reverse-proxy as the Mapping File server 707
CentOS 7 Kernel Hardening 708
IPtables Hardening 710
Restrict Client Connections 713
Block Client Connections 713
SELinux 714
Verifying Reverse-Proxy Configuration 717
Finesse 717
Unified CCX and Customer Collaboration Platform 718
Cisco Identity Service 718
Brute Force Attack Prevention Configuration 718
Attack Detection Parameters 718
Logging 719

Install and Configure Fail2ban 719

Troubleshoot 721

Troubleshoot SELinux 721

Preface

- Change History, on page xxxi
- About This Guide, on page xxxi
- Audience, on page xxxii
- Conventions, on page xxxii
- Related Documents, on page xxxiii
- Documentation and Support, on page xxxiv
- Documentation Feedback, on page xxxiv

Change History

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

Change	See	Date
Initial Release of Document for Release 12.5(1) SU3		**May 2023**
Added new CLI commands "license smart hostname enable" and "license smart hostname disable"	Command Line Interface chapter	

About This Guide

Cisco Unified Contact Center Express (Unified CCX), a member of the Cisco Unified Communications family of products, manages customer voice contact centers for departments, branches, or small to medium-size companies planning to deploy an entry-level or mid-market contact center solution.

The *Cisco Unified CCX Administration Guide* provides instructions for using the Administration web interface to provision the subsystems of the Unified CCX package and to configure Unified CCX applications.

This guide shows you how to implement the following two systems that integrate with the Unified CCX:

- Cisco Unified Contact Center Express (Unified CCX)
- Cisco Unified IP IVR

This guide also includes a reference section that describes all the menus and menu options of the Unified CCXAdministration web interface.

This guide will help you to:

- Perform initial configuration tasks
- Administer applications such as the Unified CCXEngine and other components of the CiscoUnified Communications family of products
- Familiarize yourself with the menus and menu options of the Unified CCXAdministration web interface

Audience

The *Cisco Unified CCX Administration Guide* is written for business analysts and application designers who have the domain-specific knowledge required to create multimedia and telephony customer response applications. Experience or training with Java is not required but is useful for making best use of the capabilities of the Cisco Unified Communications family of products.

Conventions

This manual uses the following conventions.

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example: • Choose **Edit** > **Find** • Click **Finish**.
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • For emphasis. Example: *Do not* use the numerical naming convention. • An argument for which you must supply values. Example: IF (*condition*, *true-value*, *false-value*) • A book title. Example: See the *Cisco Unified Contact Center Express Installation Guide*.

Convention	Description

`window` font	Window font, such as Courier, is used for the following:
	• Text as it appears in code or information that the system displays. Example:
	`<html><title> Cisco Systems,Inc. </title></html>`
	• File names. Example: `tserver.properties`.
	• Directory paths. Example:
	`C:\Program Files\Adobe`

string	Nonquoted sets of characters (strings) appear in regular font. Do not use quotation marks around a string or the string will include the quotation marks.
[ ]	Optional elements appear in square brackets.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
< >	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.
^	The key labeled Control is represented in screen displays by the symbol ^. For example, the screen instruction to hold down the Control key while you press the D key appears as ^D.

Related Documents

Document or Resource	Link
Cisco Unified Contact Center Express Documentation Guide	https://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_documentation_roadmaps_list.html
Cisco Unified CCX documentation	https://www.cisco.com/en/US/products/sw/custcosw/ps1846/tsd_products_support_series_home.html

Document or Resource	Link
Cisco Unified Intelligence Center documentation	https://www.cisco.com/en/US/products/ps9755/tsd_products_support_series_home.html
Cisco Finesse documentation	https://www.cisco.com/en/US/products/ps11324/tsd_products_support_series_home.html
Cisco Customer Collaboration Platform documentation **Note** From Unified CCX Release 12.5(1), CCP documents are available in the Cisco Unified CCX documentation folder.	https://www.cisco.com/en/US/products/sw/custcosw/ps1846/tsd_products_support_series_home.html
Cisco Unified CCX Virtualization Information	https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-contact-center-express.html
Cisco Unified CCX Compatibility Information	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html

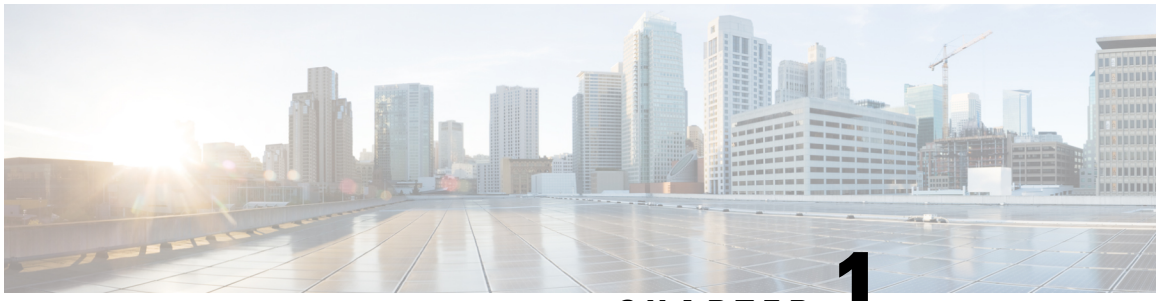
Documentation and Support

To download documentation, submit a service request, and find additional information, see *What's New in Cisco Product Documentation* at https://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Documentation Feedback

To provide your feedback for this document, send an email to:

contactcenterproducts_docfeedback@cisco.com



CHAPTER 1

Unified CCX Introduction

- Unified CCX Components, on page 1
- Unified CCX Product Family, on page 2
- Unified CCX Cluster Architecture, on page 4
- Unified CCX Engine, on page 6
- Set Up Unified CCX, on page 7
- Manage Unified CCX, on page 13

Unified CCX Components

This section describes the following components of the Unified CCX system:

- Unified Gateway—Connects the Cisco Unified Communications family of products to the Public Switched Telephone Network (PSTN) and to other private telephone systems such as PBX.
- Unified CM Server—The Cisco Unified Communications Manager (Unified CM) provides the features required to implement IP phones, manage gateways, provide failover and redundancy service for the telephony system, and direct Voice over IP (VoIP) traffic to the Unified CCX system.

Note Cisco Unified Communications Manager was previously known as Unified Call Manager. This guide uses Cisco Unified Communications Manager at the first occurrence and Unified CM for later occurrences.

- Unified CCX Server—Contains the Unified CCXEngine that runs applications, including Cisco script applications, Busy applications, Ring No Answer applications, and Voice Extensible Markup Language (VXML) 2.0 applications.

  You can position your Unified CCX application server anywhere on the IP network and administer your applications from a web browser on any computer on the IP network. Because Unified CCX uses an open architecture that supports industry standards, you can integrate your applications with a wide variety of technologies and products, such as Enterprise databases. The Unified CCX Server has the following components:

  - Unified CCX Configuration Datastore (CDS)—Manages configuration, component, and application information within the Unified CCX cluster and communicates with Unified CM.

- Historical Reports Database Server—Dedicated server that stores Unified CCX database for the following datastores: Configuration Datastore (CDS), Historical Datastore (HDS), and Repository Datastore (RDS).
- Cisco Customer Collaboration Platform—Acts as the endpoint that hosts the widgets that end users and agents use during chat and email sessions. Customer Collaboration Platform accepts chat request, communicates with Unified CCX to allocate an agent for the chat and then establishes the chat session between agent and end user.

  Customer Collaboration Platform fetches email messages from the email server, communicates with Unified CCX to allocate an agent, and provides the email management user interface components via the Finesse desktop.

- Unified CCXEditor—Allows application developers to use a simple Graphical User Interface (GUI) to create, modify, and debug Unified CCX scripts for automating customer interactions. Each script consists of a series of steps, implemented as Java Beans.
- Unified CCX Administration and Unified CCX Serviceability web interfaces—Provides access through a web browser for administrators to configure and manage Unified CCX datastores, servers, and applications.
- Cisco Finesse Agent and Supervisor Desktops—Desktop programs that allow Unified CCX agents and supervisors to log in to the system, change agent states, and monitor status.
- Media Resource Control Protocol (MRCP) Automatic Speech Recognition (ASR) server—(optional) Dedicated server that performs real-time speech recognition.
- MRCP Text-to-Speech (TTS) server—(optional) Dedicated server that converts text into speech and plays it back to the caller.

Note Support for high availability and remote servers is available only in multiple-server deployments.

- Cisco Unified Intelligence Center—A web-based reporting solution for historical reports that provides detailed Call Contact Call Detail Records (CCDRs), application performance, and traffic analysis information.

Unified CCX Product Family

The Unified CCX product family provides contact-processing functions for your Cisco Unified Communications solution.

The software package that you choose determines which steps, components, and subsystems you receive. Each Unified CCX product includes Unified CCXEngine and Unified CCXEditor.

Unified IP IVR

The Unified IP IVR is a multimedia (voice, data, web) IP-enabled interactive voice response solution that offers an open and feature-rich foundation for the creation and delivery of Unified IP IVR applications through Internet technology.

Unified IP IVR automates call handling by autonomously interacting with contacts. Using Unified IP IVR, you can create applications that answer calls, provide menu choices for callers, obtain caller data such as passwords or account identification, and transfer calls to caller-selected extensions. You can also create Unified IP IVR applications that respond to HTTP requests, perform outbound calling, send e-mail, and process VXML 2.0 commands.

The Unified IP IVR package provides the following features:

- Java Database Connectivity (JDBC) support—Unified IP IVR applications can access Oracle, Sybase, and IBM DB2 databases.
- Real-time reporting client—Unified IP IVR applications can generate a variety of reports that provide detailed information about the real-time status of your system.
- Cisco Unified Intelligence Center—A web-based reporting solution for historical reports that provides detailed Call Contact Call Detail Records (CCDRs), application performance, and traffic analysis information.
- Automatic Speech Recognition (ASR)—Unified IP IVR applications can take advantage of ASR to provide callers with the option to use speech to navigate through menu options.
- Text-to-Speech (TTS)—Unified IP IVR applications can use TTS to read back documents and prescripted prompts to callers.

Unified Contact Center Express

Cisco Unified Contact Center Express (Unified CCX) is an IP-based Automated Call Distribution (ACD) system that queues and distributes incoming calls to Unified CCX agents, who can be groups of Unified CM users for Unified CM integration.

You can use Unified CCX applications to route calls to specific agents. You can also integrate Unified CCX with Unified IP IVR to gather caller data and classify incoming calls.

Unified CCX includes a web-based real-time and historical reporting system that you can use to monitor system, Contact Service Queue (CSQ), and resource performance.

The Unified CCX system consists of the following major components:

- Resource Manager—Application program that monitors Unified CCX agent phones and allows you to organize agents into resource groups or skills-based partitions according to the types of calls each group can handle.
- CSQ—Application program that places incoming calls in a queue and distributes them to the appropriate set of agents as the agents become available.

The following licensing options are available for the Unified CCX system:

- Unified CCX Premium—Adds full Unified IP IVR support (except for Unified ICM integration) including database integration, Voice eXtensible Markup Language (VoiceXML), HTML web integration, custom Java extensions, and e-Notification services. The outbound feature is now bundled with the Premium

package. You will receive one outbound seat free with each premium seat. The maximum number of outbound seats supported will be based on the hardware type.

- Unified CCX Outbound—You need to have a Unified CCX Outbound license in addition to a Unified CCX Premium license to enable the IVR and agent outbound feature. You can increase the number of ports and agents for an existing Outbound license. For all the IVR and agent based outbound campaigns that are running currently in your Unified CCX, the Display License submenu option displays these IVR ports and agent seats:
  - The licensed IVR ports for outbound.
  - The licensed agent seats for outbound.
  - The sum of the dedicated IVR ports configured for IVR-based outbound campaigns.
  - The agent seats that currently in use for agent-based outbound campaigns.

Note The dedicated outbound IVR ports for a campaign is the number of IVR ports that you want to reserve for a campaign from the total number of CTI ports available in the outbound call control group.

Note The Unified CCX Enhanced package and the Unified CCX Premium package are provisioned in the same way.

Unified CCX Cluster Architecture

Note Support for high availability and remote servers is available only in multiple-server deployments.

The Unified CCX cluster consists of one or more servers (nodes) that are running Unified CCX components in your Unified CCX deployment.

If you deploy Unified CCX components on a single server, the Unified CCX cluster (often referred to as *cluster* in this manual) consists of that server. If you deploy Unified CCX on multiple servers, the cluster includes the Unified CCX server and standby server on which you installed Unified CCX. The Unified CCX cluster can support up to two Unified CCX Servers, one designated as the *active Unified CCX Server* and the other designated as the *standby Unified CCX Server* for high availability purposes.

When you install or upgrade Unified CCX on a server, you designate the cluster to which the server will belong by designating the cluster profile for that cluster.

Cluster architecture accommodates high availability and failover because if a component fails, a secondary server will take over the functionality lost by that failed component.

All Unified CCX servers within the cluster are configured identically and installed with the same features. One server is designated the *active server*.

Unified CCX Active Server

Note Support for high availability and remote servers is available only in multiple-server deployments.

The Unified CCX active server makes global decisions for the cluster and keeps track of calls in the CSQs, agent states (if Unified CCX is installed) and generating historical detail records.

Note Only one server in the cluster can be the active server at any given time.

If the active server fails, the Unified CCX provides automatic failover to the standby server. If the active server fails (for example, in the event a hardware failure occurs or the Unified CCX Engine process terminates), some calls being handled by the server are lost. The lost calls are restricted to those being handled by the system (those in the IVR stage or in queue). Calls answered by agents continue to remain live even though related data on the agent desktop is lost. When the standby server takes over as the new active server, call processing continues.

A Unified CCX cluster consists of the one or more servers (nodes) that run Unified CCX components in your Unified CCX deployment.

Cluster management consists of two main elements:

Cluster Manager

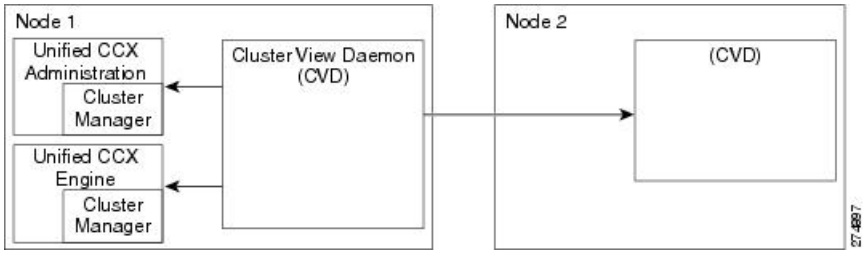
Receives updates about cluster status and subsystem states.

Cluster View Daemon (CVD)

Java code that interacts with Platform Service Manager and implements internode communication on behalf of the cluster. It detects availability of the other nodes, components and services, provides consistent cluster view, and dynamically elects a master service.

Figure 1: Components of the CVD Interaction with Nodes

The following figure shows the components of the CVD interaction with nodes.



The CVD has two interfaces:

- One that monitors *inside* the node, using:
  - Node Manager to monitor and control local processes
  - Cluster Manager publisher or subscriber to communicate with local applications, such as Engine and Application Administration

- One that monitors *outside* the node and communicates with other nodes in the cluster

Unified CCX Engine

The Unified CCXEngine enables you to run multiple applications to handle Unified CM Telephony calls or HTTP requests.

The Unified CCXEngine uses the Unified CM Telephony subsystem to request and receive services from the Computer Telephony Interface (CTI) manager that controls Unified CM clusters. The Unified CCXEngine is implemented as a service that supports multiple applications.

You can use a web browser to administer the Unified CCXEngine and your Unified CCX applications from any computer on the network. Unified CCX provides you the following two web interfaces:

- Unified CCX Administration web interface— Used to configure system parameters, subsystems, view real-time reports that include total system activity and application statistics, and so on
- Unified CCXServiceability web interface— Used to view alarm and trace definitions for Unified CCX services, start and stop the Unified CCX Engine, monitor Unified CCX Engine activity, and so on

Note Ensure that the popup blocker is disabled on your browser.

Depending on the Unified CCX products that you are using, the Unified CCX server may employ as many as 14 subsystems for communicating with other services:

Applications
Manages the applications in the Unified CCXEngine and other features such as session management.

Cisco Media
Configures CiscoMediaTermination (CMT) dialog control groups, which can be used to handle simple Dual Tone Multifrequency (DTMF)-based dialog interactions with customers.

Core Reporting
Provides information for Unified IP IVR real-time reports.

Database
Handles the connections between the Unified CCX server and the enterprise database.

eMail
Adds components to the Unified CCX Engine that allows the engine to send email messages.

HTTP
Adds components to the Unified CCX Engine that allow the engine to respond to HTTP requests.

ICM Subsystem
Manages the connection between the Unified CCX server and ICM.

Unified CM Telephony
Manages the connection between Unified CM CTI Manager and the Unified CCXEngine.

MRCP ASR
Allows a script to respond to voice input in addition to DTMF using the MRCP protocol.

MRCP TTS
Composes voice prompts that are generated real-time from text, such as speaking the words in the text of an email message using the MRCP protocol.

Resource Manager-Contact Manager (RmCm)
Allows Unified CCX to monitor agent phones, control agent states, route and queue calls, and manage the historical reporting feature.

NonVoice Subsystem

Allows Unified CCX to configure and manage Chat and Email.

Voice Browser
Manages Voice Browser functionality.

Set Up Unified CCX

After you install the Unified CCX system and perform the initial setup as described in *Cisco Unified Contact Center Express Installation Guide*, you can start provisioning and configuring the system:

- *Provisioning* is the process of allocating resources and devising strategies for using the resources to support the needs of your business.
- *Configuring* is the process of making applications available to the Unified CCX system.

Provision Telephony and Media Subsystems

The Unified CCX telephony and media subsystems manage telephony and media resources and communicate with supporting telephony and media systems.

Depending on the Unified CCX applications you plan to use, you need to provision some or all of the following subsystems:

- **Unified CM Telephony—**The Unified CM Telephony subsystem controls the Unified CM Telephony resources for the Unified CCX system.

Caution While Unified CM supports Unicode characters in first and last names, those characters become corrupted in Unified CCX Administration web pages for Real-Time Reporting.

- **Cisco Media—**The Cisco Media subsystem controls the CMT media resources for the Unified CCX system.
- **MRCP ASR—**The MRCP ASR subsystem controls the ASR media resources for the Unified CCX system.
- **MRCP TTS—**The MRCP TTS subsystem controls the TTS media resources for the Unified CCX system.

Configure Unified CCX Subsystems

You need to provision your Unified CCX subsystems to enable the Unified CCX Engine to run multiple applications to handle Unified Communications calls or HTTP requests.

Note You need to configure a particular subsystem only if you are using Unified CCX applications that require it and which are installed and activated using the appropriate license.

To continue the Unified CCX system configuration process, connect to the Unified CCX Administration web interface and perform the task in the links listed in the Related Topics section.

Provision Unified CCX Subsystem

If you have purchased any of the three versions of Unified CCX, you must provision the Unified CCX subsystem.

Provision the following settings on the Unified CCX subsystem:

- **RmCm Provider**

  The Resource Manager (RM) of the Unified CCX system uses a Unified CM user (called a Unified CM Telephony provider) for monitoring agent phones, controlling agent states, and routing and queueing calls.

- **Resources**

  Agents that answer calls are also called *resources*. After you create a resource group, you must assign agents (resources) to that group.

- **Resource Groups**

  Collections of agents that your CSQ uses to handle incoming calls. To use resource group-based CSQs, you must specify a resource group.

- **Skills**

  Customer-definable labels that are assigned to agents. You can route incoming calls to agents who have the necessary skills or set of skills to handle the call.

- **CSQs**

  After you assign an agent to a resource group or assign skills to an agent, you need to configure the agent for the CSQ to which the agent will be assigned.

- **Agent-Based Routing Settings**

  You can configure Automatic Work and Wrapup Time settings for the agent-based routing feature from the Agent-Based Routing Settings page.

- **Teams**

  If you want to create or associate teams with various agents, CSQs, and supervisors, you need to configure team settings.

Provision Additional Unified CCX Subsystems

The additional Unified CCX subsystems provide HTTP, Database, and email features.

Provision the following subsystems:

- **HTTP—**The HTTP subsystem enables Unified CCX applications to respond to requests from a variety of web clients.
- **Database—**The Database subsystem enables Unified CCX applications to communicate with enterprise database servers.
- **eMail—**The eMail subsystem enables Unified CCX applications to create and send email.

View License Information

The initial license configuration is part of the Setup Wizard procedure (during installation). The uploaded licenses define the feature set for a Unified CCX system. See *Cisco Unified Contact Center Express Install and Upgrade Guide* for more information on obtaining and installing licenses for Cisco Unified CCX.

You can add additional licenses using the **Add Licenses** submenu option.

Note

- If two licenses with the same feature name are uploaded, the Unified CCXAdministration Display Licenses web page will display the earlier date as the expiry date. Although the expiry date refers to the earlier date, it does not mean that the license expires on the date displayed in the "Display Licenses" page if you upload a permanent license.
- If a permanent license is uploaded over an already existing temporary license, a license expiry message is displayed for the temporary license for the feature. This license expiry message is displayed both in License Information and Appadmin home page. The Appadmin home page displays a popup message.

For Unified CCX, if you have a premium license with an outbound license, the Unified CCXAdministration Display Licenses web page displays:

- The number of licensed IVR ports and dedicated IVR ports for IVR outbound.
- The number of licensed agent seats and In Use agent seats for progressive and predictive agent outbound.

Note The number of In Use IVR ports and In Use agent seats are displayed only for the master node.

Caution Deleting or reducing the number of IVR ports for outbound in the license is not a supported scenario in Unified CCX. Doing this might lead to inaccurate data in Dedicated Licensed Ports, which in turn might lead to more abandoned calls.

To view license details, perform the following procedure:

Procedure

Choose **System** > **License Information** > **Display License(s)** from the Unified CCXAdministration menu bar.

The License Information web page opens, displaying the details of the configured licenses, including the expiry date in the case of time-bound licenses.

Upload Licenses

Software for all of the Unified CCX feature components are loaded on the system during installation. However, no feature is available for use unless a license for that feature is added and activated.

You can upload and display licenses using the License Information page. To upload a license, complete the following steps.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **System** > **License Information** > **Add License(s)**.

The License Information web page opens.

Step 2 Specify a License file or click **Browse** to locate a file.

You can either specify a single file with a .lic extension or a .zip file containing multiple .lic files.

Note
While you are upgrading from a previous release, if there are multiple licenses, zip all the .lic files into a single .zip file and then upload the zip file. If specifying a .zip file, ensure that all .lic files that need to be added are in the root of the .zip file and are not in subfolders in the .zip file.

Step 3 Click **Upload**.

On successful upload of the license, you will see the following confirmation message in the status bar at the top of this web page : `License has been uploaded successfully`

If you upload an Add-on license to increase the existing licensed Outbound IVR ports, the following message will be displayed :

`As the number of licensed Outbound IVR Ports have increased, please increase the number of ports in the Outbound Call Control Group to utilize all the licensed ports.`

Enable Smart Licensing

License Type

Use this page to select and enable the appropriate **Smart License Type**. Select one of the following license types:

- **Flex**
- **Perpetual Enhanced**
- **Perpetual Premium**

If you select **Perpetual Enhanced** or **Perpetual Premium**, you have to select the **Named Licenses** and enter the **No. of Seats** for each of the selected named license.

Click Enable, a confirmation message is displayed.

Click Yes to enable the Smart license.

On the Unified CCX menu bar, choose **System** and click **License Information**. Select **Smart License** and click **Next**.

Before the **Smart License** page, the **License Selection** window appears.

Note The **License Selection** appears only once when you configure Smart License for the first time for your deployment.

The **License Selection** window displays the following types of licenses:

- Flex license
- Perpetual license

Select the appropriate license type as applicable.

Smart License

Smart License page displays the following:

- **Transport Settings** button—Click this button to configure the transport to Cisco Smart Software Manager (CSSM).

  For more information about transport settings configuration, see Configure Transport Settings for Smart Licensing, on page 12.

- **Register** button—Click this button to **Register** the licenses.

  For more information about registration, see Register with Cisco Smart Software Manager, on page 276.

- The **Smart Software Licensing Status** section which displays the following details:
  - The license **Registration Status**.
  - The **License Authorization Status**, such as `Evaluation mode`,
- The **Smart License Usage** drop-down menu—Select the license type for which you want to see the license usage details.

The **Smart License Usage** table displays the license usage details for the specific license type you select in the drop-down box.

The following details of the license usage displayed in the table are as follows:

- License (Version/Type)—The type or version of the license.
- Count—The number of concurrent licenses in use.
- Status—The status of the licenses such as `Evaluation`.
- Description—Describes the function of the license, for example, *Enables base features*.

Configure Transport Settings for Smart Licensing

Configure the connection mode between Unified CCX and Cisco SSM.

Procedure

Step 1 From Unified CCX Administration, navigate to **System** > **License Management**.

Step 2 Click **Transport Settings** to set the connection method.

Step 3 Select the connection method to Cisco SSM:

- **Direct**—Unified CCX connects directly to Cisco SSM on cisco.com. This is the default option.
- **Transport Gateway**—Unified CCX connects to Cisco SSM On-Prem for smart licensing. Enter the Cisco SSM On-Prem URL.
- **HTTP/HTTPS Proxy**—Unified CCX connects to a proxy server, which connects to Cisco SSM. Enter the Fully Qualified Domain Name (FQDN) of the proxy server along with the port.

  Note
  Proxy servers that require authentication are not supported for this connection method.

Step 4 Click **Save** to save the settings.

Available Applications

There are several types of applications you can configure for Unified CCX:

- Script applications perform such functions as receiving calls, playing back prompts, receiving caller input, transferring calls, and queueing calls.
- The Busy application simulates a busy signal.
- The Ring-No-Answer application simulates a ringtone.

After adding a Unified CCX application, you need to define a *trigger* so that this application can respond to telephone calls and HTTP requests. Triggers are specified signals that invoke application scripts in response to incoming contacts.

Manage Scripts Prompts, Grammars, and Documents

The process of configuring Ciscoscript applications includes uploading Unified CCX scripts and prerecorded prompts, installing grammars and customized languages, and adding triggers to applications.

Depending on your particular Unified CCX implementation, you may need to perform most or all of the following tasks to configure a Ciscoscript application:

- Manage scripts—Ciscoscript applications are based on scripts that you must upload to the repository and make available to the Unified CCX system.

- Manage prompts—Many applications make use of prerecorded prompts, stored as .wav files, which are played back to callers to provide information and elicit caller response. You must upload these .wav files to the repository and make them available to the Unified CCX system.
- Install grammars—A *grammar* is a specific set of all possible spoken phrases and Dual Tone Multi-Frequency (DTMF) digits to be recognized by Unified CCX applications and acted upon during run time. The Unified CCX system uses specific grammars when recognizing and responding to caller responses to prompts. You must store these grammars in a directory to make them available to the Unified CCX system.
- Install customized Unified CCX languages—Language packs, such as American English and Canadian French, are installed with Unified CCX.

Configure Unified CCX Historical Reporting

When you install the Unified CCX system, the installation process creates a database named db_cra. This database contains:

- Information for historical reports, including Unified CCX configuration information, stored procedures, and some call statistics
- The ContactCallDetail table, which is the main table for call statistics

To conclude the Unified CCX system configuration process, connect to the Unified CCX Administration web interface and perform the following Historical Reporting Configuration tasks:

Procedure

Step 1 Define the maximum number of database connections for report client sessions.

Step 2 Assign historical reporting capability to users.

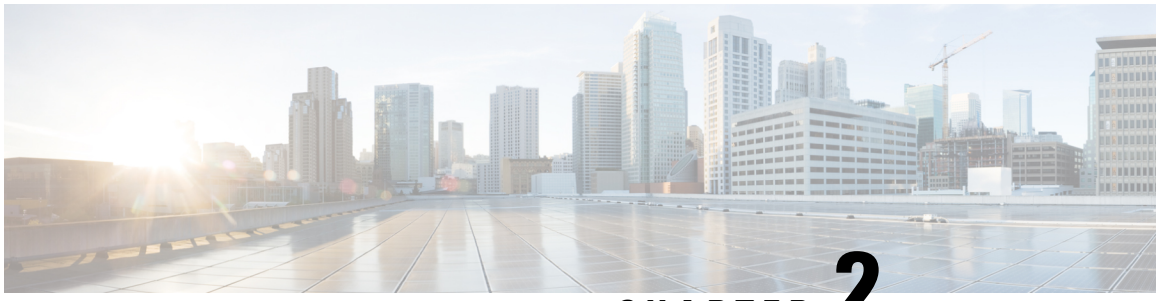
Step 3 Configure the Daily Purge Schedule and specify notification parameters.

Manage Unified CCX

To manage your Unified CCX, you must first provision and configure it. The day-to-day administration of the Unified CCX system and datastores consist of many tasks, such as:

- Starting and stopping the Unified CCX Engine and processes.
- Managing and monitoring the status of Unified CCX servers and components across the cluster.

Note Support for high availability and remote servers is available only in multiple-server deployments.



CHAPTER 2

Unified CCX AdministrationWeb Interface

- Access Unified CCX Administration Web Interface, on page 15
- Cisco Unified CCX Administration Menu Bar and Menus, on page 16
- Cisco Unified CCX Administration Navigation, on page 17
- Unified CCX Configuration Web Pages, on page 19

Access Unified CCX Administration Web Interface

The web pages of the Unified CCX Administration web interface allow you to configure and manage the Unified CCX system and its subsystems.

Use the following procedure to browse into the server and log in to Unified CCX Administration web interface.

Procedure

Step 1 Open the Unified CCX Administration Authentication page from a web browser on any computer on your network and enter the following case-sensitive URL:

```
https://<servername>/appadmin
```

In this example, replace <*servername*> with the hostname or IP address of the required Unified CCX server.

A Security Alert dialog box is displayed.

Step 2 Click the appropriate button.

The Authentication page appears.

Note

- Ensure that Cisco Tomcat and Cisco Unified Cluster View Daemon services are running before you log in to the Unified CCX Administration using the URL in Step 1.
- Ensure that the popup blocker is disabled on your browser.
- If a custom logon message is set up in Cisco Unified OS Administration, the message appears in a pop-up window. You must acknowledge the message to log in. For more information about setting up custom logon message, see the *Set Up Customized Logon Message* section in *Cisco Unified Operating System Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR*.

Step 3 On the main Cisco Unified CCX Administration web page, enter your Unified CCX username and password.

Note
If you are accessing Unified CCX for the first time, enter the Application User credentials that are specified during installation of the Unified CCX. See the *Cisco Unified Contact Center Express Install and Upgrade Guide* for further instructions.

User IDs are case-sensitive when logging into the Unified CCX Administration web interface. To make them case-insensitive, you must install 12.5(1) SU1 ES02.

Step 4 Click **Login**.

A web page opens listing information about Cisco Unified CCX Administration and the Cisco Unified CCX Administration menu bar appears at the top of the page.

Note
- Unified CCX Administration detects web-based cross-site request forgery attacks and rejects malicious client requests. It displays the error message, "The attempted action is not allowed because it violates security policies."
- Avoid using multiple sessions of the Unified CCX Administration at the same time.
- To log in again to the Cisco Unified CCX Administration after you clicked **Logout** click the link, **Click here to log in again**.
- For a complete logout from all applications, sign out of the respective applications and close the browser window. In a Windows desktop, you may achieve this by logging out of the Windows account. In a Mac desktop, you may quit the browser application.
- Single Sign-On enabled agents have the risk of others misusing their account. If the browser is not closed completely the **Click here to log in again** link does not require the agent to enter credentials to log in to the application.
- The Unified CCX Administration interface and the Unified CCX User Options (appuser) web interface should not be logged in to the same window on different tabs.
- To configure session-timeout, use the **set webapp session timeout** command. You can specify the session-timeout between 5 and 35000 minutes. For example, if you have configured session-timeout for 5 minutes, the user is logged out after a session is inactive for 5 minutes. The configuration is updated only on the node where the command is run. Ensure to run this command on both the nodes. You must reboot the node for the configuration to take effect.

Supported Languages

Unified CCX Administration supports only English.

Cisco Unified CCX Administration Menu Bar and Menus

The Cisco Unified CCX Administration menu bar appears at the top of every web page of the Unified CCX Administration web interface. You begin every Unified CCX configuration and administration task by choosing a menu and submenu option from the menu bar.

The Cisco Unified CCX Administration menu bar contains the following menu options:

- **System**—Contains options for configuring new servers in the cluster, Unified CM information, language information, changing system parameters, custom file configuration, standalone CUIC configuration, adding or displaying licenses, and single sign-on.
- **Applications**—Contains options for managing applications, scripts, prompts, grammars, documents, and AAR files.
- **Subsystems**—Contains options for configuring parameters for the subsystems that are licensed for your Unified CCX server. Your Subsystems menu may include submenu options for one or more of the following subsystems: Unified CM Telephony, Unified CCX, Database, HTTP, Chat and Email, CiscoMedia, MRCP Automatic Speech Recognition (ASR), and MRCP Text-To-Speech (TTS).
- **Wizards**—Contains options that provide access to the following wizards of your Unified CCX server: Application and RmCm.
- **Tools**—Contains options that allow you to access system tools such as Plug-ins, Real-Time Reporting, Real-Time Snapshot Config. You can also assign access levels to administrators and supervisors and reset passwords.
- **Help**—Provides access to online help for Unified CCX.

Cisco Unified CCX Administration Navigation

After you log in, the main Cisco Unified CCX Administration web page appears.

Note The minimum supported screen resolution specifies 1024 x 768. Devices with lower screen resolutions may not display the applications correctly.

The choices in the drop-down list include the following Cisco Unified CCX Administration applications:

- **Cisco Unified CCX Administration** — Uses Cisco Unified CCX Administration to configure system parameters, subsystems, wizards, and much more.
- **Cisco Unified CCX Serviceability** — Takes you to the main Cisco Unified CCX Serviceability web page that is used to configure trace files, alarms, and to activate and deactivate services.
- **Cisco Finesse Administration** — Uses Cisco Finesse Administration to configure system settings in Cisco Finesse.
- **Cisco Unified Serviceability** — Takes you to the main Cisco Unified Serviceability web page that is used to save alarms and traces for troubleshooting, provide alarm message definitions, activate and deactivate services and so on.
- **Cisco Unified OS Administration** — Takes you to the main Cisco Unified OS Administration web page, so that you can configure and administer the Cisco Unified Communications platform.
- **Disaster Recovery System** — Takes you to the Cisco Disaster Recovery System, a program that provides data backup and restore capabilities for all servers in a Cisco Unified CCX Administration cluster.
- **Cisco Identity Service Management**- Takes you to the Identity Service Management page where the Identity Service configurations can be done.

You can log in to Cisco Unified CCX Administration either as an administration user or an application user.

Note An administration user is an end user that is configured on the Unified CM with Administrator capability in Unified CCX.

An application user is an user that is configured during the installation of Unified CCX having administrator capability by default.

If you log in as an Administrator, you can access the following applications that display in the navigation drop-down list in the top right corner of the Administration menu bar:

- Cisco Unified CCX Administration
- Cisco Unified CCX Serviceability
- Cisco Finesse Administrator
- Cisco Identity Service Management

If you log in as an application user, you can seamlessly traverse between the Unified CCX web applications as well as the Cisco Identity Service Management and Cisco Unified Serviceability without logging in again.

Note For security purposes, Cisco Unified CCX Administration and Cisco Unified CCX Serviceability logs you out after a configured session timeout for an inactive session and you must log back in. This session timeout can be configured using the platform based command line interface command **set webapp session timeout**. For more information on this command, see *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Note An application user can log in to these four Unified CCX web applications even when Unified CM is down.

To access these applications from Cisco Unified CCX Administration, you must first choose the desired application from the navigation drop-down list in the upper right corner and click **Go**.

Note Cisco Finesse Administration Console opens in a new tab or in a new window based on the browser settings.

To log in to Cisco Finesse Administration, you must be a user with administrator privileges.

When the Cisco Tomcat service is down on any of the Unified CCX nodes, you will not be able to launch Cisco Unified CCX Administration from any of the Unified CCX nodes; therefore, you will not be able to launch the Cisco Finesse Administration from within it.

In that case, you can launch the Cisco Finesse Administration directly from the browser.

To launch the Finesse Administration Console, direct your browser to *https://hostname or IP address:8445/cfadmin*, where *hostname* or *IP address* is the hostname or IP address of the server.

You can access the following platform-based web applications using the platform user credentials as configured during installation of Unified CCX:

- Cisco Unified Operating System Administration
- Disaster Recovery System

Unified CCX Configuration Web Pages

When you choose any menu and submenu option from the Unified CCXAdministration menu bar, a configuration or administration web page opens. Use this web page to continue your configuration or administration task.

In some cases, you will perform your configuration or administration task on this one web page.

In other cases, the web page that first opens when you choose a submenu item leads to a series of web pages. For example, the Unified CM Telephony Call Control Group Configuration web page contains both a tool bar in the top with a few icons that link to other web pages and a configuration area.

The following table describes the **Refresh All** button and the **Copy**, **Delete**, and **Refresh** icons that are found on several Unified CCX web pages.

Icon/Button	Description
Copy	Click this icon to copy the information in that specific row. **Note** When you click **Copy**, the web page displays the copied configuration so you can make changes, if d
Delete	Click this icon to delete the information in that specific row.
Refresh	Click this icon to refresh the information in that specific row.
Refresh All	Click this button to refresh the information listed on this page.

Details for Advanced Configuration

In Unified CCX Administration web interface, advanced configuration with **Show More** and **Show Less** options exists. On the applicable pages, all configuration details can be displayed or minimised based on user preferences and requirements.

A page by default displays fewer parameters. Parameters configured with default values and not requiring modification or user input are now available in the advanced configuration section. You can access this advanced configuration section by clicking the **Show More** button at the bottom of the page. When you click this button, the extra parameters become visible and the button changes to **Show Less**. When you click **Show Less**, the page reverts to its original list of parameters.

Note If you are using Unified CCX with Cisco Contact Center Gateway solution, see the *Cisco IPCC Gateway Deployment Guide for Cisco Unified ICME/CCE/CCX*. The instructions for configuring Unified CCX with that solution differs from what is described in this guide. The Unified Gateway provides for the integration of the Unified ICME system with Unified CCX by way of Unified Gateway. For more information, see the *Cisco Unified Contact Center Enterprise Install and Upgrade* guides available at https://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_installation_guides_list.html . The Unified Gateway is a Peripheral Gateway (PG), which you configure on the Unified ICME software.

Toolbar and Buttons

On the top left toolbar of many web pages, you will find an **Add New** icon and the same **Add New** will also be displayed as a button at the bottom of the web page.

For example, the Unified CM Telephony Call Control Group Configuration web page contains **Add New** and **Refresh All** icons on the top left toolbar and the same are displayed as buttons at the bottom of the web page. When you click the **Add New** icon or button, another Unified CM Telephony Call Control Group Configuration web page opens. Use this area to add a new Unified CM Telephony Call Control Group.

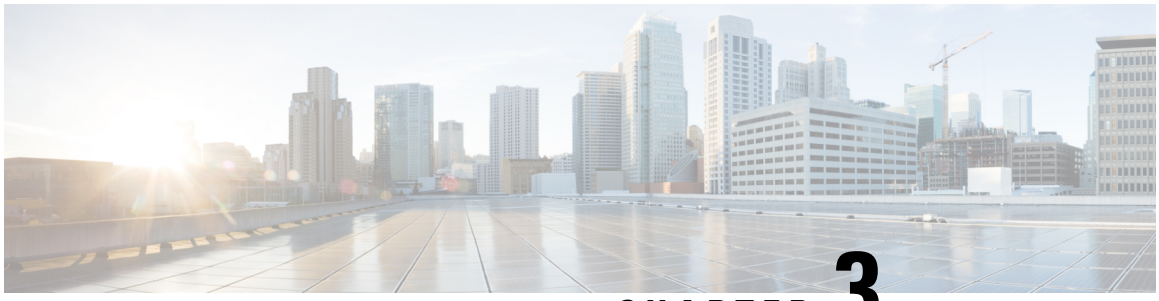
Many web pages contain icons or buttons that perform a variety of functions. For example, the **Refresh All** button on the Unified CM Telephony Call Control Group Configuration web page refreshes all the Unified CM Telephony call control group configurations in the Unified CCX server.

A few web pages (for example, **Subsystems** > **Database** > **Parameters** page) also contain a **Reset to Default** icon and button. This allows you to revert to the software set defaults for each parameter on this page.

Application and RmCm Wizards

In Unified CCX, two wizards are available in the main menu: the Application Wizard and the RmCm Wizard.

To improve the usability and configuration process, these wizards take you through the configuration pages in the required order and help ease the configuration process for these two features. You can access these wizards from a new main menu option called **Wizards**.



CHAPTER 3

Unified CCX Provision Checklist

- Unified CCX, on page 21
- Provision Unified CCX, on page 22
- Change Licensing Packages, on page 23

Unified CCX

The Unified CCX system uses the Unified CCX subsystem as part of an ACD system to provide resource distribution and queueing to call centers.

Two types of routing are available:

- **Contact Service Queue (CSQ)-based routing—**CSQs are entities that route calls to your resources (agents). Each CSQ controls incoming calls and determines where an incoming call is placed in the queue and to which agent the call is sent.

  Each CSQ selects resources from an associated resource pool that you define or from resource skills for all Unified CCX license packages. When an agent becomes available to take a call, the system chooses a queued call from one of the CSQs whose resource pool includes the agent, and routes that call to that agent.

- **Agent-based routing—**Agent-based routing provides the ability to send a call to a *specific* agent, rather than any agent available in a CSQ.

A Unified CCX agent can participate in both CSQ-based and agent-based routing. A Unified CCX agent can be any one of the following:

- Cisco Finesse
- IP Phone Agent
- Extension Mobility (EM) Agent
- Supervisor (if the supervisor is taking calls)

Note A supervisor who is not taking calls is not considered to be an agent.

Calls are queued in the Unified CCX server and sent to agents by the Unified CCX server.

The machine you install your Unified CCX system on determines how many agents and IVR ports Unified CCX can accommodate. However, be aware of the following general configuration rules:

- Each agent cannot be associated with more than:
  - 25 CSQs (This is a configuration design guideline; Unified CCX Administration does not enforce the rule.)
  - 50 skills (Unified CCX Administration enforces this rule.)
- Each CSQ cannot be associated with more than 50 skills. (Unified CCX Administration enforces this rule.)
- A call should not queue for more than 25 CSQs. (This is a configuration design guideline; Unified CCX Administration does not enforce the rule.)

Provision Unified CCX

To provision Unified CCX, complete the following tasks:

Step	Task	Unified CM
Step 1	Configure Unified CM users who will be agents in your Unified CCX system.	Provision Unified CM for Unified CCX, on page 25
Step 2	Provision resources information for Unified CCX telephony and media.	Provision Unified CM Telephony Subsystem, on page 61
Step 3	Provision RmCm Provider to allow RmCm Subsystem to be in service.	RmCm Provider Configuration, on page 89
Step 4	Create resource groups.	Resource Groups, on page 91
Step 5	Create skills.	Skills Configuration, on page 92
Step 6	Assign agents to resource groups and assign skills to agents.	Agent Configuration, on page 95
Step 7	Create Contact Service Queues.	Contact Service Queue Configuration, on page 99
Step 9	Provision agent-based routing—if using Unified CCX Enhanced or Premium.	Configure Agent-Based Routing, on page 107
Step 10	Create teams and assign agents to teams.	Teams Configuration, on page 108

Change Licensing Packages

Now, the Unified CCX system can be upgraded from Enhanced to Premium.

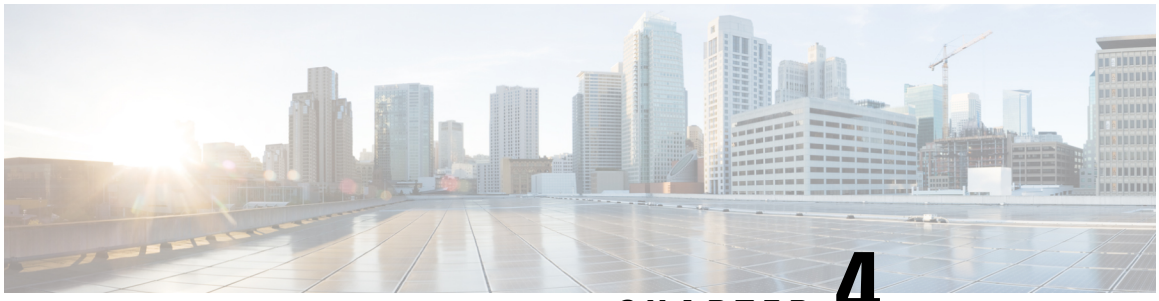
While upgrading the licenses, you need to configure the following system parameters:

- **Enhanced to Premium—**You need to configure the Number of Direct Preview Outbound Seats while upgrading to a Premium license.

Note Downgrade of license is not supported in Unified CCX.

Procedure

Choose **System** > **System Parameters** from the Cisco Unified CCX Administration menu bar to open the System Parameters Configuration web page where you can update these values.



CHAPTER 4

Provision Unified CM for Unified CCX

When you access Unified CCX Administration for the first time in a cluster, the system automatically initiates the cluster setup procedure once for each cluster to perform the following tasks:

- Identify Unified CCX license files
- Enter information about Unified CM Administrative XML Layer (AXL) and Unified CM Telephony and RmCm providers

You can modify the Unified CM information from Unified CCX. See the *Cisco Unified Contact Center Express Install and Upgrade Guide* for detailed information on how to perform the initial system setup using the Unified CCX Administration web interface.

The following topics explain how to modify the Unified CM information from Unified CCX:

- Configure Unified Communications Manager Information, on page 25
- Unified Communications Manager for Unified CCX Configuration, on page 30

Configure Unified Communications Manager Information

During initial setup of Unified CCX using the Unified CCX Administration web interface, the administrator who installed the Unified CCX should have already provided the Unified Communications Manager IP address and hostname(s). Upload the Cisco Unified Communications Manager Tomcat certificate from Cisco Unified Communications Manager (CUCM) into the Unified CCX Tomcat trust store using the Cisco Unified OS Administration interface. The administrator must also provide the Administrative XML Layer (AXL) authentication (user ID and password) information.

The Unified Communications Manager Configuration web page allows you to configure and update the AXL authentication information, Unified Communications Manager Telephony subsystem information, and RmCm Provider configuration information from within Unified CCX.

This page has three blocks of information: AXL service details, Unified Communications Manager Telephony Provider details, and RmCm Provider details.

If the same user ID (Application User in CUCM) is used as CUCM admin and is also configured as AXL user in Unified CCX, the user ID may get locked if wrong password is used multiple times to login to CUCM. If the user ID gets locked, you will not be able send AXL requests such as, Create Call Control groups, Triggers, and so on from Unified CCX to CUCM. The best practice is to create AXL specific admin credentials.

Note Before regenerating CUCM certificates, disable **SRTP** in **System Parameters Configuration** page of Unified CCX Administration.

For any modification related to CUCM certificates, see *Administration Guide for Cisco Unified Communications Manager*. After completing all the modifications related to CUCM certificates, enable **SRTP** in Unified CCX Administration.

Modify AXL Information

To change previously configured AXL information, complete the following steps.

Note If you want to change the credentials, change first in Unified Communications Manager and then in Unified CCX. Otherwise, Unified CCX might have issues communicating with Unified Communications Manager.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **System** > **Cisco Unified CM Configuration**.

The Cisco Unified Communications Manager Configuration web page opens.

Step 2 Go to the **AXL Service Provider Configuration** section to modify the AXL information using the following fields:

Field	Description
AXL Service Provider Configuration	
Selected AXL Service Providers	Lists the AXL service providers that are configured. You can have a maximum of two AXL service providers in the list. Select one or both the AXL service providers and click the right arrow to remove them from the selected list. The removed AXL Service Providers are moved to the available list for future use. Arrange the order of the selected entries using the up and down arrows.
Available AXL Service Providers	Lists the AXL service providers that are available in the Unified CM cluster. Select one or two AXL service providers and click the Left arrow to add them to the selected list. **Note** Make sure you configure multiple AXL providers running the AXL Service for a redundant system.
Cluster Wide Parameters	
User Name	The Unified Communications Manager User ID. This information is provided during cluster setup in the Unified CCX installation process. When you select an AXL Service Provider, the corresponding username is automatically displayed in this field. This is a mandatory field.

Field	Description
Password	Password for the Unified Communications Manager User ID. This information is provided during cluster setup in the Unified CCX installation process. When you select an AXL Service Provider, the corresponding user password is automatically displayed in this field. This is a mandatory field.

Step 3 After logging in to the Unified CCX Administration web interface, follow these steps to update the AXL password:

a) Log in to Unified Communications Manager Administration web interface and update the password for the application user (AXL provider).

b) Navigate back to **System** > **Cisco Unified CM Configuration** web page of Unified CCX and enter the new password in the Password field.

A dialog box prompts you to confirm the AXL username and password. Reenter the AXL user ID and password and click **Login**.

The system validates the data and takes you back to the Unified Communications Manager configuration page.

c) Enter the updated password once again to validate and click **Update**.

The AXL password is updated successfully and you should be able to log in to Unified CCX Administration web interface of Unified CCX with the new AXL password.

Step 4 Click **Update** at the top of the Cisco Unified Communications Manager Configuration web page or the **Update** button that displays at the bottom of the web page to save the changes. The Unified Communications Manager Configuration web page refreshes to display the new settings.

The selected AXL services are now enabled. If the selected AXL services cannot be enabled, an error message instructs you to reselect AXL service providers.

Modify Unified Communications Manager Telephony Information

Note The Unified Communications Manager Telephony client is installed in the background after you configure the Unified Communications Manager Telephony user. The Unified Communications Manager Telephony client runs in the background and verifies that the right version and the right client are installed.

Configuring the Unified Communications Manager Telephony user does not automatically install the Unified Communications Manager Telephony client. This is normally done during activation of Unified CCX Engine in component activation (see *Cisco Unified Contact Center Express Serviceability Administration Guide*). To install it manually, go to **Subsystems** > **Unified CM Telephony** and select the **Cisco JTAPI Resync** submenu option from the Unified CCX Administration menu bar.

The updated list of CTI Managers within a cluster are listed in this section. If for any reason the Unified Communications Manager is not functioning or if the Unified CCX cannot connect to the Unified Communications Manager, information that is obtained from the most recent connection is saved as part of the bootstrap information.

To change previously configured Unified Communications Manager Telephony information, complete the following steps.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **System** > **Unified CM Configuration**.

The Cisco Unified Communications Manager Configuration web page opens.

Step 2 Scroll down to the **Unified CM Telephony Subsystem - Unified CM Telephony Provider Configuration** section and reconfigure the Unified Communications Manager Telephony information using the following fields.

Field	Description
Unified CM Telephony Subsystem—Unified CM Telephony Provider Configuration	
Selected CTI Managers	Lists the CTI Managers that are configured. You can have a maximum of two CTI Managers in the list. Select one or both the CTI Managers and click the right arrow to remove them from the selected list. The removed CTI Managers are moved to the available list for future use. Arrange the order of the selected entries using the up and down arrows. **Note** SRTP settings remain unchanged, even if the **Selected CTI Managers** are changed.
Available CTI Managers	Lists the CTI Managers that are available in the Unified CM cluster. Select one or two CTI Managers and click the Left arrow to add them to the selected list.
Cluster Wide Parameters	
User Prefix	The syntax of the User ID is: <*userprefix*>_<*nodeid*> For example, if you set this field to **cti_user**, the User ID for Node 1 will be **cti_user_1**. This is a mandatory field.
Password	Password that you defined for the User ID in Unified Communications Manager. If a CTI Manager is already selected, the corresponding password is displayed in this field. This is a mandatory field.
Confirm Password	Reenter the password that you provided in the Password field. This is a mandatory field.

Step 3 Click **Update** at the top of the Cisco Unified Communications Manager Configuration web page or click the **Update** button that displays at the bottom of the web page to save the changes.

The Unified Communications Manager Configuration web page refreshes to display the new settings.

The newly selected CTI Manager is now enabled. If the selected CTI Manager cannot be enabled, an error message instructs you to reselect CTI Managers.

Note

In a HA over WAN deployment of Unified CCX, the JTAPI user will be created only for the selected node. To create JTAPI user for the HA node, you have to explicitly select the HA node, make necessary updates, and click **Update**.

Modify RmCm Provider Information

The list of all CTI Managers available in a cluster are saved as part of the bootstrap information. You can select any available CTI Managers listed in the Available CTI Managers list box in this page.

Note The RmCm Provider specified through the Unified CCX Administration is automatically created in Unified Communications Manager. You do not need to use the Unified Communications Manager web interface to create the user.

To change previously configured RmCm provider information or to configure a new RmCm Provider, complete the following steps.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **System** > **Unified CM Configuration**.

The Unified Communications Manager Configuration web page opens.

Step 2 Scroll down to **RmCm Subsystem - RmCm Provider Configuration** and reconfigure the selected CTI Manager using the following fields:

Field	Description
RmCm Subsystems—RmCm Provider Configuration	
Selected CTI Managers	Lists the CTI Managers that are configured. You can have a maximum of two CTI Managers in the list. Select one or both the CTI Managers and click the right arrow to remove them from the selected list. The removed CTI Managers are moved to the available list for future use. Arrange the order of the selected entries using the up and down arrows.
Available CTI Managers	Lists the CTI Managers that are available in the Unified CM cluster. Select one or two CTI Managers and click the Left arrow to add them to the selected list.
User ID	User prefix for the Unified Communications Manager User IDs to be created in Unified Communications Manager. **Note** The RmCm User Id must neither be a standard user created on Cisco Unified CM by default nor be a part of Standard CM Super Users group. If a CTI Manager is already selected, the corresponding user name is displayed in this field. If you change the CTI Managers, be sure to enter the corresponding user prefix for the selected service. This is a mandatory field.

Field	Description
Password	Password you defined for the User ID in Unified Communications Manager. If a CTI Manager is already selected, the corresponding password is displayed in this field. If you change the CTI Manager, be sure to enter the corresponding password for the selected service. This is a mandatory field.
Confirm Password	Reenter the password that you provided in the Password field. This is a mandatory field.

Step 3 Click **Update** at the top of the Cisco Unified Communications Manager Configuration web page or click the **Update** button that displays at the bottom of the web page to save the changes.

The Unified Communications Manager Configuration web page refreshes to display the new settings.

The newly selected RmCm Provider is now enabled. If the selected RmCm Provider cannot be enabled, an error message instructs you to reselect RmCm Provider.

Unified Communications Manager for Unified CCX Configuration

To enable Unified CCX to communicate with Unified Communications Manager, you also need to assign extensions for the users who will be agents in your Unified CCX system.

Note If you delete a Unified CCX user with Administrative rights from Unified Communications Manager, you can still log in to the Unified CCX Administration web interface as an application user.

Note Q Signaling (QSIG) and Path Replacement (PR) features of Unified Communications Manager are not supported by Unified CCX.

Invoke Unified Communications Manager Administration

Begin the process of configuring Unified Communications Manager by connecting to the Unified Communications Manager Administration web interface.

To connect to the Unified Communications Manager Administration web interface, complete the following steps.

Procedure

Step 1 From a web browser on any computer on your network, enter the following URL: **https://***servername***/ccmadmin**.

In this example, *servername* is the hostname or IP address of your Unified Communications Manager server.

A Security Alert dialog box is displayed.

Step 2 Click the appropriate button.

Step 3 At the main Cisco Unified Communications Manager Administration web page, enter the Unified Communications Manager username and password, and then click **Login**.

The Unified Communications Manager Administration web page appears.

You are now ready to use the Unified Communications Manager Administration web interface to configure users for Unified CCX.

Unified Communications Manager Users as Unified CCX Agents

Warning Do not configure Unified Communications Manager users having the same username/password as the application administration credentials (configured during installation). Doing so may restrict the Unified Communications Manager when shared across multiple Unified CCX servers.

Note When there is a change in the configuration data on the Unified Communications Manager, the team configuration is lost on the Unified CCX. You must reconfigure the teams in the Unified CCX or restore data from DRS.

Agent ID

When logging in to the desktop, agents use the Unified Communications Manager user ID and password. Unified Communications Manager limits agent IDs to 128 alphanumeric characters, but Unified CCX limits the agent IDs to 31 alphanumeric characters. For more information about Agent ID configuration, see the Agent Configuration, on page 95 section.

Agent Name

Agent name includes the first name and last name. The following is the limit for agent name in Unified CCX:

- English-based script (German, Spanish, English, and so on)—50 characters
- Non-English script (Arabic, Chinese, Cyrillic, and so on)—16 characters

Attention If the agent name exceeds the limit, Unified CCX truncates the name to 50 or 16 characters respectively and stores.

RmCm uses the Unified Communications Manager database to determine which devices it can control and provides an interface method for getting the Media Access Control (MAC) address of the calling party.

After you install RmCm, you get access to the Unified Communications Manager database. The database stores parameters that initialize Unified Communications Manager Telephony, user profiles, application logic, network-specific configuration information, and Directory Number Associations such as Primary Extension and Unified CCX Extension.

The Primary Extension field represents the primary directory number for the end user. End users can have multiple lines on their phones. From the drop-down list box, choose a primary extension when associating devices for this end user.

Unified CCX Extension allows you to define Unified Communications Manager users as Unified CCX agents in Unified Communications Manager.

To assign Unified CCX devices to end users and application users in the Unified Communications Manager, these users must first exist in Unified Communications Manager. If these users do not exist, you must first add the users. See the *Cisco Unified Communications Manager Administration Guide* to obtain detailed information about the Unified CCX web interface and configuration procedures. After adding the end user and the application user, be sure to modify their Unified CCX settings.

Agents and Supervisors with IDs That Match Reserved Words Cannot Sign In

Do not use the following reserved words for agent ID or supervisor ID because these IDs conflict with system account names that are used internally within the Unified CCX server:

System\Components	Reserved words
Unified CCX Web Chat	admin
Cisco Finesse	admin
	finesse
	FIPPA
	xmpprootowner
	presencelistener

Note

- If a user tries to sign in with a reserved word for the agent ID or supervisor ID, the sign-in fails.
- Do not use the reserved words for IDs whether they are upper case, lower-case, or any combination of both cases. For example, admin, ADMIN, or Admin.

Guidelines for Agent Phone Configuration

Follow these guidelines when configuring agent phones for Unified CCX agents:

- Choose **Device** > **Phone** in Unified Communications Manager Administration. The Find and List Phones window is displayed.

  Enter search criteria to locate a specific phone and click **Find**. A list of phones that match the search criteria is displayed. Click the device name of the phone to which you want to add a directory number. The Phone Configuration window is displayed.

  In the Unified Communications Manager Administration Phone Configuration web page, select the required Association Information (on the left) to get to the Directory Number Configuration web page. On this page, make the following changes:

- In the Multiple Call/Call Waiting Settings section, set the Maximum Number of Calls to 2 (default is 4) for Cisco Unified IP Phones 7900 Series and 3 for Cisco Unified IP Phones 8961, 9951, and 9971.

Note If you are using Cisco Finesse for your agent desktop, you must set the Maximum Number of Calls to 2 for all agent phones.

- In the Multiple Call/Call Waiting Settings section, set the Busy Trigger value to 1 (default is 2).
- In the Call Forward and Call Pickup Settings section, verify that you do not forward any Unified Communications Manager device to the Unified CCX extension of an agent.
- In the Call Forward and Call Pickup Settings section, verify that you do not configure the Unified CCX extension of an agent to forward to a Unified CCX route point.

- Secure Real-Time Transport Protocol (SRTP) based recording is now supported. You can disable Secure Real-Time Transport Protocol (SRTP) when configuring a Cisco Unified Communications product. You can disable SRTP for a specified device or for the entire Unified Communications Manager:
  - For a specified device—Choose **Device** > **Phone**. In the Find and List Phone page, select the required phone device. In the Phone Configuration page for the selected phone, scroll down to the Protocol Specific Information section. To turn off SRTP on the phone device, select any one of the **Non Secure SCCP Profile auth by** choices from the drop-down list in **SCCP Phone Security Profile** or **SCCP Device Security Profile** field.
  - For the entire Unified Communications Manager cluster—Choose **System** > **Enterprise Parameters**. In the Enterprise Parameters Configuration page, scroll down to the Securities Parameters section, to verify that the corresponding value for the Cluster Security Mode field is 0. This parameter indicates the security mode of the cluster. A value of 0 indicates that phones will register in nonsecure mode (no security).

- The Unified CCX extension for the agent must be listed within the top 4 extensions on the device profile. Listing the extension from position 5 on will cause Unified CCX to fail to monitor the device, so the agent will not be able to log in.
- Do not forward any Unified Communications Manager device to the Unified CCX extension of an agent.
- Do not configure the Unified CCX extension of an agent to forward to a Unified CCX route point.
- Do not use characters other than the numerals 0 to 9 in the Unified CCX extension of an agent.
- Do not configure two lines on an agent phone with the same extension when both lines exist in different partitions.
- Do not assign a Unified CCX extension to multiple devices.
- Do not configure the same Unified CCX extension in more than one device or device profile. (Configuring a Unified CCX extension in one device or device profile is supported.)
- To use Cisco Unified IP Phones 9900 Series, 8900 Series, and 6900 Series as agent devices, the RmCm application user in Unified Communications Manager needs to have “Allow device with connected transfer/conference” option assigned to itself.

To determine a list of Unified CCX agent devices supported by Cisco Finesse Desktop, see the Unified CCX Compatibility related information, located at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

Modify Existing Unified Communications Manager Users

To use any version of Unified Communications Manager, you must first ensure that you define Unified Communications Manager users as Unified CCX agents in Unified Communications Manager. After you perform this task, these Unified CCX agents can be combined into Resource Groups, assigned Skills, and placed in CSQs.

Note In Unified CCX, this operation is called “associating a device.”

Note Be sure to assign Unified CCX devices to both end users and application users in the Unified Communications Manager web interface.

To assign devices to an end user, you must access the End User Configuration window for that user. The End User Configuration window in Unified Communications Manager Administration allows the administrator to add, search, display, and maintain information about Unified Communications Manager end users.

To assign devices to an application user, you must access the Application User Configuration window for that user. The Application User Configuration window in Unified Communications Manager Administration allows the administrator to add, search, display, and maintain information about Unified Communications Manager application users.

Note If Enterprise Mobility (EM) is used together with both Cisco Unified Communications Manager release 8.0 or later and Cisco Unified Communications Manager, the Resource Manager application user must be associated with the device profile and not with the device.

To modify the Unified CCX Extension settings for existing Unified Communications Manager users who are Unified CCX agents, complete the following steps:

Note If you change or update an end user ID in Unified Communications Manager, Unified CCX resets the end user's resource name, skills, and team to default values.

Procedure

Step 1 Connect to the Unified Communications Manager Administration web interface.

The Unified Communications Manager Administration web page appears.

Step 2 Choose **User Management** > **End User**.

The Find and List End Users page displays. Use the two drop-down list to search for an end user.

Tip
To find all end users that are registered in the database, click **Find** without entering any search text. A list of discovered end users is displayed. Then, skip to Step 6.

Step 3 From the first Find end user where drop-down list, choose one of the listed criteria.

Step 4 From the second Find end user where drop-down list, choose one of the listed criteria.

Step 5 Specify the appropriate search text, if applicable, and click **Find**.

A list of discovered end users is displayed.

Step 6 From the list of records, click the end user name that matches your search criteria.

The End User Configuration page opens, displaying the configuration information for the end user that you chose.

Step 7 In the Controlled Devices list box below the Device Information section, select the device and click the Down arrow below the Available Profiles list box. If the device that you want to associate with this end user is not displayed in this pane, do the following to associate devices with an end user:

a) From the Device Information pane, click **Device Association**. The User Device Association page opens.
b) Finding a Device: Because you may have several devices in your network, Cisco Unified Communications Manager lets you locate specific devices on the basis of specific criteria. Click **Find**. All or matching records are displayed. You can change the number of items that is displayed in each page by choosing a different value from the Rows per Page drop-down.
c) Associating a Device: From the Device association for (this particular end user) pane, choose the devices that you want to associate with this end user by checking the box to the left of the device names. You can also use the buttons at the bottom of the window to select and deselect devices to associate with the end user.
d) To complete the association, click **Save Selected/Changes**.
e) From Related Links drop-down list in the upper right corner of the web page, choose **Back to User**, and click **Go**.

The End User Configuration page is displayed, and the associated devices that you chose are displayed in the Controlled Devices pane.

Step 8 Select the required device and save your changes to associate that device with this end user.

After the device is associated, the Controlled Devices field displays the description information (for example, the MAC address) that the end user controls.

Step 9 In the End User Configuration page, scroll down to the **Directory Number Associations** section.

Step 10 In the **Primary Extension** field drop-down list and the **IPCC Extension** field drop-down list, choose the required agent extension for this device.

These fields represent the primary directory number for the end user. End users can have multiple lines on their phones. If you have a single line, be sure to select the same extension for both fields.

Step 11 Click **Update** to apply the changes.

The specific End User Information page for this user appears, with the message that the update was successful.

Step 12 From the Unified Communications Manager Administration menu bar, choose **User Management** > **Application User**. RmCm Providers are referred to as application users in Unified Communications Manager.

Note
When you associate one device with the Unified CCX agent (end user), you must also be sure to associate the same device with the Unified CCX RmCm Provider (application user).

The Find and List Application Users window is displayed. Use the two drop-down list to search for the application users in Unified Communications Manager.

Tip
To find all application users registered in the database, click **Find** without entering any search text. A list of discovered end users is displayed. Then, skip to Step 16.

Step 13 From the first Find application user where drop-down list, choose one of the listed criteria.

Step 14 From the second Find application user where drop-down list, choose one of the listed criteria,

Step 15 Specify the appropriate search text, if applicable, and click **Find**.

A list of discovered application users is displayed.

Step 16 From the list of records, click the application user name that matches your search criteria.

The window displays the application user that you choose.

Step 17 Repeat Step 7 and Step 8 for the selected Application User.

These steps ensure that the Unified Communications Manager application users are also defined as Unified CCX agents in Unified Communications Manager.

Step 18 Click **Update** to apply the changes.

The specific Application Information page for this user appears, with the message that the update was successful.

See the "User Management Configuration" section in the *Cisco Unified Communications Manager Administration Guide* for detailed information on how to configure an end user and application user using Unified Communications Manager.

Now that you have defined the agent in Unified Communications Manager, you can configure agents in Unified CCX. Before you configure the agent, you will also need to configure resource groups and CSQs.

Assign Unified Communications Manager Users as Cisco TelePresence Virtual Agents

The Cisco TelePresence application enables enterprises to create a live, face-to-face interaction with customers over the network. This solution allows rapid deployment of a virtual contact center infrastructure. Agents using Cisco TelePresence are referred to as virtual agents in this guide. Virtual agents connect to callers using Unified CCX, which incorporates ACD, CTI, and Unified IP IVR with Cisco Unified Communications Manager and providing the entire solution on one server.

Note For more information on the Cisco TelePresence solution, see https://www.cisco.com/en/US/products/ps7060/index.html.

The following guidelines apply for the Cisco TelePresence integration with Unified CCX:

- The only commonly supported codec for Unified CCX and Cisco TelePresence is G711.
- The following supervisor features are not supported:

- Monitoring and Recording is not supported for Cisco TelePresence integration with Unified CCX.

Follow this procedure to assign Unified Communications Manager users as virtual agents:

Procedure

Step 1 Identify the required Cisco TelePresence system that will participate as a virtual agent in the Unified CCX application.

a) Note the Unified Communications Manager extension of the Cisco TelePresence deployment.

Note
The Cisco Unified IP Phone 7970G and Cisco TelePresence system must be assigned the same extension in Unified Communications Manager, because they both share the same line.

b) Note the MAC address or the Directory Number of the Cisco Unified IP Phone 7970G connected to the identified Cisco TelePresence system.

Tip
From the Unified CCX perspective, this is another SIP endpoint.

Step 2 Associate the Cisco Unified IP Phone 7970G with the Unified Communications Manager user to configure this user as a virtual agent.

Step 3 Associate the Cisco Unified IP Phone 7970G with the RmCm provider.

Note
Do not associate the corresponding Cisco TelePresence system with the RmCm provider.

Configure Tool for Auto-Registered Phones Support (TAPS)

The Tool for Auto-Registered Phone Support (TAPS) loads a preconfigured phone setting on a phone. The TAPS works in conjunction with the Bulk Administration Tool (BAT). After the BAT is used to bulk add phones with dummy MAC addresses to Cisco Unified Communications Manager Administration, you can plug the phones into the network.

The administrator or users can then dial a TAPS directory number that causes the phone to download its configuration. At the same time, the phone gets updated in the Unified Communications Manager database with the correct MAC address of the phone. Refer to Configuring the Bulk Administration Tool (BAT) if you are not familiar with the BAT.

For the TAPS to function, you must make sure that Auto-registration is enabled in Cisco Unified Communications Manager Administration (select **System** > **Cisco Unified CM**). Follow the instructions in the procedure below to install and configure TAPS application with Unified CCX.

Procedure

Step 1 Log in to Cisco Unified Communications Manager Administration and choose **Application** > **Plugins** from the Cisco Unified Communications Manager Administration menu bar.

Step 2 In the Find and List Plugins web page, search for “Cisco TAPS” and click **Find**.

Step 3 Download the TAPS_AAR.aar file to your client PC, which is used for accessing Unified Communications Manager Administration and Unified CCX Administration.

Step 4 Install Unified CCX. See the *Cisco Unified Contact Center Express Install and Upgrade Guide*, available at https://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html.

Step 5 After installing Unified CCX, follow these steps from the User Configuration page in Unified CCX Administration:

a) In the Cisco Unified Communications Manager Users list, select the Cisco Unified Communications Manager user whom you want to designate as the Cisco Unified CCX administrator and who can configure TAPS.

b) Click the **left arrow** (<) to move the selected user to the Cisco Unified CCX Administrator list.

c) Click **Finish**. The Cisco Unified CCX Setup Result Information window is displayed. This window confirms the result of the initial setup. The Cisco Unified CCX engine will restart.

d) Close your web browser.

Step 6 Log in to Cisco Unified CCX Administration as the Unified CCX application administrator, who can configure TAPS. After installing and configuring Unified CCX and Unified Communications Manager, follow this procedure to set up TAPS:

a) From the Unified CCX Administration menu bar, choose **Applications** > **AAR Management**. Click **Browse** and upload the TAPS_AAR.aar file that you downloaded in Step 3 from Unified Communications Manager.

On successful upload, you will see a confirmation message in the status bar at the top of the AAR Management web page.

Note
For TAPS configuration, you need to restart the Unified CCX engine and Unified CCX Cluster View Daemon (CVD). You can restart the CVD using the CLI command,

utils service service name stop/start.

b) After restarting the CVD, log in once again to Cisco Unified CCX Administration as the Unified CCX application administrator. From the Unified CCX Administration menu bar, choose **Subsystems** > **Unified CM Telephony** > **Call Control Group**. Click **Add New** and provide the Call Control Group Configuration values for TAPS using the following fields:

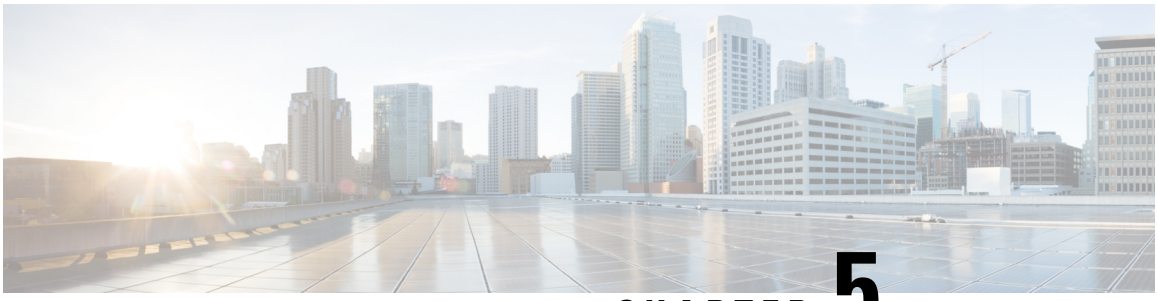
- Group ID
- Number of CTI Ports
- Media Termination Support
- Device Name Prefix
- Starting Directory Number

c) From the Unified CCX Administration menu bar, choose **Subsystems** > **Cisco Unified CM Telephony** > **Triggers**. Click **Add New** and specify values for the following mandatory fields:

- Directory Number
- Language
- Application Name
- Device Name
- Description
- Call Control Group:

The call control group types can be Inbound or Outbound for Unified CCX running with Unified Communications Manager.

d) Choose **Subsystems** > **Cisco Unified CM Telephony** > **Data Resync** from the Cisco Unified CCX Administration menu bar to check and resynchronize the JTAPI data between Cisco Unified Communications Manager and Cisco Unified CCX.
e) From the Unified CCX Administration menu bar, choose **Applications** > **Application Management**. The Application Management web page opens, displaying the details of existing applications.
f) Click the **Add New** icon or button. The Add a New Application web page opens.
g) From the Application Type drop-down menu, choose Cisco Script Application and click **Next**. The Cisco Script Application configuration web page opens.
h) In the Script field, select the script "/TAPS.aef" from the drop-down list and enter the IP address of the Cisco Unified Communications Manager in the text box below the Script drop-down list.
i) Check the check box against **Cisco_Unified_CM_IP_Address** field.
j) Click the **Yes** radio button in the Enabled field.
k) Click **Update**.
l) Log in to Cisco Unified Communications Manager Serviceability Page and restart the TAPS Service.



CHAPTER 5

Update Unified CM IP Address Change in Unified CCX

• Update Unified CM IP Address Change in Unified CCX , on page 41

Update Unified CM IP Address Change in Unified CCX

The following section details the procedure to update any change in Unified CM IP Address in Unified CCX.

Note Unified CCX supports changing one or more IP addresses of Unified CM servers but does not support changing the Unified CM cluster.

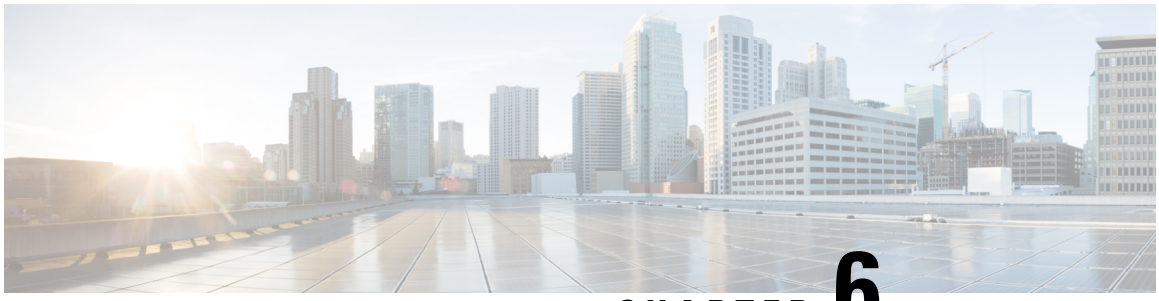
Procedure

Run the following CLI commands on the Unified CCX publisher using the new IP address of Unified CM as input.

- **set uccx provider ip axl** - Sets the Unified CCX AXL provider IP address.
- **set uccx provider ip jtapi** - Sets the Unified CCX JTAPI provider IP address.
- **set uccx provider ip rmcm** - Sets the Unified CCX Resource Manager-Contact Manager provider IP address.

Note
After you run the above CLI commands, restart the Unified CCX Engine service on the publisher node. After Unified CCX Engine service starts successfully, restart Cisco Tomcat.

Update Unified CM IP Address Change in Unified CCX



CHAPTER 6

Cisco Applications Configuration

- About Unified CCX Applications, on page 43
- Application Triggers, on page 49
- Script Management, on page 52

About Unified CCX Applications

The Unified CCX system uses applications to interact with contacts and perform a wide variety of functions.

Note Unified CCX licenses you purchase and install determine the applications available on your system.

Unified CCX provides the following application types:

- Script
- Busy
- Ring-No-Answer

Configure Script Applications

The Unified CCX *script* applications are applications based on scripts created in the Unified CCXEditor. These applications come with every Unified CCX system and running scripts created in the Unified CCX Editor.

Use the Unified CCXEditor to create scripts that direct the Unified CCX system to automatically answer calls and other types of contacts, prompt callers for information, accept caller input, queue calls, distribute calls to available agents, place outbound calls, respond to HTTP requests, and send email messages.

Note The Unified CCX system includes a number of sample scripts. For a description of these sample scripts, and for more information on creating scripts with the Unified CCX Editor, see the *Cisco Unified Contact Center Express Getting Started with Scripts*. In addition, a script repository is available at https://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_implementation_design_guides_list.html. This repository provides some examples of scripting techniques that can leverage Unified CCX abilities.

Cisco script applications can make use of many components, such as scripts, prerecorded prompts, grammars, languages, locales, and custom Java classes.

Tip Upload these components to the repository before you configure a Cisco script application that uses them.

Depending on your particular Unified CCX implementation, you may need to perform most or all of the following tasks to configure a Cisco script application:

- Manage scripts—Cisco script applications are based on scripts that you must upload to the repository and make available to the Unified CCX system.
- Manage prompts—Many applications make use of prerecorded prompts, stored as .wav files, which are played back to callers to provide information and elicit caller response. You must upload these .wav files to the repository and make them available to the Unified CCX system.
- Install grammars—The Unified CCX system uses specific grammars to recognize and respond to caller response to prompts. You must store these grammars in a directory to make them available to the Unified CCX system.

  Unified CCX support only W3C XML grammar for speech recognition with Nuance adapter. The following XML and regular expression (regex) grammars are supported:

  - Nuance extensions for XML grammar.
  - regex grammar for DTMF input.

- Install customized Unified CCX languages—Language packs, such as American English, Canadian French, and so on, are installed with Unified CCX. You install language packs in a directory accessible by the Unified CCX system.
- Install Java files—In addition to the Java files automatically installed as part of the Unified CCX installation process, you can install your own custom classes and Java Archive (JAR) files to customize the performance of your Unified CCX system.
- Add a Cisco script application—Scripts created in the Unified CCXEditor are used as the basis for Cisco script applications.
- Add an application trigger—Triggers are specified signals that invoke application scripts in response to incoming contacts. After adding a new Cisco script application, you need to add a trigger so that this application can respond to telephone calls and HTTP requests.

Add New Cisco Script Application

To add a new Cisco script application, complete the following steps:

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Applications** > **Application Management**.

The Application Management web page opens, displaying the details of any existing applications.

Step 2 Click **Add New** icon that is displayed in the tool bar in the upper left corner of the window or the **Add New** button that is displayed at the bottom of the window.

The Add a New Application web page opens.

Step 3 From the Application Type drop-down menu, choose **Cisco Script Application** and click **Next**.

The Cisco Script Application configuration Web page opens.

Step 4 Specify the following fields:

Field	Description
Name	A name for the application. This is a mandatory field.
ID	Accept the automatically-generated ID, or enter a unique ID. This is a mandatory field. **Note** The Historical Reporting feature uses this ID to identify this application.
Maximum Number Of Sessions	The maximum number of simultaneous sessions (instances) that the application can handle. This is a mandatory field.
Script	**Note** This field is available only for Cisco Script Application type. This is a mandatory field. Perform one of the following actions: • Choose a script from the drop-down list to run the application. If the script contains parameters, the parameters are displayed below the Script drop-down menu. Each parameter has a check box, which enables you to override the default value for that parameter. If you want to override the value, check the check box for that parameter. **Note** All scripts under the default directory are listed in the drop-down list of the Script field in the Cisco Script Application Configuration web page. • Click **Edit**, enter the script name in the dialog box, and click **OK**. The User Prompt dialog box closes, and the name you entered appears in the Script field. **Note** If you enter the script name as a file URL, enter the value with double backslashes (\\). For example, file://c:\\temp\\aa.aef
Description	Use the Tab key to automatically populate this field. **Note** For the Busy and Ring-No-Answer application types, this field is visible only when you click **Show More**.
Enabled	Click the required radio button to accept (**Yes** = default) or reject (**No**) **Note** For the Busy and Ring-No-Answer application types, this field is visible only when you click **Show More**.

Field	Description

Enable Cisco Webex Experience Management post-call survey	This field is not enabled by default. For the procedure to enable the Cisco Webex Experience Management post-call survey and information about the script variables required for Cisco Webex Experience Management post-call survey, see *Cisco Unified Contact Center Express Features Guide*.
	After you select the **Enable Cisco Webex Experience Management post-call survey** check box:
	• If you want to play the inline survey to the customer, then select the **IVR** option and select the survey from the drop-down list.
	• If you want to provide an offline SMS/Email survey to the customer:
	  • Select the **SMS/Email** option and select the survey from the drop-down list. After you select the survey, the associated questionnaire and associated channels are displayed. The associated channels can be sms, email, or both.
	  • Ensure that the script selected for the application has all the variables required for SMS/Email survey to work. Select the check box **All the variables required for the survey have been defined in the script**.

Step 5 Click **Add**.

The Cisco Script Application page is refreshed, the **Add New Trigger** hyperlink appears in the left navigation bar, and the following message is displayed in the status bar on top:

```
The operation has been executed successfully.
```

Click **Back to Application List** icon or button to view the list of existing applications.

Step 6 Add a trigger for the application.

Configure Busy Application

The Cisco Busy application comes with each Unified CCX system. This application returns a busy signal when a call reaches a Computer Telephony Interface (CTI) route point and the extension is busy.

Before you begin

To configure the Busy application, you will need to perform the following tasks:

- Add the Busy application.
- Add a Unified CM Telephony trigger to the Busy application. The Busy application is activated when it is triggered by a Unified CM Telephony trigger. The Busy application does not support HTTP triggers.

To configure the Unified CCX server with the Busy application, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Applications** > **Application Management**.

The Application Management web page opens, displaying the details of existing applications, if any.

Step 2 Click **Add New** icon that displays in the tool bar in the upper, left corner of the window or the **Add New** button that is displayed at the bottom of the window.

The Add a New Application web page opens.

Step 3 From the Application Type drop-down menu, choose **Busy**, and then click **Next**.

The Busy Application Configuration web page appears.

Step 4 Specify the following fields:

Field	Description
Name	A name for the application. This is a mandatory field.
ID	Accept the automatically-generated ID, or enter a unique ID. This is a mandatory field. **Note** The Historical Reporting feature uses this ID to identify this application.
Maximum Number Of Sessions	The maximum amount of simultaneous sessions (instances) that the application can handle.
The following fields are displayed only on click of **Show More** button.	
Description	Use the Tab key to automatically populate this field.
Enabled	Click the required radio button to accept - **Yes** (the default).

Step 5 Click **Add**.

The Busy web page refreshes, the **Add New Trigger** hyperlink appears in the left navigation bar, and the following message is displayed in the status bar on top:

```
The operation has been executed successfully
```

Step 6 Add a trigger for the application.

Configure Ring-No-Answer Application

The Cisco Ring-No-Answer application comes with each Unified CCX system. This application returns a ring tone signal when a call reaches a CTI route point.

Before you begin

To configure the Ring-No-Answer application, you will need to perform the following tasks:

- Add the Ring-No-Answer application.
- Add a Unified CM Telephony trigger to the Ring-No-Answer application. The Ring-No-Answer application is activated when it is triggered by a Unified CM Telephony trigger.

To configure the Unified CCX server with the Ring-No-Answer application, complete the following steps:

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Applications** > **Application Management**.

The Application Management web page opens, displaying the details of existing applications, if any.

Step 2 Click **Add New** icon that is displayed in the tool bar in the upper, left corner of the window or the **Add New** button that is displayed at the bottom of the window.

Step 3 From the Application Type drop-down menu, choose **Ring-No-Answer**, and then click **Next**.

The Ring-No-Answer web page opens.

Step 4 Specify the following fields.

Field	Description
Name	A name for the application. This is a mandatory field.
ID	Accept the automatically-generated ID, or enter a unique ID. This is a mandatory field. **Note** The Historical Reporting feature uses this ID to identify this application.
Maximum Number Of Sessions	The maximum amount of simultaneous sessions (instances) that the application can handle. This is a mandatory field.
The following fields are displayed only when you click the **Show More** button:	
Description	Use the Tab key to automatically populate this field.
Enabled	Click the required radio button to accept - **Yes** (the default).

Step 5 Click **Add**.

The Ring-No-Answer web page refreshes, the **Add New Trigger** hyperlink appears in the left navigation bar, and the following message is displayed in the status bar on top:

```
The operation has been executed successfully
```

Step 6 Add a trigger for the application.

Application Triggers

After adding a new Cisco application, you need to add one or more *triggers* so that the application can respond to Unified CM Telephony calls and HTTP requests.

Triggers are specified signals that invoke application scripts in response to incoming contacts. The Unified CCX system uses Unified CM Telephony triggers to trigger responses to telephone calls and HTTP triggers to respond to HTTP requests.

You can use either of the below two methods to add a trigger to an application:

- Add the trigger from the Cisco Application web page or add the trigger from the Unified CM Telephony.
- HTTP Triggers web pages available from the Subsystem menu.

Unified CM Telephony Trigger

You must add Unified CM Telephony triggers to invoke Cisco applications in response to incoming contacts.

A Unified CM Telephony trigger responds to calls that arrive on a specific route point by selecting telephony and media resources to serve the call and invoking an application script to handle the call.

Add Unified CM Telephony Triggers from Application Web Page

To add a Unified CM Telephony trigger directly from the Cisco Application Configuration web page, complete the following steps.

Procedure

Step 1 From the configuration web page for the application you want to add a trigger for, click **Add New Trigger**.

The Add a New Trigger window opens.

Step 2 From the Trigger Type drop-down menu, choose **Unified CM Telephony** and click **Next**.

The Unified CM Telephony Trigger Configuration window opens.

Step 3 Follow the procedure described in **Add Unified CM Telephony Trigger**.

Add Unified CM Telephony Triggers from Unified CCX

To add a Unified CM Telephony trigger to an application from the Unified CM Telephony subsystem, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **Unified CM Telephony** > **Triggers**.

The Unified CM Telephony Trigger Configuration summary web page opens.

Step 2 Click the **Add New** icon that is displayed in the tool bar in the upper, left corner of the window or the **Add New** button that is displayed at the bottom of the window.

Step 3 The Cisco Unified CM Telephony Trigger Configuration web page opens. Follow the procedure described in Add Unified CM Telephony Trigger, on page 70 (Steps 3 and 4) for detailed instructions on adding and configuring a Unified CM Telephony trigger.

Note
For triggers created in Unified CCX, Unified CM will always show the IPv4 Address of the CTI Route point, as the IP address is of the primary node or the first node in the Unified CCX cluster.

HTTP Trigger Provision

A Cisco application can be used to handle HTTP requests when the Unified CCX system is provisioned with an HTTP trigger.

Note HTTP/HTTPS triggers are available if your system has a license installed for one of the following Cisco product packages: Unified IP IVR or Unified CCX Premium.

An HTTP trigger is the relative URL a user enters into the client browser to start the application. You can upload either eXtensible Style Language Transformation (XSLT) templates or Java Server Pages (JSP) templates to serve as your HTTP trigger.

The following path is an example of an HTTP-triggered request (using the HTTP trigger name "/hello"):

```
http://www.appserver.acme.com:9080/hello
```

In this example, the URL starts the application with the HTTP trigger "/hello" on a web server running on port 9080 with the hostname www.appserver.acme.com.

You can add the HTTP trigger from the Cisco Script Application web page or add the trigger from the HTTP subsystem.

Add HTTP Trigger from Application Web Page

To add an HTTP trigger directly from a Cisco Application Configuration web page, complete the following steps.

Procedure

Step 1 From the configuration web page for the application you want to add a trigger for, click **Add New Trigger** hyperlink.

The Add a New Trigger window opens.

Step 2 From the Trigger Type drop-down menu, select **HTTP** and click **Next**.

The HTTP Trigger Configuration window opens.

Step 3 Specify the following fields.

Field	Description
URL	The relative URL For example: `/hello`
Language	Perform one of the following actions: • Choose a default language from the drop-down list. • Click **Edit**, specify a default language in the dialog box that appears, and click **OK**.
Maximum Number Of Sessions	The maximum amount of simultaneous sessions that can be served by the HTTP subsystem for this trigger.
Idle Timeout (in ms)	Maximum amount of time (in milliseconds) that the system will wait to invoke the application before rejecting a contact.
Enabled	Click the required radio button to accept - **Yes** (the default). **Note** If you disable the trigger, the user receives an error message when browsing to the defined trigger URL.

Step 4 Click **Add**.

The Cisco Application Configuration web page appears, and the URL of the HTTP trigger appears on the navigation bar.

Step 5 Test the trigger by entering the URL you just configured in the address bar of your browser.

For example,

`/hello`

The browser should display “hello”.

Add HTTP Trigger from HTTP Subsystem

To configure a HTTP trigger from the HTTP subsystem, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **HTTP**.

The HTTP Trigger Configuration web page opens.

Step 2 Click the **Add New** icon that is displayed in the tool bar in the upper, left corner of the window or the **Add New** button that is displayed at the bottom of the window.

The HTTP Trigger Configuration window opens.

Step 3 Specify the following mandatory fields.

Field	Description
URL	The relative URL. For example: `/hello`
Language	Perform one of the following actions: • Choose a default language from the drop-down list. • Click **Edit**, specify a default language in the dialog box that appears, and click **OK**.
Application Name	Choose the name of the application from the drop-down list.
Maximum Number Of Sessions	The maximum amount of simultaneous sessions that can be served by the HTTP subsystem for this trigger.
Idle Timeout (in ms)	Maximum amount of time (in milliseconds) that the system will wait to invoke the application before rejecting a contact.
Enabled	Click the required radio button to accept - **Yes** (the default) **Note** If you disable the trigger, the user receives an error message when browsing to the defined trigger URL.

Step 4 Click **Add**.

The Cisco Application Configuration web page appears, and the URL of the HTTP trigger appears on the navigation bar.

Step 5 To test the trigger, enter the URL you just configured in the address bar of your browser.

For example,

`/hello`

The browser should display “hello”.

Script Management

Scripts are created with the Unified CCX Editor, and can perform a wide variety of functions. For example, scripts can prompt callers for extension numbers to transfer calls, place callers in a queue, route calls to available agents, and place outbound calls.

The Unified CCX Administration web interface contains options for managing the Unified CCX scripts. The options are available at **Applications > Script Management**.

Note Your Unified CCX system includes sample scripts stored as .aef files.

Caution If a large number of VRU scripts are configured for your system, the **Upload a New Script** and **Refresh Scripts** operations can take a long time to complete. These tasks can also result in high CPU utilization.

Upload New Scripts

To make a script available for use as a Unified CCX application, you must first upload the script to the repository. The Repository Datastore (RDS) database contains the uploaded scripts along with prompts, grammars, and files. The scripts are grouped into folders and subfolders. The uploaded user scripts get synchronized to the local disk and are accessible from there.

To upload a script to the repository, complete the following steps:

Procedure

Step 1 Choose **Applications** > **Script Management** from the Unified CCX Administration menu.

The Script Management page opens.

Note
The Script Management page allows you to only work with user scripts; it does not have language-based directories.

The following table describes the available columns on the Script Management web page.

Field	Description
Folder Path	The level of the directory in the folder drop-down list.
Name	The name of the script. **Note** Click the icon in front of the script name to download the script file. **Note** Unified CCX does not support the use of special characters—Dollar ($), ampersand (&), percent (%), colon (:), asterisk (*), question mark (?), double quotes(" "), angle brackets(< >), pipe (|), single quotes (' '), forward slash (/), backward slash (\), square brackets ([ ]), parentheses (( )).
Size	The size of the script file is prefixed with **KB**. The file size is in kilobytes. **Note** This column is blank on the root page because the items on the page are usually folders.

Field	Description
Date Modified	The date, time, and time zone when the document was changed.
Modified by	The user ID of the person who modified the document.
Delete	To delete the corresponding folder. **Caution** When you delete a folder, you permanently remove it from the repository and make it unavailable to the Unified CCX system.
Rename	To rename the required subfolder within the **default** folder.
Refresh	To refresh the corresponding script.

Step 2 Click the **Upload New Scripts** icon. Alternatively, you can also click the **Upload New Scripts** button.

The Upload Script dialog box opens.

Step 3 In the **File Name** field, click **Browse** and navigate to the directory in which the scripts are located. Select a script, and click **Open**.

The script path for the profile appears in the **File Name** field.

Step 4 Click **Upload** to upload the script to the repository.

On successful upload of the license, a confirmation window appears.

You can now manage any existing scripts shown in the **Script Management** page. You can also add prompts to your applications.

Download Script File

To view or download a script file, complete the following steps:

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Applications** > **Script Management**.

The Script Management page opens to display the contents of the **default** folder.

Step 2 Click the **Download Script** icon that appears before the name of the script file that you want to view or download.

The File Download dialog box opens.

Step 3 Perform one of the following tasks:

a) To view the script file, click **Open**.

The script file opens in the Unified CCX Editor.

b) To download the script file, click **Save**, and then follow the prompts to choose a directory and file name for the script file.

The file is saved to the specified directory.

Refresh Scripts

Caution The size of the script determines the loading time of script properties. Larger the size, longer the processing time. If a large number of VRU scripts are configured for your system, the **Upload a New Script** and **Refresh Scripts** operations can take a long time to complete. These tasks can also result in high CPU utilization.

The size of the script determines the loading time of script properties. Larger the size, longer the processing time.

When you make changes to a script, you must refresh the script to direct all the applications and subsystems that use this script to reload the new version. There are two script refresh options:

- Refresh Scripts Individually, on page 55
- Refresh Bulk Scripts, on page 55

Refresh Scripts Individually

To refresh an individual script on the Unified CCX server from the repository (RDS), complete the following steps:

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Applications** > **Script Management**.

The Script Management page opens to display the contents of the **`default`** folder.

Step 2 In the row that contains the script, click **Refresh**.

The script information refreshes and the Script Management page reappears.

Refresh Bulk Scripts

Note Support for high availability and remote servers is available only in multiple-server deployments.

Bulk scripts refers to multiple .aef script files within one .zip file.

Note This option is available only when you upload .zip files. You will see the option to refresh scripts after the selected file is uploaded successfully.

To refresh all scripts (within a zip file) with one command, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Applications** > **Script Management**.

The Script Management page opens to display the contents of the **default** folder.

Step 2 Click the **Upload New Scripts** icon or button.

The Upload Script dialog box opens.

Step 3 To locate the script, click the **Browse** button next to the File Name field, navigate to the directory in which the scripts are located, select a file, and click **Open**. The script path for the profile appears in the File Name field.

Tip
You can only upload .zip files containing .aef files. The total size of the.zip file cannot exceed 20 MB.

Step 4 Click **Upload** to upload the script to the repository.

A window opens, informing you that the script upload succeeded.

Step 5 Click **Refresh** icon in the Script Management page.

The Script Management web page opens, giving you the option of refreshing the script and the applications that reference it, or just refreshing the script.

Step 6 Specify one of the following options:

- If you want all applications and subsystems that reference the script (in the repository) to use the new version, click **Yes**.
- If you only want to refresh the scripts, click **No**.
- If you want to cancel the operation, click **Cancel**.

The script information refreshes and the Script Management page reappears to display the newly loaded .zip file.

Rename Script or Folder

To rename a script or folder, complete the following steps:

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Applications** > **Script Management**.

The Script Management page opens to display the contents of the **default** folder.

Step 2 Click **Rename** icon for the folder or script that you want to rename. A dialog box opens displaying the name of the selected folder or script.

Step 3 Enter a new name for this folder or script in the text box.

Step 4 Click **Rename** button.

The dialog box refreshes to state that the folder was successfully renamed.

Step 5 Click **Return to Script Management** button.

The dialog box closes and the **default** folder's updated Script Management page displays the new script name.

Delete Script or Folder

When you delete a script or a folder, you remove it permanently from the repository.

To delete a script or folder, complete the following steps:

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Applications** > **Script Management**.

The Script Management page opens to display the contents of the **default** folder.

Step 2 To delete a folder, click **Delete** icon for the folder or script that you want to delete.

A dialog box opens to confirm your action on the selected script or folder.

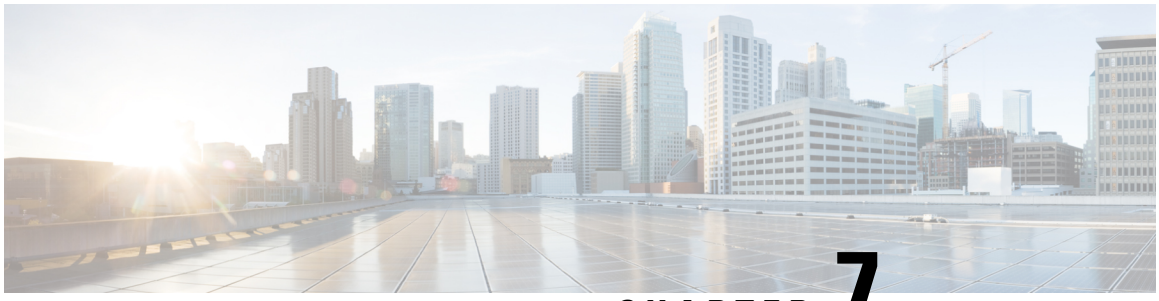
Step 3 Click **OK**.

The dialog box closes and the **default** folder's updated Script Management page refreshes to display the updated list of folders and scripts.

Sample Scripts

Your Unified CCX system includes sample scripts stored as .aef files. These scripts have been built using Unified CCXEditor steps, including prerecorded prompts. You can use these scripts to create applications without performing any script development, or you can use these scripts as models for your own customized scripts.

Note The included scripts are bundled with the Unified CCX system only as samples; they are not supported by Cisco. For more information on these sample scripts, see the *Cisco Unified Contact Center Express Getting Started with Scripts*.



CHAPTER 7

Telephony and Media Provision

- Unified CCX Telephony and Media, on page 59
- Provision Unified CM Telephony Subsystem, on page 61
- Additional Unified CM Telephony Information, on page 74
- Cisco Media Subsystem, on page 75
- ASR and TTS in Unified CCX, on page 77

Unified CCX Telephony and Media

The Unified CCX system uses a telephony resource called Computer Telephony Interface (CTI) ports to accept incoming calls and to place outbound calls. The Unified CCX system uses the following media resources to provide interactive services for calls:

- Unified CM Telephony—The Unified CCX Engine uses the Unified CM Telephony subsystem to send and receive calls from the Unified CM by interfacing with the CTI Manager through the Unified CM Telephony client.
- Cisco Media Termination (CMT)—The CMT channels provide media terminations in the Unified CCX for Unified CM Telephony Call Contacts. These channels enable the Unified CCX to play media to the connected party. DTMF digits are received out of band by the Unified CM Telephony subsystem.
- MRCP Automated Speech Recognition (MRCP ASR)—The ASR media resource allows callers to use speech to navigate menus and to provide other information to Unified CCX applications.
- MRCP Text-To-Speech (MRCP TTS)—The TTS media resource enables Unified CCX applications to play back documents to callers as speech.

Note Media resources are licensed and sold as Unified IP IVR ports. Although you can provision more channels than you are licensed for, licensing is enforced at run-time. If more channels are provisioned than licensed, the system will not accept the extra calls, because doing so would violate your licensing agreements.

The Unified CCX system uses *groups* to share telephony and media resources among different applications:

- *Call control groups* allow you to control how the system uses CTI ports. For example, you can reserve more ports for higher-priority applications or provide access to fewer ports for applications with less traffic.
- *Media resource groups* allow you to share media resources among different applications. For example, you can share ASR media resource groups with applications that collect caller information and applications that transfer calls to specific extensions.

The Unified CCX system also uses *triggers*, which are specified signals that invoke application scripts in response to incoming contacts.

Media Termination Groups

Media termination groups are associated with CTI port groups.

Note For Unified CM deployment, you can create and use additional CTI port groups as required.

If a CTI port group is selected to support media termination and if the number of channels are identical to both groups, the CTI port group is automatically created in the background. This auto creation feature eliminates the manual CTI port group creation process.

If you choose to override media termination, the call control channel chooses the media termination automatically. If you want to select a new dialog group, you can have more than one media termination option. The options are used in the order that is displayed in the drop-down list.

Channels Required to Process Calls

Unified CCX needs two types of channels to process calls:

- A *call control channel*, which is provisioned through the Unified CM Telephony subsystem and corresponds to CTI port resources in Unified CM.
- A *media channel*, which is provisioned through either the CMT subsystem or the MRCP subsystem and corresponds to the kernel resources for handling the media voice path with the caller.

Note MRCP channels also correspond to additional resources on the MRCP server for performing speech recognition.

Unified CCX needs access to a channel of each type to successfully process a call. However, the capabilities of the two channel types are not identical.

For example, consider a Unified CCX system provisioned with a single Unified CM Telephony call control channel (that is, a CTI port) and a single CMT channel. The system can handle one call at a time; when that call terminates, the system must reinitialize the channel resources before it can accept another call.

However, the time each channel takes to reinitialize is not equal—CMT channels take more time to reinitialize than CTI ports. For example:

- The Unified CM Telephony call control channel may take approximately 1 millisecond to reinitialize.

- The CMT channel may take approximately 200 milliseconds to reinitialize.

This example implies that the system will not be able to accept a new incoming call for 200 milliseconds after the first call terminates; although the Unified CM Telephony channel is available after one millisecond, the CMT channel is not and Unified CCX needs both channels to process a call.

Such a delay can become an issue when a Unified CCX system is experiencing a high load condition or needs to handle a burst of incoming calls. Consequently, CMT channels require a higher channel count provisioning.

Tip To provision Unified CCX systems to handle burst calls equally among all required resources, you must configure approximately 10 percentage more CMT channels than CTI ports, and approximately 10 percentage more MRCP channels than ASR licenses.

Provision Telephony and Media Resources

To provision telephony and media resources, complete the following tasks:

Procedure

Step 1 Provision the Unified CM Telephony subsystem.

Unified CM Telephony subsystem controls telephony resources for Unified CCX system.

Step 2 Provision the CiscoMedia subsystem.

CiscoMedia subsystem controls CMT media resources for Unified CCX system.

Step 3 Provision the MRCPASR subsystem.

MRCPASR subsystem controls ASR media resources for Unified CCX system.

Step 4 Provision the MRCP TTS subsystem.

MRCP TTS subsystem controls TTS media resources for Unified CCX system.

Provision Unified CM Telephony Subsystem

The Unified CM Telephony subsystem is the subsystem of the Unified CCXEngine that sends and receives call-related messages from the Unified CM CTI Manager through the Unified CM Telephony client. To enable your Unified CCX server to handle Cisco Unified Communications requests, you must provision the Unified CM Telephony subsystem. The Unified CM Telephony subsystem is available in all the Unified CCX license packages.

Note In previous versions of Unified CCX, it was necessary to configure Unified CM Telephony information using Unified CM. In Unified CCX, Unified CM Telephony configuration tasks are performed directly through Unified CCX Administration web pages.

To provision the Unified CM Telephony subsystem, complete the following tasks:

Procedure

Step 1 Configure a Unified CM Telephony Provider, if not already configured. Specify the server on which Unified CM CTI Manager is running, and provide a Unified CM user ID and password.

Step 2 Provision Unified CM Telephony call control groups.

Unified CM Telephony call control groups pool together a series of CTI ports, which the system then uses to serve calls as they arrive at the Unified CCX server.

Step 3 Provision a Unified CM Telephony trigger.

Unified CM Telephony triggers invoke application scripts in response to incoming contacts.

Step 4 Resynchronize Unified CM Telephony versions.

Resynchronize Cisco JTAPI Client

During the resynchronizing process, an additional check ensures that the Unified CM Telephony Client (also known as the Cisco JTAPI Client) are the same between the clients installed on the Unified CCX node and the Cisco Unified CM. If the Unified CCX detects a mismatch, the system downloads and installs the required version of Cisco JTAPI Client.

To resynchronize and view the status of Cisco JTAPI client, complete the following steps.

Procedure

Step 1 Choose **Subsystems** > **Cisco Unified CM Telephony** > **Cisco JTAPI Resync** from the Unified CCX Administration menu bar.

Step 2 The Cisco JTAPI Resync web page opens, displaying the status of Cisco JTAPI Client resynchronization.

At this point, if there is an incompatible version, it automatically downloads the new client.

Resynchronize Unified CM Telephony Data

This resynchronizing process ensures that the Unified CM Telephony user, the call control groups, and the triggers match the data of Unified CM being used.

To resynchronize the Unified CM Telephony data, complete the following steps.

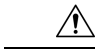
Procedure

From the Unified CCX Administration menu bar, choose **Subsystems** > **Cisco Unified CM Telephony** > **Data Synchronization** .

The Cisco Unified CM Telephony Data Synchronization web page opens after resynchronization, displaying the Data Resync status of Unified CM Telephony Port Groups and Unified CM Telephony Triggers.

Configure Unified CM Telephony Provider

The Unified CM Telephony Provider web page is a read-only page that displays the latest configured information.



Caution Some setups may prevent the Unified CM directory administrator from creating new Unified CM Telephony providers in a multiserver configuration. If this setup applies to you, be sure to delete preexisting Unified CM Telephony providers before creating new Unified CM Telephony providers. For example, if the Unified CM Telephony provider prefix is *cmtelephony* and you have a two-server configuration (*node_id1* and *node_id2*), you must delete both *cmtelephony_<node_id1>* and *cmtelephony_<node_id2>*. If you do not verify and delete preexisting Unified CM Telephony providers, the Unified CM Telephony subsystem issues an error and will not allow you to create Unified CM Telephony providers from the Unified CM Telephony Provider Configuration web page.

Procedure

Step 1 Choose **Subsystems** > **Cisco Unified CM Telephony** > **Provider** from the Unified CCX Administration menu bar.

The Cisco Unified CM Telephony Provider web page opens.

The following table describes the read-only fields displayed in the Unified CM Telephony Provider Configuration web page.

Field Heading	Description
Primary Unified CM Telephony Provider	IP address of the Server, running Unified CM CTI Manager in the cluster. This is usually the first CTI Manager or Cisco Unified CM Telephony Provider selected by the Unified CCX user for Unified CM Telephony subsystem using **System** > **Cisco Unified CM Configuration** web page.

Field Heading	Description
Secondary Unified CM Telephony Provider	IP address of the second Server, running Unified CM CTI Manager in the cluster. This is usually the second CTI Manager or Cisco Unified CM Telephony Provider selected by the Unified CCX user for Unified CM Telephony subsystem using **System** > **Cisco Unified CM Configuration** web page. **Note** If you have selected only one Unified CM Telephony provider, this field will be blank.
User Prefix	User prefix for the Unified CM user IDs created in Unified CM.

Step 2 To modify the Unified CM Telephony subsystem, click **Modify Cisco Unified CM Telephony Provider Information** icon that displays in the tool bar in the upper left corner of the window. The Cisco Unified CM Configuration web page opens.

Add New Call Control Group

The Unified CCX system uses Unified CM Telephony call control groups to create a series of CTI ports. The system uses the CTI ports to serve calls as they arrive at or depart from the Unified CCX server. You can create multiple Unified CM Telephony call control groups to share and limit the resources that are used by specific applications.

To configure a new Unified CM Telephony call control group, complete the following steps.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Unified CM Telephony** > **Call Control Group**.

The Cisco Unified CM Telephony Call Control Group Configuration web page opens, which displays the existing Unified CM Telephony Call Control Group information, if any.

Step 2 Click the **Add New** icon that is displayed in the tool bar in the upper left corner of the window or the **Add New** button at the bottom of the window to create a new CTI port. The Cisco Unified CM Telephony Call Control Group Configuration web page opens.

Note
You can create only one call control group of the Outbound type, in which the number of CTI ports must be always equal to or greater than the licensed Outbound IVR ports.

Create the CTI ports through the Publisher for both nodes in a HA over WAN deployment.

Step 3 Use this web page to specify the following information:

Page Area	Field	Description
Group Information	Group ID	Corresponds to the trunk group number reported to Cisco Unified Intelligent Contact Management Enterprise (Unified ICME) when the Unified CCX server is part of the Unified ICME solution. The value for this field is automatically generated. **Note** If a Stop icon appears beside the Group ID (on the Cisco Unified CM Call Control Group Configuration list page), it indicates that the data is invalid or out of sync with Unified CM data; if a Head icon appears, the group is valid.
	Description	Description of the Group ID. Press the **Tab** key to automatically populate the Description field.
Group Information (continued)	Number of CTI Ports	Number of CTI ports assigned to the call control group. This is a mandatory field. If you have a Premium license with an Outbound license, you can create only one Outbound call control group with a minimum licensed number of IVR ports or more. The number of CTI ports for an outbound type of call control group can be modified but not below the licensed ports for Outbound IVR. This rule does not apply to inbound type call control groups. You can continue to create more inbound type call control groups. **Note** If this field is set to <*n*>, the system creates <*n*> ports for each Unified CCX Engine node (node in which Unified CCX Engine component is enabled).
	Media Termination Support	Enables the auto-creation of media termination groups. This is a mandatory field. Yes = Provides automatic media termination if the CTI port group is successful. No = Media termination port group is not created (default).
	Group Type	Select the group type for the call control group using this radio button. The choices are Inbound and Outbound. This is a mandatory field and Inbound radio button is enabled by default. You cannot change the group type from Outbound to Inbound and conversely. The Outbound type call control group will be displayed only if you have uploaded the Outbound license on top of the premium license in your Unified CCX.
Directory Number Information	Device Name Prefix	The Device Name Prefix (DNP) given to all of the CTI ports in this group. This is a mandatory field. The CTI ports for this port group are restricted to a maximum of 5 characters and has the following format: `<deviceprefix>_<directoryno>` For example, if the Device Name Prefix is CTP and the starting Directory Number is 7000, the CTI port that is created in Unified CM can have the device name CTP_7000.

Page Area	Field	Description
Select **Server for Telephony Port Group Configuration** (displayed only in a HA over WAN deployment).		
	Select Server	This field is displayed only in a HA over WAN deployment and it displays the different Unified CCX nodes that are available in a HA over WAN deployment in a drop-down list. In a HA over WAN setup, you need to configure directory information along with Unified CM-specific information for the ports in each node. Once you select a node, all configuration details displayed below this field will be specific to the selected node only. So, if you update any node-specific parameters (below the **Select Server** field), it will be applicable only to the ports specific to the selected node. But, if you update any configuration data above the **Select Server** field, it will be applicable for the ports in both the nodes except for the **Number of s** field. **Note** You need to ensure that the values in **Number of s** field for both the nodes are the same. If you modify this field, the number of ports is modified for the selected node only as the device pool selection for both nodes could be different in a HA over WAN deployment. If you click **Add** before updating this value for either of the node, the port group for that node will be marked with a red cross in the main Cisco Unified CM Telephony Call Control Group Configuration web page to signify the fact that the number of ports between the two nodes is different and the other node should also be updated. In such a scenario, click the hyperlink for the node that is tagged in red; and from the Cisco Unified CM Telephony Call Control Group Configuration page for the selected node, update the value in the **Number of CTI Ports** field and click **Update** to ensure the number of CTI ports for both the nodes are the same. After you configure the data for the selected node and click **Add** or **Update**, the updated configuration information will be saved. For detailed information on behavior in HA over WAN scenario, refer to the *Solution Design Guide for Cisco Unified Contact Center Express* https://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_implementation_design_guides_list.html. In case of LAN deployment, this field is not displayed, as the same configuration data will be applicable for both the nodes in the cluster.

Page Area	Field	Description
Directory Number Information	Starting Directory Number	A unique phone number. The Starting Directory Number contains numerals, and can have an asterisk (*) or a hash (#), or both as a prefix or a suffix. To support E.164 compliance, Unified CCX allows you to add the plus sign (+) before the directory number. The specified number of ports will be created starting from the value specified in this field. The Directory Number that you enter can appear in more than one partition. This is a mandatory field. **Note** When a pattern is used as a Directory Number, the phone display and the caller ID display on the dialed phone will contain characters other than digits. To avoid this, provide a value for Display (Internal Caller ID), Line Text Label, and External Phone Number Mask.
	Device Pool	Set of common characteristics for devices, such as region, date/time group, softkey template, and MLPP information to which you want to assign this phone. **Note** The support for having multiple device pools associated with the call control group(s) has been withdrawn in Unified CCX. Manually assign a single device pool to each call control group if you have multiple device pools associated with call control group(s) in an older version of Unified CCX. In a HA over WAN setup, you need to configure directory information along with Unified CM-specific information for the ports in each node. Once you select a node, all configuration details displayed below this field will be specific to the selected node only. So, if you update any node-specific parameters (below the **Select Server** field), it will be applicable only to the ports specific to the selected node. But, if you update any configuration data above the **Select Server** field, it will be applicable for the ports in both the nodes except for the **Number of CTI Ports** field. **Note** You need to ensure that the values in **Number of CTI Ports** field for both the nodes are the same. If you modify this field, the number of ports is modified for the selected node only as the device pool selection for both nodes could be different in a HA over WAN deployment. If you click **Add** before updating this value for either of the node, the port group for that node will be marked with a red cross in the main Cisco Unified CM Telephony Call Control Group Configuration web page to signify the fact that the number of ports between the two nodes is different and the other node should also be updated. In such a scenario, click the hyperlink for the node that is tagged in red; and from the Cisco Unified CM Telephony Call Control Group Configuration page for the selected node, update the value in the **Number of CTI Ports** field and click **Update** to ensure the number of CTI ports for both the nodes are the same.
	DN Calling Search Space	A collection of partitions that are searched to determine how a dialed number should be routed. The calling search space for the device and the calling search space for the directory number get used together. The directory number calling search space takes precedence over the device calling search space.

Page Area	Field	Description
	Location	The Cisco Unified Communications phone location setting specifies the total bandwidth that is available for calls to and from this location. A location setting of **HUB_NONE** means that the location feature does not keep track of the bandwidth that this Cisco Unified Communications phone consumes.
Advanced Directory Number Information (only available if you click **Show More**)		
Directory Number (continued)	Alerting Name ASCII	This information is automatically populated based on the configuration in the Unified CM setup and displays the ASCII name filed used in one of the following situations: • If the device is not capable of handling the Unicode strings • If the locals on endpoint devices do not match • If the Unicode string is not specified
	Redirect Calling Search Space	A collection of partitions that are searched to determine how a redirected call is routed. Redirect Calling Search Space options: **Note** **DN Calling Search Space** is deprecated. Use **Calling Party** or **Redirect Party** instead. • **DN Calling Search Space—**This option enables the CTI port to use its directory number CSS when performing a redirect transfer. • **Calling Party—**This option enables the CTI port to use the calling party's CSS when performing a redirect / consult transfer. • **Redirect Party—**This option enables the CTI port to use the CTI port's CSS to control the redirect.
	Media Resource Group List	A prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from the available media resources according to the priority order that is defined in a Media Resource Group List. If you choose <none>, Unified CM uses the Media Resource Group that is defined in the device pool.

Page Area	Field	Description
Directory Number Setting	Voice Mail Profile	A list of profiles defined in the Voice Mail Profile Configuration. The first option is <None>, which is the current default Voice Mail Profile that is configured in the Voice Mail Profile Configuration.
	Presence Group	See the *Cisco Unified Communications Manager Administration Guide* for detailed information on how to configure presence groups.
	Require DTMF Reception	A Unified CM radio button to determine if DTMF reception is required. Yes is selected by default. If you select No, a warning message is displayed.
	AAR Group	Automated Alternate Routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of <None> specifies that no rerouting of blocked calls will be attempted.
	User Hold Audio Source	Audio source heard by the caller when the Unified CCX Script places the caller on Hold by using the Hold Step (when you press the hold key).
	Network Hold Audio Source	Audio source heard by the caller when Unified CCX performs a Consult Transfer (when Unified CCX calls an agent). Use this entry for the .wav file (for example, a .wav file playing a ringback tone) to be played to the caller during this Consult Transfer.
Call Forward and Pickup Settings	Call Pickup Group	The number that can be dialed to answer calls to this directory number in the specified partition.
	Display	Use a maximum of 30 alphanumeric characters. Typically, use the user name or the directory number (if you use the directory number, the person receiving the call may not see the proper identity of the caller). Leave this field blank to have the system display the extension.
	External Phone Number Mask	Phone number (or mask) that is used to send Caller ID information when a call is placed from this line. You can enter a maximum of 24 number, the international escape character +, *, # and "X" characters. The X characters represent the directory number and must appear at the end of the pattern. For example, if you specify a mask of 972813XXXX, an external call from extension 1234 displays a caller ID number of 9728131234.

Step 4 Click **Add** or **Save**.

The Unified CM Telephony Call Control Group Configuration summary web page opens. The corresponding CTI ports are created in the Unified CM Telephony call control group. The new call control group appears in the list of call control groups in the Cisco Unified CM Telephony Call Control Group Configuration web page.

Add Unified CM Telephony Trigger

You must configure Unified CM Telephony triggers to invoke application scripts in response to incoming contacts. A Unified CM Telephony trigger responds to calls that arrive on a specific route point by selecting telephony and media resources to serve the call and invoking an application script to handle the call. The Unified CM Telephony triggers are available with all Unified CCX license packages.

Unified CM Telephony trigger settings include:

- **Session** information, such as the application to associate with the trigger, Maximum Number of sessions allowed, and the Idle Timeout value.
- **CTI** information, such as a CTI port device and CTI route points for each call Unified CCX simultaneously places or accepts.
- **Directory Number** information, such as the Voice Mail Profile and Calling Search Space.
- **Call Forward and Pickup** instructions.

To add and configure a Unified CM Telephony trigger, complete the following steps.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Cisco Unified CM Telephony** > **Triggers**.

The Unified CM Telephony Trigger Configuration web page opens displaying the following fields.

Field	Description
Route Point	Available CTI route point, which is the directory number associated with the trigger.
Application	Application name to associate with the trigger.
Sessions	Maximum number of simultaneous calls that the trigger can handle.
Enabled	True if the trigger is enabled; False if the trigger is disabled.

Note
If you try to delete a trigger associated with an outbound call control group, then the campaigns associated with the trigger become invalid and the application also gets deleted. In such cases, when you click the **Delete** icon or button, a dialog box opens to confirm your action. Click **OK** if you want to delete the trigger and disassociate the campaigns associated with it. If you delete a trigger and navigate to the Campaign Configuration web page, you will also see an alert regarding the missing trigger association for that campaign.

Step 2 Click the **Add New** icon that is displayed in the tool bar in the upper left corner of the window or the **Add New** button that is displayed at the bottom of the window.

The Unified CM Telephony Trigger Configuration web page opens.

Step 3 Use this web page to specify the following mandatory fields:

Field	Description
Directory Information	

Field	Description
Directory Number	A unique phone number. To support E.164 compliance, Unified CCX allows you to add a plus sign (+) before the agent extension or a route point directory number followed by 15 characters which consist of numerals and the following special characters: uppercase letter X, hash (#), square brackets ([ ]), hyphen (-), and asterisk (*). • Supports only route point directory numbers and Finesse agent and supervisor extensions. **Note** • +1234 and 1234 are two different directory numbers. • The square brackets ([ ]) enclose a range of values. • For more information, see the "Wildcards and Special Characters in Route Patterns and Hunt Pilots" section in the *System Configuration Guide for Cisco Unified Communications Manager*. **Examples:** • Valid directory numbers—+1223* or *#12#* • Invalid directory numbers—91X+ or +-12345 **Note** Use of two(2) wildcard CTI Route Points that overlap with each other is not supported. For example, Route Point 1: 123XXXX and Route Point 2: 1234XXX overlap with one another and is not supported. However, a wildcard CTI Route point can overlap with a full DID (best match pattern) that doesn't contain a wildcard. For example, Route Point 1: 123XXXX and Route Point 2: 1234567 is supported.
Trigger Information	
Language	Choose the default language to associate with the incoming call when the application is started from this drop-down menu. **Note** To add a Language option, click **Edit** button. The User Prompt dialog box opens. Enter a locale string value and click **OK**. The User Prompt dialog box closes, and the name of the language opens in the Language field in the Unified CM Telephony Configuration web page.
Application Name	From the drop-down menu, choose the application to associate with the trigger.
Device Name	A unique identifier for this device, consisting of alphanumeric characters, dots, dashes, or underscores.
Description	A descriptive name for the CTI route point.
Call Control Group	Choose the call control group to associate with the trigger from this drop-down menu. For Outbound IVR Dialer, you must select the call control group from Outbound type call control group list. The route point should be created on Unified CM. Once you assign the Outbound group for a trigger, you cannot change it to an Inbound group and vice versa.

Field	Description
Advanced Configuration (available only if you click **Show More**).	
Advanced Trigger Information	
Enabled	Radio buttons to choose the required option: • **Yes—**enable the trigger (default) • **No—**disable the trigger.
Maximum Number of Sessions	The maximum number of simultaneous calls that this trigger can handle. The number is actually governed by the Unified CM (10,000 for each separate line). However in Unified CCX, this number is restricted to the maximum number of sessions. Any call after this number is exceeded gets the busy tone.
Idle Timeout (in ms)	The number of milliseconds (ms) the system should wait before rejecting the Unified CM Telephony request for this trigger.
Override Media Termination	Radio buttons to choose the required options: **Yes—**Override media termination. **No—**Enable media termination (default). If you select Yes, two panes open: • Selected Dialog Groups displays the default or selected group. • Available Dialog Groups lists the configured dialog.
CTI Route Point Information	
Alerting Name ASCII	This information is automatically populated based on the configuration in the Unified CM setup and displays the ASCII name filed used in one of the following situations: • If the device is not capable of handling the Unicode strings • If the locals on endpoint devices do not match • If the Unicode string is not specified
Device Pool	The device pool to which you want to assign this route point. A device pool defines sets of common characteristics for devices, such as region, date/time group, softkey template, and MLPP information.
Location	The total bandwidth that is available for calls to/from this location. A location setting of **HUB_NONE** indicates that the locations feature does not keep track of the bandwidth used by this route point.
Directory Number Settings	

Field	Description
Partition	The partition to which the Directory Number belongs. The Directory Number field value must be unique within the partition that you choose. If you do not want to restrict access to the Directory Number, select <**None**> as the partition setting.
Voice Mail Profile	A list of profiles defined in the Voice Mail Profile Configuration. The first option is <**None**>, which is the current default Voice Mail Profile that is configured in the Voice Mail Profile Configuration.
Calling Search Space	A collection of partitions that are searched for numbers that are called from this directory number. The specified value applies to all devices that use this directory number. For example, assume you have two calling search spaces: Building and PSTN. Building only allows users to call within the building, while PSTN allows users to call both in and outside the building. You could assign the phone to the Building calling search space and the line on your phone to the PSTN calling search space. For more information, see the *System Configuration Guide for Cisco Unified Communications Manager*.
Calling Search Space for Redirect	By default, Cisco Unified Communications Manager uses the original calling party's calling search space (CSS) to process the redirected call from a Unified CCX Trigger to a Unified CCX CTI Port. This default behavior requires the partition of the Unified CCX CTI ports to be a member of the original calling party's CSS even if the partition of the CTI Route Point/Unified CCX Trigger is accessible to the calling device's CSS and the CSS of the CTI Route Point/Unified CCX Trigger contains the partition of the Unified CCX CTI Ports. You can modify this behavior using the drop-down list to instruct Cisco Unified Communications Manager which CSS to use when redirecting the call from the CTI Route Point to the CTI Port. Calling Search Space for Redirect options: • **Default Calling Search Space—**CSS of the calling device • **Calling Address Search Space—**CSS of the calling device • **Route Point Address Search Space—**CSS of the CTI Route Point (Trigger)
Presence Group	A list of groups to integrate the device with the iPass server. The device/line information is provided for integrating applications.
Call Forward and Pickup Settings	

Field	Description
Forward Busy	Check one of the following options: **Voice Mail—**Check this box to use settings in the Voice Mail Profile Configuration window. **Note** When this box is checked, Unified CM ignores the settings in the Destination box and Calling Search Space. **Destination—**To use any disable phone number, including an outside destination. **Calling Search Space—**To apply the above setting all devices that are using this directory number. **Note** For limiting the number of calls per application in Unified CCX system, see the Unified CM Telephony Triggers for Unified CCX Queuing, on page 74 section.
Display	Use a maximum of 30 alphanumeric characters. Typically, use the user name or the directory number (if using the directory number, the person receiving the call may not see the proper identity of the caller). Leave this field blank to have the system display an extension.
External Phone Number Mask	Phone number (or mask) that is used to send Caller ID information when a call is placed from this line. You can enter a maximum of 24 number, the international escape character +, *, # and "X" characters. The X characters represent the directory number and must appear at the end of the pattern. For example, if you specify a mask of 972813XXXX, an external call from extension 1234 displays a caller ID number of 9728131234.

Step 4 Click **Add** or **Save** to save the changes. The specified route point is created on the Unified CM.

The Unified CM Telephony Trigger Configuration web page opens and displays the new Unified CM Telephony trigger.

Additional Unified CM Telephony Information

This section includes the following topics:

- Unified CM Telephony Triggers for Unified CCX Queuing, on page 74
- Unified CM Telephony Information Resynchronization, on page 75

Unified CM Telephony Triggers for Unified CCX Queuing

When limiting the number of calls per application in Unified CCX applications, you need to take care to coordinate the Unified CM Telephony trigger Maximum Number of Sessions limit with the Media Group session limit.

For example, if you are using Unified CCX for queuing calls and set the Unified CM Telephony trigger Maximum Number of Sessions limit on Unified CCX to 4 and set the Call Forward and Pickup Settings to

send the fifth call to voice mail. To make this happen, you must configure the Media Group Session Limit to the identical setting (4). This will cause Unified CM to forward the next incoming call to voice mail (once the CTI New Call Accept timer setting expires).

The disadvantage of this approach is that you need to define more media groups for each application and you cannot share the same set of media groups across multiple applications.

Unified CM Telephony Information Resynchronization

If the Unified CM Telephony information (Unified CM Telephony users, CTI ports, triggers, SRTP) in the Unified CM is missing or not in sync with Unified CCX data, choose **Subsystems** > **Cisco Unified CM Telephony** > **Data Resync** from the Unified CCX Administration menu bar. Unified CCX checks whether:

- The Unified CM Telephony users exist in Unified CM.
- All the ports belonging to the Port Group exist in Unified CM.
- The port group's data is in sync with Ports data in Unified CM.
- The ports' association to users are correct.
- The route point exists in Unified CM.
- The triggers data is in sync with the Route Point data in the Unified CM.
- The route points have been associated with all the Unified CM Telephony users in Unified CM.
- The Unified CM configuration is in sync with Unified CCX for SRTP.

Unified CCX synchronizes the data by:

- Creating any missing users
- Creating any missing ports
- Modifying out-of-sync ports
- Associating CTI Ports to Unified CM Telephony users. (For example, associating CTI Ports created for Node 1 to the Unified CM Telephony User for Node 1, and so on.)
- Creating any missing route points
- Modifying out-of-sync route points
- Associating route points to all the Unified CM Telephony users.
- Modifying Unified CM configuration, such as user roles and CAPF profiles for JTAPI telephony users to match SRTP configuration.

Cisco Media Subsystem

The Cisco Media subsystem is a subsystem of the Unified CCX Engine. The Cisco Media subsystem manages the CMT media resource. CMT channels are required for Unified CCX to be able to play or record media.

The Cisco Media subsystem uses *dialog groups* to organize and share resources among applications. A dialog group is a pool of *dialog channels* in which each channel is used to perform *dialog interactions* with a caller, during which the caller responds to automated prompts by pressing buttons on a touch-tone phone.

Note The built-in grammars and grammar options that are supported by Unified CCX when using an MRCP dialog channel is determined by the MRCP speech software you purchase. See the software vendor for information about what built-in grammars and features are supported.

To enable your Unified CCX applications to handle simple DTMF-based dialog interactions with customers, you must provision the Cisco Media subsystem to configure CMT dialog groups.

Caution All media termination strings begin with `auto` and contain the same ID as the call control group—not the CMT dialog group. If the default media termination is configured and the ID differs, follow the procedure provided in the **Add CMT Dialog Control Group**.

Add CMT Dialog Control Group

To add a CMT dialog control group, complete the following steps.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Cisco Media**.

The Cisco Media Termination Dialog Group Configuration web page opens. Any preconfigured entry is listed on this page with the following information:

Field	Description
GroupID	The unique Group ID associated with the media.
Description	CMT group description. **Note** The ID in this field need not necessarily match the CMT group ID.
Channels	Number of channels associated with the group.

Step 2 Click **Add New** icon at the top or **Add New** button at the bottom of the window. The Cisco Media Termination Dialog Group Configuration web page opens.

Note
By default, a Unified CM Telephony Call Control Group with Group ID 0 is created.

Step 3 Use this web page to specify the following fields.

Field	Description
Group ID	A Group ID value unique within all media group identifiers, including ASR group identifiers. This is a mandatory field.
Description	Description for the Cisco Media Termination Dialog group.
Number of Licensed IVR ports	Number of licensed IVR ports. Display only.
Maximum Number Of Channels	Maximum number of channels associated with this group. This is a mandatory field. **Note** You can specify any value for Maximum Number Of Channels, but restrictions are placed on the system when a call is made. This restriction is imposed by the number of licensed IVR ports on your system. This is a mandatory field.

Step 4 Click **Add** icon that displays in the tool bar in the upper left corner of the window or the **Add** button that displays at the bottom of the window.

The CMT Dialog Group Configuration web page opens, displaying the new CMT dialog group.

You are now ready to provision MRCP ASR and MRCP TTS subsystems.

ASR and TTS in Unified CCX

Unified CCX supports ASR and TTS through two subsystems:

MRCP ASR
This subsystem allows users to navigate through a menu of options by speaking instead of pressing keys on a touch-tone telephone.

MRCP TTS
This subsystem converts plain text (UNICODE) into spoken words to provide a user with information, or prompt a user to respond to an action.

Note Only G.711 codec is supported for ASR/TTS integrations.

Prepare to Provision ASR/TTS

It is the responsibility of the customer to perform the following tasks:

- Order ASR/TTS speech servers from Cisco-supported vendors.

Note For more information on supported speech servers for Unified CCX, see the Unified CCX Compatibility related information, located at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

- Work with the ASR/TTS vendor to size the solutions.
- Provision, install, and configure the ASR/TTS vendor software on a different server (in the same LAN) and not where the Unified CCX runs. (see the Unified CCX Compatibility related information, located at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.).
- Before uploading a ASR/TTS script to Unified CCX Administration, validate the script against the capabilities and specifications supported by the ASR/TTS vendor.

Provision of MRCP ASR Subsystem

The MRCP ASR subsystem allows users to navigate through a menu of options by speaking instead of pressing keys on a touch-tone telephone. When a user calls local directory assistance, for example, ASR can prompt the user to say the city and state in which to locate the information, then connect the user to an appropriate operator.

To provision the MRCP ASR subsystem, define the following information:

- **MRCP ASR Providers**—Information about the vendor of your speech server, including the number of licenses and the grammar type.
- **MRCP ASR Servers**—Information about the ASR server's name, port location, and available languages.
- **MRCP ASR Groups**— Information about the MRCP ASR dialog control groups and associated locales, which enable Unified CCX applications to use speech recognition.

Provision MRCP ASR Providers

Use the MRCP ASR Provider Configuration web page to specify information about the vendor of your speech server.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystem** > **MRCP ASR** > **MRCP ASR Providers**.

The MRCP ASR Provider Configuration web page opens, displaying the list of currently configured MRCP providers, licenses, and the corresponding status.

Step 2 Click **Add New** icon that displays in the tool bar in the upper left corner of the window or the **Add New** button that is displayed at the bottom of the window.

The MRCP ASR Provider Configuration web page opens.

Step 3 Specify the following mandatory fields:

Field	Description
Provider Name	Enter the name of the MRCP ASR provider supported by Unified CCX.
Number of Provider Licenses	The number of ASR port licenses purchased from the ASR vendor.
Grammar Variant	Vendor-specific grammar setting. Valid options: • Nuance Open Speech Recognizer servers version 9.0 and above (OSR 3.1.x) • Nuance 11.x and below version ASR servers (Nuance) • IBM WVS ASR servers (2003 SISR)

Step 4 Click **Add** icon in the tool bar in the upper left corner of the window or the **Add** button that displays at the bottom of this window to apply changes.

Note
After you update MRCP ASR/TTS Providers, Servers, and Groups, the corresponding provider needs to be refreshed for changes to take effect. The Unified CCX Engine does not need to be restarted. However, during a Refresh, Unified CM Telephony triggers using affected groups will fall back to the dialog group that is configured and the MRCP Provider being refreshed will go NOT_CONFIGURED until the reload is complete.

Your changes appear in the MRCP ASR Providers List page. You are now ready to provision MRCP ASR Servers.

Note
If you delete an ASR/TTS provider and all of its associated servers and then create a new ASR/TTS provider, its status might become IN_SERVICE immediately, even before you create any servers for it. In this situation, click **Refresh** for that ASR/TTS provider, or click **Refresh** All. These actions change the status of the ASR/TTS provider to NOT_CONFIGURED.

Provision MRCP ASR Servers

Use the MRCP ASR Server Configuration web page to specify information about the speech server's name, port location, and available language.

Note You must have an MRCP ASR Provider defined before you can provision an MRCP ASR Server.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystem** > **MRCP ASR** > **MRCP ASR Servers**.

The MRCP ASR Server Configuration web page opens, displaying a list of previously configured servers, if applicable with the following information:

Column	Description

Computer Name	Hostname or IP address in which the ASR server software is installed. **Note** ASR server deployment over WAN is not supported in Unified CCX. The ASR server should be in the same LAN where Unified CCX is. You need to specify the ASR server hostname or IP address that is local with the Unified CCX node while installing the ASR server software in this field.
Provider	The MRCP ASR Provider to which this server is associated.
Port	The default TCP port number that is used to connect to a MRCP server. • OSR 3.1.x—4900 for MRCPv1 and 5060 for MRCPv2 • 2003 SISR—554 • Nuance—554
Status	Status or state of the subsystem.

Step 2 Click **Add New** icon that is displayed in the tool bar in the upper, left corner of the window or the **Add New** button that is displayed at the bottom of the window to provision a new MRCP ASR Server.

The MRCP ASR Server Configuration web page opens.

Step 3 Use this web page to specify the following fields.

Field	**Description**
Server Name	Hostname or IP address of the server where the MRCP ASR server software is installed.
Provider Name	Select the name of the MRCP ASR Provider to which this server is associated from this drop-down list.
Port Number	The default TCP port number that is used to connect to a MRCP server. Though the default value is shown as 4900. You need to provide any one of the following values in this field based on the TCP provider or grammar variant you have selected while configuring an MRCP ASR provider: • OSR 3.1.x—4900 for MRCPv1 and 5060 for MRCPv2 • 2003 SISR—554 • Nuance—554

Locales	Languages supported by the ASR Provider. Select a language (or multiple languages) from the drop-down list and click **Add Language**; the selected language appears with a check box in the Enabled Languages list. **Note** Use the check box to enable or disable a language.

Step 4 Click **Add** to apply changes.

Your changes appear in the MRCP ASR Server list web page. You are now ready to provision MRCP ASR Groups.

Provision MRCP ASR Dialog Groups

Use the MRCP Groups Configuration web page to specify information about MRCP ASR dialog control groups, which enable Unified CCX applications to use speech recognition.

Note You must have a MRCP ASR Provider defined before you can provision a MRCP ASR Group. Also, you should configure MRCP ASR Servers for the specific MRCP Provider before configuring the MRCP ASR Groups. This allows users to configure languages for the groups based on the languages supported by the configured servers.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystem** > **MRCP ASR** > **MRCP ASR Dialog Groups**.

The MRCP ASR Dialog Group Configuration web page opens to display a list of preconfigured entries, if applicable with the following information:

Field	Description
Group ID	Identifier for the group.
Description	Description of this dialog group.
Provider	Name of the MRCP ASR provider.
Channels	Maximum number of sessions.

This web page also displays the Number of Licensed IVR Channels.

Step 2 Click **Add New** icon that displays in the tool bar in the upper, left corner of the window or the **Add New** button that displays at the bottom of the window to provision a MRCP ASR Group.

The MRCP ASR Dialog Group Configuration web page opens.

Step 3 Use this web page to specify the following fields:

Field	Description
Group ID	Associated group ID.
Description	Description of this dialog group. **Tip** Include languages that will be used by this Group to the description. Doing so will provide insight into the languages this Group uses when you set up the dialog group in the Unified CM Telephony trigger configuration. This also ensures that the locales used by the application configured in the Unified CM Telephony trigger match the locales supported by the MRCP ASR dialog group being selected.
Number Of Provider Licenses	Display only.
Number Of Licensed IVR Ports	Display only.
Maximum Number Of sessions	Maximum number of sessions associated with this dialog group. **Note** You can assign any value for Maximum Number Of Channels, but restrictions are placed on the system when a call is made. This restriction is imposed by the number of licensed IVR ports on your system. **Caution** Under heavy load, calls that utilize a channel from an MRCP ASR Dialog Control Group, might have a reduced call completion rate as the MRCP channels used by calls can take some additional time to clean up all the sessions set up with MRCP resources. To address this situation, you can overprovision the value of this field by a factor of 1.2 or by an additional 20 percent. For example, if your application requires 100 MRCP ASR channels, modify the value in this field to be 120 MRCP ASR channels.
Provider Name	Select a MRCP Provider name from the drop-down list that contains a list of all previously defined provider names.
Enabled Languages	Select the languages that you wish to configure for this group from the list displayed. The displayed languages represent the locales configured for all MRCP ASR servers for the specified provider. If there are no MRCP ASR servers configured, no languages are displayed. In this case, you must update the group configuration once MRCP ASR servers have been configured for the specified provider.

Step 4 Click **Add** to apply changes.

Your changes appear in the MRCP ASR Groups list web page.

MRCP TTS Subsystem

The MRCP TTS subsystem converts plain text (UNICODE) into spoken words to provide a user with information, or prompt a user to respond to an action.

For example, a company might use TTS to read back a customer's name, address, and telephone number for verification before the company ships a requested product to the customer's location. Or a customer might dial into a pre-designated phone number, access a voice portal, and listen to the latest weather report or stock quotes. TTS can also convert email text to speech and play it back to the customer over telephone.

To provision the MRCP TTS subsystem, define the following information:

- **MRCP TTS Providers**—Information about the vendor of your TTS system.

Note If you delete an ASR/TTS provider and all of its associated servers and then create a new ASR/TTS provider, its status might become IN_SERVICE immediately, even before you create any servers for it. In this situation, click Refresh for that ASR/TTS provider, or click Refresh All. These actions change the status of the ASR/TTS provider to NOT_CONFIGURED.

- **MRCP TTS Servers**—Information about the TTS server's name, port location, and available languages.
- **MRCP TTS Default Genders**—Information about the default gender setting for the Locales specified during TTS Server provisioning.

Note You will need at least one MRCP TTS Provider for each vendor requiring TTS server installation.

Provision MRCP TTS Providers

Use the MRCP TTS Providers Configuration web page to specify information about the vendor of your TTS server.

Note After you update MRCP ASR/TTS Providers, Servers, and Groups, the corresponding provider needs to be refreshed for changes to take effect. The Unified CCX Engine does not need to be restarted. However, during a Refresh, Unified CM Telephony triggers using affected groups will fall back to the dialog group that is configured and the MRCP Provider being refreshed will go NOT_CONFIGURED until the reload is complete.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **MRCP TTS** > **MRCP TTS Provider**.

The MRCP TTS Provider Configuration web page opens. If providers are already configured, this page lists the provider name and corresponding status.

Step 2 Click **Add New** icon that displays in the tool bar in the upper, left corner of the window or the **Add New** button that displays at the bottom of the window.

Use this web page to specify the MRCP TTS Provider supported by Unified CCX.

The MRCP TTS Provider Configuration web page reopens. The Provider Name drop-down list displays the existing MRCP TTS Providers. Choose the MRCP TTS Provider supported by Unified CCX from this list.

Note
Support for High Availability and remote servers is available only in multiple-server deployments.

Step 3 Click **Add** to apply changes.

Your changes appear in the MRCP TTS Provider Configuration web page. You are now ready to provision MRCP TTS Servers.

Configure Default TTS Provider for Unified CCX System

Optionally, you can configure a default TTS provider. The Unified CCX Prompt Manager uses the default TTS provider for rendering TTS prompts if a TTS provider is not configured in the TTS Prompt. This usually happens in the case of VXML applications. For additional information on supported VXML tags for Unified CCX, see *Cisco Unified Contact Center Express Getting Started with Scripts* and for supported grammars see *Cisco Unified Contact Center Express Editor Step Reference Guide*.

To configure a default TTS provider, follow these steps.

Procedure

Step 1 Choose **System** > **System Parameters**.

Step 2 In the Default TTS Provider drop down list below Media Parameters section, select the provider you wish to be the system default. You must select only a preconfigured TTS provider as the Default TTS Provider.

Note
If you are deploying an VXML applications and the only TTS functionality you need is to play pre-recorded `.wav` files, select the **Cisco LiteSSMLProcessor** option as the Default TTS Provider. This option allows you to run SSML that has .wav file references in them.

Step 3 Click **Update**.

Provision MRCP TTS Servers

Use the MRCP TTS Servers Configuration web page to configure the TTS server's name, port location, and available languages.

You need at least one MRCP TTS Server associated with each configured provider.

Note You must have an MRCP TTS Provider defined before you can provision an MRCP TTS Server.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **MRCP TTS** > **MRCP TTS Server**.

The MRCP TTS Server Configuration web page opens, displaying a list of previously configured servers, if applicable, with the following information:

Column	Description
Computer Name	Hostname or IP address of the server in which the TTS server software is installed. **Note** TTS server deployment over WAN is not supported in Unified CCX. In other words, the TTS server should be in the same LAN where Unified CCX is. Thus, you need to specify the TTS server hostname or IP address that is local with the Unified CCX node while installing the TTS server software in this field.
Port	TCP port number used to connect to an MRCP server. Following are the different TCP Provider names: • MRCP Server • Nuance Vocalizer • Scansoft Realspeak
Provider	The MRCP TTS Provider to which this server is associated.
Status	Status or state of the subsystem.

Step 2 Click **Add MRCP TTS Server** icon that displays in the tool bar in the upper, left corner of the window or the **Add New** button that displays at the bottom of the window to provision a new MRCP ASR Server.

The MRCP TTS Server Configuration web page opens.

Step 3 Specify the following fields:

Field	Description
Server Name	Hostname or IP address of the server the MRCP TTS server software is installed.
Provider Name	Select the name of the MRCP TTS Provider to which this server is associated from this drop-down list.

Port Number	The default TCP port number used to connect to a MRCP TTS server. The port number is automatically displayed based on the provider or grammar variant that you have selected while configuring an MRCP TTS provider. Following are the different TCP Provider names along with their port numbers: • MRCP Server—554 • Nuance Vocalizer—4900 for MRCPv1 and 5060 for MRCPv2 • Scansoft Realspeak—4900
Locales	Languages supported by the TTS Provider. Select a language (or multiple languages) from the drop-down list and click **Add Language**; the selected language appears in the Enabled Language list. **Note** Use the check box to disable/enable a language.

Step 4 Click **Add** to apply changes.

Your changes appear in the MRCP TTS Server Configuration web page. You are now ready to provision MRCP TTS Default Genders.

Note
Whenever a new language is added for an MRCP Server—and if this is the first instance of this language being added for the corresponding MRCP Provider—then the default gender for that locale and for the specified provider is set to Neutral. You should check the MRCP Locales page to review the default genders that are set automatically per locale per provider. Default genders are used when a prompt for a specific locale is used without specifying any gender.

Provision MRCP TTS Default Genders

Use the MRCP TTS Default Genders Configuration web page to configure the default gender settings per Locale per Provider. TTS uses default genders when a prompt for a specific locale is used without specifying the gender.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **MRCP TTS** > **MRCP TTS Default Genders**.

The MRCP TTS Default Gender Configuration web page opens, displaying the default genders currently configured for each locale for every MRCP TTS Provider that is currently configured.

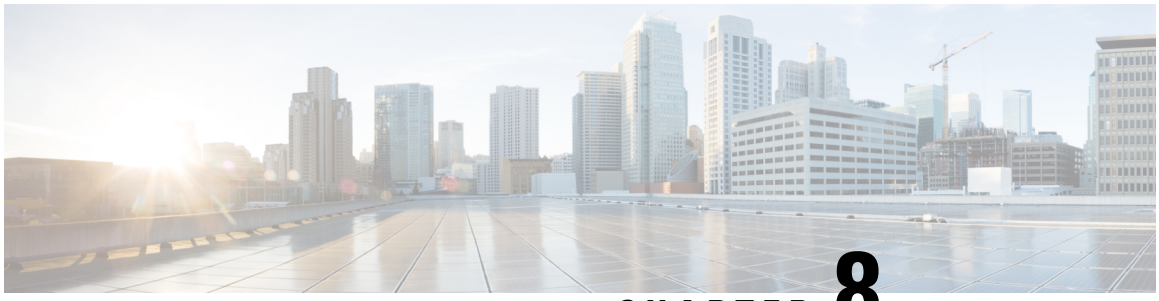
Step 2 Optionally, change the default gender setting for each locale for each provider.

Note

The Locale radio button has the Male, Female, or Neutral options. By default, the “Default Gender” is set to “Neutral” unless configured explicitly.

Step 3 Click **Update** to apply changes.

The system updates the default gender setting for each Locale per Provider.



CHAPTER 8

Provision of Unified CCX

To provision the Unified CCX subsystem, you must provision your telephony and media resources (see the Provision Telephony and Media Resources, on page 61).

Attention Do not edit users, teams and permissions in Unified Intelligence Center. The Unified CCX to Unified Intelligence Center sync runs as part of daily purge and synchronizes these settings on Unified Intelligence Center according to Unified CCX settings.

The following topics introduce the Unified CCX subsystem and explain how to provision it in the Unified CCX system:

- RmCm Provider Configuration, on page 89
- Resource Groups, on page 91
- Skills Configuration, on page 92
- Agent Configuration, on page 95
- Contact Service Queue Configuration, on page 99
- Configure Agent-Based Routing, on page 107
- Teams Configuration, on page 108

RmCm Provider Configuration

The Unified CCX Resource Manager (RM) uses a Unified CM Telephony user (called the RmCm Provider) to monitor agent phones, control agent states, and route and queue calls. For information on adding Unified CM users, see section "Access Control Group Overview" section in the *Cisco Unified Communications Manager Administration Guide* available here:

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Note The RmCm user specified through Unified CCX Administration is updated automatically in Unified CM.

RmCm Provider Modification

Note This section only applies to Unified CCX deployments with Unified CM.

Caution While Unified CM supports Unicode characters in first and last names, those characters become corrupted in Unified CCX Administration web pages for RmCm configuration and real-time reporting .

The RmCm Provider web page is a read-only page that displays the latest configured information. To access this configuration area, choose **Subsystems** > **RmCm** > **RmCm Provider** from the Unified CCX Administration menu bar. The RmCm Provider web page opens, displaying the following read-only fields.

Field	Description
Primary RmCm Provider	The hostname or IP address of the server, running CTI Manager (Unified CM that runs CTI Manager). The RmCm subsystem registers with the CTI Manager so that it can observe an agent's device when the agent logs in. When the CTI Manager fails, the RmCm subsystem registers with the second CTI Manager, if there is one configured.
Secondary RmCm Provider	The hostname or IP address of the secondary RmCm Provider.
User ID	The RmCm user ID.

To modify the RmCm Provider, click **Modify RmCm Provider Information** icon in the tool bar in the upper, left corner of the window. The Cisco Unified CM Configuration web page opens.

Associating Agent Extensions with the RmCm Provider

Note This section only applies to Unified CCX Deployments with Unified CM.

For every agent/resource created in Unified CM, make sure that the agent phone is also associated with the RmCm Provider. You do this from the Unified CM User Page for the RmCm Provider. In other words, even though you *create* the RmCm User in Unified CCX Administration, you still need to use the Unified CM interface to *associate* the RmCm user with an agent phone. These phones are the same as those associated with each agent.

Note If you use Extension Mobility (EM), ensure that the IPCC extension is associated with the Extension Mobility (EM) User Device Profile (UDP) and not to the physical phone. The Extension Mobility (EM) profile needs to be associated with the RmCm user and the physical phones that the agents may be expected to use should not be associated to the RmCm user.

Resource Groups

Resource groups are collections of agents that your CSQ uses to handle incoming calls. To use resource group-based CSQs, you must specify a resource group.

Create Resource Group

To create a resource group, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **RmCm** > **Resource Groups**.

The Resource Group web page opens with a list of configured resource groups (if any).

Step 2 Click **Add New** icon in the tool bar in the upper, left corner of the window or **Add New** button at the bottom of the window.

The Resource Group Configuration area opens.

Step 3 In the Resource Group Name field, enter a resource group name.

Enter a name that identifies the resource group to which you want to assign agents (for example, “Languages”).

Step 4 Click **Add**.

The Resource Groups page opens displaying the resource group name in the Resource Group Name column.

Modify Resource Group Name

To modify a resource group name, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **RmCm** > **Resource Groups**.

The Resource Group web page opens.

Step 2 In the Resource Group Name column, click the resource group that you want to modify.

The Resource Group Configuration area opens.

Step 3 Type the name of the resource group in the Resource Group Name text field.

Step 4 Click **Update** to apply the modifications.

The Resource Groups area opens, displaying the modified resource group name in the Resource Group Name column.

Delete Resource Group

When you delete a resource group, the resource group is removed automatically if it is not associated with any agents and CSQs. If the resource group is associated with any agents or CSQs and if you click **Delete**, you will be directed to another web page, where you can see a list of the associated CSQs and agents, and you are prompted to confirm whether you want to delete the same.

Tip To delete resource groups, you can use the following procedure or open a Resource Group and click the **Delete** icon or button in the Resource Group Configuration web page.

To delete a resource group, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **RmCm** > **Resource Groups**.

The Resource Group web page opens.

Step 2 Click **Delete** icon next to the name of the Resource Group that you want to delete.

A dialog box opens, warning that the resource group is about to be permanently deleted.

Step 3 Click **Continue**.

The resource group is deleted.

Skills Configuration

Skills are customer-definable labels assigned to agents. All the Unified CCX license packages can route incoming calls to agents who have the necessary skill or sets of skill to handle the call.

Create a Skill

To create a skill, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **RmCm** > **Skills**.

The Skills web page opens to display the Skill Name (customer-definable label assigned to an agent), if configured.

Step 2 Click **Add New** icon in the tool bar in the upper, left corner of the window or **Add New** button at the bottom of the window.

Note
When the system reaches the maximum number of skills that can be created, the **Add New** icon or button no longer appears.

The Skill Configuration web page opens.

Step 3 In the Skill Name field, enter a description of a relevant skill (for example, French).

Note
Unified CCX does not support the following special characters for Skill name.

Table 1: Unsupported Characters in Skill and CSQ Name

Symbol	Description	Symbol	Description
`	apostrophe	~	tilde
!	exclamation mark	@	at sign
$	dollar	%	percent
^	circumflex	&	ampersand
*	asterix	()	parentheses
=	equals sign	[]	square brackets
{}	braces	;	semicolon
\	backslash	?	question mark
"	double quotes	<>	angle brackets
'	single quote	+	add
|	pipe	:	colon
.	period	/	forward slash
,	comma	#	hash

Step 4 Click **Add**.

The Skills web page opens, showing the skill in the Skill Name column and the total number of skills that exist in the system. You can add a maximum of 150 skills.

Modify a Skill Name

To modify a skill name, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **RmCm** > **Skills**.

The Skills web page opens.

Step 2 In the Skill Name column, click the skill that you want to modify.

The Skill Configuration web page opens.

Step 3 Modify the name of the skill in the Skill Name text field.

Note
Unified CCX does not support special characters for the skill name. To see the list of unsupported characters, see Table 1: Unsupported Characters in Skill and CSQ Name, on page 93.

If you have upgraded to Unified CCX Release 12.5(1) and above and are facing errors when making changes to the Skill name, remove the special characters and modify the skill name.

Step 4 Click **Update** to apply the modifications.

The Skills Configuration summary opens, displaying the modified skill name in the Skill Name column.

Delete a Skill

When you delete a skill, the skill is removed automatically if it is not associated with any agents and CSQs. If the skill is associated with any agents or CSQs and if you click **Delete**, you are directed to another web page, where you can see a list of the associated CSQs and agents, and you are prompted to confirm whether you want to delete the same.

Tip To delete a skill, you can use the following procedure or open a skill and click **Delete** icon or button in the Skills Configuration web page.

To delete a skill, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **RmCm** > **Skills**.

The Skills web page opens.

Step 2 Click the **Delete** icon next to the name of the skill that you want to delete.

A dialog box opens, warning that the skill is about to be permanently deleted.

Step 3 Click **Continue**.

The skill is deleted.

Agent Configuration

Once the end users in Cisco Unified Communications[1] are defined as agents, the list of agents and their associated Unified CCX devices are displayed in the **Subsystems** > **RmCm** > **Resources** page. These agents are also called resources. After you create a resource group, you can assign agents (resources) to that group.

You can add skills to agents once the skills have been created. You can also select the competence level of agents in assigned skills. Competence level indicates agent level of expertise in that skill.

You can assign resource groups and skills to agents either individually or in bulk. The bulk option enables you to assign skills and resource groups to multiple agents at the same time.

Once you assign agents to resource groups and skills, you can create a CSQ.

Warning After an agent is added, wait for 10 minutes for Unified CCX to automatically synchronize or force synchronization before the agent can sign in to Cisco Finesse.

The maximum allowed length of an agent's IPCC Extension is 15.

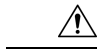
Special Characters

- Unified CM supports the use of special characters—square brackets ([ ]), dollar ($), ampersand (&), single quotes (' '), colon (:), angle brackets(< >), forward slash (/), question mark (?), backward slash (\), parentheses ({ }), double quotes(" "), hash(#), percent (%), semicolon (;), comma (,), pipe (|), tilde(~) and space in a user ID when you configure end users. However, Unified CCX restricts the use of these characters when you configure end users as agents or supervisors.
- Unified CCX does not support the use of special characters—square brackets ([ ]), dollar ($), ampersand (&), single quotes (' '), colon (:), angle brackets(< >), forward slash (/), question mark (?), backward slash (\), parentheses ({ }), double quotes(" "), hash(#), percent (%), semicolon (;), comma (,), pipe (|), tilde(~), period (.).
- With Cisco Finesse for Unified CCX, agent IDs (or usernames) are case-sensitive and can contain letters, numbers, hyphens (-), underscores (_), at (@), and periods (.) They cannot begin or end with a period or contain two periods in a row. Finesse agent usernames are restricted to 7-bit printable ASCII characters (any of the 94 characters with the numeric values from 33 to 126). They do not support double quotes (" "), forward slash (/), backward slash (\), square brackets ([ ]), colon (:), semicolon (;), pipe (|), equal to (=), comma (,), add (+), star (*), question mark (?), angle brackets (< >), hash (#), percent (%), SPACE and the characters restricted by Unified Communications Manager and Unified CCX.
- Finesse agent passwords are restricted to 7-bit printable ASCII characters (any of the 94 characters with the numeric values from 32 to 126). They do not support control characters (for example, Tab) or international characters.
- Agent Alias name now supports the use of SPACE in the name.

[1] Unified Communications users in a Unified CM deployment refers to a Unified CM user.

Implications of Deleting Agents in Unified CM

If you modify an agent's record in Unified CM (for example, changing the Unified CCX extension or deleting the agent), ensure to refresh the user page on Unified CCX Administration interface so that the agent information in the Unified CCX RmCm subsystem is updated. Choose **Subsystems** > **RmCm** > **Resources** option to update the Unified CCX information in the Unified CCXAdministration any time. If you change the Unified CCX extension of an agent who is currently logged in, the agent will continue to use the old extension until the agent logs off. The agent must log off and then log back in to the Cisco Finesse desktop to get the new extension. When Unified CCX performs an agent sync and detects that the agent no longer exists in Unified CM, the contact is marked as inactive in the **Resource** table of the Unified CCX Historical Reporting Database (db_cra). The resource is not deleted as the resource information is referenced for the HR reports.



Caution Deleting Inactive Agents removes the agent details and records from the Historical Reporting Database, and HR reports will not display historical information of these agents.

If Unified CM connection errors have occurred, all agents will not be visible to Unified CCX. In this case, Unified CCX interprets these agents as deleted agents. As a result, the Inactive Agents list will not be accurate. When the errors are resolved, click **Inactive Agents** again to see an accurate list.

Assign Resource Groups and Skills to One Agent

To assign a resource group and skills to an individual agent, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **RmCm** > **Resources**.

The Resources web page opens.

Note
Only agents or supervisors who have assigned Unified CCX extensions are displayed in the list of resources in the Resources area.

Step 2 Click the name of the agent in the Resource Name column.

The Resource Configuration web page opens.

Step 3 Specify the following fields.

Field	Description
Resource Name	Name of the agent (display only).
Resource ID	Unique identifying number of the agent (display only). This is the alpha-numeric user id assigned in the Unified CM End User Configuration page.
Unified CCX Extension	Unified CCX Extension assigned to the resource group (display only). This is the IP Phone extension assigned to the user from the Unified CM End User Configuration page as IPCC Extension.

Field	Description
Resource Group	A resource group with which to associate the agent (optional).
Automatic Available	Accept the default (**Enabled**) to automatically put the agent into the Available or Ready state after the agent finishes a call and disconnects. **Note** When a logged on agent in Ready, Not Ready, or Work state answers a call, the agent state is subject to the Automatic Available setting.
Assigned/Unassigned Skills	Select one or more skills from the Unassigned Skills list and click < to add the skills to the Assigned Skills List. Select one or more skills from the Assigned Skills List and click > to remove skills from the Unassigned Skills list. You can assign up to 50 skills to the agent.
Competence Level	Select a skill from the Assigned Skills list and choose a number from the Competence Level drop-down menu Changes the competence level of an assigned skill (1 = Beginner, 10 = Expert). **Note** You can change the competency level one skill at a time, only. You cannot change skill competency level as a bulk procedure.
Team	A group of agents who assign the team to which the resource belongs.
Agent Alias	Agent alias is the name used instead of the agent ID when an agent chats with a customer. This option is available only when Finesse is used by the chat agent.

Step 4 Click **Update** to apply the changes.

The Resources area of the RmCm Configuration summary web page opens, and the agent is now assigned to the resource group and skills (if skills were assigned).

Assign Resource Groups and Skills to Multiple Agents

To assign resource groups and skills to agents in bulk, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, select **Subsystems** > **RmCm** > **Assign Skills**.

The Assign Skills summary web page opens.

Tip
Only agents or supervisors who have assigned Unified CCX extensions are displayed in the list of resources in the Resources area.

Step 2 In the Resource Name column, check the check box beside each agent to whom you want to assign set of same resource group and skills. In the Resource Name column, check the check box next to each agent you want to assign set of same resource group and skills.

Note
You can check the **Select All** check box to select all agents.

The Skill summary web page shows the total number of skills created.

Step 3 Click **Add Skill** icon that displays in the tool bar in the upper, left corner of the window or the **Add Skill** button that displays at the bottom of the window.

The Add Skill web page opens.

Step 4 Specify the following fields.

Field	Description
Resource Group	To assign a resource group to all the selected agents, choose a resource group from the Resource Group drop-down menu.
Skills to Add	Select one or more skills from the Skills list and click < to add the skills to the Skills to Add List. **Note** The Skills to Add list contains all skills, not just the skills that agents already have.
Skills	List of the available skills.
Competence Level	Select a skill from the Assigned Skills list and choosing a number from the Competence Level drop-down menu

Step 5 Click **Update** to apply the changes.

The Assign Skills area of the RmCm Configuration web page opens, and the agents are now assigned to the resource group and their skills (if skills were assigned).

Remove Skills from Agents

Note If a resource is not assigned a skill that you attempt to remove, the resource is not updated. However, the system will still generate a related message.

To remove skills from agents, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **RmCm** > **Assign Skills**.

The Assign Skill summary web page opens.

Step 2 In the Resource Name column, click the check box next to the agent you want to remove skills from.

Note
You can click **Select All** check box to select all agents.

Step 3 Click **Remove Skill** icon that displays in the tool bar in the upper, left corner of the window or the **Remove Skill** button that displays at the bottom of the window.

The Remove Skill Configuration web page opens.

Step 4 Remove skills by choosing one or more skills from the Skills list and clicking > to move the skills to the Skills to Remove list.

Step 5 Click **Update** to apply the changes.

The Assign Skills area of the RmCm Configuration web page opens, and the agents are no longer assigned to the skills.

Contact Service Queue Configuration

The Contact Service Queue (CSQ) controls incoming calls by determining where an incoming call should be placed in the queue and to which agent the call is sent.

After you assign an agent to a resource group and assign skills, you need to configure the CSQs.

You assign agents to a CSQ by associating a resource group or by associating *all* skills of a particular CSQ. Agents in the selected resource group or who have *all* the selected skills are assigned to the CSQ.

Skills within the CSQ can be *ordered*. This means, when resources are selected, a comparison is done based on the *competency* level (highest for “most skilled” and lowest for “least skilled”) of the first skill in the list. If there is a “tie” the next skill within the order is used, and so on.

Skills within the CSQ can also be *weighted*. The weight value is an integer from 1 to 1000. Each competency level is multiplied by the skill's associated weight, and a final comparison is done on the sum of all the weighted skill competencies (highest value for “most skilled” and lowest for “least skilled”). The maximum number of CSQs in the system depends on the type of server on which the engine is running.

For more information, see the Unified CCX Data Sheets at https://www.cisco.com/c/en/us/products/contact-center/unified-contact-center-express/datasheet-listing.html

Each agent can belong to up to 25 CSQs. To ensure that agents are not assigned to more than 25 CSQs, click **Resources** submenu option in the RmCm Configuration web page, and click **Open Resources Summary Report** icon. The report opens, listing each agent and the number of CSQs to which the agent belongs. If the agent belongs to more than 25 CSQs, modify the skills and resource groups to which the agent is assigned so that the agent does not belong to more than 25 CSQs.

Create a Contact Service Queue

To create a new CSQ and assign agents, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **RmCm** > **Contact Service Queues**.

The Contact Service Queues web page opens.

Use this web page to view the following fields:

Field	Description
Name	Name of the resource or skill group.
Contact Queuing Criteria	Algorithm used to order the queued calls (contacts).
Resource Pool Selection Model	The resource selection criteria chosen for this CSQ.
Resource Pool	The skills or resource group used for this CSQ.
CSQ Type	The type of the CSQ.
Delete	Deletes the selected CSQ.

Step 2 Click **Add New** icon that displays in the tool bar in the upper, left corner of the window or the **Add New** button that displays at the bottom of the window.

The Contact Service Queue Configuration web page opens.

Note
If this link does not appear on the page, it means that the system has reached the maximum number of CSQs that can be created. The CSQ Summary page displays the total number of created CSQs.

Step 3 Use the Contact Service Queue Configuration web page to specify the various fields. For more information on the fields, see **Contact Service Queue Configuration Web Page**.

Step 4 Click **Next**.

The second Contact Service Queue Configuration area opens with the newly-assigned CSQ Name.

Step 5 Select an option from the Resource Selection Criteria drop-down menu.

Note
The Resource Pool Selection Model settings determine the options available in this drop-down menu.

- **Longest Available**—Selects the agent who has been in the Available state for the longest amount of time.
- **Most Handled Contacts**—Selects the agent who has handled the most calls.
- **Shortest Average Handle Time**—Selects the agent who generally spends the least amount of time talking to customers.
- **Most Skilled**—Used for expert agent call distribution. Selects the agent with the highest total competency level. The total competency level is determined by adding the agent's competency levels for each of their assigned skills that are also assigned to the CSQ.

- Example 1: If Agent1 is assigned Skill1(5), Skill2(6), and Skill3(7) and CSQ1 specifies Skill1(min=1) and Skill3(min=1), the total competency level for Agent1 for CSQ1 is 12.
- Example 2: If Agent1 is assigned Skill1(5) and Skill2(6) and Skill3(7) and CSQ1 specifies Skill1(min=1), only, the total competency level for Agent1 for CSQ1 is 5.

- **Least Skilled**—Used for expert agent call distribution. Selects the agent with the lowest total competency level. The total competency level is determined by adding the agent's competency level in each assigned skill.
- **Most Skilled by Weight**— Used for expert agent call distribution. Selects the agent with the highest total competency level multiplied by the skill's associated weight.
- **Least Skilled by Weight**—Used for expert agent call distribution. Selects the agent with the lowest total competency level multiplied by the skill's associated weight.
- **Most Skilled by Order**— Used for expert agent call distribution. Selects the agent with the highest total competency level in the ordered list.
- **Least Skilled by Order**— Used for expert agent call distribution. Selects the agent with the lowest total competency level in the ordered list.

Note
If two or more agents have equal competency level, the selection automatically defaults to **Longest Available** selection criteria.

Step 6 Specify the following settings, as necessary:

Note
The Resource Pool Selection Model setting determines the availability of these options.

a) Use the Select Skills list to highlight the skills you want; click the **Add** button next to the list.
b) Specify a Minimum Competence Level for the skills assigned to the CSQ. Depending on the Resource pool criteria you chose, specify a Weight value between 1 and 1000.
c) If the Resource Selection Criteria is Most Skilled by Order or Least Skilled by Order, use the arrow icons to order the skills by moving them up or down in the list.

Note
Use the **Delete** icon next to a skill to delete that skill from the Skills Required list.

Step 7 If you selected one of the Least/Most Skilled options as shown in the list below for the Resource Selection Criteria, you can view the agent order using **Show Resources** icon or button.

Note
The order of the agents determines the priority, with the agent at the top of the list having the highest priority.

To change the order of the agents belonging to the CSQ, you should modify the skill set of the agents. The Least/Most Skilled Resource Selection Criteria option comprises the following:

a) Most Skilled
b) Least Skilled
c) Most Skilled by Order
d) Least Skilled by Order
e) Most Skilled by Weight
f) Least Skilled by Weight

Step 8 If you selected *Resource Groups* as the Resource Pool Selection Model on the previous page, follow these steps:

a) Select an option from the Resource Selection Criteria drop-down menu.

- **Longest Available**—Selects the agent who has been in the Available state for the longest amount of time.
- **Linear**—Selects the next available agent with the highest priority, as determined by the agent order in the Resources list.
- **Circular**—Selects the next available agent with the highest priority, based on the last agent selected and the agent order in the Resources list.
- **Most Handled Contacts**—Selects the agent who has handled the most calls.
- **Shortest Average Handle Time**—Selects the agent who generally spends the least amount of time talking to customers.

b) Choose the resource group for this CSQ from the Resource Group drop-down menu.
c) Click **Show Resources** icon to show all agents who meet the specified criteria.
d) If you selected *Linear* or *Circular* as the Resource Selection Criteria, if necessary, rearrange the order of agents in the Resources list by highlighting an agent and using the up and down arrows to move the agent in the list.
e) Click **Add** to apply changes and update the system.

The new CSQ is now displayed, and all agents who belong to the resource group or all selected skill groups are now a part of this CSQ.

Contact Service Queue Configuration Web Page

Contact Service Queue Configuration web page:

Field	Description
Contact Service Queue Name	Enter a meaningful name that is concise, yet easy to recognize (for example, Language Experts). This is a mandatory field. **Note** Unified CCX does not support special characters for the Call Service Queue name. To see the list of unsupported characters, see Table 1: Unsupported Characters in Skill and CSQ Name, on page 93.
Contact Service Queue Type	Display only. Voice—Agents in this CSQ can handle inbound and outbound voice calls.
Contact Queuing Criteria	Display only. Displays the criteria used for queuing the contacts. For example, First In, First Out (FIFO).

Field	Description
Automatic Wrapup	Determines whether agents handling calls that are routed through this CSQ automatically enter the Wrapup state when a call ends. This field is mandatory. Options are: • Enabled—Agents associated to a CSQ that has the Automatic Wrapup option enabled, enter the Wrapup state automatically when on a call. CSQ ends. If agents are associated to a CSQ that has the Automatic Wrapup option disabled handle transferred calls that were originally delivered by a CSQ that has Automatic Wrapup enabled, they also enter the Wrapup state automatically when a call ends. • Disabled (default)—Agents enter Ready or Not Ready state when a call ends, depending on the Automatic Available setting.
Wrapup Time	Determines the length of the Wrapup state for this CSQ when a call ends. Options are: • Enabled button with Seconds field—The Seconds field specifies the length of the Wrapup state phase. • Disabled—No limit on how long the agent can stay in the Wrapup state.
Resource Pool Selection Model	Select one of the following options from the drop-down menu: • Resource Skills—To create a skills-based CSQ. • Resource Group—To create a resource group-based CSQ. This is a mandatory field.
Service Level	The target maximum number of seconds a call is queued before it is connected to an agent. This is a mandatory field.
Service Level Percentage	The target goal for percentage of contacts that meet the service level. This is a mandatory field. For example, a call center that has a service level of 20 and a service level percentage of 80 percent has a goal of answering 80 percent of its calls within 20 seconds.

Field	Description
Prompt	.wav prompt file to associate with the CSQ. You can retrieve the prompt file that you select from this **Prompt** drop-down list using the Create CSQ Prompt Step in the Unified CCX Editor. In the Unified CCX Editor, Create CSQ Prompt Step is one of the steps used to create scripts for the Unified CCX engine. In this step, you need to give the CSQ ID that is displayed as the last number in the AppAdmin address bar of the web page that is displayed when you click on an existing CSQ. For example, the CSQ ID will be 3 if the address bar of an existing CSQ Configuration web page ends with "&csdid=3". When you run the script, it will return the prompt associated with the specific CSQ ID. Use the Play Prompt Step within the script to play this prompt. See the *Cisco Unified CCX Editor Step Reference Guide* for detailed information on scripting. **Note** The Prompt field is available only if you have licensed the Cisco Unified CCX Enhanced or Premium product package.

Modify a Contact Service Queue

Note Changes take effect when all agents affected by the changes have left the Ready state. Emails Contact Service Queues cannot be modified. It is for display only.

To modify an existing CSQ, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **RmCm** > **Contact Service Queues**.

The Contact Service Queues web page opens.

Step 2 In the Name list, click the CSQ that you want to modify.

The Contact Service Queue Configuration page opens.

Step 3 Modify the Contact Service Queue Configuration information as necessary.

Note
If you change an existing CSQ name, the old name still exists in the HR reports and the CSQ is not removed even if all the data is purged.

Step 4 Click **Next** icon that displays in the tool bar in the upper, left corner of the window or the **Next** button that displays at the bottom of the window to view and update the remaining fields.

Step 5 Click **Update** icon in the top of the window or the **Update** button that displays at the bottom of the window to apply the modifications.

Note
Ensure that the **Resource Selection Criteria** is changed only when there are no agents signed in. If there are active agents, these changes take effect only when all the active agents sign out and sign in again.

Delete a Contact Service Queue

When you delete a CSQ, any skills or resource groups assigned to that CSQ are automatically removed from the CSQ, and any application using that CSQ can no longer access it. Before deleting the CSQ, change the applications to use a different CSQ. If the application is using a CSQ when the CSQ is deleted, new incoming calls will get an error and existing queued calls will not be routed to agents.

Note
- Existing Email Contact Service Queues can be deleted.

To delete a CSQ, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **RmCm** > **Contact Service Queues**.

The Contact Service Queues web page opens.

Step 2 Click the **Delete** icon next to the name of the CSQ that you want to delete.

Note
You can also delete a CSQ from its Contact Service Queue Configuration page using the Delete icon or button.

Resource Pool Selection Criteria: Skills and Groups

The resource selection criteria available for CSQs with Resource *Skills* is different from that of CSQs with Resource *Groups*.

Example—In a banking application with two skills (Banking and CreditCard) and one Resource Group (General Queries), assume that the following agents, skills, and resource groups are defined:

Agent ID	Assigned Skills	Resource Group
Agent1	Banking (Competence Level 10) CreditCard (Competence Level 6)	GeneralQueries
Agent2	Banking (Competence Level 5) CreditCard (Competence Level 10)	GeneralQueries
Agent3	None	GeneralQueries

In addition, suppose you had the following Contact Service Queue information defined:

Table 2: Agent Skill and Resource Group Settings

CSQ Name	Resource Pool Selection Model	Resource Selection Criteria	Skill/Competence	Available Agents
CSQ1	Resource Skills	Most Skilled	BankingMinimum competency: 5	Agent1 Agent2
CSQ2	Resource Skills	Most Skilled	CreditCardMinimum competency: 5	Agent1 Agent2
CSQ3	Resource Group	Longest Available	GeneralQueries	Agent1 Agent2 Agent3

In this scenario, if a caller calls with a question about CreditCard information and there are no CSQs currently available with CreditCard skills (that is, Agent1 and Agent2), there is a possibility for Agent3—who has no CreditCard skill—to get selected as the Longest Available Agent.

To avoid such a situation, you could design the script to always look into CSQ2 for available agents since it has the highest competency of 10 for CreditCard, and agent selection here is based on most skilled.

Note If two or more agents have equal competency level, the selection automatically defaults to **Longest Available** selection criteria.

Resource Skill Selection Criteria within a Contact Service Queue

Resource selection *within* a CSQ is based on the resource competency levels of the skills associated to the CSQ. You can choose between the most and least skilled.

The Unified CCX system defines a Level 10 competency to be the highest skill level, while a Level 1 denotes the lowest skill level. When more than one skill is involved, each skill is given the same weight, meaning no preference is given to any skill. A comparison is performed on the sum of all the competency levels for the associated skills. (Skills assigned to resources but not associated to the CSQ are ignored.) In the case of a tie when skill competencies are equal, the resource that has been ready for the longest amount of time will be chosen.

The following table provides examples of how Unified CCX selects resources within a CSQ.

Table 3: Resource Skill Selection Criteria

Example	CSQ Skills	Agent Competency Levels	Sequence Agents Become Ready	Selection Order
Most skilled resource selection model	Technical Support	Agent A = 10 Agent B = 10 Agent C = 5	A, B C	A, B, C
			C, A, B	A, B, C
			A, C, B	A, B, C
			C, B, A	B, A, C
Least skilled resource selection model	Technical Support	Agent A = 10 Agent B = 10 Agent C = 5	A, B, C	C, A, B
			C, A, B	C, A, B
			A, C, B	C, A, B
			C, B, A	C, B, A
Note The ordering in the two examples above are not opposite because the selection criteria has changed from most to least skilled—when competency levels are equal, both selection models choose the resources that have been available for the longest time.				
Most skilled resource selection model	SalesSupport	Agent A = Sales (10) Support (5) Agent B = Sales (5), Support (10) Agent C = Sales (5) Support (1)	A, B, C	A, B, C
			C, A, B	A, B, C
			A, C, B	A, B, C
			C, B, A	B, A, C
Least skilled resource selection model	SalesSupport	Agent A = Sales (10) Support (5) Agent B = Sales (5), Support (10) Agent C = Sales (5) Support (1)	A, B, C	C, A, B
			C, A, B	C, A, B
			A, C, B	C, A, B
			C, B, A	C, B, A

Configure Agent-Based Routing

Agent-based routing provides the ability to send a call to a *specific* agent, rather than any agent available in a CSQ.

Use the Agent Based Routing Settings web page to configure system-wide parameters to be used in an agent-based routing application.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **RmCm** > **Agent Based Routing Settings**. The Agent Based Routing Settings area opens.

Note
The Agent Based Routing Settings are available only if you are using Unified CCX Enhanced or Premium license packages.

Step 2 Specify the following fields:

Field	Description
Automatic Wrapup	Determines whether agents handling calls that are routed through this CSQ automatically enter the Automatic Wrapup state when a call ends. • Enabled—Agents associated to a CSQ that has the Automatic Wrapup option enabled enter the Wrapup state automatically when on a call. If agents are associated to a CSQ that has the Automatic Wrapup option disabled handle transferred calls that were originally delivered by a CSQ that has Automatic Wrapup enabled, they also enter the Wrapup state automatically when a call ends. • Disabled (default)—Agents enter Ready or Not Ready state when a call ends, depending on the Automatic Available setting.
Wrapup Time	Determines if agents automatically enter Wrapup when a call ends. • Enabled button with seconds field—Controls how long the agent can stay in the Wrapup state if Automatic Wrapup is enabled. The seconds field specifies the Wrapup time length. • Disabled (default)—No limit of how long the agent can stay in the Wrapup state if Automatic Wrapup is enabled.

Step 3 Click **Save** icon that displays in the tool bar in the upper, left corner of the window or the **Save** button that displays at the bottom of the window to apply changes.

Wrap-Up Data Usage

Contact centers use wrap-up data to track the frequency of activities or to identify the account to which a call is charged, and other similar situations. Like reason codes, wrap-up data descriptions are set up by your system administrator to reflect the needs of your contact center. By default this feature is disabled.

Teams Configuration

A *team* is a group of agents who report to the same Supervisor. A team can have one primary Supervisor and optional secondary Supervisors. A Supervisor can also monitor CSQs that are assigned to the team being supervised.

Barge-in is when a Supervisor joins an existing call between an agent and a customer.

Intercept is when the Supervisor joins a call and drops the agent from the call.

A *default team* is automatically created by the system and cannot be deleted. If agents are not assigned to any team, they belong to the default team. When an agent is assigned to a team, the team Supervisor can barge-in and intercept any call being handled by the agent.

Note Before creating a team, you must set up Supervisors using the User Management page.

Note The Advanced Supervisor Capability of Queue Management is removed when:

- Supervisor is not associated to any team.
- Supervisor is not the primary or secondary Supervisor of any team.
- There are no CSQs assigned to the teams associated to the Supervisor.

Note A team that accesses Live Data reports is limited to 50 agents.

Assign Supervisor Privilege to a User

Perform the following procedure to assign supervisor privilege to a user.

Procedure

Step 1 From the Unified CCX Administration menu, choose **Tools > User Management > User View**.

The User Configuration page displays the list of all users.

Step 2 Click the user to whom you want to assign supervisor capability.

The User Configuration page displays information about that user. In the Capabilities section, the left pane displays the list of assigned capabilities and the right pane displays the list of capabilities.

Step 3 Using the left arrow, assign Supervisor capability.

Step 4 Click **Update** to save your changes.

Agents, who have logged in must logout and login again to use supervisor specific features.

For agents with chat or email skill, who have logged in, it may take maximum of 30 mins to reflect the change.

Create Teams

Use the Teams area of the RmCm Configuration web page to create or associate teams with various agents, CSQs, and supervisors.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **RmCm** > **Teams**.

Step 2 Click **Add New** icon that displays in the tool bar in the upper left corner of the window or the **Add New** button at the bottom of the window.

The Team Configuration page appears.

Step 3 Enter the **Team Name**.

Step 4 Select the **Primary Supervisor** from the drop-down list.

Step 5 (Optional) Select the secondary supervisor name from the **Available Supervisors** list and use the arrow icon to move it into the **Secondary Supervisors** list.

Step 6 (Optional) To add an agent to this team, select an agent name in the **Available Resources** list and use the arrow icon to move it into the **Assigned Resources** list.

Step 7 (Optional) Select the CSQ name in the **Available CSQs** list and use the arrow icon to move it into the **Assigned CSQs** list to add the CSQ to this team.

Step 8 In the **Team Settings** section, specify the following information:

Parameter Name	Parameter Value	Global Settings
Change Agent State to Not Ready when Agent Busy on Non ACD Line	Radio button that enables the agent state to change from the Ready state to the Not Ready state when the monitored Non ACD lines are used for Incoming or Outgoing calls. The options are: • Enable—Enables the state change of the agent in the team. • Disable (default)—Disables any state change of the agent in the team. • Allow team settings to override global settings—A check box to override the global settings. The global settings is available at **System** > **System Parameters** > **Agent Settings**. **Note** When you select the check box, a popup message reminds you that your team settings are different from the global settings. Click **OK** to proceed or **Cancel** to discard the changes. When you click OK, the team level settings override the global settings.	Displays the global settings.

Parameter Name	Parameter Value	Global Settings
Auto Answer	Enables the incoming calls to be auto answered. The options are: • Enable with Zip tone—For agents, belonging to the team, all the incoming calls to the IPCC extension is auto answered provided the agent is in the Ready state in the Cisco Finesse desktop. A zip tone plays to alert the agent. • Enable without Zip tone—For agents, belonging to the team, all the incoming calls to the IPCC extension is auto answered provided the agent is in the Ready state in the Cisco Finesse desktop. The zip tone does not play to alert the agent. • Disable (Default)—Auto answer is not enabled.	

Note

- To configure **Change Agent State to Not Ready when Agent Busy on Non ACD Line** at a team level, you must install UCCX 12.5(1) SU1 ES01.
- This functionality is applicable only for the agents and not for the supervisors of the team.

Step 9 Click **Save** to apply changes or **Cancel** to exit.

Modify Teams

Use the Teams area to modify the supervisors, agents, CSQs, or auto answer configuration on an existing Team.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **RmCm** > **Teams**.

Step 2 Click a name in the **Team Name** column.

The Team Configuration page appears.

Step 3 Select the **Primary Supervisor** from the drop-down list.

Step 4 (Optional) Select the secondary supervisor name from the **Available Supervisors** list and use the arrow icon to move it into the **Secondary Supervisors** list.

To remove the secondary supervisor name from this team, select the supervisor name in the **Secondary Supervisors** list and use the arrow icon to move it into the **Available Supervisors** list. This supervisor now belongs to the default team.

Step 5 (Optional) Select an agent name in the **Available Resources** list and use the arrow icon to move it into the **Assigned Resources** list to add an agent to this team.

To remove an agent from this team, select an agent name in the **Assigned Resources** list and use the arrow icon to move it into the **Available Resources** list. This agent now belongs to the default team.

Step 6 (Optional) Select the CSQ name in the **Available CSQs** list and use the arrow icon to move it into the **Assigned CSQs** list to add the CSQ to this team.

To remove a CSQ from this team, select a CSQ name in the **Assigned CSQs** list and use the arrow icon to move it into the **Available CSQs** list. This CSQ now belongs to the default team.

Step 7 In the **Team Settings** section, specify the following information:

Parameter Name	Parameter Value	Global Settings
Change Agent State to Not Ready when Agent Busy on Non ACD Line	Radio button that enables the agent state to change from the Ready state to the Not Ready state when the monitored Non ACD lines are used for Incoming or Outgoing calls. The options are: • Enable—Enables the state change of the agent in the team. • Disable (default)—Disables any state change of the agent in the team. • Allow team settings to override global settings—A check box to override the global settings. The global settings are available at **System** > **System Parameters** > **Agent Settings**. **Note** When you select the check box, a popup message reminds you that your team settings are different from the global settings. Click **OK** to proceed or **Cancel** to discard the changes. When you click OK, the team level settings override the global settings.	Displays the global settings.
Auto Answer	Enables the incoming calls to be automatically answered. The options are: • Enable with Zip tone—For agents, belonging to the team, all the incoming calls to the IPCC extension is auto answered provided the agent is in the Ready state in the Cisco Finesse desktop. A zip tone plays to alert the agent. • Enable without Zip tone—For agents, belonging to the team, all the incoming calls to the IPCC extension is auto answered provided the agent is in the Ready state in the Cisco Finesse desktop. The zip tone does not play to alert the agent. • Disable (Default)—Auto answer is not enabled.	

Note
To configure **Change Agent State to Not Ready when Agent Busy on Non ACD Line** at a team level, you must install UCCX 12.5(1) SU1 ES01.

Step 8 Click **Save** or **Update** to apply changes, **Cancel** to exit or **Delete** to delete this team.

Delete a Team

Use the Teams area of the RmCm Configuration web page to delete an existing Team.

Procedure

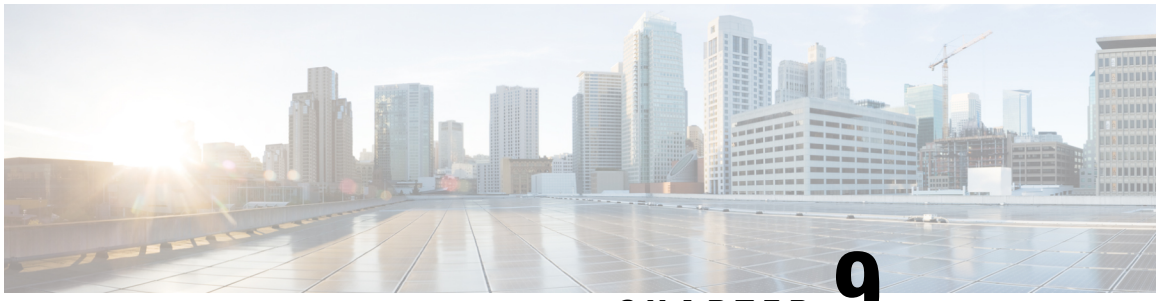
Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **RmCm** > **Teams**.

The Teams web page opens.

Step 2 Click the **Delete** icon beside the Team Name icon you want to delete.

The system prompts you to confirm the delete.

Step 3 Click **OK**.



CHAPTER 9

Provision of Additional Subsystems

- About Additional Subsystems, on page 115
- Provision of HTTP Subsystem, on page 115
- Provision of Database Subsystem, on page 117
- Provision eMail Subsystem, on page 120

About Additional Subsystems

Your Unified CCX system may include some or all of the following additional subsystems:

- The HTTP subsystem—The Unified CCX system uses the HTTP subsystem to enable Unified CCX applications to respond to requests from a variety of web clients, including computers and IP phones.
- The Database subsystem—The Unified CCX system uses the Database subsystem to enable Unified CCX applications to interact with customer-provided enterprise database servers to make database information accessible to contacts.
- The eMail subsystem—The Unified CCX system uses the eMail subsystem to communicate with your email server and enable your applications to create and send email.

If you plan to run applications that use any of the additional Unified CCX subsystems included in your Unified CCX package, you should now provision those subsystems. The Unified CCX system uses these additional subsystems to communicate with supporting systems such as web servers, database servers, and email servers.

Note You need to provision a particular subsystem only if you are using Unified CCX applications that require it.

Provision of HTTP Subsystem

Note The HTTP subsystem is available if your system has a license installed for one of the following Cisco product packages: Unified IP IVR or Unified CCX Premium.

The Unified CCX system uses the HTTP subsystem to enable Unified CCX applications to respond to requests from a variety of web clients, including computers and IP phones.

Note If you are not using HTTP applications, you do not need to provision the HTTP subsystem.

The Unified CCX system uses subdirectories in the Unified CCX installation directory to store text substitution, eXtensible Style Language (xsl) templates, static and dynamic web pages, and Java Servlet Pages (JSPs).

Note Use the Document Management page to upload these documents.

To provision the HTTP subsystem, you need to provision HTTP triggers. HTTP applications use triggers to activate the application in response to an incoming HTTP message.

Note You cannot change the TCP/IP port numbers used by the HTTP subsystems or triggers in Unified CCX.

Configure HTTP Triggers

You need to create an application using **Applications** > **Application Management** menu from the Unified CCX Administration menu bar. After you create an application, you can configure HTTP triggers for the application using the following procedure.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **HTTP**.

The HTTP Trigger Configuration web page opens.

Step 2 Specify the following fields:

Field	Description
URL	The relative URL. For example: `/hello`
Application Name	Select an application for which you want to add a HTTP trigger from this list box.
Sessions	The maximum amount of simultaneous sessions (instances) that the application can handle.
Enabled	Click the required radio button to accept - **Yes** (the default). **Note** If you disable the trigger, the user receives an error message when browsing to the defined trigger URL.

Step 3 Click **Add New**.

The HTTP Trigger Configuration web page closes, and the trigger information appears on the HTTP Trigger Configuration summary web page.

You are now ready to provision any additional subsystems your Unified CCX applications require or to begin configuring Unified CCX applications.

Provision of Database Subsystem

Note The Database subsystem is available if your system has a license installed for either the Unified IP IVR or Unified CCX Premium product packages. If you are not using Unified CCX applications that require access to databases, you do not need to provision the Database subsystem.

The Unified CCX system uses the Database subsystem to enable Unified CCX applications to interact with database servers to make database information accessible to contacts.

Caution The Database subsystem does not support database views or running the store procedures.

Database Subsystem Configuration

The Database subsystem enables the Unified CCX applications to obtain information from data sources, which are databases configured to communicate with the Unified CCX system. You can connect the Unified CCX system with enterprise databases such as Microsoft SQL Server, Sybase, Oracle, or IBM DB2.

You can upload JDBC driver files using **Subsystems** > **Database** > **Drivers** menu option.

Note To determine a list of enterprise databases supported for the Database subsystem, see the Unified CCX Compatibility related information, located at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

Add New Datasource

After uploading the JDBC driver, you need to use this to create the datasource in the Database subsystem.

To add a new data source, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **Database** > **DataSource**. Click **Add New** icon that displays in the tool bar in the upper, left corner of the window or the **Add New** button that displays at the bottom of the page.

The Datasource Configuration web page opens. For more information on the web page fields, see **Datasource Configuration Web Page**.

Step 2 Click **Add** to save the changes.

The Enterprise Database Subsystem Configuration web page opens. You are now ready to provision any additional subsystems your Unified CCX applications require or to begin configuring Unified CCX applications.

Datasource Configuration Web Page

Datasource Configuration web page.

Field	Description
Secure Connection	When enabled, encrypts the connections to enterprise database servers. By default, it is disabled.
Data Source Name	Data source name for referring to the datasource. This is a mandatory field.
User Name	Username defined for connecting to the enterprise database. This is a mandatory field.
Password	Password defined for connecting to the enterprise database.
Confirm Password	Re-enter the password that you provided in the Password field.
Maximum Number of Connections	Maximum number of connections allowed to connect to the database. This database is usually an external database to which the customer script can connect. While the limit is set by that database and governed by your license, if this number in this setting is exceeded, the corresponding workflow is aborted and the caller receives an error message. However, you can avoid this error by configuring the appropriate number of sessions in the corresponding script or application. Also, the script writer can provide information about how many connections are used per call (or instance of application). This is a mandatory field.
Driver	Displays the list of available drivers for the enterprise database. One or more datasources can use the same driver. Select a driver for this datasource from this list box. This is a mandatory field.

Field	Description
JDBC URL	JDBC URL that is used to obtain a connection to the enterprise database. This is a mandatory field. The JDBC URL provided will be used by Unified CCX to connect to the enterprise database using JDBC. The URL to be used is dependent on the database you are connecting. The examples provided in the Datasource Configuration web page can be used as a reference to define the URL. Refer to the driver documentation for more information. **Note** • If the test connection fails for Oracle JDBC drive connection, try the following connection `url:` `jdbc:oracle:thin:[user/password]@[host][:port]:SID` • Encrypted connections to enterprise database servers are supported. This is applicable from Unified CCX release 12.5(1) SU3 ES03. • If you enable **Secure Connection**, ensure that the communication ports on the external database server are configured to be secure. Otherwise, the communication is not restricted.

Note If you enable FIPS, then the password length must be minimum 14 characters for Oracle users connecting to external datasource configuration.

Poll Database Connectivity

To poll connectivity to the database on a periodic basis, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **Database** > **Parameters**.

The Parameters web page opens to display the parameter-related fields.

Step 2 Specify the following fields:

Field	Description
RetryConnectInterval	Specifies the interval between two connection attempts when a data source is initialized. The default is 15,000 milliseconds.
NumAttempt	Specifies the number of attempts to establish connections to the database when a data source is initialized. The default is 3 attempts.
LoginTimeout	Sets the maximum time in seconds that a driver will wait while attempting to connect to a database. The default is 0 (disabled).

Step 3 Click **Update** to apply changes (or **Reset to Default** if you prefer to retain the default values).

The window refreshes and Unified CCX updates the parameters with your changes. You are now ready to provision any additional subsystems your Unified CCX applications require or to begin configuring Unified CCX applications.

Provision eMail Subsystem

Note The eMail subsystem is available if your system has a license installed for one of the following Cisco product packages: Unified IP IVR or Unified CCX Premium.

The Unified CCX system uses the eMail subsystem to communicate with your email server and enable your applications to create and send email. You must provision the eMail subsystem if you intend to create scripts that use messaging steps to create and send email.

Tip If your email system is configured to receive acknowledgments, you should process the mailbox you identify in your configuration to determine whether or not an email was successfully sent.

The email configuration process identifies the default email address and server to be used for sending email (including e-pages and faxes) and for receiving acknowledgments.

Note If you are not using email applications, you do not need to provision the eMail subsystem.

Complete the following steps.

Procedure

Step 1 Choose **Subsystems** > **eMail**.

The eMail Configuration web page opens.

Step 2 Specify the following fields:

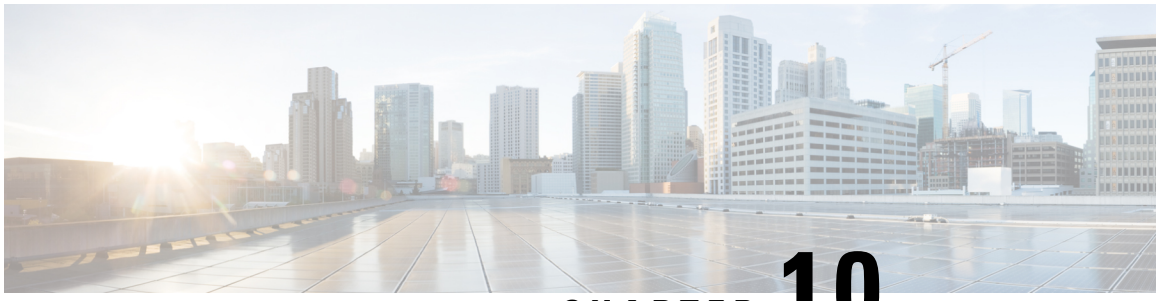
Field	Description
Mail Server	A fully-qualified email server name. (Example: server.domain.com)
email Address	An existing fully qualified e-mail address for the administrative account. Example:administrator@domain.com **Note** Unified CCX supports alphanumeric IDs and special characters (only hyphen "-" , underscore "_", and dot ".").

Step 3 Click **Update**.

The Unified CCX system saves your changes and the Unified CCXAdministration web page opens.

Note
Cisco does not currently support multiple email configurations. To remove the email information, you must erase the fields and click **Update**.

You are now ready to provision any additional subsystems your Unified CCX applications require, or to begin configuring Unified CCX applications.



CHAPTER 10

Management of Prompts, Grammars, Documents, and Custom Files

- Manage Prompt Files, on page 123
- Manage Grammar Files, on page 124
- Manage Document Files, on page 126
- Language Management, on page 127
- Upload of Prompt Files, on page 130
- Management of Custom Files, on page 132
- AAR File Management, on page 132

Manage Prompt Files

Many applications make use of pre-recorded prompts stored as .wav files, which are played back to callers to provide information and elicit caller response.

Several system-level prompt files are loaded during Unified CCX installation. However, any file you create needs to be made available to the Unified CCX Engine before a Unified CCX application can use them. This is done through the Unified CCX cluster's Repository datastore, where the prompt, grammar, and document files are created, stored, and updated.

Note Support for High Availability and remote servers is available only in multiple-server deployments.

The Unified CCX Server's local disk prompt files are synchronized with the central repository during Unified CCX Engine startup and during run-time when the Repository datastore is modified.

To access the Prompt Management page, perform the following steps:

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Application** > **Prompt Management**.

Step 2 The Prompt Management web page opens to display the following fields and buttons.

Field or Button	Description
Language	Lists the location of the items listed in the Name column.
Folder	Path of the current item selected in the Name column with respect to the root folder.
Name	Name of the language.
Size	The size of the prompt file prefixed with KB. The file size is converted from bytes to KB. **Note** This column is usually blank on the root page because the items on this page are usually folders.
Date Modified	The date and time when the document was last uploaded or changed along with time zone.
Modified by	The user ID of the person who performed these modifications.
Delete	Click **Delete** icon to remove the folder and its contents from the repository.
Rename	Click **Rename** icon to rename the folder in the repository.
Refresh	Click **Refresh** icon to refresh the folder in the repository.
Create Language	Displays a dialog box that lets you create a new language folder.
Upload Zip Files	Displays a dialog box that lets you locate and upload a zip file. **Note** The zip file must contain language folders in the root directory. Be sure to place the grammar files in folders and then zip the folders.

When you click a hyperlink (if configured) in the Name folder column, a secondary page appears. From this page, you can create a new subfolder or upload a new prompt.

Manage Grammar Files

The Unified CCX system uses specific grammars when recognizing and responding to caller response to prompts. A grammar is a specific set of all possible spoken phrases and Dual Tone Multi-Frequency (DTMF) digits to be recognized by Unified CCX applications and acted upon during run time.

Several system-level grammar files are loaded during Unified CCX installation. However, any file *you* create needs to be made available to the Unified CCX Engine before a Unified CCX application can use them. This is done through the Unified CCX cluster's Repository datastore, where the grammar files are created, stored, and updated.

Note Support for High Availability and remote servers is available only in multiple-server deployments.

The Unified CCX Server's local disk grammar files are synchronized with the central repository during Unified CCX Engine startup and during run-time when the Repository datastore is modified.

To access the Grammar Management page, perform the following steps:

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Applications** > **Grammar Management**.

Step 2 The Grammar Management web page opens to display the following fields and buttons.

Field or Button	Description
Language	Lists the location of the items listed in the Name column.
Folder	Path of the current item selected in the Name column with respect to the root folder.
Codec	The codec chosen during installation for this Unified CCX server. Display only.
Name	Name of the language folder.
Size	The size of the grammar file prefixed with KB. The file size is converted from bytes to KB. This column is usually blank on the root page as the items on this page are usually folders.
Date Modified	The date and time when the document was last uploaded or changed along with time zone.
Modified by	The user ID of the person who performed these modifications.
Delete	Displays a dialog box that lets you delete an existing language folder.
Rename	Displays a dialog box that lets you rename an existing language folder.
Refresh	Refreshes the specified folder in the repository.
Create Language	Displays a dialog box that lets you create a new language folder.
Upload Zip Files	Displays a dialog box that lets you locate and upload a zip file. **Note** The zip file must contain language folders in the root directory. Be sure to place the grammar files in folders and then zip the folders.

When you click a hyperlink (if configured) in the Name folder column, a secondary page appears. From this page, you can create a subfolder or upload a new Prompt, Grammar, or Document.

Manage Document Files

Documents might consist of .txt, .doc, .jsp, or .html files. Documents can also include custom classes and Java Archive (JAR) files that allow you to customize the performance of your Unified CCX system.

Several system-level document files are loaded during Unified CCX installation. However, any file you create needs to be made available to the Unified CCX Engine before a Unified CCX application can use them. This is done through the Unified CCX cluster's Repository datastore, where the document files are created, stored, and updated.

Note Support for High Availability and remote servers is available only in multiple-server deployments.

The Unified CCX Server's local disk document files are synchronized with the central repository during Unified CCX Engine startup and during run-time when the Repository datastore is modified.

To access the Document Management page, perform the following steps:

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Applications** > **Document Management**.

Step 2 The Document Management web page opens to display the following fields and buttons.

Field or Button	Description
Language	Lists the location of the items listed in the Name column.
Folder	Path of the current item selected in the Name column with respect to the root folder.
Name	Name of the language folder.
Size	The size of the grammar file prefixed with KB. The file size is converted from bytes to KB. This column is usually blank on the root page as the items on this page are usually folders.
Date Modified	The date and time when the document was last uploaded or changed along with time zone.
Modified by	The user ID of the person who performed these modifications.

Field or Button	Description
Delete	Displays a dialog box that lets you delete an existing language folder.
Rename	Displays a dialog box that lets you rename an existing language folder.
Refresh	Refreshes the specified folder in the repository.
Create Language	Displays a dialog box that lets you create a new language folder.
Upload Zip Files	Displays a dialog box that lets you locate and upload a zip file. **Note** The zip file must contain language folders in the root directory. Be sure to place the grammar files in folders and then zip the folders.

When you click a hyperlink (if configured) in the Name folder column, a secondary page appears. From this page, you can create a subfolder or upload a new Prompt, Grammar, or Document.

Language Management

The topics in this section describe the procedure for managing languages.

Create New Language

Follow this procedure to create a new Prompt, Grammar, or Document language folder in the Repository datastore:

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Applications** > **Prompt Management** or **Grammar Management** or **Document Management**.

The corresponding Management web page opens.

Step 2 Click **Create New Folder** or **Create Language** icon that displays in the tool bar in the upper, left corner of the window or the **Create New Folder** or **Create Language** button that displays at the bottom of the window.

The Create New Folder or Create Language dialog box opens.

Step 3 Perform any one of the following actions:

- Select a value from the Language drop-down list.

- If you are unable to find a particular language or if the Language drop-down list is empty, click **Edit** button to add a new Language. The Explorer User Prompt dialog box opens. Enter the name of the new language in the Language Name field and click **OK**.

Step 4 Click **Create**.

A new language folder Name appears on the summary web page.

Note
Ensure that the language created is supported in the Script Editor. For more information on the list of languages supported by the Script Editor, see the "Language Class and Code Specifications on the Web" section of the *Cisco Unified Contact Center Express Expression Language Reference Guide* at https://developer.cisco.com/docs/contact-center-express/#language-class-and-code-specifications-on-the-web.

Rename Language

Follow this procedure to rename a Prompt/Grammar/Document language folder in the Repository datastore:

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Applications** > **Prompt Management** or **Grammar Management** or **Document Management**.

The corresponding Management web page opens.

Step 2 Select the **Rename** icon against the folder you want to rename.

The Rename Folder dialog box opens.

Step 3 From the Select Language Folder To Rename field, choose the name of the folder to be renamed.

Step 4 In the Rename Folder To field, enter the new name.

Step 5 Click **Rename**.

The web page then refreshes itself to provide a summary and status. Click **Return to Document Management** to navigate to the respective Prompt or Grammar or Document Management page.

Delete Language

Follow this procedure to delete a Prompt/Grammar/Document language folder in the Repository datastore:

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Applications** > **Prompt Management** or **Grammar Management** or **Document Management**.

The corresponding Management web page opens.

Step 2 Select the **Delete** icon against the respective folder, that you want to delete.

A dialog box opens to confirm the Delete action for the specific folder.

Step 3 Click **OK** to delete.

Upload Zip Files to Language Folder

In addition to adding Prompt or Document files individually, you can upload multiple files from a Zip file.

Note The maximum upload file size is 20 MB, whether it is a single file or a Zip file.

Tip Be sure to upload (or download) large zip files in Prompt, Grammar and Document Management pages during off-peak hours.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Applications** > **Prompt Management** or **Grammar Management** or **Document Management**.

The corresponding Management web page opens.

Step 2 Click **Upload Zip Files** icon that displays in the tool bar in the upper, left corner of the window or the **Upload Zip Files** button that displays at the bottom of the window to upload a new prompt or zip file.

The Upload Document dialog box opens.

Step 3 Enter the path for the script file or click **Browse** to locate the script or the zip file containing the script files. Select the required script file and click **Open**.

Note
You can upload only files with extension .aef or .zip.

Step 4 Click the **Upload** button to upload the new script to the repository. A dialog box confirms the successful upload of the files.

Note
If you try to upload invalid script files, the upload will be unsuccessful and an error message will be displayed on the upload dialog box. You can also create user-defined directories using “Create a New folder” option and uploads scripts to those directories.

Step 5 By default, the files are unzipped after uploading. If you want to change this option, uncheck the **Unzip after uploading** check box.

Caution
In the Documents Management summary web page, you have the option to zip or to unzip the file before uploading. By default, this check box is checked to unzip the file before uploading. Ensure to uncheck the check box if you want to upload it as a zipped file.

The maximum upload file size of the Zip file is 20 MB.

Step 6 The contents of the zip file is uploaded to the folder. On successful uploading of the zip file, the status icon is updated accordingly. Click **Return to Document Management** button to go back to the respective Management web page.

Upload of Prompt Files

Prompts are messages that the Unified CCX system plays back to callers. Unified CCX applications often use prompts to obtain caller response so that the Unified CCX system can transfer calls, receive account information, and perform other functions.

To use prompts in your Unified CCX applications, you must first create a folder to store them. You can then record and upload new user prompts, delete prompts, and modify existing prompts.

You store pre-recorded prompts as `.wav` files. The Unified CCX system also allows users to record spoken names, which you can upload to be used in the playback of prompts.

Note
- Unified CCX supports audio playback of RIFF header .wav files only though your MRCP vendor may support multiple `.wav` file header formats.
- Unified CCX supports u-Law and A-Law prompts when G.711 voice codec is selected.
- Ensure that your prompt file (.wav) size is minimum of one byte. If you try to upload a prompt file that is less than one byte, the following error message is displayed:

  `Failed to upload file with path:`

ScanSoft uses RIFF headers. When generating a `.wav` file prompt specifically for Nuance, ensure that you consider the server playing the prompt:

- If the prompt is played by the Nuance Speech Server, the `.wav` file requires a SPHERE header.
- If the prompt is played by the Unified CCX server, the `.wav` file requires a RIFF header.

Nuance provides a tool to convert `.wav` files from RIFF headers to SPHERE headers.

Managing prompts can include one or more of the following activities:

- **Creating a folder:** You must create a folder to store the `.wav` files that the Unified CCX system uses as prompts.
- **Recording a prompt:** You can record prompts by using Recording Step in Unified CCX or any third-party utility.
- **Upload one or more prompts:** You can replace any of the stored prompts used by Cisco script applications with a different `.wav` file by uploading the new.wav file. If necessary, you can also add

spoken name prompts. Some Unified CCX applications play back the pre-recorded names of the people that callers are trying to reach, to allow the caller to confirm the transfer of the call.

Note In a HA setup, subscriber goes to Partial Service state while recording a prompt by using Unified CCX or uploading prompts.

Record a Prompt

You can record prompts and save in .wav format to be used in Unified CCX applications. You can use any third-party recording application to record prompts. You can save the prompts for the standard:

- G711- The G711 is a freely distributed public domain codec that has several recording options and is available to any sound recording application. You can save the prompts in μ-Law or A-Law. While saving a prompt file, ensure that the **8.000 kHz, 8 Bit, Mono 7 kb/sec** attribute is selected.
- G729 - The G729 is a freely distributed public domain codec and has several recording options. Some of these options are included in Microsoft Windows systems and are available to any sound recording application.

After you record a prompt, upload the prompt, associate the prompt with an application, and run the application to ensure that the prompt is playing properly.

Add Spoken-Name Prompts

Some Unified CCX applications play back the pre-recorded names of people that callers are trying to reach, to allow callers to confirm the transfer of a call.

To upload .wav files of the spoken names of users, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Tools** > **User Management** > **Spoken Name Upload**.

Step 2 The Spoken Name Prompt Upload web page opens with the following fields:

Field	Description
User Id	Unique identifier of the user for which the spoken name is to be uploaded. This is a mandatory field.
Codec	The codec chosen during installation for this Unified CCX server. Display only.
Spoken Name (.wav)	Location of the .wav file. This is a mandatory field.

Step 3 In the User Id field, enter an ID number that will identify the user.

Step 4 In the Spoken Name (.wav) field, enter the path for a .wav file or click **Browse** to navigate to the directory that contains the Spoken Name .wav file.

The Choose File dialog box opens. Select the required script file and click **Open**.

Step 5 Click **Upload** icon that displays in the tool bar in the upper, left corner of the window or click the **Upload** button that displays at the bottom of the window to upload the file.

Step 6 Repeat this process as needed to upload all spoken name .wav files.

Management of Custom Files

Use the Custom File Configuration web page to configure the classpath location of custom classes.

Specify Custom Classpath Entries

Use the Custom Classes Configuration web page to specify the available classpath entries.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **System** > **Custom File Configuration**.

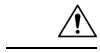
The Custom Classes Configuration web page opens. You can:

- Select required entries from the Available Classpath Entries list and arrange them in the order you want.
- Use the arrow icons to move items between the Available Classpath Entries and Selected Classpath Entries lists.

Step 2 Click **Update** when your selections are complete.

Click **Upload Custom Jar Files** icon that displays in the tool bar in the upper, left corner of the window or the **Upload Custom Jar Files** button that displays at the bottom of the window to upload Jar files. The Document Management web page opens.

AAR File Management



Caution Ensure that the contents of the AAR file are correct and conform to the specifications detailed in this section. If you upload AAR files that do not conform to these specifications, the Unified CCX Engine may not function as designed. Consequently, you need to manually reconfigure some of the applications uploaded through AAR.

AAR files are archives of prompt, grammar, document, scripts, applications, and custom classes that you use as building blocks for applications and extensions.

An AAR file can be simple—for instance, consisting of a single prompt—or complex—for example, containing all the prompts for all languages application uses, the workflow, and the configuration information for an application.

An AAR file is essentially a zip file that contains an optional META-INF directory. The META-INF directory, if it exists, stores configuration data, including security, versioning, extensions, and services.

You create AAR files using Java tools. After creating a file, you need to upload it to Unified CCX.

The following example shows a sample AAR Main Manifest and a sample AAR Application Manifest.

Sample AAR Main Manifest

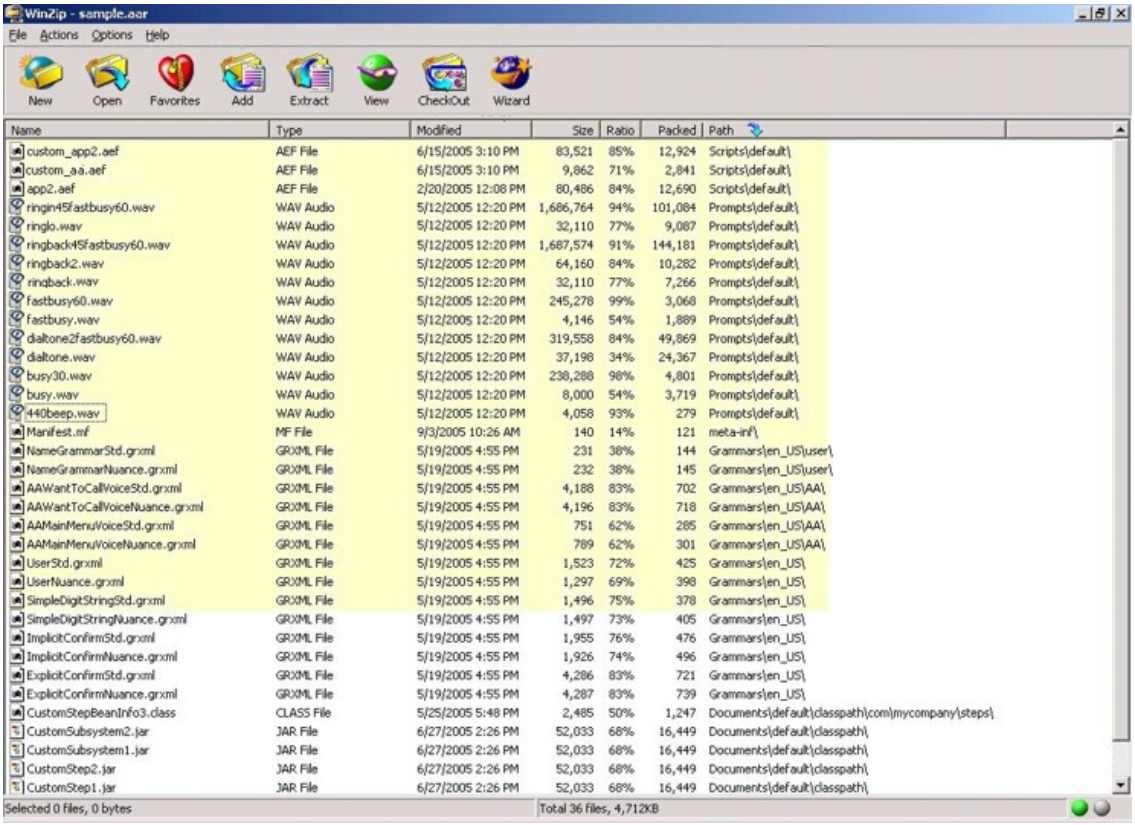
```
Manifest-Version: 1.1Created-By: 1.4.2_05 (Sun Microsystems Inc.)
Built-By: aaruser
Sealed: false
Cisco Unified CCX-Version: 9.0(1)
Class-Path:
Application-List: customApp1.mf customApp2.mf
Subsystem-List: sub1.mf sub2.mf
Palette-List: Custom1 Custom2
Custom1-Palette-Name: Category1
Custom2-Palette-Name: Category2
Custom1-Step-List: step1.mf
Custom2-Step-List: step2.mf step3.mf
Implementation-Title: AAR Test File
Implementation-Version: 4.5(1)
Implementation-Vendor: Cisco Systems, Inc.
Implementation-Vendor-Id: 12345
Implementation-URL: https://www.cisco.com
```

Sample AAR Application Manifest

```
Application-Version: 1.1Created-By: 1.4.2_05 (Sun Microsystems Inc.)
Built-By: aaruser
Sealed: false
Implementation-Title: AAR Application MF
Implementation-Version: 9.0(1)
Implementation-Vendor: Cisco Systems, Inc.
Implementation-Vendor-Id: 12345
Implementation-URL: https://www.cisco.com
Application-Name: Custom AA
Application-Type: Cisco Script Application
Application-Description: Cisco Unified CCX Cisco Custom Application
Application-Id: 100
Max-Sessions: 300
Enabled: true
Script: SSCRIPT[aa.aef]
Default-Script: SSCRIPT[aa.aef]
Initial-Script: SSCRIPT[aa.aef]
```

Figure 2: Sample AAR File

The figure below shows a sample AAR file.



To deploy custom applications, steps, and subsystems through an AAR file, you must first create the AAR file using a jar or zip tool and then upload the file through the Unified CCX Administration web page.

AAR File Creation

You create an AAR file using a jar or WinZip tool.

An AAR file format is similar to a Zip file format. It includes an optional META-INF directory, which is used to store configuration data, including security, versioning, extension, and services.

Upload AAR Files

To upload an AAR file, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Applications** > **AAR Management**.

The AAR Management web page opens to display the following fields and buttons.

Field or Button	Description
Enter a Valid AAR File to Upload	You can either enter the name of the AAR file or click **Browse** button next to this field to navigate to the directory in which the file is located. This is a mandatory field.
Overwrite existing files	Enable this checkbox in case you want to overwrite the existing files.
Upload	Click this button to upload the AAR file.
Clear	Click this button to clear the selected file.

Enter the path for the AAR file or click **Browse** button to upload the file. The Choose File dialog box opens. Select the required script file and click **Open**.

Step 2 Click **Upload**.

The contents of the AAR file are uploaded to the respective folders.

Note
Unified CCX generates an error if the AAR file is not formatted correctly or is missing some custom files.

META-INF Directory

Unified CCX uses the following files and subdirectories in the META-INF directory to configure applications, extensions and services:

- **MANIFEST.MF**. The file used to define extension and application related data.
- **applications**. This directory stores all application configuration files.

Directories for Prompts, Grammars, Documents, and Scripts

The AAR files features also provides directories to store prompts, grammars, documents, and scripts to be uploaded to the Repository.

The AAR directory structure mirrors the function of the Unified CCX Prompt, Grammar, Documents, and Scripts Management web pages. Each directory corresponds to each language for which to install prompts, grammars, documents and scripts. Languages are defined using the Java Locale standard, and the special default directory is used for prompts, grammars, and documents that are common to all languages.

Only Unified CCX supported prompt files and extensions are allowed within each directory. The maximum length of each individual folder name and file name within a directory is 64 characters.

Prompts Directory

The Prompts directory stores prompts that must be uploaded to the prompt repository (to make it seem like they were uploaded through Unified CCX Prompt Management).

Grammars Directory

The Grammars directory stores grammars that must be uploaded to the grammar repository (to make it seem like they were uploaded through Unified CCX Grammar Management).

Documents Directory

The Documents directory stores documents that must be uploaded to the document repository (to make it seem like they were uploaded through Unified CCX Document Management).

Scripts Directory

The Scripts directory stores scripts that must be uploaded to the script repository (to make it seem like they were uploaded through Unified CCX Script Management).

Note The Script directory must define a single directory named **`default`** under which all script files must be listed.

AAR Manifest

An AAR file manifest consists of a main section followed by a list of sections for individual AAR file entries, each separated by a newline.

Information in a manifest file contains *name-value* pairs—which are also referred to as *headers* or *attributes*. Groups of name-value pairs are known as a *section*; sections are separated by empty lines.

The following table describes the expected syntax of the manifest file.

Table 4: Manifest File Syntax

Name	Value
section:	*header +newline
nonempty-section:	+header +newline
newline:	CR LF | LF | CR (not followed by LF)
header:	name: value
name:	alphanum *headerchar
value:	SPACE *otherchar newline *continuation
continuation:	SPACE *otherchar newline
alphanum:	{A-Z} | {a-z} | {0-9}
headerchar:	alphanum | - | _
otherchar:	any UTF-8 character except NUL, CR and LF

Name	Value
Note To prevent corruption of files sent through email, do not use “From” to start a header.	

The main section, which is terminated by an empty line:

- Contains security and configuration information about the AAR file itself, as well as the applications or extensions that this AAR file is defining.
- Defines main attributes that apply to every individual manifest entry. No attribute in this section can have its name equal to “Name”.

The individual sections define various attributes for directories or files contained in this AAR file. Not all files in the AAR file need to be listed in the manifest as entries. The manifest file itself must not be listed. Each section must start with an attribute with the name as “Name”, and the value must be a relative path to the file or directory.

If there are multiple individual sections for the same file entry, the attributes in these sections are merged. If a certain attribute has different values in different sections, the last one is recognized.

Attributes that are not understood are ignored. Such attributes may include implementation-specific information used by applications.

The following table describes the specification for any file that can be archived in the AAR.

Table 5: Syntax for AAR Files

Name	Value
manifest-file	main-section newline *individual-section
main-section	version-info newline *main-attribute
version-info	Manifest-Version: version-number
version-number	digit+{.digit+}*
main-attribute	(any legitimate main attribute) newline
individual-section	Name: value newline *perentry-attribute
perentry-attribute	(any legitimate perentry attribute) newline
newline	CR LF | LF | CR (not followed by LF)
digit	{0-9}

Attribute Types

Attributes that appear in the main section are called main attributes. Attributes that appear in individual sections are called per-entry attributes. Some attributes appear in both the main and individual sections, in which case the per-entry attribute value overrides the main attribute value for the specified entry.

Main Attributes

Main attributes are the attributes that are present in the main section of the manifest:

General main attributes as shown in the following table.

Table 6: General Main Attributes

Attribute	Description
Manifest-Version	The manifest file version. The value is a legitimate version number.
Created-By	The version and the vendor of the java implementation on top of which this manifest file is generated. This attribute is generated by the jar tool.
Cisco Unified CCX-Version	The minimum Unified CCX version release compatible with the AAR file. Unified CCX-version is the accumulation of the Unified CCX release, Unified CCX Service Release, and Unified CCX Engineering Special defined in that order. For example, if the AAR file is compatible with Cisco Unified CCX release 4.5(1)_Build705, SR1_Build001, ES2_Build002, the Cisco Unified CCX-Version would be defined as 4.5(1)SR1ES2_Build002. Only the last build number is taken. So for instance, if the AAR file is compatible with Cisco Unified CCX release 4.5(1)_build705, SR1_Build001, then the Cisco Unified CCX-Version is 4.5(1)SR1_Build001. As a last example, if AAR file is compatible with Cisco Unified CCX release 4.5(1)_Build705 and above, then Cisco Unified CCX-Version would be 4.5(1)_Build705.
Class-Path	The directories or JAR files that need to be installed and accessed by scripts directly. Entries are separated by one or more spaces. The Unified CCX class loader uses the value of this attribute to construct its internal search path where each entry is defined relative to the /Documents/default/classpath directory in this AAR file.
Application-List	The application configuration files from the META-INF/applications/ directory to be installed. Entries are separated by one or more spaces.
Subsystem-List	The subsystem configuration files from the META-INF/subsystems/ directory to be installed. Entries are separated by one or more spaces.
Palette-List	The step palettes that need to be installed. Each palette listed in this attribute will have a set of additional attributes that the Unified CCX editor uses to specify the palette name and the palette steps to install. Entries are separated by one or more spaces.
Palette-Name	The unique name of the palette to define in the Unified CCX editor where the specified steps will be grouped and accessible.
Step-List	The step configuration files from the META-INF/steps/ directory to be installed under the palette. Entries are separated by one or more spaces.

Attribute defined for extension identification: Extension-Name

This attribute specifies a name for the extension contained in the AAR file. The name should be a unique identifier.

The following tables shows attributes defined for extension and directory versioning and sealing information. These attributes define features of the extension which the AAR file is a part of. The values of these attributes apply to all the directories in the AAR file, but can be overridden by per-entry attributes.

Table 7: Implementation Category in Main Attributes

Attribute	Description
Implementation-Title	The title of the extension implementation.
Implementation-Version	The version of the extension implementation.
Implementation-Vendor	The organization that maintains the extension implementation.
Implementation-VendorId	The ID of the organization that maintains the extension implementation.
Implementation-URL	The URL from which the extension implementation is downloaded.
Sealed	Defines if this AAR file is sealed. Sealing a directory means that the files uploaded to the corresponding repository will not be modifiable once installed unless the AAR file is reinstalled. If set to true, then all directories in the AAR file default to be sealed, unless individually defined otherwise. If set to false, then all directories are modifiable.

Per-entry Attributes

Per-entry attributes apply only to the individual AAR file entry with which the manifest entry is associated. If the same attribute also appears in the main section, then the value of the per-entry attribute overwrites the main attribute value.

- Example 1: If AAR file a.aar has the following manifest content, then all the files archived in a.aar are sealed, except US English prompts. If the same attributes also appeared in an entry representing a parent directory of another entry, then the value of the per-entry attribute overwrites the parent directory per-entry attribute value.

```
Manifest-Version: 1.1 Created-By: 1.2 (Sun Microsystems Inc.)
Sealed: true
Name: Prompts/en_US/
Sealed: false
```

- Example 2: If AAR file a.aar has the following manifest content, then all the US English prompts archived in a.aar are sealed, except US English prompts located in the AA/ directory.

```
Manifest-Version: 1.1 Created-By: 1.2 (Sun Microsystems Inc.)
Name: Prompts/en_US/
Sealed: true
Name: Prompts/en_US/AA/
Sealed: false
```

The per-entry attributes fall into the following groups:

- Attributes defined for file contents: Content-Type

This attribute specifies the MIME type and subtype of data for a specific file entry in the AAR file. The value should be a string in the form of type/subtype. For example, image/bmp is an image type with a subtype of bmp (representing bitmap). This indicates that the file entry is an image with the data stored as a bitmap. RFC 1521 and 1522 discuss and define the MIME types definition.

- Attributes defined for directory versioning and sealing information:

  These are the same set of attributes defined in Table 7: Implementation Category in Main Attributes, on page 139 for the main attributes. When used as per-entry attributes, these attributes overwrite the main attributes for the individual file specified by the manifest entry.

META-INF Directory Attributes

The Unified CCX recognizes the x.MF file in the applications, subsystems, and steps subdirectories in the META-INF directory and interprets each to configure applications, subsystems, and steps respectively. The x is the base file name as listed on the Application-List main attribute of the manifest file. The X.MF file contains one section defining the configuration of a particular application.

Application Subdirectory Attributes

The following table describes the syntax of the manifest file for the application subdirectory.

Table 8: Application Subdirectory Manifest File Syntax

Name	Value
application-file	version-info newline *application-attribute
version-info	Application-Version: version-number
version-number	digit+{.digit+}*
application-attribute	(any legitimate application attribute) newline
newline	CR LF | LF | CR (not followed by LF)
digit	{0-9}

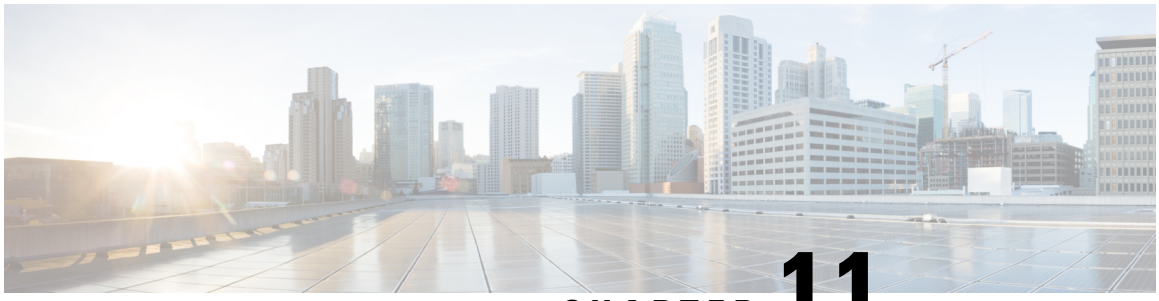
The application attributes fall into the following groups:

Table 9: Application Attributes

Attribute	Description
Application-Version	The application configurations file version. The value is a legitimate version number. For example, Cisco Unified CCX Release 4.5 starts with version 1.1.
Application-Name	The unique name of the application (see Unified CCX Application Management).
Application-Type	The type of the application (Cisco Script Application, Busy, Ring-No-Answer.

Attribute	Description
Application-Description (optional)	The description for the application (see Unified CCX Application Management).
Application-Id	A unique identifier for the application (see Unified CCX Application Management).
Max-Sessions	The maximum number of sessions for the application (see Unified CCX Application Management).
Enabled	The application is enabled if the value is set to true (see Unified CCX Application Management). If the value is set to false, the case is ignored.
Script	The main script of a Cisco Script Application (see Unified CCX Application Management). The value must be relative to the Scripts directory. Unified CCX does not support configuring script parameters.
Default-Script	The default script of a Cisco Script Application, Unified ICME Translation or Post Routing application (see Unified CCX Application Management). The value must be relative to the Scripts directory. Unified CCX does not support configuring script parameters.
Initial-Script	The initial script of a Unified CCX Post Routing application (see Unified CCX Application Management). The value must be relative to the Scripts directory. Unified CCX does not support configuring script parameters.

- Attributes defined for application versioning and sealing information: These attributes define features of the application to which the AAR file belongs. These attributes are the same as those listed in Main Attributes, on page 138.



CHAPTER 11

Unified CCX System Management

- Basic Terminology, on page 143
- High Availability and Automatic Failover, on page 144
- Unified CCX CDS Information Management, on page 145
- Manage System Parameters, on page 145
- Unified CCX IP Address/hostname Management, on page 146
- Set Up Certificates, on page 162
- Exit Unified CCX Administration, on page 164

Basic Terminology

This section provides information about different Unified CCX terminology.

- **Cluster**. A Unified CCX cluster (often referred to as cluster in this manual) consists of one or more servers (nodes) that are running Unified CCX components in your Unified CCX deployment. If you deploy Unified CCX components on a single server, the Unified CCX cluster consists of that server. If you deploy Unified CCX on multiple servers, the cluster includes the Unified CCX server and standby server on which you installed Unified CCX. The Unified CCX cluster supports up to two Unified CCX servers, one designated as the *active Unified CCX server* and the other designated as the *standby Unified CCX server* for high availability purposes.

Note Support for High Availability and remote servers is available only in multiple-server deployments.

- **Cluster profile**. The Unified CCX Administration web page (home page) displays information about the cluster profile. A cluster profile includes data relating to the Unified CCX servers, components, and licenses installed in a cluster.
- **Node (server)**. A server that is part of the Unified CCX cluster.
- **Active Server**. The active server provides all system services and resources. You can deploy one active server in each Unified CCX subsystem. If the active server fails, the Unified CCX subsystem automatically fails over to the standby server.

- **Standby Server**. You can deploy up to two servers in each Unified CCX system for high availability—one active server (master) and one standby (not active) server. With high availability, if an active server becomes unavailable, the standby server automatically becomes the active server.
- **Component**.The software units in the Unified CCX system. The main software components of the Unified CCX server are the Engine, datastores, monitoring, recording, and the Cluster View Daemon (CVD). See the *Cisco Unified Contact Center Express Install and Upgrade Guide* for more information on setup and installation procedures.
- **Service**. An executable unit. A service may have other services as its children. (For example, subsystems and managers are children of the engine service).
- **Feature**. A logical representation of the functional unit.
- **Master service**. A specially-elected service. Only one service from the Engine service, or database services set can be the master within the Unified CCX Engine component.
- **Standby service**. An active service that can take over the master functionality in case the master service becomes unavailable within the Unified CCX Engine component. You cannot configure the standby service. The Cluster View Daemon (CVD) dynamically elects the services on the active node to be the master.

High Availability and Automatic Failover

Note Support for High Availability (HA) and remote servers is available only in multiple-server deployments. Unified CCX does not support more than two nodes in a HA setup. Expansion servers where the Database, Monitoring, or Recording components are running on separate servers are not supported.

Unified CCX provides high availability and automatic failover capability through the use of two servers, the *active server* and the *standby server*.

The active server provides all system services and resources; no services or resources are available from the standby server. When you make administrative changes on the active server, both the servers are synchronized.

If the active server fails, there is automatic failover to the standby server. For detailed information on HA over WAN deployment, see *Solution Design Guide for Cisco Unified Contact Center Express*.

Note After a Unified CCX failover or failback the agent state changes to Not Ready state.

Network Partitions

Network malfunction or misconfiguration can create network partitions and split the network into separate *islands*. If a node enters this state, the node is referred to as being in the island mode. Nodes in the island mode are hard to detect. While these nodes can communicate within a partitioned island, they cannot communicate between partitioned islands. If the islands do not communicate, then each island will select its own active server.

Generally, you can connect to the Unified CCX administration on any node, and see a consistent cluster view. If a node is in the island mode, you will see different cluster views when you connect to nodes in each island.

Note Support for High Availability and remote servers is available only in multiple-server deployments.

If your node enters the island mode, it should recover from the island mode as soon as the underlying network issue is resolved. If the island mode persists, check the network connectivity/reachability between the two CCX servers and take action accordingly.

Unified CCX CDS Information Management

The Unified CCX system stores configuration information in the Cisco Configuration Datastore Server (CDS). The Unified CCX Administration configurations are stored in the CDS.

Note Support for High Availability and remote servers is available only in multiple-server deployments.

The Unified CCX server can receive directory information from one Cisco Unified Communications directory and application configuration and script logic from a repository on another server.

Manage System Parameters

The parameters in the System Parameters Configuration page are grouped logically into sections with headings. Each parameter has a corresponding suggested or default value on the right side of the page. Where applicable, radio buttons are used to toggle between the parameter options.

In this web page, you can configure the port settings, default session timeout, and codec.

Note Changing some system parameters like IP address, Network Time Protocol (NTP) and so on can result in a different License MAC. You need to get rehosted license files (with new License MAC) in such cases within 30-day grace period beyond which the system will stop working.

Procedure

Step 1 Choose **System** > **SystemParameters** from the Unified CCXAdministration menu bar.

The System Parameters Configuration web page appears.

Step 2 Click the **Update** icon that displays in the tool bar in the upper, left corner of the window or the **Update** button that displays at the bottom of the window.

The system notifies all nodes in the cluster about the changes.

Note

If Cluster View Daemon is in Shutdown state during this operation, then the changes just made are synchronized on that node when Cluster View Daemon is started again.

Unified CCX IP Address/hostname Management

This section provides the steps you need to follow whenever there is a change in IP address/hostname for the following Unified CCX deployments:

- Unified CCX Cluster with Single-node
- Unified CCX Cluster with High Availability (HA)

You may want to change the IP address/hostname for a variety of reasons, including moving the server from one segment to another or resolving a duplicate IP address/hostname problem.

Note Hostname change is supported in Cisco Unified CCX.

The character limit for Hostname is 63 characters.

Prepare System for IP Address/hostname Change

Perform the following tasks to ensure that your system is prepared for a successful IP address/hostname change.

Note If you do not receive the results that you expect when you perform these tasks, do not continue with this procedure until after you resolve any problems that you find. DB replication across the entire cluster is essential for this process. Also, if the DNS check fails then the IP Address/hostname change will not happen.

Procedure

Step 1 List all servers in the cluster and note whether the nodes are defined by using IP addresses or hostnames.

- From **Cisco Unified CCX Administration** menu bar on the first node, navigate to **System** > **Server**. A list of all servers in the cluster displays.
- See whether the servers are defined using IP addresses or hostnames and capture this list of servers for later reference. Ensure that you have saved an inventory of both the hostname and IP address of each node in your cluster.

Step 2 Ensure that all servers in the cluster are up and available by checking for any active ServerDown alerts. You can check by using either the Real Time Monitoring Tool (RTMT) or the Command Line Interface (CLI) on the first node.

- To check by using RTMT, access Alert Central and check for ServerDown alerts.

- To check by using the CLI on the first node, enter the following command and inspect the application event log:

```
file search activelog syslog/CiscoSyslog ServerDown
```

Step 3 Check the DB replication status on all the Cisco CRS nodes and Cisco Unified Communications nodes in the cluster to ensure that all servers are replicating database changes successfully using the following substeps:

a) **For Unified CCX**: In a High Availability deployment of Unified CCX, you can check the DB replication status for the datastores across all servers in the cluster using Unified CCX Serviceability Administration. Choose **Tools** > **Datastore Control Center** > **Replication Servers** from the Unified CCX Serviceability menu bar to view the replication status. The value in State field for both the servers in this web page should display ACTIVE/ CONNECTED.

b) **For Cisco Unified Communications Platform**: You can check the DB replication status on all the Cisco Unified Communications nodes in the cluster by using either RTMT or a CLI command.

- To check by using RTMT, access the Database Summary and inspect the replication status.
- To check by using the CLI, enter the command that is shown in the following example:

```
admin: show perf query class "Number of Replicates Created and
 State of Replication"
==>query class :

- Perf class (Number of Replicates Created and State of
Replication)
has instances and values:
ReplicateCount  -> Number of Replicates Created   = 344
ReplicateCount  -> Replicate_State                = 2
```

Be aware that the Replicate_State object shows a value of 2 in this case. The following list shows the possible values for Replicate_State:

- 0—Replication Not Started. Either no subscribers exist, or the Database Layer Monitor service is not running and has not been running since the subscriber was installed.
- 1—Replicates have been created, but their count is incorrect.
- 2—Replication is good.
- 3—Replication is bad in the cluster.
- 4—Replication setup did not succeed.

Step 4 Run a manual DRS backup and ensure that all nodes and active services are backed up successfully.

Step 5 Run the CLI command **`utils diagnose module validate_network`** through Platform CLI on all nodes in the cluster to ensure network connectivity and DNS server configuration are intact.

IP Address Modification

This section describes how to change the IP address.

Caution Changing the IP address on any node in a Cisco CRS cluster can interrupt call processing and other system functions. Also, changing the IP address can cause the system to generate certain alarms and alerts such as ServerDown and automatic failover to a backup server may not operate. Because of this potential impact to the system, you must perform IP address changes during a planned maintenance window.

Note When there is a change in the Unified CCX server subnet, you must change the default gateway IP address. Ensure the following:

- The new default gateway IP address is configured on the Unified CCX server.
- The DNS is reachable and the DNS record exists for the Unified CCX server.

Change IP Address for Server in Single-Node Deployment

Use this procedure to change the IP address of the server in a single-node deployment.

Caution Ensure that the server on the same subnet or that is moved to the new subnet has access to the configured default gateway before proceeding to change the IP address of the server.

Procedure

Step 1 Change the DNS record of the server to point to the new IP address. Ensure that you correctly update both the forward (A) and reverse (PTR) records, and there are no duplicate PTR records.

Step 2 If you want to change the IP address of the server on the same subnet or a different subnet that requires a new default gateway address, use either of the following methods:

- CLI commands
- Cisco Unified Communications Operating System Administration interface

Using CLI commands:

a) To change the default gateway, enter the following CLI command:

`set network gateway` <*IP Address*>

The following sample output displays:

```
admin:set network gateway 10.3.90.2

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue(y/n):
Continue (y/n)?y
```

b) To change the IP address of the server, enter the following CLI command:

set network ip eth0 <ip_address> <netmask> <default gateway> where ip_address specifies the new server IP address and netmask specifies the new server network mask and default gateway specifies the default gateway of the new server.

The following sample output displays:

```
admin: set network ip eth0 10.3.90.21 255.255.254.0 10.3.90.1
** W A R N I N G ***
If there are IP addresses (not hostnames)
configured in UCCX Administration
under System -> Servers then you must change
the IP address there BEFORE changing it here
or call processing will fail. This will cause the
system to restart
=======================================================
Note: To recognize the new IP address all nodes within
the cluster will have to be manually rebooted.
=======================================================
Do you want to continue?
Enter "yes" to continue and restart or any other key
to abort
```

Enter **y** and press **Enter**. This will automatically reboot this server with the new IP address.

Using Cisco Unified Communications Operating System Administration interface:

Alternatively, you can change the IP address and default gateway of the server from **Cisco Unified Communications Operating System Administration** interface as follows:

- Choose **Settings** > **IP** > **Ethernet**.
- Change the IP address, default gateway, and netmask, and click **Save**. The server restarts automatically with the new IP address.

If you change the IP address, License MAC of the server will also change. Rehost the new license. Old license enters its grace period.

What to do next

When the Cloud Connect services are enabled, after the Unified CCX IP address has been changed, run the following CLI command to restart the services.

```
utils cloudconnect reinit services
```

Note In a high availability (HA) deployment, run this CLI command on other nodes of the cluster.

IP Address Modification in High-Availability (HA) Deployment

Note Ensure that the IP Address is sequentially changed first in the Publisher and then the Subscriber node of the Unified CCX servers.

Change IP Address for Publisher Server in HA Deployment

Use this procedure to change the IP address of the publisher server in a HA deployment.

Caution Before changing the IP address of the server, ensure that the server has access to the configured default gateway. This applies whether the server is on the same subnet or is moved to a new subnet.

Procedure

Step 1 Change the DNS record of the publisher server to point to the new IP address. Ensure that you correctly update both the forward (A) and reverse (PTR) records, and there are no duplicate PTR records.

Step 2 Verify that the DNS change propagates to other nodes. To verify, use the **utils network host** <*IP Address*> CLI command on all the cluster nodes.

Step 3 From the Cisco Unified Operating System Administration page of the subscriber server in the cluster, perform the following tasks:

a) Navigate to **Settings** > **IP** > **Publisher**.
b) Change the IP address of the publisher server.

Step 4 To update the new IP of the publisher server in the subscriber, enter the following CLI command on the subscriber server:

```
utils uccx modify remote_IPAddress <Old_IP_of_Publisher>
<New_IP_of_Publisher>
```

The following output appears:

```
admin:utils uccx modify remote_IPAddress 10.3.90.21  10.3.90.28

 Old Remote IP Address: 10.3.90.21
 New Remote IP Address: 10.3.90.28

This command should be executed only in case you are changing IP Address of remote server.
Are you sure you want to run this command?
Continue (y/n)?
```

Enter **y** and press **Enter**.

Step 5 To change the IP address of the server on the same subnet or a different subnet that requires a new default gateway address, use either of the following methods:

- CLI commands
- Cisco Unified Operating System Administration interface

Using CLI commands:

a) To change the default gateway, enter the following CLI command:

set network gateway <*IP Address*>

The following sample output appears:

```
admin:set network gateway 10.3.90.2

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
```

```
Continue(y/n):
Continue (y/n)?y
```

Caution
Ensure that the server is in the new subnet and has access to the default gateway before proceeding to the following sub-step.

b) To change the IP address of the publisher server, enter the following CLI command:

set network ip eth0 <ip_address> <netmask> <default gateway> where ip_address specifies the new server IP address, netmask specifies the new server network mask and default gateway specifies the default gateway of the new server.

The following sample output appears:

```
admin:set network ip eth0 10.78.92.55 255.255.255.0 10.78.92.1

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue (y/n)?y
           ***   W A R N I N G   ***
This command will cause the system to restart
======================================================
 Note: Please verify that the new ip address is unique
       across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
       To recognize the new ip address all nodes within
       the cluster will have to be manually rebooted.
======================================================
Continue (y/n)?y
```

Enter **y** and press **Enter**. The server is automatically rebooted with the new IP address.

Using Cisco Unified Operating System Administration interface:

Alternatively, you can change the IP address and default gateway of the server from the **Cisco Unified Operating System Administration** interface as follows:

- Choose **Settings** > **IP** > **Ethernet**.
- Change the IP address, default gateway, and netmask, and click **Save**. The server restarts automatically with the new IP address.

Step 6 Reboot the publisher server in the cluster by using the **utils system restart** CLI command. After 10 minutes, reboot the subscriber server with the same command.

Note
If you do not reboot the subscriber after the IP address change, all the services on the publisher may not start properly.

If you change the IP address, the License MAC also changes. Rehost the new license for the new License MAC. Old license enters its grace period.

Change IP Address for Subscriber Server in HA Deployment

Use this procedure to change the IP address of a subscriber server in a HA deployment.

Caution Before changing the IP address of the server, ensure that the server has access to the configured default gateway. This applies whether the server is on the same subnet or is moved to a new subnet.

Procedure

Step 1 Change the DNS record of the subscriber server to point to the new IP address. Ensure that you correctly update both the forward (A) and reverse (PTR) records, and there are no duplicate PTR records.

Step 2 Verify that the DNS change propagates to the other nodes. To verify, use the **utils network host** <*IP Address*> CLI command on all the cluster nodes.

Caution
Skip Step 3 if the server is defined by hostname and you are changing only the IP address.

Step 3 From **Cisco Unified CCX Administration** page, perform the following tasks:

a) Navigate to **System** > **Server**. From the List Servers web page, click the IP address of the subscriber server.

The Server Configuration page for the subscriber server opens.

b) Enter the new IP address in the **Host Name/IP Address** field and click **Save**.

Note
You can use the CLI command **run sql select name,nodeid from ProcessNode** to check whether the new IP address has been replicated on all the servers.

Step 4 To update the new IP of the subscriber in the publisher, enter the following CLI command on the publisher server:

utils uccx modify remote_IPAddress <Old_IP_of_Subscriber> <New_IP_of_Subscriber>

The following output appears:

```
admin:utils uccx modify remote_IPAddress 10.3.90.21  10.3.90.28

 Old Remote IP Address: 10.3.90.21
 New Remote IP Address: 10.3.90.28

This command should be executed only in case you are changing IP
Address of remote server.
Are you sure you want to run this command?
Continue (y/n)?
```

Enter **y** and press **Enter**.

Step 5 If you want to change the IP address of the server on the same subnet or a different subnet that requires a new default gateway address, use either of the following methods:

- CLI commands
- Cisco Unified Communications Operating System Administration interface

Using CLI commands:

a) To change the default gateway, enter the following CLI command:

set network gateway <*IP Address*>

The following sample output appears:

```
admin:set network gateway 10.3.90.2

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue(y/n):
Continue (y/n)?y
```

Caution
Ensure that the server is in the new subnet and has access to the default gateway before proceeding to the following sub-step.

b) To change the IP address of the server, enter the following CLI command:

set network ip eth0 <ip_address> <netmask> <default gateway> where ip_address specifies the new server IP address, netmask specifies the new server network mask and default gateway specifies the default gateway of the new server.

The following sample output appears:

```
admin:set network ip eth0 10.78.92.55 255.255.255.0 10.78.92.1

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue (y/n)?y
           ***   W A R N I N G   ***
This command will cause the system to restart
======================================================
 Note: Please verify that the new ip address is unique
       across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
       To recognize the new ip address all nodes within
       the cluster will have to be manually rebooted.
======================================================
Continue (y/n)?y
```

Enter **y** and press **Enter**. The server is now automatically rebooted with the new IP address.

Using Cisco Unified Communications Operating System Administration interface:

Alternatively, you can change the IP address and default gateway of the server from **Cisco Unified Communications Operating System Administration** interface as follows:

- Choose **Settings** > **IP** > **Ethernet**.
- Change the IP address, default gateway, and netmask, and click **Save**. The server restarts automatically with the new IP address.

Step 6 Reboot all the servers in the cluster including the publisher using the CLI command **utils system restart**.

Note
If you do not reboot the subscriber after the IP address change, all the services on the publisher may not start properly.

HostName and Domain Name Modification

Changing the hostname or domain name on any node in the Unified CCX cluster can interrupt call processing and other system functions. It can cause the system to generate certain alarms and alerts such as ServerDown and automatic failover to a backup server may fail. To prevent these failures, ensure to change the hostname or domain name during a planned maintenance window.

As a prerequisite ensure that the DNS is reachable and the DNS record exists for the server with its current fully qualified domain name (FQDN) and the IP address.

Note

- Ensure Single Sign-On is disabled before modifying the hostname or domain name.

HostName Modification

This section describes how to change the hostname.

Change HostName for Server in a Single-Node Deployment

Use this procedure to change the hostname of the server in a single-node deployment.

Note The hostname can have a maximum of 63 characters.

Ensure Single Sign-On is disabled before modifying the hostname.

Procedure

Step 1 Change the DNS record of the server to point to the new hostname. Ensure that you correctly update both the forward (A) and reverse (PTR) records, and there are no duplicate PTR records.

Step 2 You can change the hostname of the server either using the CLI (command line interface) command or using **Cisco Unified OS Administration** interface. To change the hostname using CLI command, go to step 3 or to change the hostname using **Cisco Unified OS Administration** interface go to step 4.

Step 3 At the CLI prompt, perform the following tasks:

a) Enter the CLI command **`set network hostname`** and press **Enter**.

The following sample output displays:

```
admin:set network hostname

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue(y/n):
Continue (y/n)?y
ctrl-c: To quit the input.



         ***   W A R N I N G   ***
Do not close this window without first canceling the command.
```

```
This command will automatically restart system services.
The command should not be issued during normal operating
hours.

======================================================
Note: Please verify that the new hostname is a unique
       name across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
======================================================

Security Warning : This operation will regenerate
       all UCCX Certificates including any third party
       signed Certificates that have been uploaded.

Continue (y/n)?y
Enter the hostname:
```

b) Enter **y** twice to continue and enter the hostname and press **Enter**.

Step 4 From **Cisco Unified OS Administration** interface, perform the following task:

a) Choose **Settings** > **IP** > **Ethernet**.
b) Change the hostname.
c) Click **Save**. The server automatically reboots with the new hostname.

Step 5 On changing the hostname/IP address, License MAC of the server changes. Rehost the new license. Old license enters its grace period.

Step 6 Verify the status of Customer Collaboration Platform:

Step 7 Regenerate the SAML certificate through the **Cisco Identity Service Administration**.

If Single Sign-On must be enabled, then perform the following steps:

a. Establish the trust between the Cisco Identity Service and Identity Provider.

b. Log in to the Cisco Unified CCX Administration and navigate to **System** -> **Single Sign-On**.

c. Click **Register** to onboard the SSO components even if you had onboarded the components earlier.

d. You can now enable Single Sign-On after you perform **SSO Test** again.

HostName Modification in High-Availability (HA) Deployment

The character limit for Host Name is 24 characters.

Change HostName for Publisher Server in HA Deployment

Use this procedure to change the hostname of publisher server in a HA deployment.

Note Ensure Single Sign-On is disabled before performing the change in hostname.

Procedure

Step 1 Change the DNS record of the publisher server to point to the new hostname. Ensure that you correctly update both the forward (A) and reverse (PTR) records, and there are no duplicate PTR records.

Step 2 Verify that the DNS change propagates to other nodes by using the **utils network host** <*IP Address*> CLI command on all the cluster nodes.

Step 3 To change the hostname of the publisher on the subscriber node, use either of the following methods:

- CLI commands
- Cisco Cisco Unified OS Administration interface

Using CLI commands:

a) Run the following CLI command on the subscriber node:

set network cluster publisher hostname <hostname>

where `hostname` is the new publisher.

The following output displays:

```
admin:set network cluster publisher hostname hijk-lmn-n1

New Remote hostname: hijk-lmn-n1
```

Using Cisco Unified OS Administration interface:

From interface of the subscriber server, perform the following tasks:

a) Navigate to **Setting** > **IP** > **Publisher**.
b) The Server Configuration page for the publisher server opens. Change the hostname of Publisher server in the **Host Name** or **IP Address** field and then click **Save**.

Step 4 Run the following CLI command on the Subscriber node to update new hostname of the Publisher server :

```
utils uccx modify remote_hostname <Old_hostname_of_Publisher> <New_hostname_of_Publisher>
```

The following output displays:

```
admin:utils uccx modify remote_hostname abcd-efg-n1 hijk-lmn-n1

 Old Remote hostname: abcd-efg-n1
 New Remote hostname: hijk-lmn-n1

This command should be executed only in case you are changing Hostname of remote server.
Are you sure you want to run this command?
Continue (y/n)?
```

Enter **y** and press **Enter**.

Step 5 To change the hostname of publisher server, use either of the following methods:

- CLI commands

Using CLI commands:

a) Run the following CLI command on the publisher node:

```
set network hostname
```

The following output displays:

```
admin:set network hostname


***   W A R N I N G   ***
Do not close this window without first canceling the command.

This command will automatically restart system services.
The command should not be issued during normal operating
hours.

=====================================================
 Note: Please verify that the new hostname is a unique
       name across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
=====================================================
Security Warning : This operation will regenerate
       all UCCX Certificates including any third party
       signed Certificates that have been uploaded.

Continue (y/n)?
```

Enter **y** and press **Enter**.

b) Enter the hostname when prompted. The system services will automatically restart.

Using Cisco Unified OS Administration interface:

Change the hostname using Cisco Unified OS Administration interface of the publisher server:

a) Choose **Settings** > **IP** > **Ethernet**.
b) Change the hostname.
c) Click **Save**. The system services will automatically restart.

Step 6 Reboot all the servers in the cluster including the publisher using the CLI command **utils system restart**.

Note
If you do not reboot the subscriber, all the services on the publisher may not start properly.

Step 7 From the publisher node, run CLI command **utils dbreplication reset all** to resetup Unified CM database replication across the entire cluster.

Step 8 From the publisher node, run CLI command **utils uccx dbreplication reset** to setup Unified CCX database replication across the cluster.

Step 9 On changing the hostname, License MAC changes. Rehost the new license for the new license MAC. Old license enters its grace period.

Step 10 Verify the status of Customer Collaboration Platform:

Step 11 Regenerate the SAML certificate through the **Cisco Identity Service Administration**.

If Single Sign-On must be enabled, then perform the following steps:

a. Establish the trust between the Cisco Identity Service and Identity Provider.

b. Log in to the Cisco Unified CCX Administration and navigate to **System** -> **Single Sign-On**.

c. Click **Register** to onboard the SSO components even if you had onboarded the components earlier.

d. You can now enable Single Sign-On after you perform **SSO Test** again.

Change HostName for Subscriber Server in HA Deployment

Use this procedure to change the hostname of a subscriber server in a HA deployment.

Note Ensure Single Sign-On is disabled before performing the change in hostname.

Procedure

Step 1 Change the DNS record of the subscriber server to point to the new hostname. Ensure that you correctly update both the forward (A) and reverse (PTR) records, and there are no duplicate PTR records.

Step 2 Verify that the DNS change propagates to other nodes by using the **utils network host** <*IP Address*> CLI command on all the cluster nodes.

Step 3 To update new hostname of the subscriber in publisher, enter the following CLI command on the publisher server:

utils uccx modify remote_hostname <Old_hostname_of_Subscriber> <New_hostname_of_Subscriber>

The following output displays:

```
admin:utils uccx modify remote_hostname abcd-efg-h1  ijkl-mno-p2

 Old Remote hostname: abcd-efg-h1
 New Remote hostname: ijkl-mno-p2

This command should be executed only in case you are changing Hostname
of remote server.
Are you sure you want to run this command?
Continue (y/n)?
```

Enter **y** and press **Enter**.

Step 4 To change the hostname of the subscriber server, perform either of the following methods:

- CLI commands
- Cisco Unified OS Administration interface

Using CLI commands:

a) Run the following CLI command on the subscriber server:

set network hostname

The following output displays:

```
admin:set network hostname

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue (y/n):
Continue (y/n)?y
***   W A R N I N G   ***
This command will cause the system to restart
```

```
=====================================================
 Note: Please verify that the new ip address is unique
       across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
       To recognize the new ip address all nodes within
       the cluster will have to be manually rebooted.
=====================================================
Continue (y/n)?y
```

Enter **y** and press **Enter**. The system services will automatically restart.

Using Cisco Unified OS Administration interface:

Change the hostname using Cisco Unified OS Administration interface of the subscriber server:

a) Choose **Settings** > **IP** > **Ethernet**.
b) Change the hostname.
c) Click **Save**. The system services will automatically restart.

Step 5 Restart all the servers in the cluster using the CLI command **utils system restart** .

Note
If you do not reboot the subscriber, all the services on the publisher may not start properly.

Step 6 From the publisher node, run CLI command **utils dbreplication reset all** to resetup Unified CM database replication across the entire cluster.

Step 7 From the publisher node, run CLI command **utils uccx dbreplication reset** to setup Unified CCX database replication across the cluster.

Step 8 Verify the status of CCP.

a) Choose **Subsystems** > **Chat and Email** > **CCP Configuration**.
b) Click **Save** and verify that the **CCP Status** displays green for all the components.

Step 9 If Single Sign-On must be enabled, then reestablish the trust between the Cisco Identity Service and Identity Provider in the Publisher node.

Step 10 Log in to the Cisco Unified CCX Administration and navigate to **System** -> **Single Sign-On**.

Step 11 Click **Register** to onboard the SSO components even if you had onboarded the components earlier.

Step 12 You can now enable Single Sign-On after you perform **SSO Test** again.

Verify Proper Function of System after IP Address/hostname Change

After you change the IP addresses/hostnames of your cluster, complete the following tasks:

Procedure

Step 1 Ensure that all the servers in the cluster are up and available.

Step 2 Check the DB replication status as described in Step 3 of Prepare System for IP Address/hostname Change, on page 146 to ensure all the servers are replicating database changes successfully.

Step 3 Run a manual DRS Backup and ensure that all nodes and active services are successfully backed up.

Step 4 Run the CLI command `utils diagnose module validate_network` through platform CLI on all nodes in the cluster to ensure network connectivity and DNS server configuration are intact.

Step 5 If you have changed the IP address to move the Unified CCX server to a different network, then any firewall configuration on the other network must be changed to permit or deny traffic from the new IP address.

Step 6 If you have created any DSN using old IP address, change the DSN to point to the new IP. For example, the DSN created for Wallboard.

Step 7 Update the new IP address in the following web pages as well:

- **Work Flow Configuration** > **User Interface** > **Browser Setup** - URL and Home Page
- **Work Flow Configuration** > **HTTP Action** - Host
- **Work Flow Configuration** > **IPC Action** - IP Address
- Update the Recording configuration and the Cisco Customer Collaboration Platform configuration in the Unified CCX Administration page on the Publisher server.

Step 8 For Cisco Identity Service, Cisco Finesse and Unified Intelligence Centers users, delete the certificates entries for the old hostname/IP Address from the web browser before you log in to Cisco Identity Service, Cisco Finesse Agent Desktop or Unified Intelligence Center.

Step 9 Reregister the SSO components if the components were registered earlier.

Step 10 Perform the **SSO Test** to check if all the SSO components like CCX, CUIC and Finesse are registered and the test is successful for each component.

Domain Name Modification

This section describes how to change the domain name on single node and HA deployment.

Change the UCCX Domain Name

You can change the Unified CCX domain name based on the requirement. After changing the domain name, you must restart the server (in case of HA setup both publisher and subscriber nodes must be restarted). This regenerates all Unified CCX certificates including any third-party signed certificates. Unified CCX domain name change will not affect your existing license MAC unless the DNS server details are changed.

Before you begin

Before you change the Unified CCX domain name, ensure that you complete the following prerequisites:

- Change the Unified CCX fully qualified domain name (FQDN) in DNS server to reflect the new domain name.
- Ensure that both the forward and reverse lookups on the DNS server returns the fully qualified domain name (FQDN).
- Ensure that all the services are running. Run the following command in the Unified CCX OS platform CLI to verify that all the services are running:

  utils service list

Note If verification fails then identify the cause, resolve the issues to ensure that all the services are running.

- If you are using a HA setup, run the following command to check the database replication status:

  utils dbreplication runtimestate

Note Check if the database replication status is in sync on both the nodes.

Procedure

Step 1 Log in to Cisco Unified Communications OS Platform CLI using administrator username and password.

Step 2 Run the following command on the Unified CCX to set the new domain name:

set network domain <domain-name>

Step 3 Restart the node. Run the following command to restart the node:

utils system restart

Note
If you are using a HA setup, first change the domain name of the publisher node, restart the publisher node and verify that all the services are running. Then change the domain name of the subscriber node, restart the subscriber node, and verify that all the services are running.

What to do next

After changing the Unified CCX domain name, perform the following:

- After restarting the node, run the following command to verify that all the services are running:

  utils service list

- Once the services are running, check if the new domain name is updated. Run the following command to check the domain name:

  show network eth0 detail

- If you are using a HA setup, run the following command to check the database replication status:

  utils dbreplication runtimestate

Note Check if the database replication status is in sync on both the nodes.

- Run the following command to check if all the system tests are passing:

utils diagnose test

- Check the license MAC to find out the difference if the DNS server details and the domain name are changed. Run the following command to check the license MAC:

  show status

- Regenerate the SAML certificate through the **Cisco Identity Service Administration**.

If Single Sign-On must be enabled, then perform the following steps:

1. Establish the trust between the Cisco Identity Service and Identity Provider.
2. Log in to the Cisco Unified CCX Administration and navigate to **System** -> **Single Sign-On**.
3. Click **Register** to onboard the SSO components even if you had onboarded the components earlier.
4. You can now enable Single Sign-On after you perform **SSO Test** again.

Set Up Certificates

Client Requirements

For more information on client requirements, see *Compatibility Information* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

Note Finesse Desktop client machines should be time synchronized with a reliable NTP server for the correct updates to the Duration fields within Live data reports.

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 FQDN of the Unified CCX server to access the desktop.

Procedure

Step 1 From the Firefox browser menu, choose **Options**.

Step 2 Go to **Privacy and Security** tab.

Step 3 Under Certificates section, click **View Certificates**.

Step 4 Select **Authorities**.

Step 5 Click **Import** and browse to the *ca_name*.cer file.

Note

Here the *ca_name* is the name of your certificate.

Step 6 Check the **Validate Identical Certificates** check box.

Step 7 Restart the browser for the certificate to install.

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.

Note
When using Chrome, it is recommended you import your certificates to the Chrome trust store to avoid issues with the Cisco Unified CCX Administration interface. Refer to CSCwa89310 for more details.

Manage Expired CA Certificates

If you receive a certificate expiry alert, it means that the validity of your CA certificate is about to expire, and you can delete it after expiry.

The following table lists the CA certificates, their expiry dates, and the action required.

Certificate Name	Date of Expiry	Action Required
QuoVadis Root CA	17th Mar 2021	None. Delete after expiry.
Sonera class2 CA	6th Apr 2021	None. Delete after expiry.
DST Root CA X3	30th Sep 2021	None. Delete after expiry.
GeoTrust Global CA	21st May 2022	None. Delete after expiry.
Staat der Nederlanden EV Root CA	08th Dec 2022	None. Delete after expiry.

Exit Unified CCX Administration

To exit Unified CCXAdministration without closing your web browser, you can do either of the following:

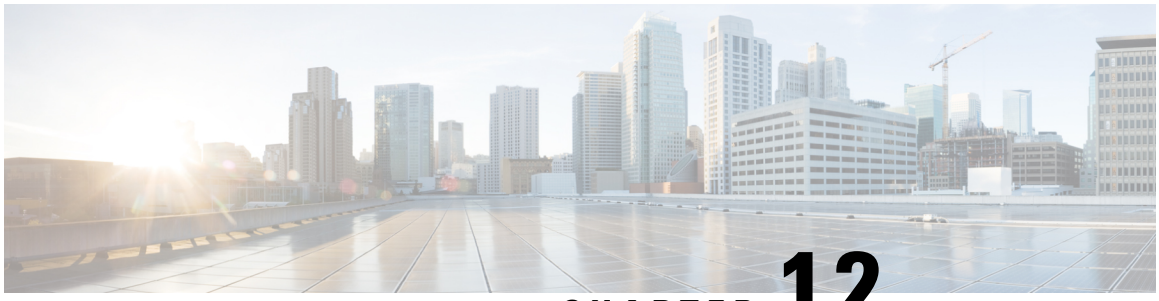
Note You can also exit Unified CCXAdministration by closing your web browser.

Procedure

Step 1 Click the **Logout** link displayed in the top right corner of any Cisco Unified CCX Administration web page

Step 2 Choose **System** > **Logout** from the Unified CCXAdministration menu bar.

The system logs you out of Unified CCX and displays the Unified CCX Authentication web page.



CHAPTER 12

Unified CCX Reporting

- Reporting Administration on Unified CCX, on page 165
- Reporting Administration on Unified Intelligence Center, on page 204
- Start Unified Intelligence Center, on page 205
- Administrator Overview, on page 205
- Security Overview, on page 206
- User List, on page 206
- Create a User, on page 207
- User Groups, on page 209
- Manage User Permissions, on page 211
- Run As, on page 214
- Audit Trail Logging in Cisco Unified Intelligence Center, on page 215
- Audit Trail Report, on page 215
- Security Considerations, on page 216

Reporting Administration on Unified CCX

Import of Stock Reports

If you import stock reports from Unified Intelligence Center, run the CLI **utils uccx synctocuic permission all** command to reset the permissions of the user groups. For more information, see *utils uccx synctocuic* command in the *Cisco Unified Contact Center Express Administration and Operations Guide*.

Note Do not create a sub-category under the **Stock** category as the permissions for the **Stock** category is automatically reset at midnight.

You can now rename the Stock Reports folder name.

Unified CCX Historical Reports

Historical reports are the preconfigured reports in Unified Intelligence Center. These reports access past data from the historical data source to display information for the specified period of time.

Unified CCX Historical Datastore

In a Unified CCX Cluster, there can be one or more Historical datastores.

Note Support for High Availability and remote servers is available only in multiple-server deployments.

The Historical Unified CCX Datastore can be co-located with the Unified CCX.

Note In a Unified CCX High Availability server with co-resident Cisco Unified Intelligence Center, Cisco Unified Intelligence Center will intelligently point to the appropriate datasource. This will require no manual configuration during failover or in island mode scenario. For more information about Historical datastore, see *Cisco Unified Contact Center Express Serviceability Administration Guide*.

Historical Reporting Configuration

The Unified CCX Historical Reporting subsystem provides you with a way to set up and manage the purging of the Historical Reporting databases.

Setting up Unified CCX for Historical Reporting consists of the following tasks:

1. Configure Automatic Purging, on page 168

Configure Database Server Limits

To limit the performance impact of historical reporting on a particular Unified CCX server, you can configure a maximum number of five client/scheduler database connections per server.

To do so, complete the following steps:

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Tools** > **Historical Reporting** > **Database Server Configuration**.

The Database Server Configuration web page opens with the following fields:

Field	Description
Server Name	The hostname or IP Address of the database server.
Maximum DB Connections for Report Clients Sessions	The maximum number of client and scheduler connections that can access the Historical Reports Database server. There is a limit of instances for the reporting client sessions and the scheduler sessions based on the load that can be run on each server. The following are the limits: • Standalone Setup—1 to 8 instances • High Availability Setup—1 to 16 instances

Step 2 Enter a value in the **Maximum DB Connections for Report Client Sessions** field next to a Server Name.

Step 3 Click **Update**.

The configuration changes take effect.

View Historical Reports

You can view historical reports through the Unified Intelligence Center.

Procedure

Choose **Tools** > **User Management** > **Reporting Capability View**

The User Configuration web page opens.

Purge of Historical Data

As the Unified CCX Engine runs, it collects information about the status and performance of the Unified CCX system. Historical information is stored in a database that can then be accessed to provide reports.

When the database approaches its maximum size, some or all of the data in it must be removed. Removing data from a database is called *purging*.

When the system purges data, it removes data from the db_cra database. It determines what information to purge based on the number of months you specify and on the current date. For example, if you instruct the system to purge data older than 12 months, a purge on January 15 will purge data older than January 15 of the previous year.

Note When you purge data, you permanently delete it. If you want to keep data that will be purged, back up the database.

Unified CCX Administration provides the following features for purging historical reports from the database:

- Daily comparison of the size of the database to a user-specified maximum size
- User-specified time at which the system purges data
- Automatic purging of the database when it exceeds the user-specified maximum sizes
- Automatic purging of the database based on user-specified parameters
- Manual purging of the database

Caution Not configuring the Purge parameters may make your database to be overloaded with large number of records. This leads to call data not being written to database.

Configure Automatic Purging

The Unified CCXEngine performs automatic purging each day at a preset time.

To help keep your system running most efficiently, schedule automatic purging to run when your system is least busy. By default, daily purges are scheduled to run at 01:00 a.m. (01:00 Hrs), but you can change this time.

The system bases its purging activities on a variety of parameters. You can change the default value for any parameter as needed.

The following section contains the procedure for setting the daily purge schedule and auto purge.

Configure Purge Schedule Configuration Parameters

You can change the time of day that the system assesses the need to purge data and the age of data to purge.

When data is purged, the Unified CCX sends a “Database purged” message. This message announces that a purge has taken place and includes an explanation of the purging activity. If the database is approaching its maximum size, then the Unified CCX sends the following message - “Database approaching maximum size”.

The system can send notifications through the following two methods:

- Syslog (system log)
- SNMP traps

To set the purge schedule configuration parameters, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Tools** > **HistoricalReporting** > **Purge Schedule Configuration**.

The Purge Schedule Configuration area opens. The following fields are displayed in the Purge Schedule Configuration area.

Field	Description
Purge Schedule	
Daily purge at	Time of day for the daily purge along with the time zone. The time that appears here is based on the primary time zone, which is specified during initial setup of Unified CCX Administration. In a High Availability over WAN deployment, the purge schedule will happen at the time zone of the primary node. **Note** Unified CCX to Unified Intelligence Center sync runs as part of the purge. It synchronizes the users, teams and grants Live Data report permissions.
Purge data older than	Data can persist for a number of months before being purged.
Purge run time	The total duration for which the purge process should run.

Field	Description
Auto Purge Configuration	
Initiate automatic purge when database exceeds	Percentage of the maximum database size at which an automatic purge is initiated (as compared to the total available size).
Initiate automatic purge when extent size exceeds	Percentage of the maximum extents size of any table above which an automatic purge is initiated.
Auto purge data for the oldest	Age of data to be purged.

Step 2 From the drop-down list in the Daily purge at field, choose a time of day at which the system determines if purging is necessary.

Step 3 From the drop-down list in the Purge data older than field, choose the required number of months.

If the system determines that purging is necessary, it will purge both databases of data that is older than the number of months specified in this field.

Step 4 From the drop-down list in the Purge run time field, specify the required number of hours.

If the system determines that purging is necessary, it will purge both databases of data within the specified duration of time.

Step 5 From the drop-down list in the Initiate automatic purge when database size exceeds field, accept the default, or choose another number.

Step 6 From the drop-down menu in the Auto purge data for the oldest field, accept the default of **15**, or choose another number.

Step 7 From the drop-down list in the initiate automatic purge when extent size exceeds field, accept the default , or choose another number.

Step 8 Click **Update** icon that displays in the tool bar in the upper, left corner of the window or the **Update** button that displays at the bottom of the window.

The new purge schedule configuration is added to the Unified CCX system.

Purge Manually

You can manually purge the databases at any time. This action will not affect the automatic purging schedule.

Note Support for High Availability is available only in multiple-server deployments.

To manually purge historical data, complete the following steps.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Tools** > **HistoricalReporting** > **Purge Now**.

The Purge Now web page opens. The Purge data older than field is displayed in the Purge Now web page. You can specify this field in months and days.

Step 2 From the drop-down list in the Purge data older than *N* months field, keep the default (13 months) or specify the required number of months.

If the system determines that purging is necessary, it will purge both databases of data that is older than the number of months specified in this field.

The Initiate automatic purge when database exceeds field displays the current historical database size as compared to the total available size.

Step 3 From the drop-down list in the Purge data older than *N* days field, keep the default (15 days) or specify the required number of days.

If the system determines that purging is necessary, it will purge both databases of data that is older than the number of days specified in this field.

Step 4 From the drop-down list in the Purge run time, keep the default (7 hours) or specify the required number of hours.

If the system determines that purging is necessary, it will purge both databases of data within the specified duration of the time .

Step 5 Click **Purge Now**.

The database purge is initiated in the server and the Purge Now area refreshes.

Unified CCX to Unified Intelligence Center Synchronization

The Unified CCX to Unified Intelligence Center synchronization runs as part of daily purge at midnight.

The following updates occur during the synchronization:

- Based on the user role (agent, supervisor, or reporting user) configured in Unified CCX, the corresponding user in Unified Intelligence Center gets added to the respective group (agent, supervisor or reporting group). The groups have predefined permissions for folders, reports and report definitions. If you edit the permissions manually in Unified Intelligence Center, these changes are reset to the predefined settings during the daily purge.
- Unified CCX sets the group association for its users based on the highest level role (reporting user, supervisor or agent) for the user. Any custom group associations that may have been done on Unified Intelligence Center is retained.
- Users created directly in the co-resident Unified Intelligence Center are removed. However, users created in the standalone Unified Intelligence Center are retained.
- Custom user groups remain unchanged unless they refer to agent, supervisor, and reporting groups and these groups get reset during the synchronization.

File Restore

Use the File Restore menu option to restore the database records written to HR files when the database goes down.

Unified CCX Real-Time Reports

When the Unified CCX system is configured and functioning, you can run reports to monitor real-time activity using the Unified CCXAdministration web interface.

You must be logged into the Unified CCX Administration web interface to run Unified CCX real-time reports.

Available Unified CCX Real-Time Reports

Unified CCX real-time reporting provides real-time reports you can use to monitor Unified CCX system activity. The following table briefly describes each of these reports.

Report	Description
Application Tasks	Provides information about currently active applications.
Application Tasks Summary	Provides a summary of specific application activity.
Applications	Provides a list of all applications loaded on the Unified CCX server.
Contacts Summary	Provides information for call contacts, email contacts, and HTTP contacts. Also provides the total number of contacts. **Note** Calls made by the Outbound subsystem will not be displayed in the Contacts Summary Real-Time Report.
Contacts	Provides information about currently active contacts.
Chat CSQ Cisco Unified Contact Center Express Stats	Provides information about Chat CSQ activity. This report is available only if Unified CCX has been configured.
Chat Resource Cisco Unified Contact Center Express Stats	Provides information about Chat Unified CCX resources activity.
CSQ Cisco Unified Contact Center Express Stats	Provides information about CSQ activity. This report is available only if Unified CCX has been configured.
Data Source Usage	Provides information about configured data source names (DSNs).
Engine Tasks	Provides information about currently active Engine tasks.

Report	Description
Preview Outbound Campaign Cisco Unified Contact Center Express Stats	Provides information about real-time Unified CCX information for the Outbound preview dialer.
Outbound Campaign Stats	Provides real-time statistics on IVR and agent based progressive and predictive Outbound campaigns since the statistics were last reset. **Note** This report will be available only if you have an Outbound license on top of the Unified CCX premium license in your Unified CCX.
Overall Outbound Stats	Provides real-time statistics across all IVR and agent based progressive and predictive Outbound campaigns since the statistics were last reset. **Note** This report will be available only if you have an Outbound license on top of the Unified CCX premium license in your Unified CCX.
Overall Chat Cisco Unified Contact Center Express Stats	Provides information about Chat Unified CCX resources and contact information. This report is available only if Unified CCX has been configured.
Overall Cisco Unified Contact Center Express Stats	Provides information about Unified CCX resources and calls. This report is available only if Unified CCX has been configured.
Resource Cisco Unified Contact Center Express Stats	Provides information about Unified CCX resources activity.
Sessions	Provides information on all active sessions.

Related Topic

Report Menu, on page 176

Open Real-Time Reports

Real-Time reporting is available from the Unified CCXAdministration web interface.

Real-Time Reporting requires the Java plug-in. If the Java plug-in is not already installed on the PC on which you are viewing the reports, the Unified CCX system automatically installs it when you choose **Tools** > **Real Time Reporting Tool**.

Note Real Time Reporting (RTR) tool is downloaded as a .jnlp file and is launched using Java Web Start (JWS). Support for JWS is deprecated from Java 9. To use RTR tool with later versions of Java, use OpenWebStart. For more information on OpenWebstart, go to Install OpenWebStart, on page 339.

Note Use Google Chrome, Mozilla Firefox, or Microsoft Edge to run Real Time Reporting tool.

The Application Reporting web page is a stand-alone component of the Unified CCXAdministration interface. It has its own menu bar, which replaces the Unified CCXAdministration menu bar.

To open real-time reporting, complete the following steps.

Procedure

Step 1 If you are running Real-Time Reporting for the **first time** on this system, log into Unified CCXAdministration as an **Administrator**.

The system prompts you to download the Java plug-in; follow the prompt instructions.

Note
After you perform the initial download of the Real-Time Reporting Java plug-in, non-Administrative users can access Real-Time Reporting on this system.

Step 2 Choose **Tools** > **Real-Time Reporting** from the Unified CCXAdministration menu bar.

The Application Reporting web page opens in a new window. The real-time reporting tool requires a Java plug-in. If the plug-in is not installed on the machine you are using, the Unified CCX system prompts you to accept the automatic installation of the plug-in. If you do not accept the installation, you cannot use real-time reporting.

Run Reports

Open the real-time reporting tool from the Unified CCXAdministration web interface to run reports.

To run a real-time report, complete the following steps.

Procedure

Step 1 From the Application Reporting menu bar, choose **Reports**.

Step 2 From the Reports menu, choose the report to run.

The report opens in the Application Reporting window.

View Detailed Subreports

You can view more detailed information for selected items in these four reports:

- Application Tasks report
- Contacts report
- Applications report
- Sessions report

To view detailed subreports, complete the following steps.

Procedure

Step 1 Run the Application Tasks, Contacts, Applications, or Sessions report.

Step 2 Click a line in the report for which you want to view more detailed information. For example, click an email address in the Contacts report.

Step 3 From the Application Reporting menu bar, choose **Views** and click the subreport that you want to run.

You can also open a subreport by right-clicking the selected item and choosing a subreport.

The subreport opens.

Print Reports

To facilitate printing, you can open a printable version of a report.

To print a report, complete the following steps.

Procedure

Step 1 Run a report.

Step 2 From the Application Reporting menu, choose **Tools** > **Open Printable Report**.

A printable version of the report opens in a separate window.

Step 3 Print the report using your browser print functionality.

Reset Report Statistics

The Unified CCX system automatically resets all statistics each day at midnight. You can reset the accumulated statistics manually at any time. Resetting statistics does not reset active statistics, such as active contacts and active tasks.

To reset report statistics, complete the following steps.

Procedure

Step 1 From the Application Reporting menu bar, choose **Tools** > **Reset All Stats**.

The Reset Stats dialog box opens for you to confirm the reset.

Step 2 Click **Yes**.

Accumulated statistics are reset.

Clear Contact Option for Stuck Calls

You may sometimes see a Contact/Call as waiting in Real Time Reports in CSQ Stats, and even though there are available Agents in the queue, the call does not seem to get routed to these Agents. The waiting time for the Queued call accumulates and will not clear even if the user activates “Reset All Stats” option from the Real-Time Reporting menu.

To enable clearing such stuck call entries from the system, Unified CCX system provides the Clear Contact option. This has the ability to clear stuck calls in the system without requiring a restart of the engine.

Set Report Options

You can set the following reporting options:

- Refresh interval
- Number of times that the Unified CCXAdministration web interface should attempt to reconnect to the Unified CCX server
- Whether logged off users appear in reports

To set report options, complete the following steps.

Procedure

Step 1 From the Application Reporting menu bar, choose **Settings** > **Options**.

The Options dialog box opens.

Step 2 From the Polling Interval drop-down menu, choose the refresh rate in seconds.

Step 3 From the Server Connect Retry Count drop-down menu, choose the number of times that the Unified CCXAdministration web interface should attempt to reconnect to the Unified CCX server.

Step 4 From the Show Logged Off Resources drop-down menu, choose whether logged-off agents appear in reports.

Step 5 Click **Apply** to apply the settings.

Set Report Appearance

You can select from three report appearances:

- Windows, which displays reports in colors based on your Windows settings
- Motif, which displays reports in purple and menu items in brown
- Metal, which displays reports in grey and menu items in black

To set the report appearance:

Procedure

Choose **Settings** from the Application Reporting menu bar and click the appearance that you want.

Application Reporting User Interface

Note Support for High Availability and remote servers is available only in multiple-server deployments.

When you choose **Tools** > **Real-Time Reporting** from the Unified CCXAdministration menu, the Application Reporting tool opens a web page in a new window.

The Application Reporting tool menu bar contains the following options:

- **Report**—Choose this option to display a list of the available top-level real-time reports.
- **Tools**—Choose this option to reset all the statistics and refresh connections.
- **Settings**—Choose this option to set the look and feel of the real-time Reporting client, set the polling (refresh) interval times, and set the amount of times the server will attempt to reconnect.
- **Help**—Choose this option to display system information and to access Unified CCX online help.

Report Menu

Note All real-time reports display a **Last Updated At** field, which indicates the time of the snapshot. All summary reports display both a start time (which indicates when the summary statistics started being collected) and the current time. All real-time reports display a Connected or Not Connected status for each node in the cluster.

The Report menu provides access to a variety of top-level reports. It contains the following menu options:

- Contacts Summary Real-Time Report, on page 178
- Application Tasks Summary, on page 179
- Application Tasks Real-Time Report, on page 180
- Engine Tasks Real-Time Report, on page 180
- Contacts Report, on page 181
- Applications Report, on page 184
- Sessions Report, on page 185

- Data Source Usage Report, on page 185
- Overall Cisco Unified Contact Center Express Stats Report, on page 186
- CSQ Cisco Unified Contact Center Express Stats Report, on page 189
- Preview Outbound Campaign Cisco Unified Contact Center Express Stats Report, on page 190
- Outbound Campaign Stats Report, on page 195
- Overall Outbound Stats Report, on page 197
- Resource Cisco Unified Contact Center Express Stats Report, on page 198
- Failover Behavior for Unified CCX Stats, on page 200

High Availability (HA) Setup

In an HA setup, real-time reports obtain data from both nodes in the cluster.

Note

- Support for High Availability and remote servers is available only in multiple-server deployments.
- In case of island mode where each node (on either side of the network) assumes mastership and handles calls, the real-time reports may not report accurate data.

Failover in a two-node cluster is available for Unified IP IVR reports as described in the following table.

Failover Scenario	Connection Status	Node 1 Status	Node 2 Status
Both nodes are up	Fully Connected	Node ID current/start-time	Node ID current/start-time
Node 1 is up Node 2 is down	Partially Connected	Node ID current/start-time	Node ID Not Connected
Node 1 is down Node 2 is up	Partially Connected	Node ID Not Connected	Node ID current/start-time
Both nodes are down	Not Connected	Node ID Not Connected	Node ID Not Connected

Unified CCX real-time reports obtain data only from the current master node—failover in a two-node cluster is available as described in the following table.

Failover Scenario	Connection Status	Node 1 Status	Node 2 Status
Both nodes are up Node 1 is master	Fully Connected	Node ID current/start-time	Node ID Not Connected
Node 1 is master Node 2 is down	Fully Connected	Node ID current/start-time	Node ID Not Connected
Node 1 is down Node 2 is master	Fully Connected	Node ID Not Connected	Node ID current/start-time

Failover Scenario	Connection Status	Node 1 Status	Node 2 Status
Both nodes are down	Not Connected	Node ID Not Connected	Node ID Not Connected

Contacts Summary Real-Time Report

Use the Contacts Summary report to view specific contact information for call contacts, email contacts, HTTP contacts, and total number of contacts.

To access the Contacts Summary real-time report, choose **Reports** > **Contacts Summary** from the Application Reporting menu bar.

Note You display the data on this report as numbers or percentages by clicking the Display Value/Display % toggle button.

The following fields are displayed on the Contacts Summary report.

Field	Description
Active	Active contacts that are currently running.
Inbound	Number of inbound contacts since the statistics were last reset.
Outbound	Number of outbound contacts since the statistics were last reset.
Connected	Number of connected contacts since the statistics were last reset. Provides a total for contacts that are connected to resources (for example, a call connected to an ACD agent).
Terminated	Number of terminated contacts since the statistics were last reset. This row reports contacts that are ended generally by the application (for example, a caller stops responding and the application terminates), indicating whether the contact was terminated: • Locally—On the local server. • Remotely—On a remote server in the cluster. **Note** Use the + toggle button to access these statistics.

Field	Description
Rejected	Number of rejected contacts since the statistics were last reset. This row reports contacts that are not accepted and processed (as a result, for example, of insufficient resources or the rejection of the contact based on some customer-defined logic). Indicates the reason code for the reject: • Channels busy • No channel license • No trigger Use the + toggle button to access these statistics.
Aborted	Number of aborted contacts since the statistics were last reset. This row reports contacts improperly ended by a task associated with the application (as when, for example, the system generates an exception or can not invoke the application because of some error in the application) and includes the associated Java exception code. **Note** Java exception codes are dynamic, as they can be generated from a variety of sources. **Note** Use the + toggle button to access these statistics.
Handled	Number of handled contacts since the statistics were last reset. This row reports contacts that are explicitly marked “Handled” by the application (typically when the application connects the contact to a Unified CCX agent).
Abandoned	Number of abandoned contacts since the statistics were last reset. This row reports contacts that end without being marked “Handled” by the application.

Application Tasks Summary

Use the Application Tasks Summary report to display statistics that summarize the activity of specific applications.

To access the Application Tasks Summary real-time report, choose **Reports** > **Application Tasks Summary** from the Application Reporting menu bar.

The following fields are displayed on the Application Tasks Summary report.

Field	Description
Application Name	Names of the applications that are running or have run.
Running	Currently running applications.
Completed	Applications that have stopped running.
Total	Number of times an application was invoked since the statistics were last reset.

Field	Description
DTMF VB and AA	Application names configured from the Unified CCX Administration.
Status	Displays the failover connection status. The possibilities are: Fully connected, Partially connected, and Not connected. See the following tables for detailed status information for Unified IP IVR and Unified CCX reports.

Application Tasks Real-Time Report

Use the Application Tasks real-time report to view information about currently active applications.

To access the Application Tasks report, choose **Reports** > **Application Tasks** from the Application Reporting menu bar. The following fields are displayed on the Application Tasks report.

Field	Description
ID	Unique application task ID.
Node ID	Unique ID for a server in the cluster.
Application	Name of the application.
Start Time	Time when the application task started.
Duration	Length of time that the application has been active.

Note If this report indicates that an application is running for an unusually long time, there may be a problem with the application. The application script may not include error handling that prevents infinite retries if a call is no longer present. If the application does not receive a disconnect signal after a call, the application repeatedly retries to locate the call, and causes the application to run for an unusually long time. To prevent this problem, include the proper error handling in the application script.

Engine Tasks Real-Time Report

Use the Engine Tasks real-time report to view information about currently active Engine tasks.

To access the Engine Tasks report, choose **Reports** > **Engine Tasks** from the Application Reporting menu bar.

The following fields are displayed on the Engine Tasks report.

Field	Description
ID	Unique identifier of the engine task. If the engine task is the main task running the application and the parent ID is empty, its identifier will match the Application Task Identifier.
Parent ID	Unique identifier for the parent of the engine task (if any).
Node ID	Unique identifier for a server in the cluster.

Field	Description
Server IP Address	IP address identifying the server in the cluster.
Script	Name of the script that is running the task (if the task is running a Unified CCX script).
Start Time	Time that the task started.
Duration	Length of time the task has been active.

Contacts Report

Use the Contacts real-time report to view information for all the active contacts for all servers across clusters.

Note Support for High Availability and remote servers is available only in multiple-server deployments.

To access the Contacts report, choose **Reports** > **Contacts** from the Application Reporting menu bar.

You can access detailed information about specific contacts listed on the Contacts web page by performing one of the following procedures:

- Call Contacts Detailed Info Report, on page 182
- Email Detailed Info Report, on page 182
- HTTP Detailed Info Report, on page 183

The following fields are displayed on the Contacts report.

Field	Description
ID	Unique identifier representing a contact.
Type	Type of contact: Unified CM Telephony call, Cisco agent call, or
Impl ID	Unique identifier provided by the particular type of contact. For example, for a call contact, this identifier would represent the Unified CM global call ID.
Node ID	Unique identifier for a server in the cluster.
Start Time	Time stamp when the contact was created.
Duration	Length of time that the contact is active.
Handled	If True, the contact is handled; if False, the contact is not handled.
Aborting	If True, the contact is aborted with a default treatment; if False, the contact is not aborted.
Application	Name of the application currently managing the contact.
Task	Unique identifier of the application task that is currently responsible for the contact.
Session	Unique identifier of the session currently managing the contact (if any).

Note The information displayed is dependent on the type of contact selected. Depending on the type of call, some fields may not be supported and will appear blank.

Call Contacts Detailed Info Report

Use the Call Contacts Detailed Info real-time report to view all information related to the call contact.

To access the Call Contacts Detailed Info report, right-click a specific call contact record on the Contacts report; information for that specific record displays.

The following fields are displayed on the Call Contacts Detailed Info report.

Field	Description
State	Current state of the contact.
Inbound	If True, this call was received by the Unified CCX server; if False, this call was placed as an outbound call by an application.
Language	The selected language context of the call.
Application ID	Unique identifier of the associated application.
Called Number	Called number for this call leg from the perspective of the called party.
Dialed Number	Dialed number for this call leg from the perspective of the calling party.
Calling Number	Calling number of the originator of this call.
ANI	Automatic number identification.
DNIS	Dialed number identification service.
CLID	Caller ID.
Arrival Type	Information on how the call contact arrived in the system.
Last Redirected Number	Number from which the last call diversion or transfer was invoked.
Original Called Number	Originally called number.
Original Dialed Number	Originally dialed number.
ANI Digits	Automatic Number Identification information indicator digit codes.
CED	Entered digits that were gathered by the network before the call was received.

Email Detailed Info Report

Use the Email Detailed Info real-time report to view all information related to the email contact.

To access the Email Detailed Info report, right-click a specific email contact record on the Contacts report; information for that specific record displays.

The following fields are displayed on the Email Detailed Info report.

Field	Description
State	Current state of the contact.
Inbound	If True, this email message was received by the Unified CCX server; if False, this email was created by an application. **Note** Inbound email messages are not currently supported.
Language	Selected language context of the email message.
Application ID	Unique identifier of the associated application.
From	Sender of this email message.
To	All the recipients of this email message.
Subject	"Subject" field of this email message.
Attachments	List of all attachments (file names) associated with this email message.

HTTP Detailed Info Report

Use the HTTP Detailed Info real-time report to view all information related to the HTTP contact.

To access the HTTP Detailed Info report, right-click a specific HTTP contact record in the Contacts report; information for that specific record displays.

The following fields are displayed on the HTTP Detailed Info report.

Field	Description
State	Current state of the contact.
Inbound	If True, this HTTP request was received by the Unified CCX server; if False, this HTTP request was created by an application. **Note** This information will always be reported as True, because the Unified CCX server does not currently track outbound HTTP requests in this way.
Language	Language currently associated with the HTTP request.
Application ID	Unique identifier of the associated application.
Authentication Type	Name of the authentication scheme used to protect the servlet; for example, "BASIC" or "SSL."
Character Encoding	Length, in bytes, of the request body, which is made available by the input stream, or -1 if the length is not known. **Note** This length is the same as the value of the CGI[2] variable CONTENT_LENGTH.

Field	Description
Content Length	MIME type of the body of the request, or null if the type is not known. **Note** This is the same as the value of the CGI variable CONTENT_TYPE.
Content Type	Type of HTTP contact request.
Request Language	Preferred language for client content (the language that the client accepts for its content), based on the Accept-Language header.
Path Info	Any extra path information associated with the URL the client sent when the HTTP request was made.
Protocol	Name and version of the protocol the request uses in the form: *protocol/majorVersion.minorVersion*; for example, HTTP/1.1 **Note** This value is the same as the value of the CGI variable SERVER_PROTOCOL.
Remote Address	IP address of the client that sent the request **Note** This value is the same as the value of the CGI variable REMOTE_ADDR.
Remote Host	Fully qualified name of the client that sent the request, or the IP address of the client, if the name cannot be determined **Note** This value is the same as the value of the CGI variable REMOTE_HOST.
Remote User	Login of the user making this request, if the user has been authenticated.
Requested Session ID	HTTP session ID as specified by the client.
Request URL	Section of the URL of the HTTP request, from the protocol name up to the query string in the first line of the HTTP request.

[2] CGI = Common Gateway Interface

Applications Report

Use the Applications real-time report to view all the applications loaded on the server.

To access the Applications report, choose **Reports** > **Applications** from the Application Reporting menu bar.

The following fields are displayed on the Applications report.

Field	Description
Name	Unique name of the currently loaded application.
ID	Application ID.
Type	Type of application that is currently running (for example, a Cisco Script Application).

Field	Description
Description	Description of the application as entered on the Unified CCXAdministration web site.
Enabled	If True, the application is enabled; if False, the application is disabled.
Max. Sessions	Maximum number of simultaneous task instances that can run simultaneously on the Unified CCX server.
Valid	If True, the application is valid; if False, the application is invalid.[3]

[3] An application is valid if it was successfully loaded and initialized from its configuration. At any time, an application can become invalid if it internally fails to be refreshed.

Sessions Report

Use the Sessions real-time report to view real-time information on all the active sessions.

To access the Sessions report, choose **Reports** > **Sessions** from the Application Reporting menu bar.

The following fields are displayed on the Sessions report.

Field	Description
ID	Session ID. **Note** This identifier is guaranteed to remain unique for a period of 12 months.
Mapping ID	User- or system-defined identifier that maps to this session.
Node ID	Unique identifier for a server in the cluster.
Parent	Sessions that were created as a result of consult calls propagated in the system.
Creation Time	Creation time of the session.
State	Current state of the session. **Note** When marked IDLE, the session is subject to being “garbage collected” by the system after a specified period of time. In addition, a session is IN_USE if it still has a contact associated or a child session.
Idle Time	Length of time that the session has been idle.

Data Source Usage Report

Use the Data Source Usage real-time report to view real-time information on all configured Data Source Names (DSNs).

To access the Data Source Usage report, choose **Reports** > **Datasource Usage** from the Application Reporting menu bar.

The following fields are displayed on the Data Source Usage report.

Field	Description
Data Source Name	Name of the data source, as configured through the Unified CCXAdministration web interface.
Available Connections	Number of connections available.
Busy Connections	Number of busy connections. **Note** Busy + available = Maximum number of connections configured.
Checkouts Granted	Number of times the database connections have been used up since the statistics were last reset.
Checkouts Denied	Number of times the Database connections have been denied since the statistics were last reset.

Overall Cisco Unified Contact Center Express Stats Report

Use the Overall Cisco Unified Contact Center Express Stats real-time report to view real-time Unified CCX resource and call information.

Note Unified CCX reports contain information for calls that have been queued in one or more CSQs. If a call is not queued (for example, the caller hangs up before being queued), the reports do not display data for that call.

Unified CCX reports retrieve the following statistics:

- Unified CCX statistics from the current Master node.
- Unified IP IVR statistics from all nodes in the cluster.

To access the Overall Unified CCX Stats report, choose **Reports** > **Overall Cisco Unified Contact Center Express Stats** from the Application Reporting menu bar.

Note Preview Outbound durations are updated when the preview outbound call disconnects and all agents (resources) involved in the call move out of the Work and Talking state.

The following fields are displayed on the Overall Cisco Unified Contact Center Express Stats report.

Field	Description
Resource Information	
CSQs	Number of CSQs currently configured. If a CSQ is added or removed, this statistic reflects that change.
Logged-in Resources	Number of resources currently logged in.

Field	Description
Talking Resources	Number of resources currently talking. **Note** This number includes resources in Talking, Work, and Reserved states.
Ready Resources	Number of resources currently ready.
Not Ready Resources	Number of resources currently not ready.
Call Information — Inbound	
Total Contacts	Number of total contacts that have arrived since the statistics were last reset. This includes contacts that are waiting, contacts connected to a resource, and contacts that have disconnected. If a resource transfers to or conferences with a route point, this value increases.
Contacts Waiting	Number of contacts waiting to be connected to a resource. **Note** A contact is shown as waiting until the call is *answered* by the agent. This means that, even if the phone is ringing at the agent, the contact will still show as waiting in RTR.
Oldest Contact in Queue	Displays the wait time for the oldest contact in the queue.
Contacts Handled	Number of contacts that have been handled by a resource.
Contacts Abandoned	Number of contacts that have arrived and disconnected before being connected to a resource.
Avg Talk Duration	Average duration (in seconds) that resources spend talking on Unified CCX contacts. Talk duration starts when a contact first connects to a resource and ends when the contact disconnects from the last resource to which it was connected. Talk duration does not include hold time.
Avg Wait Duration	Average wait time (in seconds). It begins when the contact enters the system and ends when the contact stops waiting. Wait duration does not include hold time. The time a contact spends on a CTI port prior to getting queued is included in this report.
Longest Talk Duration	Longest talk duration (in seconds) of a contact. Talk duration does not include hold time.
Longest Wait Duration	Longest wait (in seconds) for a contact to be connected to a resource. Wait duration does not include hold time.
Call Information — Preview Outbound	
Active	Total number of preview outbound calls currently previewed or connected to agents.

Field	Description
Preview	Total number of preview outbound calls currently previewed but have not been accepted, rejected. or closed by the agents.
Connected	Total number of preview outbound calls currently connected to agents. When an agent conferences in other agents, the call is counted once towards the total number of connected calls.
Offered	Total number of preview outbound calls offered. A call is considered offered when it is presented to an agent. A contact that is presented to an agent, skipped/rejected by that agent, and then presented to the same agent or to another agent is counted twice towards the number of calls offered. Offered = Accepted + Rejected + Closed + Timed-out.
Accepted	Total number of preview outbound calls accepted. A call is considered accepted if an agent has clicked Accept when presented the call. A call that is presented to an agent, skipped/rejected by that agent, presented to another agent, and then accepted by that other agent is counted once towards the number of calls accepted.
Rejected	The number of preview outbound calls that were skipped or rejected by an agent. This means that the agent selected Reject, Skip, or Cancel Reservation. These contacts will be dialed again. If a contact is rejected by multiple agents, this field increments each time the contact is rejected. The number Rejected is also incremented each time an agent drops the preview call while it is ringing at the customer's contact.
Closed	The number of preview outbound contacts that were closed by agents. This means that the agent selected Skip-Close or Reject-close. These contacts will not be dialed again.
Timed-Out	Total number of preview outbound calls that timed out. A call is considered timed out when it is presented to an agent and not accepted, rejected, or closed within the allocated time. These contacts will be dialed again. If a contact timed out multiple agents, this field is incremented each time the contact is timed out for each agent.
Invalid Number	The number of preview outbound calls that were dialed to an invalid number. This means that the agent accepted the call (by clicking Accept), got connected to the customer, and selected the Invalid Number option from the contact Reclassification drop down. It also includes the number of preview outbound calls that failed at the network level. **Note** The agent can manually reclassify the contact as Invalid Number while the customer contact is on the call or when the agent has gone into the Work state after the call.
Voice	The number of preview outbound calls that ended in successful customer contact. This means that an agent accepted the call (by clicking Accept) *and* selected a classification of Voice (default) or Do Not Call for this contact.

Field	Description
Answering Machine	The number of preview outbound calls that connected to an answering machine for this campaign. This means that the agent accepted the call (by clicking Accept), got connected to the answering machine and selected the Answering Machine option from the contact Reclassification drop down. **Note** The agent can manually reclassify the contact as Answering Machine while the customer contact is on the call or when the agent has gone into the Work state after the call.
Requested Callback	The number of contacts marked for callback. This means that the agent accepted the call (by clicking Accept), got connected to the contact, the contact requested a callback, and the agent selected the CallBack option. A call that is accepted by an agent, marked for callback, later presented to and accepted by another agent (at the callback time), and marked for callback again is counted twice towards the number of callback calls.
Avg Outbound Talk Duration	The average time in HH:MM:SS (hours, minutes, seconds) that agents spend talking on outbound calls. The durations consider all calls that were Agent Accepted and classified as Voice. If a preview outbound call is transferred or conferenced to a route point, this average outbound talk duration does not include the talk time of agents who handle the call after it came through the route point. Instead, the talk time is included in the inbound talk duration.
Longest Outbound Talk Duration	The longest talk duration of a preview outbound call in HH:MM:SS (hours, minutes, seconds). The durations consider all calls that were Agent Accepted and classified as Voice.

CSQ Cisco Unified Contact Center Express Stats Report

Use the CSQ Cisco Unified Contact Center Express Stats real-time report to view real-time information.

Note Unified CCX reports contain information for calls that have been queued in one or more CSQs. If a call is not queued, the reports do not display data for that call. .

To access the CSQ Cisco Unified Contact Center Express Stats report, choose **Reports** > **CSQ Cisco Unified Contact Center Express Stats** from the Application Reporting menu bar.

The following fields are displayed on the CSQ Cisco Unified Contact Center Express Stats report.

Field	Description
Name	Name of the CSQ.

Field	Description
Talking/Ready Resources/Not Ready Resources/Logged-In Resources	Number of resources who are in the talking, ready, and not ready states, and the number of resources logged in for this CSQ. Values for the four items are separated by colons. Values are displayed in the same order that the items appear in the column heading. **Note** This number includes resources in Talking, Work, and Reserved states. If you are logged into the Unified CCX Administration web interface as a Supervisor and opening the Real-Time Reporting plug-in, you will be able see all the logged in agents from all the teams independent of team membership.
Total Contacts	Number of total contacts since the statistics were last reset for this CSQ.
Contacts Waiting	Number of contacts waiting to be connected to a resource in this CSQ. This column also displays how long the oldest contact has been waiting.
Contacts [oldest contact in queue]	Duration of longest currently waiting contact.
Contacts Handled	Number of contacts that have been handled by this CSQ.
Contacts Abandoned	Number of contacts that have been abandoned by this CSQ.
Contacts Dequeued	Number of contacts that have been dequeued from this CSQ.
Avg Talk Duration	Average time (in seconds) agents in this CSQ spent talking to contacts.
Avg Wait Duration	Average wait time (in seconds). It begins when the call was queued (when you run the "Select Resource" step) and ends when the call reaches the agent. Wait duration does not include hold time.The time a contact spends on a CTI port prior to getting queued is not included in this wait time.
Longest Talk Duration	Longest time (in seconds) agents in this CSQ spend talking to contacts.
Longest Wait Duration	Longest wait (in seconds) for a contact to be connected to a resource.

Preview Outbound Campaign Cisco Unified Contact Center Express Stats Report

Use the Preview Outbound Campaign Cisco Unified Contact Center Express Stats real-time report to view real-time Unified Contact CCX information for the Outbound preview dialer.

To access the Preview Outbound Campaign Cisco Unified Contact Center Express Stats report, choose **Reports** > **Preview Outbound Campaign Cisco Unified Contact Center Express Stats** from the Application Reporting menu bar.

The following fields are displayed on the Preview Outbound Campaign Cisco Unified Contact Center Express Stats report.

Field	Description
Campaign	The name of the preview outbound campaign.

Field	Description
Status	The current activation state of the preview outbound campaign: • Running: an active preview outbound campaign • Stopped: an inactive preview outbound campaign
Active	Total number of outbound calls currently previewed by or connected to agents for this preview outbound campaign. Active Calls = Previewed + Connected.
Preview	Total number of outbound calls currently previewed but have not been accepted, rejected or closed by the agents as part of this preview outbound campaign.
Connected	Total number of outbound calls currently connected to agents for this preview outbound campaign. When an agent conferences in other agents, the call is counted once towards the total number of connected calls.
Offered	Total number of outbound calls offered for this preview outbound campaign. A call is considered offered when it is presented to an agent as part of this preview outbound campaign. A contact that is presented to an agent, rejected by that agent, and then presented to the same agent or to another agent is counted twice towards the number of calls offered. Offered = Accepted + Rejected + Closed + Timed-out.
Accepted	Total number of outbound calls accepted for this preview outbound campaign. A call is considered accepted if an agent has clicked Accept when presented the call. A call that is presented to an agent, rejected by that agent, presented to another agent, and then accepted by that other agent is counted once towards the number of calls accepted.
Rejected	The number of outbound calls that were rejected by an agent as part of this preview outbound campaign. This means that the agent selected Reject or Cancel Reservation. These contacts will be dialed again. If a contact is rejected by multiple agents, this field increments each time the contact is rejected. The number Rejected is also incremented each time an agent drops the preview call while it is ringing at the customer contact.
Closed	The number of outbound contacts that were closed by agents as part of this preview outbound campaign. This means that the agent selected Reject-close. These contacts will not be dialed again.
Timed-Out	Total number of outbound calls that timed out. A call is considered timed out when it is presented to an agent and not accepted, rejected, or closed within the allocated time. These contacts will be dialed again. If a contact times out for multiple agents, this field is incremented each time the contact is timed out for each agent.

Field	Description
Invalid Number	The number of outbound calls that were dialed to an invalid number for this preview outbound campaign. This means that the agent accepted the call (by clicking Accept), got connected to the customer, and selected the "Invalid Number" option from the contact Reclassification drop down. It also includes the number of outbound calls that failed at the network level. **Note** The agent can manually reclassify the contact as Invalid Number while the customer contact is on the call or when the agent has gone into the Work state after the call.
Voice	The number of outbound calls that ended in successful customer contact. This means that an agent accepted the call (by clicking Accept) *and* selected a classification of Voice or Do Not Call for this contact.
Answering Machine	The number of outbound calls that connected to an answering machine for this preview outbound campaign. This means that the agent accepted the call (by clicking Accept), got connected to the answering machine and selected the Answering Machine option from the contact Reclassification drop down. **Note** The agent can manually reclassify the contact as Answering Machine while the customer contact is on the call or when the agent has gone into the Work state after the call.
Requested Callback	The number of contacts marked for callback for this preview outbound campaign. This means that the agent accepted the call (by clicking Accept), got connected to the contact, the contact requested a callback, and the agent selected the CallBack option. A call that is accepted by an agent, marked for callback, later presented to and accepted by another agent (at the callback time), and marked for callback again is counted twice towards the number of callback calls.
Avg Talk Duration	The average time in HH:MM:SS (hours, minutes, seconds) that agents spend talking on outbound calls for this preview outbound campaign. The durations consider all calls that were Agent Accepted and classified as Voice. If a call is transferred or conferenced back to the route point, the preview outbound campaign talk duration does not handle the talk time of agents who handle the call after it came through the route point.
Longest Talk Duration	The longest talk duration of an outbound call in HH:MM:SS (hours, minutes, seconds) for this preview outbound campaign. The durations consider all calls that were Agent Accepted and classified as Voice.

Chat CSQ Cisco Unified Contact Center Express Stats Report

Use the Chat CSQ Cisco Unified Contact Center Express Stats real-time report to view real-time queue information. This report is available in Cisco Unified CCX Premium license package.

Note Unified CCX reports contain information for a chat contact that are queued with a specific CSQ. If a contact is not queued, the reports do not display data for that chat contact.

To access the Chat CSQ Cisco Unified Contact Center Express Stats report, choose **Reports > Chat CSQ Cisco Unified Contact Center Express Stats** from the Application Reporting menu bar.

The following fields are displayed on the Chat CSQ Cisco Unified Contact Center Express Stats report.

Field	Description
Name	Name of the chat CSQ
Busy Resources/ Ready Resources/ Not Ready Resources/ Logged-In Resources	Number of resources who are in the Busy, Ready, and Not Ready states, and the number of agents logged in for this chat CSQ. Values for the four items are separated by colons. Values are displayed in the same order that the items appear in the column heading. **Note** If you are logged in to the Unified CCX Administration web interface as a supervisor and you open the Real-Time Reporting plug-in, you can see all the logged-in agents from all the teams.
Total Contacts	Number of total contacts presented to this queue since last reset of statistics.
Contacts Waiting [Oldest Contact in Queue]	Number of contacts waiting in this queue with the duration of longest waiting contact in this queue.
Contacts Handled	Number of contacts that have been handled by this queue since last reset of statistics.
Contacts Abandoned	Number of contacts that have been abandoned in this queue since last reset of statistics.
Avg Contact Handling Duration	Average time (in HH:MM:SS) agents in this CSQ spent chatting with contacts.
Avg Wait Duration	Average wait time (in HH:MM:SS) a contact spent in queue waiting for an agent.
Longest Contact Handling Duration	Longest time (in HH:MM:SS) agents in this CSQ spent chatting with contacts.
Longest Wait Duration	Longest wait (in HH:MM:SS) for a contact to be connected to an agent.

Chat Resource Cisco Unified Contact Center Express Stats Report

Use the Chat Resource Cisco Unified Contact Center Express Stats real-time report to view real-time Unified CCX chat resource information. This report is available in Cisco Unified CCX Premium license package.

To access the Chat Resource Cisco Unified Contact Center Express Stats report, choose **Reports > Chat Resource Cisco Unified Contact Center Express Stats** from the Application Reporting menu bar.

The following fields are displayed on the Chat Resource Cisco Unified Contact Center Express Stats report:

Field	Description
Name (ID)	Unique identifier of the resource.
State	Current state of the resource.
Current Active Contacts	Number of active contacts that the agent is handling.
Duration in State	Length of time (in HH:MM:SS) the resource has remained in the current state.
Avg Resource Busy Duration	Average time the agent spent with contacts. The resource busy duration is the elapsed time between the resource accepting the contact and completing the chat by clicking End.
Longest Resource Busy Duration	Longest time the agent spent with a contact. The resource busy duration is the elapsed time between the resource accepting the contact and completing the chat by clicking End.
Contacts Presented	Number of contacts that have been presented to this resource.
Contacts Handled	Number of contacts that have been handled by this resource.

Overall Chat Cisco Unified Contact Center Express Stats Report

Use the Overall Chat Cisco Unified Contact Center Express Stats real-time report to view real-time Unified CCX resource and contact information. This report is available in Cisco Unified CCX Premium license package.

Note Unified CCX reports contain information for contacts that have been queued in one or more CSQs. If a contact is not queued, the reports do not display data for that contact.

To access the Overall Chat Unified CCX Stats report, choose **Reports > Overall Chat Cisco Unified Contact Center Express Stats** from the Application Reporting menu bar.

The following fields are displayed on the Overall Chat Cisco Unified Contact Center Express Stats report.

Field	Description
Resource Information	
CSQs	Number of chat CSQs currently configured. If a chat CSQ is added or removed, this statistic reflects that change.
Logged-in Resources	Number of resources currently logged in.
Busy Resources	Number of resources currently busy.
Ready Resources	Number of resources currently ready.
Not Ready Resources	Number of resources currently not ready.

Field	Description
Contact Information	
Total Contacts	Number of total contacts that have arrived since the statistics were last reset. This includes contacts that are waiting, contacts connected to a resource, and contacts that have disconnected.
Contacts Waiting	Number of contacts waiting to be connected to a resource. **Note** A contact is shown as waiting until the contact is answered by the agent.
Oldest Contact in Queue	Displays the wait time for the oldest contact in the queue.
Contacts Handled	Number of contacts that have been handled by a resource.
Contacts Abandoned	Number of contacts that are routed to the CSQ since midnight but are abandoned due to one of the following: • Customer ended the chat as the chat was not answered by an agent. • Customer chat was disconnected. • No agents were available. • All agents were busy.
Avg Contact Handling Duration	Average duration (in HH:MM:SS) that resources spent chatting on Unified CCX contacts. Chat duration starts when a contact first connects to a resource and ends when the contact disconnects from the resource to which it was connected.
Avg Wait Duration	Average wait time (in HH:MM:SS). It begins when the contact enters the system and ends when either the contact is connected with an agent or if contact was disconnected.
Longest Contact Handling Duration	Longest contact handling duration (in HH:MM:SS) of a contact.
Longest Wait Duration	Longest wait (in HH:MM:SS) for a contact to be connected to a resource.

Outbound Campaign Stats Report

If you have an Outbound license, use the Outbound Campaign Stats report to view real-time statistics on each IVR-based and agent-based progressive and predictive Outbound campaign configured in Unified CCX. This report will be available only if you have an Outbound license on top of Unified CCX premium license in your Unified CCX.

To access the Outbound Campaign Stats report, choose **Reports** > **Outbound Campaign Stats** from the Application Reporting menu bar. The following fields are displayed on the Outbound Campaign Stats report.

Note The call related fields display the data from the time the statistics were last reset.

Field	Description
Campaign Name	The name of the IVR-based or agent-based progressive or predictive campaign.
Status	The current activation state of the campaign: • Running: an active IVR-based or agent-based progressive or predictive campaign. • Stopped: an inactive IVR-based or agent-based progressive or predictive campaign.
Campaign Type	The dialer type of the campaign, which can be one of the following: • IVR Progressive • IVR Predictive • Agent Progressive • Agent Predictive
Attempted	The total number of attempted calls. If there are no customer abandoned calls, then Attempted will be equal to sum of the following counters: Voice + Answering Machine + Invalid Number + Fax/Modem + No Answer + Busy + Failed.
Voice	The total number of calls that are connected to live voice. **Note** The call will be marked as System Abandoned after it has been marked as Voice and Active due to any of the following reasons: • Whenever there is an exception while running some steps in an IVR script in case of IVR-based campaigns. For example, if there is any codec mismatch issue, there will be an exception in the Accept Step. In such cases, the same call will be marked in the following three categories voice, active, and system abandoned. • Whenever the call that is ringing on the agent's phone fails in case of agent-based campaigns.
Answering Machine	The total number of calls that reached an answering machine.
Invalid Number	The total number of calls that reached an invalid number: • A failed call when the gateway returns an invalid or not found error.
Fax/Modem	The total number of calls that reached fax or modem.
No Answer	The total number of calls that were not answered within the time configured for the No Answer Ring Limit field in the Add New Campaign web page.
Busy	The total number of calls that reached a busy destination.

Field	Description
Failed	The total number of calls that failed due to any one of the following reasons: • Dialer asked the Gateway to cancel a call that was dialed out, but not connected. • Gateway has declined the call. • Gateway failure or configuration issues at the Gateway. • Gateway is down.
Active	The total number of calls that were connected to IVR ports or agents. All the voice calls that will be connected to Outbound IVR ports or agents will be marked as active. If you have selected Answering Machine Treatment or Abandoned Call Treatment as "Transfer to IVR," the answering machine calls and abandoned calls that are getting transferred to Outbound IVR ports will also be marked as active.
Customer Abandoned	The total number of calls that were disconnected by the customer or agent within the Abandoned Call Wait Time configured in Add New Campaign web page.
System Abandoned	The total number of calls that were abandoned due to any of the following reasons: • Non-availability of ports or agents. • Any issues at system level.
Abandon Rate (in %)	Abandon Rate = (System Abandoned/Voice)*100

Note
- If you have selected Answering Machine Treatment as "End Call" for an IVR or agent based outbound campaign through Campaign Configuration web page, then Voice = Active + System Abandoned.
- If you have selected Answering Machine Treatment or Abandoned Call Treatment as "Transfer to IVR" for an IVR or agent based outbound campaign through Campaign Configuration web page, then Voice + Answering Machine = Active + System Abandoned.

Overall Outbound Stats Report

If you have an Outbound license, you can use the Overall Outbound Stats report to view real-time statistics across all IVR-based and agent-based progressive and predictive campaigns since the statistics were last reset. This report will be available only if you have an Outbound license on top of Unified CCX premium license in your Unified CCX.

To access the Overall Outbound Stats report, choose **Reports** > **Overall Outbound Stats** from the Application Reporting menu bar. The following fields are displayed on the Overall Outbound Stats report for all the configured IVR-based and agent-based Outbound campaigns.

Note The call related fields display the data from the time the statistics were last reset.

Field	Description
Attempted	The total number of attempted Outbound calls.
Voice	The total number of Outbound calls that were connected to live voice.
Answering Machine	The total number of Outbound calls that reached answering machine.
Invalid Number	The total number of Outbound calls that reached an invalid number.
Fax/Modem	The total number of Outbound calls that reached fax or modem.
No Answer	The total number of Outbound calls that were not answered.
Busy	The total number of Outbound calls that reached a busy destination.
Failed	The total number of failed Outbound calls for all IVR and agent based Outbound campaigns.
Active	The total number of Outbound calls that were connected to Outbound IVR ports or agents.
Customer Abandoned	The total number of Outbound calls that were abandoned by the customer or disconnected by the agent.
System Abandoned	The total number of Outbound calls that were abandoned by the system.

Resource Cisco Unified Contact Center Express Stats Report

Use the Resource Cisco Unified Contact Center Express Stats real-time report to view real-time Unified Contact CCX agent information.

To access the Resource Cisco Unified Contact Center Express Stats report, choose **Reports** > **Resource Cisco Unified Contact Center Express Stats** from the Application Reporting menu bar.

Note If multiple lines are configured for an agent, only the calls on the agent's primary extension are reported in Resource Cisco Unified Contact Center Express Stats report.

The following fields are displayed on the Resource Cisco Unified Contact Center Express Stats report.

Field	Description
Name (ID)	Unique identifier of the agent.
State	Current state of the agent.
Duration in State	Amount of time (in seconds) the agent has remained in the current state.
Contacts Presented	Number of contacts presented to the agent.
Contacts Handled	Number of contacts handled by the agent.
Avg Talk Duration	Average time (in seconds) the agent spent in talking state.

Field	Description
Avg Hold Duration	Average time (in seconds) the agent keeps calls on hold.
Longest Talk Duration	Longest time (in seconds) the agent spent in talking state.
Longest Hold Duration	Longest time (in seconds) the agent keeps a call on hold.
Outbound Offered	Total number of preview outbound calls offered to the agent. A call is considered offered when it is presented to an agent. The number of calls offered is counted twice if a contact that is presented to an agent is skipped/rejected by that agent and then the contact is presented to the same agent or to another agent. Offered = Accepted + Rejected + Closed + Timed-out.
Outbound Accepted	Total number of outbound calls accepted by the agent. For transferred or conferenced outbound calls, the call is considered accepted if it is answered by the agent. A preview outbound call is considered accepted if an agent has clicked Accept to accept the call and then the system places the call to the customer. The number of calls accepted is counted once if a call that is presented to an agent is skipped/rejected by that agent and then the call is presented to another agent who accepts the call. A progressive or predictive outbound call is considered accepted if an agent has answered a live voice call that is presented to the agent (if Auto Answer is disabled).
Outbound Rejected	The number of preview outbound calls skipped/rejected by the agent. This means that the agent selected Reject, Skip, or Cancel Reservation. These contacts will be dialed again. The number of calls rejected is also incremented each time an agent drops the preview call while it is ringing at the customer's contact.
Outbound Closed	The number of contacts closed by the agent for preview outbound. This means that the agent selected Skip-Close or Reject-close. These contacts will not be dialed again.
Outbound Timed-Out	Total number of preview outbound calls that timed out. A call is considered timed out when the call is presented to an agent but not accepted, rejected, or closed within the allocated time. These contacts will be dialed again. If a contact timed out for multiple agents, this field is incremented each time the contact is timed out for each agent.
Outbound Voice	The number of preview outbound calls that ended in successful customer contact for the agent. This means that the agent accepted the call (by clicking Accept) *and* selected a classification of Voice or Do Not Call for this contact.
Outbound Avg Talk Duration	The average time in HH:MM:SS (hours, minutes, seconds) that the agent spends in talking state for outbound calls. This talk duration also includes the time spent on outbound calls that were transferred or conferenced to a route point. For preview outbound, the talk duration considers all calls that were Agent Accepted and classified as Voice.

Field	Description
Outbound Avg Hold Duration	The average time in HH:MM:SS (hours, minutes, seconds) that the agent spent in holding an outbound call. For preview outbound, the hold duration considers all calls that were Agent Accepted and classified as Voice.
Outbound Longest Talk Duration	The longest time in HH:MM:SS (hours, minutes, seconds) that the agent spent in talking state for an outbound call . For preview outbound, the talk duration considers all calls that were Agent Accepted and classified as Voice.
Outbound Longest Hold Duration	The longest time in HH:MM:SS (hours, minutes, seconds) that the agent spent in holding an outbound call. For preview outbound, the hold duration considers all calls that were Agent Accepted and classified as Voice.

Failover Behavior for Unified CCX Stats

All failovers, regardless of whether the Unified CCX Engine is restarted, will cause the Unified CCX stats to reset.

The Unified IP IVR stats do not reset in all cases if the Unified CCX Engine is not restarted on a node. However, the node loses its active server status. The Unified IP IVR stats on that node will not be reset.

Tools Menu

The Tools menu gives you access to the following Application Reporting tools:

- **Reset All Stats**—Choose this option to reset all statistics.
- **Open Printable Report**—Choose this option to get a printable report of all currently active contacts in the system.
- **Refresh Connections**—Choose this option to refresh connections with the Unified CCX system.
- **Clear Contact**—Choose this option to clear contacts/calls that have been stuck in the system for a long time.

Reset All Statistics

Use the Reset All Stats option to reset all statistics accumulated since the last time the statistics were reset. It will not reset active statistics, such as active contacts, tasks, and so on.

Note The Unified CCX system automatically resets all statistics each day at midnight.

Procedure

Choose **Tools** > **Reset All Statistics** from the Application Reporting menu bar.

Open Printable Report

Use the option to get a printable report of all currently active contacts in the system.

To get a printable report:

Procedure

Choose a real-time report from the Report menu option and then **Tools** > **Open Printable Report** from the Application Reporting menu bar.

Refresh Connections

To refresh connections with the Unified CCX system:

Procedure

Choose **Tools** > **Refresh Connections** from the Application Reporting menu bar.

The Unified CCX system refreshes all connections.

Clear Contact Menu

You can use the Clear Contact menu option to clear contacts in the following three situations:

Clear Stuck Calls from Sontacts Real-Time Report

To clear stuck calls or contacts from the Unified CCX system:

Procedure

Step 1 Choose the contact from **Reports** > **Contacts**.

Step 2 From the Application Reporting menu bar, choose **Tools** > **Clear Contact**. A Clear Call dialog box is displayed to warn you. If you want to continue with the clear action, click **No**. To cancel the action, click **Yes**.

Step 3 Click **No** to proceed with the clear action. A Clear Contact dialog box is displayed for you to confirm the action. You can click **Yes** to proceed or **No** to cancel.

Step 4 Click **Yes**. The Unified CCX system removes the contact from all its queues.

Clear Stuck Calls from Overall Cisco Unified CCX Stats

To clear stuck calls/contacts from the Unified CCX system:

Procedure

Step 1 Choose **Reports** > **Overall Cisco Unified Contact Center Express Stats**.

Step 2 Choose the contact from **Views** and click **Overall Waiting Contacts Info**.

Note
Please note that the Overall Waiting Contacts Info menu option displays only those calls that are queued in CSQs and not agent-based routing calls.

Step 3 From the Application Reporting menu bar, choose **Tools** and click **Clear Contact**. A Clear Call dialog box is displayed to warn you. If you want to continue with the clear action, click **No**. To cancel the action, click **Yes**.

Step 4 Click **No** to proceed with the clear action. A Clear Contact dialog box is displayed for you to confirm the action. You can click **Yes** to proceed or **No** to cancel.

Step 5 Click **Yes**. The Unified CCX system removes the contact from all its queues.

Clear Stuck Calls from CSQ Cisco Unified CCX Stats

To clear stuck calls or contacts from the Unified CCX system:

Procedure

Step 1 Choose **Reports** > **CSQ Cisco Unified Contact Center Express Stats**.

Step 2 Choose the contact from **Views** and click **CSQ Waiting Contacts Info**.

Step 3 From the Application Reporting menu bar, choose **Tools** > **Clear Contact**. A Clear Call dialog box is displayed to warn you. If you want to continue with the clear action, click **No**. To cancel the action, click **Yes**.

Step 4 Click **No** to proceed with the clear action. A Clear Contact dialog box is displayed for you to confirm the action. You can click **Yes** to proceed or **No** to cancel.

Step 5 Click **Yes**. The Unified CCX system removes the contact from all its queues.

Views Menu

The Views menu allows you to access more detailed information for the following reports: The Application Tasks report, the Contacts report, the Applications report, the Sessions report, Overall Cisco Unified Contact Center Express Stats report, and the CSQ Cisco Unified Contact Center Express Stats report.

Note For some reports, detailed information is also available by right-clicking a record in that report.

The Views menu contains different options, depending on the report you have chosen. Possible options are:

- **Contacts by Application Task ID**—Choose this option to view contacts according to Application Task ID numbers.
- **Engine Tasks by Application Task ID**—Choose this option to view Engine tasks according to Application Task ID numbers.
- **Detailed Info**—Choose this option to view more detailed information on selected reports.
- **Application Tasks by Application Name**—Choose this option to view application tasks by application name.
- **Contacts by Session ID**—Choose this option to view contacts by session ID.
- **Overall Waiting Contacts Info**—Choose this option to view detailed information for the overall waiting contacts. To clear stuck calls in this view, see Scenario 2 in **Clear contact menu** option.
- **CSQ Waiting Contacts Info**—Choose this option to view detailed information for the CSQ waiting contacts. To clear stuck calls in this view, see Scenario 3 in **Clear contact menu** option.

Application Tasks

You can obtain reports based on the application task ID associated with application tasks.

Contacts by Application Task ID

This report displays the same report as the Contact report with the exception that the Contacts by Application Task ID report has been filtered using only the contact currently being managed by the selected application task.

Engine Tasks by Application Task ID

This report displays the same report as the Engine Task reports except that the Engine Tasks by Application Task ID report has been filtered to display only the engine tasks that are associated with the application task.

Contacts

When you use the Views options with the Contacts report, the Views menu contains only the Detailed Info option.

The Detailed Info option provides various detailed information, depending on the type of contact selected. For example, if the contact is a call, the Calling Party number, the Called Number, and so on, are displayed for that particular call.

Applications

When you use the Views options with the Application reports, the Views menu contains only the Application Tasks by Application Name option.

The Application Task By Application Name report displays the same report as the Application Task report except that the Application Task By Application Name report is filtered using only the active application tasks associated with this application.

Sessions

You can obtain reports based on the session ID associated with a session.

Contacts by Session ID

This report displays the same report as the Contact report with the exception that the Contacts By Session ID report is filtered using only the contacts associated with the selected session.

Detailed Info

Detailed info displays the time the session was created and its current state.

Settings Menu

The Settings menu of the Application Reporting menu bar allows you to adjust various settings of the Real Time Reporting tool.

The Settings menu contains the following menu options:

- **Options**—Choose this option to set the polling (refresh) interval times and to set the amount of times the server will attempt to reconnect.
- **Window**—Choose this option to display reports in colors based on your Windows settings.
- **Motif**—Choose this option to display reports in purple and menu items in brown.
- **Metal**—Choose this option to display reports in grey and menu items in black.

Options Menu

Choose **Settings** and click **Options** to access the Options dialog box. Use the Options dialog box to set the polling (refresh) interval time, set the number of times the server will attempt to reconnect, and specify whether logged off agents appear in reports.

The following fields are displayed in the Options dialog box.

Field	Description
Polling Interval	Time between two requests to the server for new statistics by the client.
Server Connect Retry Count	The number of times that the Unified CCXAdministration web interface should attempt to reconnect to the Unified CCX server. **Note** If an error occurs, an Error dialog box opens to alert you that the server is not communicating with the web interface.
Show Logged Off Resources	Specifies whether logged off agents appear in reports.

Click **Apply** to submit configuration changes.

Reporting Administration on Unified Intelligence Center

Unified Intelligence Center is the default reporting solution for Unified CCX. Unified Intelligence Center is a comprehensive, end-to-end reporting solution.

Note Do not access Unified Intelligence Center until you complete the post installation tasks for Unified CCX.

Live Data reports can only be run by agents, supervisors, and reporting users.

Note The maximum number of users who can concurrently run Live Data reports is 42 .

For more information, see the following guides:

- *Cisco Unified Contact Center Express Report User Guide*
- *Cisco Unified Contact Center Express Report Developer Guide*, located at: https://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_programming_reference_guides_list.html

Note Historical Reporting Client (HRC) is not available from 10.0(1).

Cisco Finesse

You can configure the Live Data reports that are to be displayed in the gadgets of the Cisco Finesse desktops.

Start Unified Intelligence Center

Procedure

Step 1 Open a web browser.

Step 2 Access `http://<host address>` and click **Cisco Unified Contact Center Express Reporting**.

Note
Host address is the DNS name or IP address of the Unified CCX node.

Step 3 Enter your username and password.

Step 4 Click **Log In**.

Administrator Overview

Access to the functions in the Unified Intelligence Center reporting application is controlled by the one or more users who have the user role of Security Administrator.

The initial, default Security Administrator is the user defined as the System Application User during the installation.

Security Administrators can:

- Create and maintain users.
- Assign User Roles—User roles are assigned to users to control access to drawers and what objects the user can create.
- Assign users to User Groups.
- Create and maintain user groups.
- Assign Permissions—Whereas User Roles are associated with people, permissions are associated with objects (Dashboards, Reports, Report Definitions, Data Sources, Value Lists, and Collections).
- Use the Run As feature to verify other users' permissions.

Security Overview

Unified Intelligence Center security offers multilayered and flexible functionality that allows a security administrator to create a flat or a tiered structure of access to Unified Intelligence Center functions, based on the organization's needs.

A user's access to Unified Intelligence Center functions is based on:

- Login authentication.
- License type under which the user's organization runs Unified Intelligence Center. For example, organizations that use a Standard license cannot access the Report Definition functions.
- User Role (a user can have one, some, or all seven User Roles).
- User Groups in which user is a member.
- For an object the user can access, the *object-level permissions* assigned by the person who created that object.

User List

User List page opens from the Security drawer. If a user who does not have the Security Administrator user role accesses this page, that user can see all the parameters except the user roles. The user cannot change his role or group membership.

When Security Administrators access this page, they can see all existing users; can create users, modify or delete users, review or edit user information, and use the **Run As** feature to work in Cisco Unified Intelligence Center as a user.

Table 10: Fields on User List Page

Field	Explanation
Only show currently active users	Check the check box to display users who are currently active.

Field	Explanation
Name Contains	Use this filter field to narrow the list of names or to move to a specific name.
User Name	The domain and user name (domain\name).
First Name	The user's first name.
Last Name	The user's last name.

You can perform the following actions on the user lists page:

- **Create**—Opens the User Information page.
- **Edit**—Select a user name and click **Edit** to edit the User Information page.
- **Delete**—Select a user and click **Delete** to delete the user.
- **Run As**—Select a user and click **Run As** to refresh the Cisco Unified Intelligence Center reporting interface.
- **Refresh**—Refreshes the page to show any latest changes to the User List.
- **Page**—Click the arrow to move to the next page of the User List.
- **Help**—Opens online help.
- **X**—Closes the page.

Create a User

To create a user, perform the following procedure:

Procedure

Step 1 Navigate to **Security > User List**.

Step 2 Under the General Information tab, perform the following:

a) In the **User Name** field, enter the domain and user name (domain\name).
b) In the **Alias** field, enter the alias name for this user.
c) Check the **User is active** check box to enable the user to log in and remain active.

Note
If the check box is unchecked, the user cannot log in.

d) In the **First Name** field, enter the first name of the user.
e) In the **Last Name** field, enter the last name.
f) In the **Organization** field, enter the company name or other descriptive text to be associated with the user, such as region or Line of Business.
g) In the **Email** field, enter the email address of the user.

h) In the **Phone** field, enter a phone number for the user. This can be the user's personal phone number or an emergency contact.
i) In the **Description** field, enter the description of the user.
j) In the **Time Zone** field, choose the time zone that you want to use in the report from the drop-down list.

This time zone is also used for the user's scheduled reports and takes precedence over the time zone used by the report server.

Note
If this field is left blank, the system uses the time zone of the report server.

k) For **Start Day of the Week**, perform the following:

- Select **Locale Based** to select starting day of the week based on locale.
- Select **Custom Settings** to choose one of the seven days of the week from the drop-down list.

Note
Start Day Of The Week is used in Scheduled Report, Report Views, and Permalink.

l) In the **Roles** field, select and assign one or more roles for this user.

If the Security Administrator adds or changes User Roles, the change does not take effect until the user logs out and then logs in again.

m) In the **Permissions** field, choose the user's permission setting preference for My Group when creating new objects. My Group is the object owner's default group.

Note
Settings for My Group configures whether other users who belong to this user's default group can write, or run the objects. Higher level permissions persist and override other permissions.

Step 3 Under the Groups tab, you can determine which groups this user is a member of and how to add group membership(s) for a user. You can view the following:

- **My Group**: This field shows the user's default group. The Security Administrator can change it. The group is represented as “My Group” for the user.
- **Available Groups**: This list shows all the groups that have been created and that the user is not yet a member of. You can use arrows to move groups between columns.
- **Selected Groups**: This column shows all the groups that the user is a member of. You can use arrows to move groups between columns.

Note
By default, every user has AllUsers in their Selected Groups column. You cannot remove the AllUsers group from the Selected Groups column.

User Groups

User Groups page opens from the Security drawer. Use it to see the existing groups, to create or delete groups, and to review or edit group information.

The following are the two default groups created by the system:

- The *AllUsers* group is supplied by Unified Intelligence Center. All users belong to this group by default.
- The *Administrators* group consists of administrators.

Table 11: Fields on the User Groups Page

Field	Explanation
Name Contains	Use this filter field to narrow down the list of group names or to move to a specific name.
Name	Name of the group.
Full Name	The full name shows the child relationship of a group, as indicated by a dot separator. For example, if the default group for Group3 is Group1, and Group1 is a top level group (does not have a parent), then the Full Name of Group1 is *Group1*. The Full Name of Group 3 is *Group1.Group3*.
Description	Description text of the group.

Yu can perform the following actions on the User Groups page:

- **Create**—Opens the Group Information page.
- **Edit**—Select the group name and click Edit to open the Group Information page.
- **Delete**—Select the group name and click Delete.
- **Refresh**—Refreshes the page to show any changes to the Group List.
- **Help**—Opens online help.
- **X**—Closes the page.

About User Groups

User Groups are constructs that allow security administrators to partition Unified Intelligence Center functionality.

Creating User Groups expedites the process of provisioning users when multiple users need the same access to dashboards and reports, or when users require distinct permissions and features based on regional or organizational requirements.

User groups have no impact on how data is stored in the database. They are used only for assigning permissions to all the user members of the group through one operation instead of repeating the same operation for each user.

System-Defined All Users Group

All users are automatically a member of the system-defined *All Users* group.

All Users always appears on the Manage User Groups window. The security administrator cannot delete it.

System-Defined Administrator User Group

The security administrator is automatically a member of the system-defined Administrators group and can add other security administrators to it.

Additional Security Administrators must be added to the Administrators group. Having the role does not automatically make them members of that group.

Customer-Defined User Groups

Security administrators can create any number of user groups and can add users to them. From those other user groups, one is designated as the user's *Group* (also called *My Group*).

Default Group

After creating the customer-defined groups, the security administrator can add a user to any of these groups and can configure one of them as the user's default Group (My Group). The All Users group can also be selected as the default group.

The owner of an object can set permission for its Group. Only the Security Administrator can set extra permissions to other groups or individual users on the User Permissions page. A user's access permission to an object is the highest level of the permission that user gets from all the permission sources.

Create a User Group

To create a user group, perform the following:

Procedure

Step 1 Navigate to **Security** > **User Groups**.

Step 2 Under the General Information tab, perform the following:

a) In the **Group Name** field, enter the name of the group. This field is available only when you create a new group.
b) In the **Description** field, enter or modify text to describe this group

Step 3 Under the Groups tab, perform the following:

a) **Default Group**—From the drop-down list, enter the default group.
b) **Available Groups**—Lists the groups that were created and that are available for this group to become a child of. Click **>** **or** **<** to move just that group or groups.
c) **Selected Groups**—Lists the groups that this group is a child of. Click **>** **or** **<** to move just that group or groups.

Step 4 Under the Groups Members tab, perform the following:

a) Under **Users** tab:

- **Available Users**—Lists all the users that were created and that are available to be children of this group. Click **>** **or** **<** to move just that group or groups.
- **Selected User Members**—Lists the users that are currently children of this group. Click **>** **or** **<** to move just that group or groups.

b) Under **Groups** tab:

- **Available Groups**—Lists all the groups that were created and that are available to be children of this group. Click **>** **or** **<** to move just that group or groups.
- **Selected Groups Members**—Lists the groups that are currently children of this group. Click **>** **or** **<** to move just that group or groups.

Step 5 Click **Save** to update new entry or changes to the fields.

Step 6 Click **Cancel** to cancel or close the page.

Manage User Permissions

Use this page to set extra permissions to Groups or to individual users.

User permissions page has the following tabs:

About Permissions

User Roles are associated with people and permissions are associated with objects. Unified Intelligence Center objects are Dashboards, Reports, Report Definitions, Data Sources, Categories, Value Lists, and Collections.

Permissions:

- EXECUTE: When the user has EXECUTE permissions for an object, that user can perform some actions that depend on the object.

  For example, with EXECUTE permission, a user can run, print, and refresh a report, open and refresh a dashboard and run a dashboard slide show, and see a Value List query. EXECUTE permission includes the read permission.

Note Permissions set on categories are not recursive. For all entities under Dashboard, Report, or Report Definition types, you need separate EXECUTE/WRITE permissions.

- WRITE: When the user has WRITE permission for an object, that user can alter, rename or delete the object. For example, With WRITE permission, you Save As, import, and export reports; you can edit a data source and can delete a custom Value List. WRITE permission also includes EXECUTE and read permission.

Note If no check boxes are selected when setting permission for an object, the user has no access privileges to the object.

The following rules are applicable for all category trees in Unified Intelligence Center — Reports, Report Definitions, Dashboards.

- To delete an entity, you need WRITE permissions for the entity and the entity's parent category.
- To delete a category, you need WRITE permissions for the category, the category's parent, and all the categories and/or entities belonging to the category.
- A user can only Edit or Save an entity even if the immediate parent category has no WRITE permissions.
- A user can only use the Save As feature if the entity has no WRITE permissions enabled.
- Any category owner within the **Imported Report Definitions** can delete a category if the administrator provides explicit WRITE permissions on the **Imported Report Definitions** category.

Permissions are combined and the highest level prevails.

A user receives permission for an object from different sources. Permission can be inherited from the AllUsers group, the Default Group (My Group), or the permission assigned by the Security Administrator. Among all these permissions, the highest level permission is used when the user accesses the object.

User Roles and Permissions

Your User Role allows you to "open" the drawer that corresponds to that role. If you have EXECUTE permission, you can create objects for that drawer. For example, if you are a Dashboard Designer, you can create dashboards on the Available Dashboards page.

When you create an object, you are the *owner* of that object. You have WRITE permission for the object, and you can set the permissions for that object for users in your Group only.

If the object is still a work-in-progress and you do not want anyone to access it yet, you can make it "private" by leaving all permissions unchecked for both the All Users and the Groups.

When the object is ready, set your default Group (My Group) permissions to EXECUTE or even WRITE. For example, if you create a Dashboard for your Group and the dashboard has notes, you might want others in your Group to update the notes.

Even though *you* are a Dashboard Designer, if the Available Dashboards page contains dashboards created by (owned by) other Dashboard Designers, you may not be able to see those dashboards, based on your Group permissions and on the object-level permissions those owners have set for their dashboards.

Assigned Group Permissions

Procedure

Step 1 Select the object type in the Permissions For panel. For Dashboard, Report or Report Definition type, you can select a category or an object within a category. For other object types, select an object from the list. All the groups that have already been assigned permissions for the object are displayed in the Group permissions for the selected item panel.

Step 2 Select a group in the All Groups panel. All user members of this group are displayed in the All Users for the selected group panel.

Step 3 Click **Set Permissions**. Check the level you want for the group (Execute, Write), and click **OK**.

Step 4 The **Group Permissions for the selected item** panel updates to include the group and its assigned permission you defined in **Step 3**.

Note If the Security Administrator adds or changes User Permissions, the change may not occur immediately.

Table 12: Fields on the Group Members Tab

Field	Description
Permissions For panel (top left)	Click the drop-down list to select the objects for which you want to set permissions. Options are: Data Sources, Report Definitions, Reports, Dashboards, Value Lists, and Collections. Selecting an object type refreshes the panel to show the list of items or categories for that object.
All Groups panel (top right)	This panel shows the available User Groups. Highlighting a user group refreshes the page to display an All Users for Selected Group panel that lists the member of the group.
All Users for the Selected Group panel (bottom right)	This panel shows all members in the group that is highlighted in the All Groups panel above.
Set Permissions button	Click this option to open a dialog box where you select the permission level for the selected object in the Permissions For panel and the selected group in the All Groups panel.
Group Permissions for the selected item	This panel shows the groups that have already been assigned permission for the selected object, and their permission level.

Assigned User Permissions

Procedure

Step 1 Select the object type in the Permissions For panel. For Dashboard, Report, or Report Definition type, you can select a category or an object within a category. For other object types, select an object from the list. All the users that have already been assigned permission for the object are displayed in the User permissions for the selected item panel.

Step 2 Select a user name in the User List panel.

Step 3 Click **Show Groups** to see the groups for which this user is a member.

Step 4 Click **Set Permissions**, check the level you want for this user (Execute, Write), and click **OK**.

The **All Permissions for the selected item** panel refreshes to show the user permissions you have added or changed for this user in steps 3 and 4.

Field	Description
Permissions For panel (top left)	Click the drop-down arrow to select the kinds of object for which you want to set permissions. Options are Data Sources, Report Definitions, Reports, Dashboards, Value Lists, Collections, and System Collections. Selecting an object type refreshes the panel to show the list of items or categories for that object.
User List panel (top right)	This panel shows current users. Filter the list and select one or many user names.
Show Groups button	Click this option to show the All Groups for the selected user panel.
All Groups for the selected User (bottom right)	This panel shows all groups to which the highlighted username in the User List panel above is a member.
Set Permissions button	Click this option to open a dialog box where you select the permission level for the object (Execute, Write).
All Permissions for the selected item	This panel shows users who have permission for the object, and the level of permissions they have.

Note
You cannot change the permission for the owner of an object. The owner always has Write permission for the object. For example, if a user is the owner of Report 1, then that user has WRITE permission for Report 1, and no one else can change the permission to EXECUTE.

Run As

Security Administrators can select a name on the User List page and click **Run As**. This refreshes the Unified Intelligence Center web page so that it reflects the interface that user has when logged in.

Use this tool to verify that the User Roles and permissions are configured properly.

Note

- When you Run As another user, the top of the page shows both your Logged In identity and your Run As identity.
- You cannot Run As yourself.
- You can Run As one level of user. A Security Admin cannot *Run As* User A and, as User A, then *Run As* User B.

To leave Run As mode, click **Stop Run As** at the top of the page.

Audit Trail Logging in Cisco Unified Intelligence Center

Unified Intelligence Center now supports Audit Trail Logging. This feature allows you to view the sequence of audit records of the transactions related to create, update, modify, and delete that are performed on the entities of a Unified Intelligence Center server. You can view the audit trails using the Audit Trail stock report. Only System Administrators can access and view this feature by default. However, a System Administrator can then give permissions to other Unified Intelligence Center users to use this feature.

Note Localization of Audit Trail report is not supported.

View Audit Trail Logging in Unified Intelligence Center

Procedure

Step 1 Log in to the Unified Intelligence Center Reporting Interface.

Step 2 Navigate to **Reports** > **Stock** > **Intelligence Center Admin** and click **Audit Trail**. The system opens the **Audit Trail Report Filter** window.

Step 3 Specify the required filter criteria and click **Run**. The system displays the Audit Trail report based on the filter criteria that you specified.

Audit Trail Report

Views: This report has three grid views - Non-grouped, Groupby – EntityName, Groupby –Username.

Grouping: This report has two grouped views - grouped and sorted by User and Entity Name. The third view is un-grouped which is also the default view for this report.

Value List: CUIC Users, CUIC Operations, CUIC Entity Types.

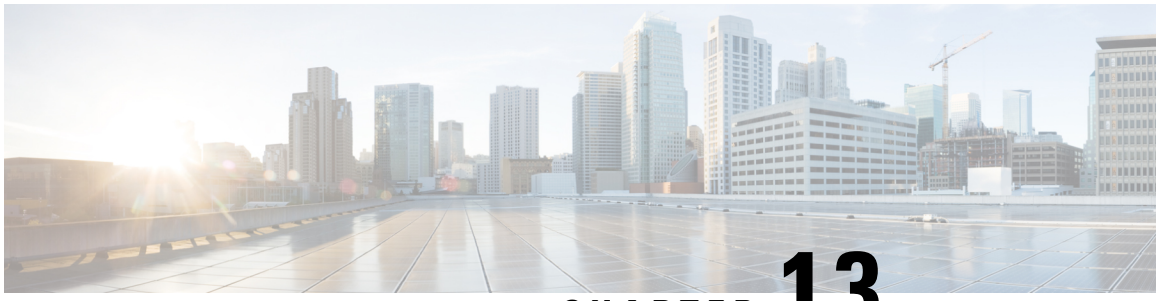
Database Schema Tables from which data is retrieved:

- CUICAUDITLOG
- CUICLOGEDENTITY

Security Considerations

If you make the user a member of one or more other groups, make one of those groups the user's default group, and set the permissions for the default group higher than those of the AllUsers group.

Higher permissions for the default group prevail over permissions in the AllUsers group. Individual user permissions prevail over group permissions.



CHAPTER 13

Unified CCX Outbound Dialer Configuration

- Outbound Feature for Unified CCX, on page 217
- Supported Dialers and Dialing Modes for Outbound, on page 220
- Configure Outbound Subsystem in Unified CCX, on page 222
- Configure General Outbound Properties, on page 222
- Configure Application and Trigger for Outbound Campaign, on page 227
- Add New Campaign, on page 227
- Import Contacts for Campaign, on page 237
- Enable Campaigns, on page 242
- Outbound Subsystem and Time Detection, on page 242
- Add Area Codes, on page 243
- Call Status Values, on page 244
- Call Result Values, on page 245
- Reclassification Status Behavior, on page 246
- Call Retrieval Priority, on page 247
- Failover and System Restarts, on page 248

Outbound Feature for Unified CCX

The Outbound feature provides outbound dialing functionality in addition to existing Unified CCX inbound capabilities.

The Unified CCX Direct Preview Outbound feature is bundled along with the Unified CCX Premium license package. The Unified CCX IVR and Agent Progressive and Predictive Outbound feature is available with the Unified CCX Outbound license. When you upload the Premium license, the Outbound subsystem will automatically appear in the Subsystems menu. With this Outbound feature, you can maintain high agent productivity by configuring contact centers for automated Outbound activities to perform Outbound calls.

Outbound Characteristics

The Outbound feature has the following characteristics:

- An Outbound subsystem that can be monitored from the control center
- IVR and Agent Progressive and Predictive Outbound
- Dialing modes - Direct preview, Progressive and Predictive

- Unified CCX Administration web pages, REST API to configure the Outbound feature
- Outbound Historical reports
- Outbound Live Data reports (Unified Intelligence Center)
- Real-Time reports are part of the Unified CCX Administration GUI real-time reporting swing application.

Note Calls made by the Outbound subsystem will not be displayed in the Contacts Summary Real-Time Report

- Access to real-time Outbound data from the GetReportingStatistics step for Direct Preview Outbound

Unified CCX Requirements

To use the Outbound feature, you must adhere to the following requirements:

Unified CCX Licensing Requirements

The licensing requirements for Outbound feature in Unified CCX will vary depending on the dialing modes.

- **For Unified CCX Outbound Direct Preview Dialer—**The Unified CCX Outbound Direct Preview Dialer feature is automatically available with Premium license package without any additional license. It is no longer available with Enhanced license.
- **For Unified CCX Outbound IVR Dialer—**You need to upload an Outbound license on top of the Unified CCX premium license with the required number of IVR ports that you would like to use for the Outbound feature.
- **For Unified CCX Outbound Agent Dialer—**You need to upload an Outbound license on top of the Unified CCX premium license with the required number of agent seats that you would like to use for the Outbound feature.

Note The sum of inbound and outbound IVR ports should be less than or equal to a maximum number of IVR ports supported for your hardware model.

Once you obtain the Outbound license for a specific number of ports, the IVR ports will be distributed between the inbound and outbound IVR calls using the following approach based on the different scenarios explained below.

You can view the licensed IVR ports for outbound and inbound and the dedicated ports for both outbound and inbound calls by navigating to **System** > **License Information** > **Display License(s)** submenu from the Unified CCX Administration menu bar.

Scenario 1:

If your Contact Center is already utilizing maximum licensed IVR ports supported for your hardware model, then:

- Inbound calls will take precedence over the configured Outbound IVR calls.

- If IVR ports are dedicated for a campaign, then the Outbound IVR ports available for the campaign will be gradually incremented as and when the inbound ports become free.

For example, if you have an UCS C220 hardware that supports maximum of 300 IVR ports and if you have 200 premium seats, then the current licensed IVR ports = 300 (Minimum of [seats*2, maximum supported for platform]).

In this case, if you upload an Outbound add-on license for 100 IVR ports and add 3 campaigns with 20 dedicated ports each running at the same time, then the 60 Outbound IVR ports will be available to the campaigns only when the number of inbound ports are freed up to support the Outbound IVR calls.

In other words, if the number of inbound ports that are used during the outbound IVR campaign time is 280, then only 20 Outbound IVR ports will be available to the campaigns. The number of Outbound IVR ports will be gradually incremented depending on the availability of free inbound ports.

Scenario 2:

If your Contact Center is close to utilizing the maximum IVR ports supported for your hardware model, then:

- Inbound calls will take precedence over the configured Outbound IVR calls.
- If IVR ports are dedicated for a campaign and if you reach the maximum inbound call limit, then the Outbound IVR ports available for the campaign will be gradually incremented as and when the inbound ports become free.

For example, if you have an UCS C220 hardware that supports a maximum of 300 IVR ports and if you have 130 premium seats, then the current licensed IVR ports = 260 (Minimum of [seats*2, max supported for platform]).

In this case, if you upload an Outbound add-on license for 50 IVR ports and add 2 campaigns with 25 dedicated ports each running at the same time and if you reach the inbound call limit of 260 during the outbound IVR campaign time, then only 40 ports (300-260) will be freed up initially for Outbound IVR calls. The number of Outbound IVR ports will be gradually incremented depending on the availability of free inbound ports.

Scenario 3:

If your Contact Center is using fewer ports than the maximum licensed ports supported for your hardware model, then the number of available IVR ports for inbound will continue to remain the same.

For example, if you have an UCS C220 hardware that supports maximum of 300 IVR ports and if you have 60 premium seats, then the current licensed IVR ports = 120 (Minimum of [seats*2, max supported for platform]).

In this case if you upload an Outbound add-on license for 50 IVR Outbound ports, and add 2 campaigns with 20 dedicated ports each running at the same time, then Unified CCX will support 40 IVR Outbound calls, and the inbound port limit will continue to be 120 as the sum of both inbound and outbound ports (160) are within the maximum licensed ports (300) for the platform.

Note The total number of dedicated IVR ports in all the IVR campaigns must be less than twice the number of Premium Seats that is equivalent to the Total Licensed Inbound IVR ports.

Unified CCX Subsystem Requirements

- The Outbound subsystem must be IN SERVICE.

- The RmCm subsystem must be IN SERVICE.
- The Unified CM Telephony subsystem must be IN SERVICE.
- The Unified CCX Database must be IN SERVICE.

Geographic Region Support

- The Outbound feature can be used in any geographic region supported by Unified CCX. The area codes and time zones mapping for North America are automatically prepopulated in the system. The system uses this information to determine the time zone of a customer's phone number.
- For regions outside North America, administrators must enter the mapping of the international area codes and their time zones using the Unified CCX Administration GUI or REST API.
- The national do_not_call list is not supported in this release. Be sure to abide by the national do_not_call list.

Outbound Components

This section provides details about the following Outbound feature components:

- Unified CCX Administration—Enables the Outbound subsystem configuration, creates campaigns, and imports contacts to generate the dialing list.
- Outbound subsystem—Is responsible for the following tasks:
  - Manages campaigns
  - Maintains Outbound system configurations
  - Manages the dialing list
  - Reserves agents
  - Makes Outbound calls
  - Updates the call data in the dialing list based on the outcome of the call
  - Decides which contact records to retrieve from a campaign

The Outbound subsystem views campaigns as logical entities that group a set of contacts together in a dialing list. Campaigns deliver outgoing calls to agents. Agents are assigned to campaigns using CSQs.

Supported Dialers and Dialing Modes for Outbound

In addition to the existing Direct Preview Outbound dialer option, Unified CCX supports IVR-based and agent-based dialing. If you select the IVR-based option for a campaign, the outbound calls are handled by IVR scripts. If you select the agent-based option for a campaign, the outbound calls are handled by agents. Typical applications include appointment and bill-payment reminders.

Unified CCX Outbound Dialing Modes

The Outbound feature in Unified CCX Release supports the following dialing modes:

- Direct preview dialing mode
- Progressive dialing mode
- Predictive dialing mode

Tip For agent predictive and agent progressive outbound calls, disable the Call Waiting option on the agent's phone to allow agents to preview a customer call on Finesse Desktop before the call is placed. The Call Waiting option must be disabled (default) in Unified Communications Manager on each Outbound agent phone to ensure that every customer call successfully transfers to an available agent.

When an Outbound call is transferred or conferenced to another agent, the second or subsequent agents are not counted towards the number of Outbound licenses. For example, if you have five seats licensed for Outbound and Agent1 gets an Outbound call, Agent1 accepts the call and conferences in Agent2 and Agent3. Now, three agents are on one Outbound call but only Agent1 is considered an Outbound agent and you are only using one licensed seat. Consequently, your system allows four more Outbound calls to agents.

Direct Preview Dialing Mode

The direct preview dialing mode allows agents to preview a customer call on Cisco Finesse before the call is placed. The advantage of this mode is that an agent is already on the call when the customer answers and can quickly begin talking with the customer immediately.

Progressive Dialing Mode

In the Progressive Dialing mode, you can specify a fixed number of lines that will always be dialed per available IVR port or per available agent. You can configure the progressive dialer settings for each campaign while creating the campaign through Unified CCX Application Administration web interface. You can also update the configuration at a later date.

Predictive Dialing Mode

The Predictive Dialing mode works similar to the Progressive Dialing mode in terms of dialing the Outbound calls. The difference remains in tuning the lines per port or per agent depending on the abandoned call-rate thus eliminating manual intervention as in the case of the Progressive Dialer.

In other words, in the Predictive Dialing mode, the Dialer adjusts the number of customers to dial per available IVR port or per available agent. The number of lines to dial is calculated by an algorithm and gets updated automatically.

Configure Outbound Subsystem in Unified CCX

Procedure

Step 1 Configure the general properties of the outbound subsystem. See **Configure General Outbound Properties**.

Step 2 (Optional) If the dialing list contains contacts outside of North America or if Unified CCX is installed outside of North America, manually add the area codes and their corresponding time zones. See **Add New Area Code**.

Step 3 Configure the SIP Gateway parameters to enable communication between Unified CCX and the SIP gateway for IVR and agent-based progressive and predictive campaigns. See **Configure SIP Gateway**.

Step 4 Configure the campaign. See **Add New Campaign**.

Configure General Outbound Properties

General Outbound properties refer to the settings that is common for all the campaigns.

Caution Area code and long distance prefix configuration changes made to the Outbound subsystem do not take effect for the calls/contacts that are currently in the Outbound subsystem's memory. For example, if you change the long distance prefix or local area code, the contacts that are already in the Outbound subsystem's memory will continue to use the old long distance prefix and local area code.

To configure general Outbound properties, complete the following steps.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Outbound** > **General**.

The General Configuration web page opens.

Step 2 Specify the following fields in the General Configuration section:

Field	Description
Customer Dialing Time Range (hh:mm) Start Time/End Time	The time range during which a customer can be called. This time range supersedes the time range of the individual campaigns and ensures that a customer is never called outside the legally allowed time range for that country. This is a mandatory field. For example, in the USA, the Federal Communications Commission (FCC) specifies the legal time range as 8 AM to 9 PM. This does not apply to callbacks, since the customer explicitly requested to be called at a certain time. This time range is always converted to the local time for each contact record. Default = 8:00 AM to 9:00 PM (USA FCC regulations)

Field	Description
Outbound Call Timeout (seconds)	If an agent does not respond to the Outbound preview call on Finesse Desktop within the timeout duration that is specified in this field, the system sets the agent to the Not Ready state. If an agent does not respond to the Outbound progressive or predictive call on Finesse Desktop within the timeout duration that is specified in this field, then the call is dropped. The system sets the agent to the Ready or Not Ready state depending on the option that is selected for Agent State after Ring No Answer field in the System Parameters Configuration Web Page. This is a mandatory field. Default = 60 seconds, Range = 5 to 3600 seconds. **Note** • If the Unified CCX Engine or Finesse Desktop restarts when an outbound campaign call is being presented to an agent, then the timeout value specified in the Outbound Call Timeout field will not be applicable for that call.
Dialing Prefix	The number that is prefixed to the phone number when the dialer dials an outgoing call (also referred to as switch prefix). This number can have a numeric value, including 0 or leading zeros. This is a user defined value. For example, if the dialing prefix is set as 9 and the phone number of the contact is 54321, then the dialer will dial out '954321'.
Long Distance Prefix	This is a user defined value that can have a numeric value, including 0 or leading zeros. When this value is set and an outgoing call is made, it helps to determine the long distance prefix in the phone number that is dialed by the dialer. It is first determined whether it is an international or domestic number by the presence of any matching International Prefix set in the **General** configurations page. When the phone number is a domestic number, based on the matching local area code set, it is determined if it is a local number or a long distance number. For example, if the long distance prefix is set as 044, the phone number of the contact is 54321, and if the **Include Long Distance Prefix** is enabled, then the dialer dials out '4454321'.
International Prefix	This is a user defined value that can have a numeric value, including 0 or leading zeros. When this value is set and an outgoing call is made, it helps to determine the international prefix in the phone number for that international number. If there is no International Prefix, then the number is considered to be a domestic number. If the imported number doesn't contain an international prefix but has a "+" sign prefixed to the phone number, then it is considered to be an international number.
Local Area Code	The area code of the location from where the PSTN call is made from. This number can have a numeric value, including 0 or leading zeros. The local area code when set in the **General** configurations page, helps to determine the prefix value in the domestic phone number which is included in the outgoing call if the **Do Not Remove Local Area Code When Dialing** is checked.

Field	Description
Do Not Remove Local Area Code When Dialing	If this box is checked, the local area code is included when dialing the phone numbers within this area code. If it is unchecked, then the local area code is stripped from the phone number before dialing the local numbers. It is expected that when contacts are imported into the system, the phone numbers include the area code. For international phone numbers, the country code must be included when importing contacts.
Include Long Distance Prefix	This field will be displayed only if you check the **Do Not Remove Local Area Code When Dialing** check box. For local numbers, the long distance prefix will be prefixed only if this check box is checked. The long distance prefix will be prefixed to the phone number for all non-local numbers (the numbers that do not start with local area code) irrespective of the status (checked/unchecked) of this check box.
Auto Answer	If this box is checked, any agent-based progressive or predictive campaign call that gets transferred to the agent is automatically answered by Unified CCX. A beep tone always notifies the agent that the call has been answered. This option is enabled by default. **Note** • If the workflow is enabled, it will be run irrespective of the status (Checked/unchecked) of the Auto Answer check box.
Assigned CSQs	Assigned CSQs are CSQs that are used by the Outbound subsystem. This is a mandatory field. To allocate CSQs for Outbound: **a.** Select a CSQ in the **Available CSQs** list. **b.** Select a value from the **% of Logged in Agents for Outbound** drop-down list to indicate what percentage of the CSQ is allocated for Outbound. **c.** Click the left arrow icon to move the CSQ to the **Assigned CSQs** list. The selected CSQ is removed from the **Available CSQs** box and appears in the **Assigned CSQs** box with the percentage allocation in parentheses next to the CSQ name.
Available CSQs	The Available CSQs pane displays all CSQs configured in the CSQ Configuration page under the RmCm subsystem configuration.
% of Logged in Agents for Outbound	The % of Logged in Agents for Outbound field indicates the percentage of logged in agents in each of the selected CSQs that are allocated for handling Outbound calls. **Note** The CSQ allocation percentage is defined at the global level and not at a campaign level. The number of agents allocated for OB is considered as the whole number of the **% of Logged in Agents for Outbound**. Any decimal value in the value is not considered. For example, If the percentage of allocation is 95% and 4 agents are logged in, then the number of agents allocated for OB are 3 [95% * 4 = 3.8 (decimal value is neglected)]. If the percentage of allocation is 80% and 4 agents were logged in, then the number of agents allocated for OB are 3 [(80% * 4 = 3.2 (decimal value is neglected)].

Step 3 Click **Update** icon that is displayed in the tool bar in the upper, left corner of the window or the **Update** button that is displayed at the bottom of the window.

The System Options components are now updated.

Callbacks

A customer can request a callback at a specific callback phone number and also specify the time/date of the callback. The Outbound subsystem stores this information (the callback phone number, date, time) in the dialing list table.

The Outbound subsystem handles the callback as follows:

- Convert to GMT—The callback date and time specified with respect to the customer's time zone is converted to GMT time zone and then stored in the database.
- Agent not Available—When the Outbound subsystem looks up the database for contacts, it first checks the callbacks. The default callback time limit is 15 minutes (can be changed) before and after the customer-specified time. If an agent is available, then the Outbound subsystem places the callback. If an agent is not available, the Outbound subsystem retries agent availability (agent state) after 10 minutes.
- Missed Callbacks—If the Unified CCX system is unable to process a callback request in the specified time, you have three action options:
  - Reschedule it to the same time on the next business day.
  - Mark it as another retry (the callback phone number is removed and the callback date time is ignored). In this case, it moves out of the call back state and into the retry state.
  - Close the record (never dialed again).

Note The selected status for the Missed Callbacks is applied at midnight.

- Agent reclassifications—If calls were retrieved and presented to the agent and if the agent reclassifies it (for example, changed it to answering machine status), then the call status is updated to the answering machine.

Outbound Area Code Functionality

In the Outbound option, the area code determines the geographical location of the phone number you dial, which correspondingly provides the Greenwich Meridian Time (GMT) zone. The db_cra database contains a mapping of the area codes to the time zones.

The U.S. area code mappings are provided along with the product. International customers should provide their own data and add it to the database.

Configuration Updates

Whenever Outbound parameters are modified in the Unified CCX Administration GUI, the changes take effect immediately. If a new CSQ is added using the **Subsystems** > **RmCm** > **Contact Service Queues** menu option, it is instantly displayed in the list of available CSQs in the General configuration page in the Unified CCX Administration GUI, as this list is dynamically updated. If a CSQ is modified and if this impacts the allocation of agents, the Outbound subsystem is aware of this change as it refreshes the list of agents in each relevant CSQ periodically.

- If a configuration change affects the Outbound contacts dialing process (for example, if a campaign is disabled or a CSQ is removed from a campaign), the Outbound subsystem stops processing the Outbound contacts, recalls these contacts to the database, and resets the call status to Pending.
- If a campaign start time is changed, the Outbound subsystem checks if the campaign is enabled. If it is enabled, and if the new start time is after the current time, it performs the following actions:
  - Sends a recall contact message to the Outbound subsystem passing the campaign ID.
  - For all Outbound contacts for this campaign in the Outbound subsystem's memory that are waiting to be dialed out, it resets all Outbound contacts to the Pending state and clears them from memory.

  If the campaign is disabled or if the new start time is before the current time, the Outbound subsystem ignores this change.
- If campaign end time is changed, the Outbound subsystem checks if the campaign is enabled. If it is enabled, and if the new end time is before the current time, it performs the following actions:
  - Sends a recall contact message to the Outbound subsystem passing the campaign ID.
  - For all the Outbound contacts for this campaign in Outbound subsystem's memory that are waiting to be dialed out, it resets all the Outbound contacts to the Pending state and clears them from memory.

  If the campaign is disabled or if the new end time is after the current time, the Outbound subsystem ignores this change.
- If a CSQ is deleted from a campaign or if the CSQ itself is deleted, the Outbound subsystem sends a recall contacts message with the csq ID of the deleted CSQ. It also reallocates any Outbound contacts in its memory that are currently allocated to this CSQ among the other existing CSQs for this campaign.

CSQ Agent Pool Allocation

You need to specify a percentage of total agents in the assigned CSQs to be allocated for Outbound calls. This pool of agents is shared by all Outbound campaigns.

Tip The CSQs for Outbound are the same as the CSQs for inbound. If you need more CSQs, you must first configure them in Unified CCX and assign the required CSQs for agents as required by your configuration, before allocating them.

Configure Application and Trigger for Outbound Campaign

For IVR campaigns, configure application and trigger before you create the campaign.

For an agent-based predictive campaign and an agent-based progressive campaign, configure the application and trigger if you configure the answering machine and the abandoned call treatment to transfer to IVR.

Procedure

Step 1 Create a Call Control Group for Outbound type with the required number of IVR ports to be used for outbound campaigns. See **Add New Call Control Group**.

Step 2 Create an application, which will be used for the outbound campaign. See **Cisco Applications Configuration**.

Step 3 Create a trigger and assign the newly created Outbound Call Control group to this trigger. See **Cisco Applications Configuration**.

Step 4 Create a new progressive or predictive outbound campaign. See **Add New Campaign**.

Step 5 Import contacts for the campaign. See **Import Contacts for Campaign**.

Add New Campaign

Use the Campaign component to configure properties for the campaign, including the campaign name and description, CSQ selection, and the time range when a campaign can call contacts.

Complete the following steps to define or modify the settings that apply to a campaign.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Outbound** > **Campaigns**.

The Campaign web page opens, displaying the details of existing campaigns, if any. Click an existing campaign to view or update the configuration settings for the campaign.

Step 2 Click the**Add New** icon in the tool bar in the upper, left corner of the window or the **Add New** button at the bottom of the window.

Add a New Campaign web page opens up where you can specify the campaign type and the dialer type for the campaign using the following fields.

Note
You need to upload an Outbound license on top of the Premium license for Unified CCX to create a campaign for Outbound.

Field	Description
Select the type of the campaign	

Field	Description
Campaign Type	Type of the campaign to be used for outbound calls. You can specify any one of the following two campaign types: • Agent-based—If you select this, all the outbound calls in a campaign will be handled by the available agents. • IVR-based—If you select the IVR-based option, the outbound calls in a campaign will be handled by the IVR scripts.
Select the type of dialer for the campaign	

Description	The dialer type options available for a campaign will vary depending on the selected Campaign Type.
	• If you select Agent-based campaign type, then you can select any one of the following dialer types:
	  • Direct Preview (default)
	  • Progressive
	  • Predictive
	• If you select IVR-based campaign type, then you can select any one of the following dialer types:
	  • Progressive (default)
	  • Predictive

Note
Once the campaign is created, you cannot change the Campaign Type and Dialer Type.

After you select the campaign type and dialer type, click **Next** to continue. The Campaign Configuration web page opens, displaying the following three column headings:

- Parameter Name
- Parameter Value
- Suggested Value

You can specify values for a new campaign or modify values for an campaign using the fields listed in the Parameter Value column. See the table below for a list of fields along with their description.

The Suggested Value displays the default configuration value for each campaign. You can refer to these values if you want to revert any changes made to one or more parameters listed in the Campaign Configuration web page.

Field	Description
Campaign Name	Name of the campaign (must be a unique identifier). This is a mandatory field.

Field	Description
Enabled	Indicates the current state of the campaign to the Outbound subsystem. Yes = The campaign is currently active. No = The campaign is currently inactive (default).
Description	Description of the campaign.
Start Time/End Time (hh:mm) AM PM Time Zone	Indicate the time range during which the campaign runs. These are mandatory fields. The name of the primary time zone is also displayed adjacent to these two field values. Default = 8:00 AM - 9:00 PM Pacific Standard Time (USA FCC regulations).
Campaign Calling Number	The campaign calling number is the number that will be displayed to the contact. This number is used by the dialer. This is a mandatory field. **Note** This field is not available if you have selected the direct preview dialer type for an agent based campaign.
Maximum Attempts to Dial Contact	The maximum number of times the Outbound subsystem attempts to dial a contact beyond which the call status will be marked as closed. You can choose this value from the drop-down list box. Default = 3, Range = 1 to 3.
Callback Time Limit	The time period before and after the scheduled callback time during which the Outbound subsystem attempts to dial out a callback. For example, if a callback was scheduled for 9:30 am and if the Callback Time Limit is set to 15 minutes, then the Outbound subsystem calls the customer anytime between 9:15 am to 9:45 am. This field is also used to determine the dialing time range for the Retries settings in the Add New Campaign web page. Default = 15 minutes, Range = 1 to 60 minutes.
Fields displayed only if you have selected IVR-based campaign type	
Application Trigger	This is the JTAPI trigger associated with this campaign. There will one-to-one mapping between a campaign and an application trigger. Only those triggers that are not associated with any other campaigns are displayed in the trigger list.
Application Name	The name of the application associated with the above-mentioned JTAPI trigger. This field is auto-populated.
Fields displayed only if you have selected Agent-based campaign type	

Field	Description
Abandoned Call Treatment	If the agent is not available to handle the call, you can choose to abandon the call or transfer it to IVR by selecting the desired radio button in this field. If you choose to transfer the call to IVR, a trigger field and an application name field appears for selection. The trigger field is a drop-down list of JTAPI triggers associated with this campaign. There is one-to-one mapping between a campaign and a trigger. Only those triggers that are not associated with any other campaigns are displayed in the trigger list. The application name is associated with the above-mentioned JTAPI trigger. This field is auto-populated. Transfer to IVR radio button is enabled by default. **Note** • This field is not applicable if you have selected the Direct Preview dialer type for an agent-based campaign. • If the agent is available to handle the call and if Unified CCX fails to transfer the call to the agent, then the call is dropped and will not be transferred to the IVR port.
Assigned CSQs	The CSQs from which agents are selected for Outbound calls for this campaign. This is a mandatory field. **Note** • For agent selection, the CSQs are used in the order in which they are assigned to the campaign. • CSQs that are associated with agent-based progressive or predictive campaigns cannot be shared across any other campaigns. • CSQs that are associated with direct preview campaigns can be shared only across other direct preview campaigns and not with agent-based progressive and predictive campaigns.
Available CSQs	For direct preview campaigns—CSQs that are allocated for outbound but not assigned to any progressive or predictive agent-based campaign. For progressive and predictive agent-based campaigns—CSQs that are allocated for outbound and not assigned to any other campaign.
Fields displayed only if you have selected Direct Preview dialer type for an Agent-based campaign	

Field	Description
Contact Records Cache Size	The number of contact records the Outbound subsystem retrieves from the database in bulk for dialing. The allowed values are 1–100. This is a mandatory field. For example, if 50 records are retrieved in bulk for campaign1 and 10 for campaign2 and they are running at the same time, the Outbound subsystem attempts to place 50 Outbound calls for campaign1 and 10 Outbound calls for campaign2. The number of Outbound calls actually placed for each campaign depends upon the number of agents available for the respective campaigns. Once all the records retrieved for a campaign have been dialed, the Outbound subsystem retrieves another batch of records for that campaign. Over a period of time, it is likely that more contacts would have been called from campaign1 than from campaign2. If two campaigns run simultaneously and share CSQs or agents, the records in both campaigns may not be processed at the same rate even if their contact cache sizes are identical. It is possible that more records from one of these two campaigns is processed before the other. Default = 20, Range = 1 to 100
Answering Machine Retry	If you select Yes, then the Outbound subsystem retries the contact after all the callbacks and pending contacts for the campaign are dialed out. Default = No
The following fields in Dialing Options are displayed if you have selected IVR-based campaign type	

Field	Description

Number of Dedicated Ports	Number of dedicated IVR ports that you want to reserve for this campaign based on the number of CTI ports available in the outbound call control group for the campaign duration. That is, the total number of dedicated IVR ports for the selected campaign cannot exceed the maximum licensed ports for outbound IVR minus the sum total of IVR ports dedicated to other campaigns running at the same time.
	
	You can enter or update this value for a campaign only after associating a trigger with the campaign. Default value = 0, Range = 0 to number of available ports for the campaign duration.
	
	For example, if you have a medium or large profile VM, which supports maximum of 300 IVR ports with 50 licensed ports for outbound IVR and you have already dedicated:
	• 20 ports for Campaign1, which runs between 10–12 pm
	• 10 ports for Campaign2, which runs between 2–4 pm, then the number of dedicated IVR ports that you can enter in this field for a new campaign cannot exceed:
	  • 30 ports if the new campaign runs between 10–12 pm and
	  • 40 ports if the new campaign runs between 2–4 pm and
	  • 50 ports if the new campaign runs during any time other than 10–12 pm and 2–4 pm
	
	If the number of configured ports for a campaign is greater than the available number of licensed ports at the specified campaign time, then an alert message stating the same will be shown while saving the campaign.
	
	Note
	Ensure that few IVR ports from the total number of licensed IVR ports are left free if you want to use the "Transfer to IVR" option available in the answering machine treatment and abandoned call treatment fields for agent-based progressive and predictive outbound campaigns.
	
	See Unified CCX Requirements, on page 218 to know how the licensed IVR ports are distributed between the inbound and outbound IVR calls in different scenarios.

Lines Per Port (1-3)	Number of lines to be dialed for each port. The dialer will try to connect as many live voices to the available port(s) where IVR script is playing and it will disconnect the remaining calls. The probability of abandoned calls increases geometrically as the lines per port increases. In an IVR based progressive campaign, you can configure the number of lines to dial per port at a time. The dialer will determine the number of calls to dial based on the following calculation - Lines per port * Available number of ports. In an IVR based predictive campaign, this is the seed value that is passed to the predictive algorithm. Initially the dialer starts dialing with this value. **Note** Predictive algorithm will pick up the LPP value, when the value is updated only while the campaign is running. The updated value will be picked when the next set of contacts are fetched for dialing. This is a mandatory field. Default value = 1.5; Range = 1 to 3.

Field	Description
The following fields in Dialing Options are displayed if you have selected Agent-based campaign type	
Lines Per Agent (1-3)	Number of lines to be dialed for each agent. The dialer will try to connect as many live voices to the available agent(s) and it will disconnect the remaining calls. The probability of abandoned calls increases geometrically as the lines per agent increases. In an agent-based progressive campaign, you can configure the number of lines to dial per agent at a time. The dialer will determine the number of calls to dial based on the following calculation - Lines per agent * Available number of agents. In an agent-based predictive campaign, this is the seed value that is passed to the predictive algorithm. Initially the dialer starts dialing with this value. **Note** Predictive algorithm will pick up the LPP value, when the value is updated only while the campaign is running. The updated value will be picked when the next set of contacts are fetched for dialing. This is a mandatory field. Default value = 1.5; Range = 1 to 3. **Note** This field is not applicable if you have selected the Direct Preview dialer type for an agent-based campaign.
Callback Missed	Determines the action that should be taken on the contacts that were not called back. The three options for this field are: • Reschedule for same time next business day (default) • Mark it for a retry • Close the record.
The following fields in Dialing Options are common if you have selected Progressive or Predictive dialer type for IVR-based and Agent-based campaigns	
Handle Low Volume as Voice	Determines whether a low volume call should be treated as voice or disconnected. Select **Yes** or **No** radio button accordingly. Default is Yes, which means low volume calls are handled as voice and they are connected to an IVR port or an agent.

Field	Description
Answering Machine Treatment	If the outbound call detects an answering machine, you can choose to end the call or transfer it to IVR by selecting the desired radio button in this field. For agent-based campaigns, if you choose to transfer the call to IVR, a trigger field and an application name field appears for selection. The trigger field is a drop down list of JTAPI triggers associated with this campaign. There is one-to-one mapping between a campaign and a trigger. Only those triggers that are not associated with any other campaigns are displayed in the trigger list. The application name is associated with the above-mentioned JTAPI trigger. This field is auto-populated. Transfer to IVR radio button is enabled by default.
The following fields in Dialing Options are common if you have selected Predictive dialer type for IVR-based and Agent-based campaigns	
Predictive Correction Pace (10-1000)	The number of calls that were answered by live voice that the predictive algorithm should consider for each iteration. This is directly proportional with the correction frequency made in the Lines Per Port or Lines Per Agent parameter. This is a mandatory field. Default value = 100, Range = 10 to 1000. **Note** It is advisable not to change this value.
Predictive Gain	The Gain parameter controls the size of the lines per port or lines per agent corrections. This is directly proportional to the size of the lines per port or lines per agent correction. This is a mandatory field. Default value = 1.0, Range = Greater than 0 to 1.0. **Note** It is advisable not to change this value.
Call Abandon Limit (0-100)	Call abandon percentage, which should be within the limit specified by Federal Trade Commission (FTC). This is a mandatory field. Default value - 3%, Range 0-100%. This means that no more than three percent of calls that are answered by a person are abandoned, measured per day per calling campaign.
The following field in Dialing Options is displayed only if you have selected Predictive dialer type for an IVR-based campaign	
Maximum Lines Per Port (1-3)	Maximum number of lines to be dialed for each port. You can configure the maximum number of lines that can be dialed per port and the predictive algorithm ensures that it does not exceed this number. This is a mandatory field. Default value = 3.0, Range = 1 to 3.
The following field in Dialing Options is displayed only if you have selected Predictive dialer type for an Agent-based campaign	

Field	Description
Maximum Lines Per Agent (1-3)	Maximum number of lines to be dialed for each agent. You can configure the maximum number of lines that can be dialed per agent and the predictive algorithm ensures that it does not exceed this number. This is a mandatory field. Default value = 3.0, Range = 1 to 3.
Dial Settings (displayed if you have selected IVR-based or Agent-based campaign types)	
No Answer Ring Limit	The duration for which the progressive/predictive dialer should allow the customer phone to ring before disconnecting an unanswered call. The duration is calculated from the time the dialer receives the ringing message from the gateway. If the dialer does not receive any ringing message from the gateway within the time duration entered for this field, then the dialer waits for the same time duration one more time before disconnecting the call. For example, if you have configured the value for No Answer Ring Limit as 30 seconds, then the dialer will wait for 60 seconds before disconnecting the call. Default = 15 seconds, Range = 1 to 60 seconds. **Note** This field is also used to determine the reservation timeout for agent-based progressive or predictive campaigns. If the agent does not receive any outbound calls, then the agent continues to remains in the reserved state up to maximum time duration of twice the value configured in the No Answer Ring Limit field. For example, if you have configured the value for No Answer Ring Limit as 30 seconds, then the range for reservation timeout is calculated as 30 to 60 (30 * 2) seconds.
Abandoned Call Wait Time	For IVR-based progressive and predictive outbound campaigns, if the customer disconnects the call within the time set here, then the call is classified as customer abandoned. For agent-based progressive and predictive outbound campaigns, if the customer or the agent disconnects the call within the time set here, then the call is classified as customer abandoned. This is a mandatory field. Default value = 2 seconds, Range = 1 to 10 seconds.
Retries (displayed if you have selected IVR-based or Agent-based campaign types): Set the value for the following four fields as “0” if you want to disable retry option for an existing IVR or agent based outbound campaign. **Note** The time duration for the below fields is calculated as the value entered for each field, plus or minus the value entered for the Callback Time Limit field in the Add New Campaign web page.	

Field	Description
No Answer Delay	The time duration (in minutes) for which the dialer waits before calling back a no-answer call. Default value = 60 minutes. Though the default value is 60 minutes, the retry attempt will not be made after 60 minutes. This is based on the value set for the Callback Time Limit configured in the subsystem. For example, if a callback was scheduled for 9:30 am and if the Callback Time Limit is set to 15 minutes, then the Outbound subsystem calls the customer anytime between 9:15 am to 9:45 am. **Note** The value set for the No Answer Delay should always be more that the value set for the Callback Time Limit.
Busy Signal Delay	The time duration (in minutes) for which the dialer waits before calling back a busy telephone number. Default value = 60 minutes. This parameter is also based on the value set for the Callback Time Limit as described above in the No Answer Delay.
Customer Abandoned Delay	• For IVR-based progressive and predictive outbound campaigns, if a customer abandons a call, the time duration (in minutes) after which the dialer should call the customer back. • For agent-based progressive and predictive outbound campaigns, if a customer or an agent abandons a call, the time duration (in minutes) after which the dialer should call the customer back. Default value = 0
Dialer Abandoned Delay	If the dialer abandons a call, the time duration (in minutes) after which the dialer should call back the customer. Default value = 0

Step 3 Click **Add** or **Save** to save the configuration changes. While saving a new or updated campaign, the Outbound subsystem validates the Session values in the application and trigger pages based on following criteria, and it might display an alert message to increase Session value in application and trigger pages:

- In case of a Progressive campaign, the outbound subsystem checks whether the Lines Per Port * Dedicated Port for IVR-based campaigns and Lines Per Agent * Dedicated Agent for agent-based campaigns is greater than the minimum of the Session value in application and trigger.
- In case of a Predictive campaign, the outbound subsystem checks whether the maximum Lines Per Port * Dedicated Port for IVR-based campaigns and maximum Lines Per Agent * Dedicated Agent for agent-based campaigns is greater than minimum of the Session value in application and trigger.

You should increase the Session values in the application and trigger to the suggested value in the alert message to reduce the number of abandoned calls in an Outbound campaign.

Once you create a campaign, you need to import contacts for the campaign.

Import Contacts for Campaign

Caution You must verify all the contacts against the national do_not_call list before importing them.

Note

- When you import contacts that have agent extension numbers, ensure that the agents are not logged in when the campaigns are running.
- When you import contacts for campaign, the order of field names is as per the last selected order for that campaign.
- When **Allow Duplicate Contacts** option is not selected in both Manual and Automatic import, there could be a difference between the number of contacts imported and the number of remaining contacts. This is because many of the contacts imported could be duplicates in the database and are overwritten.
- When Phone 1 of a contact is dialed and the CPA marks it as Busy or Unanswered the same number is retried based on the retry count and delay configured in the campaign. When the retry count reaches the maximum value, the contact is marked as closed. The other phone number for a given contact is dialed only when the called number is classified as Modem, Fax or Invalid.
- Each time contacts are imported, they are appended to the existing list of contacts for the selected campaign. If the new list contains a contact with the same Phone 1 value as the Phone 1, Phone 2, or Phone 3 value, or the same Phone 2 value as the Phone 1, Phone 2, or Phone 3 value, or the same Phone 3 value as the Phone 1, Phone 2, or Phone 3 value, of an existing contact, the existing contact is overwritten with the new contact information. The call history for the contact (if any) is retained.
- For supervisors to **Schedule Import** of contacts for a campaign, you must configure the campaign to use SFTP or HTTPS.

For a manual import of contacts:

Attention

- The contacts file should be ASCII-encoded or UTF-8 encoded if it contains special characters (for example, if the contact names are in Chinese, Russian, Japanese, and so on).
- When you want to import multiple dialing lists, ensure that you select one dialing list at a time.
- The maximum limit of contacts in the contacts file is 100 thousand.
- The maximum limit of contacts that can be imported per campaign is determined by:
  - Number of contacts that are already imported and yet to be dialed out.
  - The number of contacts present in the contacts file being imported.
- You must not initiate the manual import of contacts and automatic import of contacts using SFTP or HTTPS at the same time. If a manual import is attempted when an automatic import is in progress, it would fail.

For a scheduled import of contacts:

Attention

- The contacts file should be ASCII-encoded or UTF-8 encoded if it contains special characters (for example, if the contact names are in Chinese, Russian, Japanese, and so on).
- The maximum limit of contacts in the contacts file is 100 thousand.
- The automatic import process would stop importing contacts for a campaign after the campaign has 20,000 contacts remaining (yet to be dialed out). After the contacts are dialed out, then the next scheduled import would import additional contacts.
- The maximum limit of contacts that can be imported per campaign is determined by:
  - Number of contacts that are already imported and yet to be dialed out.
  - The number of contacts present in the contacts file being imported.

    For example: Assume a new campaign and a contacts file has 100 thousand contacts that are scheduled for import. When the import is attempted for the first time, the first 20,000 (from 1 to 20,000 contact) contacts are fetched and imported for the campaign.

    Before the next scheduled import, assume system has successfully dialed out 5000 contacts and 15000 contacts are remaining. In this, case, when next import is attempted as per the schedule, the system would import 5000 contacts for the remaining capacity of the campaign (20000-15000=5000 contacts). Thus, assuming that the contacts file has not changed across the imports, the system would import the contacts from 20001 to 25000 in the contacts file.
- You must not initiate the manual import of contacts and automatic import of contacts using SFTP or HTTPS at the same time. If a manual import is attempted when an automatic import is in progress, it would fail.
- If there are multiple imports scheduled at the same time, the import of contacts happen one at a time.
- When an automatic import of contacts is in progress and if there is a Unified CCX Engine fail over, the import will be terminated and its status is not available on the **Automatic Import Contacts** page.

Manual Import of Contacts for Campaign

To import contacts manually for a selected campaign, complete the following steps.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Outbound** > **Campaigns**.

The Campaigns web page opens, displaying the details of existing campaigns.

Step 2 Click the hyperlink below the Name column for the campaign for which you want to import the contacts.

The Campaign Configuration web page opens for the selected campaign.

Step 3 Click **Import Contacts**. The Import Contacts web page opens.

Step 4 To import contacts from a CSV or a TXT file, click the **Manual Import Contacts** tab.

Step 5 Navigate to the directory that contains the imported fields in the *same order* as they appear in the text file. Specify a filename to import the contacts from the fields being imported.

A contact list can contain up to 7 fields:

- Account Number - The account number of a contact. The account number can be a maximum length of 25 characters.
- First Name - The first name of a contact. The first name can be a maximum length of 50 characters.
- Last Name - The last name of a contact. The last name can be a maximum length of 50 characters.
- Phone1 - The phone number for the contact. This field can be 28 characters long and must be a valid phone number. Phone1 is mandatory and must be specified.
- Phone2 - The phone number for the contact. This field can be 28 characters long and must be a valid phone number.
- Phone3 - The phone number for the contact. This field can be 28 characters long and must be a valid phone number.
- Dial Time - The time to dial a number for individual contacts on the current date. The format to be used for this field is HH:MM. For example, to specify the dialing time as 08:25 am, the dial time field value should be 08:25 and for 03:45 pm, the dial time field value should be 15:45. This field is applicable only for Direct Preview Outbound campaigns.

Step 6 Check the **Allow Duplicate Contacts** option, if required.

Allow Duplicate Contacts

A record is considered duplicate when the phone number in any of the three phone fields (Phone 1, Phone 2, and Phone 3) of the records being imported:

- Exists in any of the three phone fields of the other contacts being imported.
- Exists in any of the three phone fields of the contacts previously imported for the campaign that are dialed out since last midnight or yet to be dialed out.

If this option is not selected:

- The contacts identified as duplicates are not imported for the campaign.

If this option is selected:

- The check for duplicate contacts is not performed and all contacts are imported as is.

Note
By default this option is not selected.

Step 7 Click **Import**.

What to do next

While uploading outbound contacts in a HA over WAN deployment of Unified CCX, if all the contacts that are being uploaded exist in the database and are being modified, follow these guidelines to avoid long delays:

- Upload the contacts during non-peak hours.

- Upload in batches of 500 contacts or less.

Schedule Import of Contacts Using SFTP or HTTPS

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Outbound** > **Campaigns**.

The Campaigns web page opens, displaying the details of existing campaigns.

Step 2 Click the hyperlink below the Name column for the campaign for which you want to import the contacts.

The Campaign Configuration web page opens for the selected campaign.

Step 3 Click **Import Contacts**. The Import Contacts web page opens.

Step 4 To automatically import contacts from a remote server using SFTP or HTTPS, click the **Automatic Import Contacts** tab. SFTP is the default option.

Step 5 Select the server type as **SFTP** or **HTTPS**. Enter the SFTP or the HTTPS remote server details to import contacts from a remote server using SFTP or HTTPS respectively.

If you select SFTP, enter the following details for the Remote SFTP Server:

- IP Address /FQDN—The IP address or the Fully Qualified Domain Name of the remote SFTP server.
- RSA Key—The RSA public key of the remote SFTP server. This is optional and is used for trust verification of the SFTP server by the Unified CCX server.
- User Name—The username that is required to log in to the remote SFTP server.
- Password—The password that is required to log in to the remote SFTP server.
- CSV File Path—The CSV file path (.csv or .txt file path) to import contacts from the remote SFTP server. This is the fully qualified file name. For example:

If you select HTTPS, enter the following details for the Remote HTTPS Server:

- URL—The URL to access the contacts over the remote HTTPS Server.
- User Name—The username that is required to log in to the remote HTTPS server.
- Password—The password that is required to log in to the remote HTTPS server.
- HTTPS Certificate—The check box to confirm that:
  - You have uploaded the HTTPS Certificate in the Unified OS Administration web interface at, **Security** > **Certificate Management**.

    Note
    This is required for trust verification of the HTTPS server by the Unified CCX server.

  - Restarted the Cisco Tomcat and Cisco Unified CCX Engine on both the node.

Step 6 Check the **Allow Duplicate Contacts** option, if required.

Allow Duplicate Contacts

A record is considered duplicate when the phone number in any of the three phone fields (Phone 1, Phone 2, and Phone 3) of the records being imported:

- Exists in any of the three phone fields of the other contacts being imported.
- Exists in any of the three phone fields of the contacts previously imported for the campaign that are dialed out since last midnight or yet to be dialed out.

If this option is not selected:

- The contacts identified as duplicates are not imported for the campaign.

If this option is selected:

- The check for duplicate contacts is not performed and all contacts are imported as is.

Note
By default this option is not selected.

Step 7 Click **Test Connection** to check the connectivity with the remote SFTP or HTTPS server.

Step 8 Set the order of field names and a schedule to automatically import contacts in regular intervals.

A contact list can contain up to 7 fields:

- Account Number - The account number of a contact. The account number can be a maximum length of 25 characters.
- First Name - The first name of a contact. The first name can be a maximum length of 50 characters.
- Last Name - The last name of a contact. The last name can be a maximum length of 50 characters.
- Phone1 - The phone number for the contact. This field can be 28 characters long and must be a valid phone number. Phone1 is mandatory and must be specified.
- Phone2 - The phone number for the contact. This field can be 28 characters long and must be a valid phone number.
- Phone3 - The phone number for the contact. This field can be 28 characters long and must be a valid phone number.
- Dial Time - The time to dial a number for individual contacts on the current date. The format to be used for this field is HH: MM. For example, to specify the dialing time as 08:25 am, the dial time field value should be 08:25 and for 03:45 pm, the dial time field value should be 15:45. This field is applicable only for Direct Preview Outbound campaigns.

Step 9 Set the Schedule for the automatic import of contacts.

a) Select the date.
b) Set the **Start Time**.
c) Check the **Repeat Every** checkbox and set the reoccurrence of the automatic schedule.

Note
- The Outbound schedule time is based on the Unified CCX server time zone.
- Avoid scheduling the import of contacts during peak hours.

Step 10 Select **Enable** or **Disable** option for automatic schedule of import of contacts.

Step 11 Click **Save** to save the configurations done for **Automatic Import Contacts**.

Enable Campaigns

You must verify that the configured campaigns are active and that the start and end times for the enabled campaigns are specified as required.

To verify the state of the required campaign, complete the following steps.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Outbound** > **Campaigns**.

The Campaigns web page opens, displaying following information for the existing campaigns:

Field	Description
Name	Name of the campaign.
Start Time/End Time (hh:mm) AM PM	Start Time and End Time fields indicate the time range during which the campaign runs.
Remaining Contacts	The Remaining Contacts field indicates the number of contacts that are yet to be dialed for each campaign. In addition to the contacts that have not been dialed, this number also includes contacts that have requested a callback and contacts that will be tried again because of unsuccessful prior attempt(s) (for example, the contact was busy or unavailable). A detailed breakdown of the pending contacts is provided in the Printable Reports page for each campaign.
Enabled	The Enabled field indicates to the Outbound subsystem whether this campaign is currently active.
Campaign Type	Denotes whether a specific campaign is IVR-based or Agent-based. The existing campaigns will be marked as Agent-based after an upgrade.
Delete	Click **Delete** icon next to the name of the campaign that you want to delete.

Step 2 Verify that the Enabled field is set to **TRUE** and that the start and end times are specified as required.

Outbound Subsystem and Time Detection

The Outbound subsystem uses the area code of a contact's phone number to determine the time zone of the contact's calling area. The contact's phone number can also be in E.164 format.

The subsystem provides the mapping for North American area codes to their corresponding time zones. The default North American area codes are used to determine the time zone for phone numbers that are not in the

E.164 format (for example, 234-567-8900). The Area Codes web page allows you to add, modify, and delete any area-code-to-time-zone mapping. Some area codes extend across multiple time zones. For such area codes, you can edit the default time zone for that area code and specify a different one, if required.

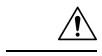
Changes to area codes take affect the next time you import contacts. For example, if the time zone of area code 603 is changed from 16 to 17, contacts already present in the system that have an area code of 603 continue to have the GMT Offset of 16. Any contacts with area code 603 that are imported after the area code change have 17 for the GMT Offset.

When Outbound contacts are imported into the database, all contacts are assigned a GMT time zone for the three phone numbers provided. The Outbound subsystem determines this GMT time zone by extracting the area code of each phone number and checking it against the Area Codes table to obtain the corresponding time zone. If the area code cannot be matched, the Outbound subsystem uses the local time zone and Daylight Savings Time (DST) setting of the server. The Outbound subsystem also considers the DST to determine if an Outbound contact can be called at a given time.

The Outbound subsystem ensures that the contacts are dialed at valid times. For Outbound contacts which have been scheduled for callback, the scheduled callback time is converted to GMT time zone and stored in the callbackDateTime field in the database.

For pending records, the Outbound subsystem ensures that Outbound contacts are called only within the Customer Dialing Time Range (hh:mm) detected by the MinCustomerDialTime and MaxCustomerDialTime, as per federal regulations. You can configure this time in the Unified CCX Administration GUI.

Add Area Codes



Caution Area code and long distance prefix configuration changes made to the Outbound subsystem do not take effect for calls/contacts currently in the Outbound subsystem's memory. For example, if you change the long distance prefix or local area code, the contacts already in the Outbound subsystem's memory will continue to use the old long distance prefix and local area code.

The Outbound subsystem provides all of the mappings from North American area codes to their corresponding time zones at the time of product release. The Area Codes page allows the administrator to add, modify, and delete any area-code-to-time-zone mappings.

Some area codes extend across multiple time zones. For such area codes, an administrator can edit the default time zone for that area code and specify a different one, if required.

The Area Codes Management page allows users to find, add, delete, and modify the mapping of area codes and time zones. The Outbound subsystem uses the area code of a contact's phone number to determine the time zone of the contact's calling area. This page can also be used for adding international area codes. International area codes must include the country code and the city code.

To add an area code, complete the following steps.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Outbound** > **Area Codes**.

The Area Codes Management web page opens.

Step 2 In the Area Code field, specify a unique identifier for the area code. This field can have any numeric value, including 0 or leading zeros. This is a mandatory field.

Step 3 Click the **Add New** icon that is displayed in the tool bar in the upper, left corner of the window or the **Add New** button that is displayed at the bottom of the window.

The new Area Code information is updated.

Call Status Values

For each contact, the call statuses and their corresponding values are recorded in the database and described in the following table:

Call Status	Value (stored in database)	Description
Pending	1	The call is pending. This is the initial state for all records.
Active	2	The record was retrieved by the Outbound subsystem for dialing.
Closed	3	The record is closed (not dialed).
Callback	4	The record is marked for a callback.
Max Calls	5	Maximum attempts have been reached for this record (considered closed).
Retry	6	The record is redialed immediately whenever there is any miss in the callbacks for Retries with Delay.
Unknown	7	If the Outbound subsystem was restarted with records in the Active (2) state, they are moved to this state.
Retries with Delay	8	The record is redialed as it was either busy, no answer, customer abandoned or system abandoned. Retry time is set as per the corresponding configuration in Unified CCX Application Administration web interface.

Contact States Reset at Midnight

The Outbound subsystem performs the following actions at midnight:

- The DialingListConfig records with a call status of Unknown are reset to Pending.

Note Outbound contacts with a call status of Unknown indicate that the these contacts were retrieved from the database but the system went down before they could be dialed out.

- Missed callback records (dialingListConfig records that have call status callback and a callBackDateTime smaller than the current time) are updated depending on the missed callback action configured in the Unified CCX Administration GUI.
  - MissedCallbackAction: Reschedule (for the same time on the next business day)
  - MissedCallbackAction: Retry (sets the call status to Retry and retries at the start of next business day)
  - MissedCallbackAction: Close (sets the call status to Closed)
  - Dialing list records with a call status of Closed or Max_Calls are moved to a separate historical data table

Note The records marked as closed today will be moved the next day at midnight. For example, the records closed on 4th June will be moved on 5th June at midnight.

- The DialingListConfig records with a call status of "Retries with delay" and which could not be retried due to lapsed time are marked for immediate retry at midnight.
- When the Unified CCX engine goes from offline to online (for example, the standby server becomes active [online] if the active [first] server fails), the dialing list records with a status of Unknown are reset to Pending.

Call Result Values

For each contact, the call results (as marked by the agent on Finesse or automatically deleted by the system) and their corresponding values are recorded in the database and described in the following table:

Call Result	Value (stored in database)	Description
Voice	1	Customer answered and was connected to agent.
Fax	2	Fax machine or modem detected.
Answering machine	3	Answering machine detected.
Invalid	4	Number reported as invalid by the network.
Callback	8	Customer requested callback.
Agent Rejected	9	Agent rejected the preview call.
Agent Closed	10	Agent rejected the preview call with the close option (not dialed).
Busy	11	Busy tone detected.

Call Result	Value (stored in database)	Description
Ring No Answer	12	Agent did not respond to the preview call within the time out duration. **Note** You can configure the time out duration using the Preview Call Timeout field detailed in the **Configure General Outbound Properties**.
Callback Failed	13	This value should not be written to the database; this is for internal use only.
Callback Missed	14	Callback missed and marked for Retry.
Timeout	15	Customer phone timed out either due to Ring No Answer (RNA) or Gateway failure.
Call Abandoned	16	Call was abandoned because IVR port was unavailable or Unified CCX failed due to transfer the call to the IVR port.
Call Failed	17	Call failed due any one of the following reasons: • Dialer asked the Gateway to cancel a call that has not yet been placed • Gateway has declined the call • Gateway is down or Gateway has timed out while placing the call • Gateway failure or configuration issues at the Gateway .
Customer Abandoned	18	Customer abandoned as customer disconnected the call within the time limit as configured in “Abandoned Call Wait Time” in Unified CCX Application Administration web interface.

Reclassification Status Behavior

When the Outbound contacts are imported into the database from the Unified CCX Administration GUI, the Call Status column in the Dialing List table is assigned the default value of 1 (Pending), indicating that these Outbound contacts are yet to be dialed. When the Outbound subsystem retrieves a batch of contacts from the database, the **Call Status** is set to 2 (Active). After a call is placed to the Outbound contact, the **Call Status** is set to 3 (Closed) and the **Call Result** is set to 1 (Voice), as all Outbound calls are classified by the agent desktop as Voice by default. If the agent clicks the reclassification button on the agent desktop and reclassifies the call as Answering Machine/Fax/Busy/Invalid or selects the Callback button and schedules a call back, the Outbound subsystem updates the **Call Result** field accordingly and, based on the call result, it also updates the **Call Status**.

The following table describes the relationship between **Call Status** and **Call Result** values and the resulting behavior of the system. The values in brackets are the actual values stored in the database.

The following information is applicable only for Preview Dialer.

Call Result	Call Status	Behavior
Voice (1)	Closed (3)	This contact is not dialed again.
Fax (2)	Retry (6)	This contact is retried, using a different phone number provided for this contact. If alternate phone numbers are not available, the call status is closed.
Answering machine (3)	Retry (6)	This contact is retried, with the same phone number as before.
Invalid Number(4)	Retry (6)	This contact is retried, using a different phone number provided for this contact. If alternate phone numbers are not available, the call status is closed.
Busy	Retry (6)	This contact is retried, with the same phone number as before.

The **Call Status** is set to 3 (Closed) when the Outbound contact is no longer dialed for this campaign. This also happens automatically if the system reaches the maximum attempts limit for an Outbound contact, which means that the system tried dialing the Outbound contact the maximum number of times configured in the Unified CCX Administration GUI.

Call Retrieval Priority

While retrieving Outbound contacts from the database, records that have scheduled callbacks have priority as the callback time must be adhered to. Outbound contacts are retrieved in the following order of priority:

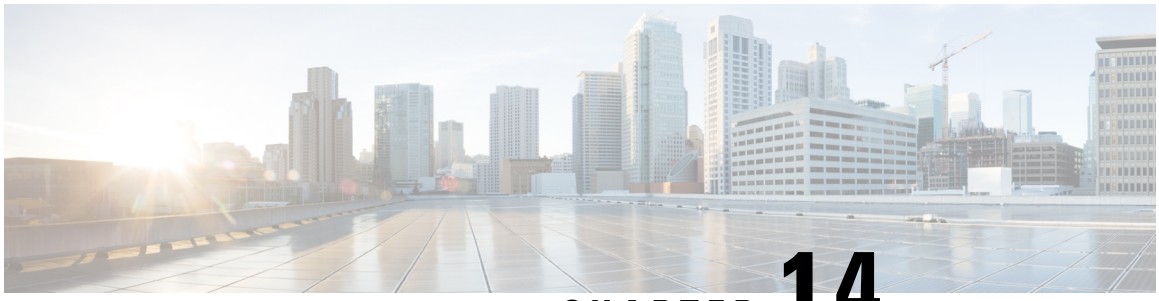
- Priority 1—Outbound contacts with a scheduled callback (call status = 4) and the current time is within the CallbackTimeLimit configured on the Campaigns page (default value is15 minutes) of the scheduled callback time.
- Priority 2—Outbound contacts to be retried after a specific delay. This is not applicable for direct preview campaigns (call status = 8).
- Priority 3—Outbound contacts in the Pending state (call status = 1).
- Priority 4—Outbound contacts in the Retry state (call status = 6).

Note The Call Retrieval Priority is on a per campaign basis. If an agent is part of multiple CSQs that are part of different campaigns, priority of callbacks may be overridden by different queues. For example, Priority 4 in a particular queue may take precedence over Priority 1 of another queue.

Failover and System Restarts

Outbound contacts with an Active call status during a failover indicate that these contacts were retrieved from the database but the system went down either before they could be dialed or after they were dialed but before the call status and call result columns were updated. When the system restarts, the call status for all such Outbound contacts is changed to 7 (Unknown). All Outbound contacts in the Unknown state will be reset to the Pending state (should be retrieved for dialing again) at midnight every night.

If there is an Outbound call in progress during a failover, they cannot be dialed again, as the call status is set to Closed as soon as an Outbound call is placed and these records will not be retrieved for dialing again when the system comes back. However, if the failover happened before the system could update the call status to Closed, these records remain in the Active state and are marked Unknown so they transition to Pending state after midnight. Once they are in the Pending state, they will be dialed again.



CHAPTER 14

Cisco Unified Contact Center Express Supervisor and User Options Plug-Ins

- About User Management, on page 249
- About Unified CCX User Capabilities, on page 249
- Unified CCX Supervisor Web Interface, on page 251
- Unified CCX User Options Web Interface, on page 252

About User Management

In earlier versions of Unified CCX, many user parameters like user ID, password, and pin were configured from the Unified CM Administrator. Some Unified CCX-related user parameters were configured through the Unified CCX Administration.

In Unified CCX, all Unified CCX user roles (capabilities) are consolidated into one User Configuration area.

Note Any changes made to the user privileges for the Unified CCX user roles after the backup operation is performed are not restored.

The Unified CM user details are stored in the Unified CM database.

About Unified CCX User Capabilities

The capability for each user refers to the Unified CCX access level assigned for each user. Unified CCX users can be assigned to one of the following four roles (or capabilities):

- Administrator
- Supervisor
- Historical Report User
- Agent

Each of these roles are described in this section.

Administrator Privileges

A Unified CCX Administrator is a user with complete access to the Unified CCX Administration and has the authority to configure the entire system. An Administrator can also be assigned a combination of other roles.

The Administrator can turn on/off the authority of a Supervisor to manage the teams and agents.

Supervisor Privileges

Supervisors can additionally modify and view skills, view the list of all teams for which this user is the supervisor, view the skills, CSQs, and resource groups configured in this system, view and manage resources, and configure the teams that they are to manage.

Unified CCX provides three types of supervisors:

- **Application Supervisor**: A basic supervisor role applicable to a Unified CCX Application server *without* a Unified CCX license. An application supervisor can only view reports.
- **ACD Supervisor**: A supervisor with an agent role. This role is applicable to a Unified CCX Application server with *any* Unified CCX license. An ACD supervisor can administer teams/agents and also view reports. Thus Unified CCX enables dynamic reskilling, the ability by which an ACD supervisor can add or remove skills from an agent without an administrator privilege.

Depending on the license allowed, Unified CCX Supervisors have the following privileges:

- View reports through Unified Intelligence Center web client.
- View agents and CSQ being monitored. This is only for a remote Supervisor.
- View the list of all teams for which this user is the Supervisor.
- Configure the teams managed by the Supervisor.
- View the skills, CSQs, and Resource Groups configured in this system.

Note The RmCm menu can be viewed by the Supervisor only when any of the following two options are selected as the parameter value for the Supervisor Access field located in **System** > **System Parameters** > **Application Parameters**:

- Access to all Teams
- Access to Supervisor's Teams only

- View and manage all the resources.

Historical Report User Privileges

A user with a historical report role can view various historical reports. The number and types of reports allowed to be viewed depends on the licenses available on a given Unified CCX system.

Agent Privileges

Note An agent capability is only available with a Unified CCX license.

Unified CM users in Unified CCX are assigned an agent role when an agent extension is associated to the user in the Unified CM User Configuration page. Consequently, this role can *only* be assigned or removed for the user using Unified CM Administrator End User Configuration web page. These users can not be assigned or removed in Unified CCX Administration.

Unified CCX Supervisor Web Interface

Use the Unified CCX Supervisor web page to:

- View and monitor permitted agents
- View and monitor permitted CSQs
- Access real-time reports, tools, and settings

Access Unified CCX Supervisor Web Page

To access the Unified CCX Supervisor web page, perform the following steps:

Procedure

Step 1 Ensure supervisor capability is assigned to the user designated as supervisor (see **Supervisor Privileges** and **User View Submenu**).

Note
If the supervisor is assigned administrator capability as well, the Unified CCX Administration window is opened instead of the Supervisor web page.

Step 2 From a web browser on any computer on your network, enter the following case-sensitive URL:

```
https://<servername>/appadmin
```

In this example, replace `<servername>` with the hostname or IP address of the required Unified CCX server.

Tip
If you have already accessed the Unified CCX Administration application or Supervisor web page in the browser, be sure to logout from the current session using **Logout** link displayed in the top right corner of any Cisco Unified CCX Administration web page or **System** > **Logout** and login with respective user credentials.

User IDs are case-sensitive when logging into the Unified CCX Administration web interface. To make them case-insensitive, you must install 12.5(1) SU1 ES02.

The Unified CCX Supervisor web page appears.

Unified CCX User Options Web Interface

Use the Unified CCX User Options web page to perform:

- Unified CCX downloads
- Alternate pronunciations for call by name
- Access the Unified CM User web page

Access Unified CCX User Options Web Page

To access the Unified CCX User Options web page, perform the following steps:

Procedure

Step 1 From the Unified CCXAdministration, enter **https***://<Cisco Unified CCX IP address>/**appuser/appusermain***.

Step 2 If prompted to do so, enter your User ID and Password.

The Unified CCX User Options web page appears.

Note
Only Unified CM users are allowed to log in.

Step 3 When finished, click **Logout**.

Add Alternative Pronunciations

Alternative Pronunciations for Call by Name is an independent feature located on the Unified CCX User Options Welcome web page. This feature lets you add one or more alternate pronunciations for your first or last name and is useful if callers might refer to you by more than one name. For example, if your first name is Bob, you might add the alternate pronunciations “Bob” and “Bobby”. Similarly, if your last name is Xhu, you might add the alternate pronunciation “Xhu”.

To access the Alternative Pronunciations for Call by Name web page, perform the following steps:

Procedure

Step 1 In the Cisco Unified CCX User Options Welcome web page, choose **User Options** > **Alternative Pronunciations for Call by Name**.

The Alternate Pronunciations web page appears.

Step 2 In the First Name field, you can enter an alternate pronunciation of your first name. For example, if your name is "Mary," you might enter "Maria."

Step 3 Click **Add>>**.

The name moves to a list of alternate first name pronunciations.

Step 4 Repeat Steps 2 and 3 as needed to add other alternate pronunciations.

To remove an alternate pronunciation for your first name, click the alternate pronunciation and then click **Remove**.

Step 5 In the Last Name field, you can enter an alternate pronunciation of your last name. For example, if your last name is "Smith," you might enter "Smitty."

Step 6 Click **Add>>**.

The name moves to a list of alternate last name pronunciations.

Step 7 Repeat Steps 5 and 6 as needed to add other alternate pronunciations.

To remove an alternate pronunciation of your last name, click the alternate pronunciation and then click **Remove**.

Step 8 Click **Save** to apply the changes.

Access Unified CM User Options Page

To access the Unified CM User Options web page, perform the following steps:

Procedure

Step 1 In the Unified CCX User Options Welcome web page, choose **User Options** > **Cisco Unified CM User Page**.

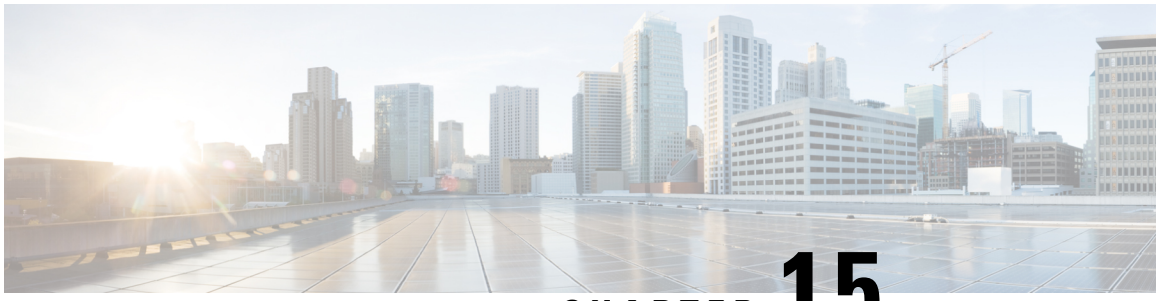
The Unified CM User Options Log On dialog box appears.

Step 2 Enter your Unified CM user ID and password, and then click **Log On**.

The Unified CM User Options web page appears.

Step 3 Click the option you want.

Step 4 When finished, click **Logout**.



CHAPTER 15

System Menu

- Access Server Menu, on page 255
- Cloud Connect, on page 257
- Unified CM Configuration, on page 259
- System Parameters, on page 259
- Single Sign-On (SSO), on page 265
- Custom File Configuration, on page 267
- Standalone Cisco Unified Intelligence Center, on page 267
- License Information, on page 269
- Language Information, on page 277
- Logout Menu, on page 278

Access Server Menu

Choose **System** > **Server** from the Cisco Unified CCX Administration menu bar to access the **List Servers** web page. Use the **List Servers** web page to view, add, remove, and view servers in the cluster.

Note **Before installing Unified CCX on the second node, you must configure the second server using this procedure. Installation of second node will fail if you do not perform this configuration**.

To view, modify, or delete the server configuration information of any server, click the respective hyperlink in the **Host Name/IP Address** field. The **Server Configuration** web page opens to display Host Name/IP Address, MAC Address, and Description of the server. Update the values in the fields and click **Save** to save the changes. Click **Delete** to delete the configuration information of a server.

Note You cannot delete the publisher.

Configure Server

To configure a new server that needs to be added to form a Unified CCX cluster for a High Availability setup, complete the following steps.

Procedure

Step 1 Click the **Add New** icon in the toolbar in the upper left corner of the **List Servers** web page or the **Add New** button at the bottom of the **List Servers** web page to add the new server.

The Server Configuration web page appears.

Note
- The **Add New** button is disabled when two servers are added to the cluster in a High Availability setup.
- A warning message appears when you click the **Add New** button without having a High Availability license.

Step 2 Complete the following fields:

Field	Description
Host Name/IP Address	Hostname or IP address of the server that you want to add.
MAC Address	MAC address of the server that you want to add.
Description	Description of the server that you want to add.

Step 3 Click **Add** to add details of the new server.

Server Deletion

This section describes how to delete a server from the Unified CCX. In Unified CCX administration, you cannot delete the first node that is also called as the publisher node, but you can delete the subscriber node.

Procedure

Step 1 Choose **System > Server** from the Cisco Unified CCX Administration menu bar to access the List Servers web page.

Step 2 Select the subscriber node and click **Delete** to delete the configuration information of the server.

Step 3 Power off the subscriber node.

Note
When a subscriber node is removed from a cluster, its certificates still exist in the publisher node. The administrator must manually remove the following:
- The certificate of the subscriber node from the trust-store of the publisher node.
- The certificates of the publisher from the trust-store of the removed subscriber node.

Step 4 Run the **utils system restart** command to restart the publisher node.

Cloud Connect

Cloud Connect enables on-premise Unified CCX solution to integrate with different cloud services. The Cloud Connect services are responsible for interacting with Webex Experience Management (WXM) cloud service for presenting surveys to users and access analytics on the survey responses to understand the Customer Experience trends.

Note To use cloud services, memory requirement is different. If you do not have the required memory an error message is displayed. For the appropriate memory requirements, see *Solution Design Guide for Unified Contact Center Express* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-implementation-design-guides-list.html.

Use the **Cloud Connect** page to perform the following:

- Check the status of Cloud Connect.
- Register and Deregister Unified CCX with Cisco Webex Cloud.
- Enable and Disable Cloud Services.
- Check Cluster Information.
- Check the status of the nodes in the cluster.

For more information, see *Cloud Connect* chapter in *Cisco Unified Contact Center Express Features Guide*.

Actions

The following table lists the actions that you can perform on this page:

Action	Procedure
Register	To use the Cisco Webex Cloud features. **Note** Ensure that all the Prerequisites are met. 1. Select the **I have received the email for the account creation in Cisco Webex Cloud and have successfully created an account in Cisco Webex Cloud** checkbox. 2. Click **Register**. The **Cisco Webex Control Hub** page is displayed. Follow the on-screen instructions to register.
Deregister	Click **Deregister**. The **Cisco Webex Control Hub** page is displayed. Follow the on-screen instructions to deregister.
Deployment Name	Enter a name to identify the Unified CCX system. By default, **Deployment ID** is displayed.

Action	Procedure
Test Connection	Click **Test Connection** to check the Unified CCX connectivity with **Cisco Webex Cloud**. In a HA environment, the connection is tested for both the nodes.
Enable Data Streaming to Cisco Webex Cloud	To publish the Unified CCX data to a database that is available in cloud: **1.** In the **Cluster Information** table, enter the **Deployment Name**. **2.** In the **Cloud Services** table, select the **Enable** checkbox for **Data Streaming to Cisco Webex Cloud**. **3.** Click **Update**.

Cluster Information

The details of **Cluster Information** table are as follows:

Field	Description
Deployment ID	Mac address of the system.
Deployment Name	Name to identify the Unified CCX system.
HTTP Proxy	HTTP Proxy value that is used by Cloud Connect. **Note** If you have configured HTTP Proxy settings in the previous versions of Unified CCX, after upgrading, you must click **Update** to get the previously configured HTTP Proxy value. If there is a mismatch of HTTP Proxy value between **System Parameters** page and **Cloud Connect** page, a **Warning** icon is displayed. Click **Update** to get the updated proxy value.

Cloud Services

You can enable and disable the cloud services that are listed. The following cloud service is available:

- **Data Streaming to Cisco Webex Cloud**

Cluster Status

The **Cluster Status** table lists the **Host Name** and **Status** of each node. The status can be any one of the following:

- In Service
- In Maintenance
- Not Configured
- Out of Service

- Unknown

Adjacent to each status, there is a link to **View Status**. Click the link to download a text file that has the status details of the node. This file is used to debug issues with Cloud Connect.

Unified CM Configuration

Choose **System** > **Unified CM Configuration** from the Unified CCXAdministration menu bar to access the Unified CM Configuration web page.

Use the Unified CM Configuration web page to update the following information:

- The Unified CM AXL provider used for Unified CCX AXL requests for agent authentication and SQL queries.
- The Unified CM JTAPI provider used by the Unified CCX Engine Unified CM Telephony subsystem to control and monitor CTI ports and route points.
- The Unified CM RmCm -JTAPI provider used by the Unified CCX Engine RmCm subsystem to control and monitor the agent phones and extensions.

System Parameters

Note When you configure a parameter for the primary node, same value is reflected for the secondary node.

The System Parameters configuration web page displays the following fields.

Table 13: System Parameters

Field	Description
Generic System Parameters	
System Time Zone	The system or primary time zone is the same as local time zone of the primary Unified CCX node configured during installation. Display only. Unified CCX Administration uses this primary time zone to display time-related data. **Note** If you have changed the primary time zone, reboot both the nodes in the Unified CCX cluster.
Network Deployment Parameters (displayed only in a HA over WAN deployment)	
Network Deployment Type	Displays the network deployment type as LAN or WAN only if we have more than one node. Display only.
Internationalization Parameters	

Field	Description
Customizable Locales	Use to specify a unique locale. Default value is blank.
Default Currency	Default currency, such as American dollars (USD), Euros, and so on. This is a mandatory field. Converts currency amounts in a playable format when no currency designator is specified Default: American Dollar [USD]
Media Parameters	
Codec	The Codec chosen during installation for this Unified CCX server. Unified CCX supports packetization intervals of 20 ms, 30 ms, or 60 ms. Default value is 30 ms. **Note** After changing the Codec, ensure that you restart Unified CCX Engine on all nodes for the settings to take effect.
MRCP Version	Select appropriate version of the protocol for ASR and TTS. When you select **MRCPv1** or **MRCPv2**, ensure that the appropriate port changes are done for MRCP ASR and MRCP TTS Servers. **Note** When you upgrade, the default value is **MRCPv1**. After changing the MRCP version, ensure that you restart Unified CCX Engine on all nodes for the settings to take effect.
Default TTS Provider	Default TTS (Text-to-Speech) provider. Default: By default, no TTS provider is configured. Select a provider from the drop-down list to configure it as the default. The system uses the default TTS provider to determine which provider to use if the TTS request does not explicitly specify the provider to use.
User Prompts override System Prompts	When enabled, custom recorded prompt files can be uploaded to the appropriate language directory under Prompt Management to override the system default prompt files for that language. By default, this is disabled.

Field	Description
SRTP	SRTP (Secure Real-Time Protocol) protects the confidentiality of the media with cryptographic procedures. When enabled, a secure media for communication (SRTP) is established between callers and CTI port. Before you enable SRTP, ensure that the CUCM Cluster Security Mode is set to Mixed mode. **Note** When SRTP is enabled, a secure JTAPI connection is established between the following subsystems and Unified CM: • Unified CM Telephony • RmCm After enabling or disabling SRTP, ensure that you restart Unified CCX Engine on all nodes for the settings to take effect. An SRTP-enabled HA setup requires distinct RmCm provider users. So, the system generates a separate **RmCm Provider User Id** with suffix "_ccxsub" for the subscriber node. Associate devices and device profiles only with the **RmCm Provider User Id** that is configured in the **Cisco Unified CM Configuration** page (primary RmCm user). During data synchronization, the devices and device profiles that are associated only with system-generated RmCm user are removed and synchronized with that of primary RmCm user.
Application Parameters	
Supervisor Access	The Administrator uses this option to allow certain privileges to supervisors (all supervisors have the same privilege). The options are: • No access to teams—The supervisor logs into the Supervisor page, but will not be able to see any team information (No RmCm info). • Access to all teams—The supervisor logs into the Supervisor page, and will be able to see all the teams (RmCm information). • Access to supervisor teams only—The supervisor logs into the Supervisor page, and can see the teams that they supervise. When this option is selected, only the Primary Supervisor can see the team-specific information. The secondary supervisor will not be able to see the team-specific information. Default: No access to teams **Note** A supervisor who does not have administrator privileges can add, modify, or remove skills from an agent.

Field	Description
Max Number of Steps that have run	The maximum number of steps an application can run before the Unified CCX Engine terminates the script or application. This is a mandatory field. This limitation is intended to prevent a script from running indefinitely. Default value is 1000. **Note** Do not change the default value.
Additional Tasks	This field allows you to control the creation of additional threads that the Unified CCX server internally initializes based on licensed Unified IP IVR ports. This is a mandatory field. Default value is 0.
Default Session Timeout	Maximum amount of time (in minutes) a user-defined mapping ID remains in the session object memory after the session is moved to the idle state. During this duration, the session remains accessible even if you have terminated that session. Use this setting to configure the time required to perform your after-call work (for example, writing variables to a database before clearing the session). This is a mandatory field. The default value is 30 minutes. If you reduce this number, you also reduce the system memory usage comparatively. You can add a user-defined mapping ID to a session using the Session Mapping step in the script editor. Once assigned, you can use this mapping ID to get the session object from another application instance. By doing so, other applications obtain access to the session context. See the *Cisco Unified Contact Center Express Getting Started with Scripts* for more information.
Enterprise Call Info Parameter Separator	A character used Get/Set Enterprise Call Info steps in the Unified CCX Editor to act as a delimiter for call data. This is a mandatory field. Default value is | (bar).
Agent State after Ring No Answer	Radio button determining how agent state should be set after a Ring No Answer event. This is a mandatory field. The options are: • Ready—If an agent does not answer a Unified CCX call, the Agent State is set to Ready. • Not Ready (default)—If an agent does not answer a Unified CCX call, the Agent State is set to Not Ready.

Field	Description
Change Agent State to Not Ready when Agent Busy on Non ACD Line	Radio button that enables the agent's state to change from Ready state to Not Ready state when the monitored Non ACD lines are used for Incoming or Outgoing calls. The options are: • Enable—Enables the state change of the agent in this scenario. • Disable (default)—Disables any state change of the agent in this scenario. This is not applicable if the Non ACD lines are shared lines. **Note** When a call is transferred from the ACD to the Non ACD monitored line on the same phone, the agent remains in the Talking state instead of Ready until the Non ACD call ends.
Number of Direct Preview Outbound seats	The maximum number of Direct Preview Outbound seats. The configuration of Outbound seats is done during the initial configuration or setup phase, after the installation. **Note** This is a mandatory field. This field is displayed only if you have a Premium license. The maximum number of direct preview outbound seats that can be configured is limited by the Premium Seat Count. If there is an invalid entry during configuration, an error message is displayed.
Live Data - Short Term Reporting Duration	This parameter applies to Live Data reports that are available to agents and supervisors on Finesse desktops. For certain fields in the live data reports, you can set a short-term value to 5, 10 or 15 minutes. Long-term value is always set to 30 minutes.
Persistent Connection	Radio button that determines whether to establish persistent connection to a remote device. The options are: • Enable (default)—Establishes persistent connection. • Disable—Does not establish persistent connection.
System Ports Parameters	
RMI Port	The port number used by the Unified CCXCVD to serve RMI requests. This is a mandatory field. Default value is 6999. **Note** After changing the RMI Port, ensure that you restart the system for the settings to take effect. On a high availability setup, restart both the nodes.

Field	Description
RmCm TCP Port	TCP port number on which the CTI server component of the RmCm subsystem opens the server socket and listens to the clients. All CTI server clients, such as Sync Server, and IP Phone Agent Server, use this port number. This is a read-only field and cannot be modified. Default value is 12028.
Proxy Parameters	
HTTP	• **Host Name**: Fully qualified domain name (FQDN) of the HTTP proxy server. Do not enter the IP address. • **Port**: Port number that is used to connect to the HTTP proxy server. Range is from 1 to 65535.
SOCKS Proxy	• **Host Name**: Fully qualified domain name (FQDN) of the SOCKS proxy server. Do not enter the IP address. • **Port**: Port number that is used to connect to the SOCKS proxy server. Range is from 1 to 65535.
SOCKS Username	Username of the SOCKS proxy server.
SOCKS Password	Password of the SOCKS proxy server.
Note Proxy parameters changes are automatically notified to Customer Collaboration Platform.	
Agent Settings	
Agent State after Ring No Answer	Radio button determining how agent state should be set after a Ring No Answer event. This is a mandatory field. The options are: • Ready—If an agent does not answer a Unified CCX call, the Agent State is set to Ready. • Not Ready (default)—If an agent does not answer a Unified CCX call, the Agent State is set to Not Ready.

Field	Description
Change Agent State to Not Ready when Agent Busy on Non ACD Line	Radio button that enables the agent state to change from the Ready state to the Not Ready state when the monitored Non ACD lines are used for Incoming or Outgoing calls. The options are: • Enable—Enables the state change of the agent. • Disable (default)—Disables any state change of the agent. This is not applicable if the Non ACD lines are shared lines. When you choose an option, a popup message informs you that this setting will be applied globally to all the teams except for the teams that have chosen to override this global setting. Click **OK** to continue or **Cancel** to discard the change. **Note** The popup message appears only if **Change Agent State to Not Ready when Agent Busy on Non ACD Line** is configured at a team level. To configure this functionality at a team level, you must install UCCX 12.5(1) SU1 ES01.
Agent Device Selection	Radio button that enables the support for the agent device selection feature which allows the agent to select the desired device (Desk Phone with EM, Desk Phone without EM, or Jabber) at the time of Finesse desktop login. The options are: • Enable—Select this option to enable the agent to select the active device at the time of Finesse desktop login. **Note** When the Agent Device Selection feature is enabled, both primary and secondary extensions can be shared with multiple devices. However, ensure that the devices using the shared extensions are not used at the same time. • Disable (default)—Select this option to disable the agent from selecting the active device at the time of Finesse desktop login. **Note** When you enable or disable the Agent Device Selection feature, restart the Unified CCX Engine on all the nodes.

Single Sign-On (SSO)

Use Single Sign-On (SSO) page to register, test, enable, and disable Single Sign-On.

Before you begin

Ensure you access the Cisco Unified CCX Administration page through a Fully Qualified Domain Name URL instead of IP address.

You need to configure Cisco Identity Service and enable trust relationship between Cisco Identity Service and Identity Provider.

For vendor specific configuration of the Identity Provider see, *Configure the Identity Provider for UCCX based on SSO* at https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200612-Configure-the-Identity-Provider-for-UCCX.html.

If Cisco Identity Service is not configured, it displays the status as `Cisco Identity Service is not configured` and provides the link to configure or update `Click here to update Cisco Identity Service configuration`. The steps 2 to 4 are disabled till the Cisco Identity Service is configured. The changes take effect when the page is refreshed.

If Cisco Identity Service is configured, it displays the status as `Cisco Identity Service is configured successfully` with the link to update `Click here to update Cisco Identity Service configuration`.

Procedure

Step 1 Choose **System** > **Single Sign-On (SSO)** from the Unified CCX Administration menu to access the Single Sign-On page. The page displays the Cisco Identity Service configuration status, options to register, test, enable, and disable Single Sign-On.

Note
If the `Cisco Identity Service` is configured successfully, then the **Register** option is enabled.

Step 2 Click **Register** on the Single Sign-On page to onboard the Single Sign-On components.
A status message is displayed on the screen to notify the status of the registration of the components. A **red** color icon indicates failure in the operation that has run. A **green** color icon indicates successful run operation. A **grey** color icon indicates the inability to capture the status of the operation that has run.

Step 3 Perform all the following prerequisites before the **SSO Test**. All the check boxes have to be checked for the **Test** option to be enabled.

a) Configure and Perform LDAP Sync in Cisco Unified CM.
b) Assign Cisco Unified CCX Administrator rights to one or more Enterprise users.
c) Assign Reporting Capability to Cisco Unified CCX Administrator (assigned in Administrator Capability View) and run the CLI command utils cuic user make-admin CCX\<Admin's User ID> to provide administrator rights to the Cisco Unified CCX Administrator in Cisco Unified Intelligence Center. Use the configured user with Unified CCX Administrator rights for the SSO Test operation.

Note
- Ensure that the browser based pop-up blocker is disabled for the **SSO Test** to work.
- For the **SSO Test** to be successful, the root domain of both the Unified CCX nodes must be the same.

Step 4 Click **Test** on the Single Sign-On page to test the status of registration of each component. You will be redirected to the Identity Provider for authentication.
A status message is displayed on the screen to notify the test status of the registered components. Single Sign-On test results are not persisted and will be lost when the page is reloaded. If the **SSO Test** is successful then the **Enable** option is enabled.

Step 5 Click **Enable** on the Single Sign-On page to enable each component for Single Sign-On.

Note
- When SSO is enabled and if the enterprise user is unable to log in, the recovery URLs can be used to log in. For troubleshooting purpose the enterprise user or system user chosen during the installation can login to Unified CCX

Administration and Unified CCX Serviceability through the following recovery URL to bypass the enterprise Identity Provider and Cisco Identity Service. However, this is not possible when SSO is enabled and the usual login URL is used.

- URL for Cisco Unified CCX Administration :
  `https://<ipaddress/fqdn>/appadmin/recovery_login.htm`
- URL for Cisco Unified CCX Serviceability :
  `https://<ipaddress/fqdn>/uccxservice/recovery_login.htm`

- To disable SSO in an SSO enabled Cisco Unified Contact Center Express solution, click **Disable** on the **Single Sign-On (SSO)** page. After SSO is disabled, you have to perform **SSO Test** again to enable SSO.

The page displays the status of each component being enabled for Single Sign-On or not.

You may close this page and open a new window of the browser to access the Cisco Unified CCX Administration. This automatically redirects you to the page to enter your credentials for the authentication with the Single Sign-On identity provider.

Note User IDs are case-sensitive when logging into the Unified CCX Administration web interface. To make them case-insensitive, you must install 12.5(1) SU1 ES02.

Custom File Configuration

Use the Custom Classes Configuration web page to specify the classpath for custom classes.

Choose **System** > **Custom File Configuration** from the Unified CCXAdministration menu bar to access the Custom Classes Configuration area.

Note Restart Unified CCX engine and Unified CCX administration services to use the custom files in scripts.

Standalone Cisco Unified Intelligence Center

Obtain and Upload SSL Certificates

Before configuring the standalone Cisco Unified Intelligence Center, you must obtain the SSL certificates from the Cisco Unified Intelligence Center nodes and upload them into the Unified CCX Tomcat trust store.

To download the SSL certificates from the standalone Cisco Unified Intelligence Center do the following:

1. Sign in to **Cisco Unified OS Administration** interface on the Cisco Unified Intelligence Center server.
2. Select **Security > Certificate Management.**

The **Certificate List** window appears.

3. In **Find Certificate List where** field, select **Certificate** and **contains** from the drop-down lists. Enter the search criteria as **tomcat** and then click **Find** to filter the certificate.

   The **Certificate List** displays the list of tomcat certificates.

4. Select the self-signed tomcat certificate.

   The **Certificate Details** dialog box is displayed.

5. Click **Download .PEM File**.

6. Save the .PEM file to your local drive.

To upload the self-signed tomcat certificates to the Unified CCX Tomcat trust store, do the following:

1. Sign in to the **Cisco Unified OS Administration** interface on the Cisco Unified CCX server.

2. Select **Security > Certificate Management**.

   The **Certificate List** window appears.

3. In the **Certificate List**, click **Upload Certificate/Certificate chain**.

   The **Upload Certificate/Certificate chain** dialog box appears.

4. From the **Certificate Purpose** drop-down list, select **tomcat-trust**.

5. In the **Upload File** field, click **Browse** and select the certificate.

6. Click **Upload File**.

7. In the CLI, restart the system using the command `utils system restart` for the changes to take effect.

Access Standalone Cisco Unified Intelligence Center Configuration

To access the Cisco Unified Intelligence Center standalone configuration webpage, perform the following steps:

Procedure

Step 1 Click **System** > **Standalone CUIC configuration** to configure standalone Cisco Unified Intelligence Center.

Step 2 Enter **FQDN** (Fully Qualified Domain Name), **DataSource Name**, **Username**, and **Password** of standalone Cisco Unified Intelligence Center.

Step 3 Click **Save**.
If the configuration is successful, a status message appears. Otherwise, an error message appears.

Note
Configurations may fail due to either of the following reasons:

- An error in input validation (DataSource Name, Username or Password).

• A failure in connectivity between Cisco Unified Intelligence Center and the Unified CCX servers.

License Information

License Management

From the Unified CCX Administration menu bar, select **Systems** > **License Management**. Based on the upgrade and usage scenarios, one of the following pages is displayed:

Page Displayed	Condition
License Management	For customers who have upgraded from Unified CCX Release 11.6(2) or earlier.
Classic License Management	For customers who have upgraded from Unified CCX Release 12.0.
Smart Licensing	This page is available only for the following customers: • Who want to migrate from Classic Licensing to Smart Licensing. • Who have newly installed Unified CCX Release 12.5.
Smart License Management	For customers who have enabled or migrated to Smart Licensing.

Use the **License Management** page to select the appropriate Unified CCX license. This page lists **Classic Licensing** and **Smart Licensing** options. By default, **Smart Licensing** is selected.

Procedure

Select one of the licenses and click **Next**.

The **License Management** page is displayed for the first time after the upgrade. After you select one of the licenses, the **Classic License Management** page or the **Smart License Management** page is displayed respectively.

Classic License Management

Use this page to manage Classic License (Add, View, and Delete).

Add License

To add a new license, perform the following steps:

1. From the Unified CCX Administration menu bar, select **Systems** > **License Management**. The **Classic License Management** page is displayed.

2. On the **Classic License Management** page, in the **Add New License** section, click **Browse** to select the Unified CCX license file.
3. Select the appropriate license file and click **Upload**.

View License Information

On the **Classic License Management** page, you can view the license files and the details of the configured licenses in the **View Licenses** section. You can select an uploaded license from the **Licenses** drop-down list. When you select **Cumulative License Information** from the list, the following details are listed:

- **Configured Licenses**
  - Package
  - Total IVR Ports
  - Cisco Unified CCX Premium Seats
  - High Availability
  - Cisco Unified CCX Preview Outbound Dialer
  - Cisco Unified CCX Quality Manager Seats
  - Cisco Unified CCX Advanced Quality Manager Seats
  - Cisco Unified CCX Workforce Manager Seats
  - Cisco Unified CCX Compliance Recording Seats
  - Cisco Unified CCX Maximum Agents
- **Inbound**
  - Available Inbound IVR Ports
- **Outbound**
  - Cisco Unified CCX Licensed Outbound IVR Ports
  - Cisco Unified CCX Outbound IVR Ports In Use
  - Cisco Unified CCX Licensed Outbound Agent Seats
  - Cisco Unified CCX Outbound Agent Seats In Use

Note All the license details that are mentioned may not be displayed. The license details are displayed as per the procurement.

Delete Licenses

You can delete only temporary licenses. You cannot delete permanent licenses. To delete a temporary license, select the required license from the **Licenses** drop-down list and click **Delete**. Click **OK** in the confirmation dialog box.

Note It is a good practice to remove redundant or expired license files before you upload new ones. Remove old temporary license files (that are expired) from the server. For the changes to take effect, you must reboot Unified CCX after uploading or deleting the licenses.

Migrate to Smart Licensing

To migrate to smart licensing, on the **Classic License Management** page, click **Smart Licensing**.

Smart Licensing

Use this page to select and enable the appropriate **Smart License Type**. After you enable the required **Smart License Type**, from the next login, **Smart License Management** page is displayed. The license types that are listed and available for selection depends on the type of installation.

Procedure

Step 1 Select one of the following license types:

- **Unified IP IVR**
- **Unified CCX**
  - **Lab**
    - **NPS**
    - **NFR**
  - **Production**
    - **Flex**
    - **Perpetual Enhanced**
    - **Perpetual Premium**

Note
For more information on the license types, see Cisco Contact Center Ordering Guide.

Step 2 Click **Enable**.
A confirmation message is displayed.

Step 3 Click **Yes** to enable Smart Licensing.

What to do next

You must register this Product Instance with **Cisco Smart Software Manager** to use Smart Licensing.

Smart License Management

The **Smart License Management** page provides the summary and detailed information on system license usage as it is reported to **Cisco Smart Software Manager (Cisco SSM)** or **Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem)**. Licenses are assigned to your Smart Account and are not node-locked to a device. That is, a single license can be used by multiple users but only one at a time.

Note **Not Node-Locked:** The same license can be used across multiple systems (nodes) but only on one node at a time.

Field	Description
Status	Displays the status of the actions that are performed on this page.
License Type Details	
Current License Type	Displays the type of license that was selected in the **Enable Smart Licensing** page. To select a different license type, click the link. The **Enable Smart Licensing** page is displayed.
License Control Displays the status of **Overage Allowance** that was configured while registering the product instance. After you register the product instance, a link is provided to update the **Overage Allowance**. **Overage Allowance** is enabled by default. You can update **Overage Allowance** only when the product instance is in the registered state. When you click the update link, the **License Control** window displays the following options:	
Current License Type	Displays the type of license that was selected in the **Enable Smart Licensing** page.
Overage Allowance	You can **Enable** or **Disable**. By default **Enable** is selected, which allows you to use more licenses than you have purchased. If you want to limit the usage of licenses to the purchased quantity or less, select **Disable**. Enter the number that you want to allow in the fields that are displayed as per the **Current License Type**. For more information on license types, see the *Overview* section of *Smart Licensing* chapter in *Cisco Unified Contact Center Express Features Guide*.
I have purchased High Availability License	If you have deployed a HA, this check box is displayed, which has to be selected.
Registration Information Displays the status of registration. If you have registered, the `You have registered successfully` message is displayed, else displays the procedure to register.	
Transport Settings	Use Transport Settings button to configure different settings through which Cisco Unified CCX can connect to Cisco SSM or Cisco SSM On-Prem.

Field	Description
Register	Use the Register button to register Cisco Unified CCX with Cisco SSM or Cisco SSM On-Prem. By default this button is disabled. You have to first configure **Transport Settings** to enable this button. After you successfully register, this button is disabled.
Smart License Details	
Registration Status	Displays the current registration status. The following are the statuses: • Registered • Unregistered or Unidentified • Unregistered-Registration Expired • Reservation In Progress • Registered - Specific License Reservation
Authorization Status	Displays one of the following status information: • Evaluation mode—Product is not registered with Cisco. • Evaluation Expired—Product evaluation period has expired. • In Compliance—Product is in authorized or in compliance state. • Not Authorized—Product is in not-authorized state. • Authorization Expired—Authorization has expired for the product. This issue usually occurs when the product has not communicated with Cisco for 90 consecutive days. After 90-days, the product instance is put into Enforcement state. • Out of Compliance—Product is in out-of-compliance state because of insufficient licenses. • Unidentified—Unable to determine current registration status. • Authorized-Reserved—License Reservation is enabled and the license usage is in-compliance state. • Not Authorized-Reserved—License Reservation is enabled, and the license usage is in out-of-compliance state.
Smart Account Name	Displays the Smart Account name. It is created from the **Request a Smart Account** option in **Administration** section of the software.cisco.com. It is the primary account that is created to represent the customer and all licenses of a company are assigned to this Smart Account. It also manages licenses of all Cisco products.
Virtual Account Name	Displays a self-defined construct to reflect the organization, which is created and maintained by the administrator on Cisco SSM or Cisco SSM On-Prem. Licenses and product instances can be distributed across virtual accounts.

Field	Description
Serial Number	Unique identifier of the product instance.
Export-Controlled Functionality	Displays one of the following status information: • Allowed—Cisco Unified CCX registered to Smart Account that allows export-controlled functionality. • Not Allowed—Cisco Unified CCX not registered to Smart Account that allows export-controlled functionality. Specifies if the Export-Controlled functionality was enabled in the token with which the product was registered. **Note** The Allow export-controlled functionality on the products that are registered with this token check box is not displayed for the Smart Accounts that are not permitted to use the Export-Controlled functionality.
Actions	This drop-down list gets activated after you successfully register the Smart License. It lists the following type of actions that can be performed: • Renew Authorization—Use this option to manually renew the authorization. The license authorization is renewed automatically every 30 days. If the product instance is not connected to Cisco SSM or Cisco SSM On-Prem, the authorization expires after 90 days. If you select the Cisco SSM On-Prem option, Cisco SSM On-Prem must have an internet connection to connect to Cisco SSM for authorization. • Renew Registration—Use this option to manually renew the registration. The initial registration is valid for one year. Registration is automatically renewed every six months, provided the product is connected to Cisco SSM or Cisco SSM On-Prem. If the Cisco SSM On-Prem option is selected, Cisco SSM On-Prem must have an internet connection to connect to Cisco SSM. • Reregister—When you select this option, the **Smart Licensing Product Registration** window is displayed. Enter the appropriate Product Instance Registration Token and click **Reregister**. • Deregister—Use this option to deregister Unified CCX from Cisco SSM or Cisco SSM On-Prem and release all the licenses from the current virtual account. All license entitlements that are used for the product instance are released to the virtual account and is available for other product instances. **Note** If Unified CCX is unable to connect to Cisco SSM or Cisco SSM On-Prem, and the product instance is deregistered, a confirmation message is displayed. This message notifies you to remove the product instance manually from Cisco SSM or Cisco SSM On-Prem to free up licenses.
License Usage	

Field	Description
License Name	Displays the different licenses as per the license type that is selected in the Smart Licensing page.
Reserved Count	Displays the number of licenses that are reserved. This column is displayed only when the specific License Reservation is enabled.
Reported Usage	Displays the number of licenses that are used by this product instance as per the details that was last reported.
Status	Displays the status of each license. The different statuses for the product instance are as follows: • Authorization Expired—The authorized period has expired. • Evaluation—This entitlement is in Evaluation mode. • Evaluation Expired—Evaluation period has expired. • In-compliance—In-compliance (authorized). • No License in Use—There are no licenses that are in use. • Invalid—In Error state. • Invalid Tag—The entitlement tag is invalid. • Not Applicable—Enforcement mode is not applicable. • Out of Compliance—Out-of-compliance (unauthorized). • Waiting—Waiting response from Cisco SSM or Cisco SSM On-Prem for entitlements that are submitted. • Authorized-Reserved—Reserved licenses are in-compliance. • Not Authorized-Reserved—Reserved licenses are out-of-compliance.

Configure Transport Settings for Smart Licensing

Configure the connection mode between Unified CCX and Cisco SSM.

Procedure

Step 1 From Unified CCX Administration, navigate to **System** > **License Management**.

Step 2 Click **Transport Settings** to set the connection method.

Step 3 Select the connection method to Cisco SSM:

- **Direct**—Unified CCX connects directly to Cisco SSM on cisco.com. This is the default option.
- **Transport Gateway**—Unified CCX connects to Cisco SSM On-Prem for smart licensing. Enter the Cisco SSM On-Prem URL.

- **HTTP/HTTPS Proxy**—Unified CCX connects to a proxy server, which connects to Cisco SSM. Enter the Fully Qualified Domain Name (FQDN) of the proxy server along with the port.

  Note
  Proxy servers that require authentication are not supported for this connection method.

Step 4 Click **Save** to save the settings.

Register with Cisco Smart Software Manager

The product instance has 90 days of evaluation period, within which, the registration must be completed. Else, the product instance gets into the enforcement state.

Register your product instance with Cisco SSM or Cisco SSM On-Prem to exit the Evaluation or Enforcement state.

Note After you register the product instance, you cannot change the license type. To change the license type, deregister the product instance.

Procedure

Step 1 In , navigate to **Overview** > **Infrastructure Settings** > **License Management.**

Step 2 From Unified CCX Administration, navigate to **System** > **License Information**.

Step 3 Click **Register**.

Note
- Before you register the product instance, ensure to select the **License Type** and the communication mechanism in **Transport Settings**.

Step 4 In the **Smart Software Licensing Product Registration** dialog box, paste the product instance registration token that you generated from Cisco SSM or Cisco SSM On-Prem.

For information on generating the Registration Token, see the *Obtain the Product Instance Registration Token* section in Cisco Unified Contact Center Express Features Guide.

License Control pane is displayed with the **Overage Allowance** option. By default **Enable** is selected, which allows you to use more licenses than you have purchased.

If you want to limit the usage of licenses to the purchased quantity or less, select **Disable**. Enter the number that you want to allow in the fields that are displayed as per the **Current License Type**.

If you have deployed a HA, the **I have purchased High Availability License** check box is displayed, which has to be selected.

For more information on license types, see the *Overview* section of *Smart Licensing* chapter in *Cisco Unified Contact Center Express Features Guide*.

Step 5 Click **Register** to complete the registration process.

After registration, the **Smart Licensing Status** displays the following details.

Table 14: Smart Licensing Status

Smart License Status	Description
On Unsuccessful Registration	
Registration Status	Unregistered
License Authorization Status	Evaluation
Export-Controlled Functionality	Not Allowed
On Successful Registration	
Registration Status	Registered (Date and time of registration) **Note** The date and time indicate the server's time zone.
License Authorization Status	Authorized (Date and time of authorization) **Note** The date and time indicate the server's time zone.
Export-Controlled Functionality	Not Allowed
Smart Account	The name of the smart account
Virtual Account	The name of the virtual account
Product Instance Name	The name of the product instance
Serial Number	The serial number of the product instance

Entitlements are a set of privileges customers and partners receive when purchasing a Cisco service agreement. Using Smart Licensing, you can view the License consumption summary for the entitlements of different license types. The License consumption summary displays the License Name, Usage Count, and Status against each entitlement name.

License usage information is updated automatically every 8 hours.

For more information, see *License Information*.

Language Information

Customized Unified CCX languages such as American English, Canadian French, and so on are installed with Unified CCX.

Use the Languages Configuration web page to:

- Enable languages that can be used to play prompts and grammars through Cisco Unified IP IVR.

Choose **System** > **Language Information** from the Cisco Unified CCX Administration menu bar to access the Languages Configuration web page. The Languages Configuration web page opens to display the following fields and buttons.

Field	Description
Choose IVR Language	
Language	You can choose a language that you wish to use with Unified IP IVR. You can select the language from the drop-down list. You can also specify the group and country-specific information for the language by selecting the desired radio button and check box respectively. Some languages have only one choice. US English (en_US) is the default. You may set the chosen language in **Set IVR Language** option. The chosen language doesn't get automatically set and the value is not persisted after it is chosen.
Set IVR Language	
IVR Language	This field is for setting the IVR language, which could be either one of the selected IVR languages or country-specific or a user-defined language entered using the **Edit** button. This is a mandatory field and you can choose from the drop-down list. Click **Edit** to add a new Language option. Default: English (United States) [en_US]

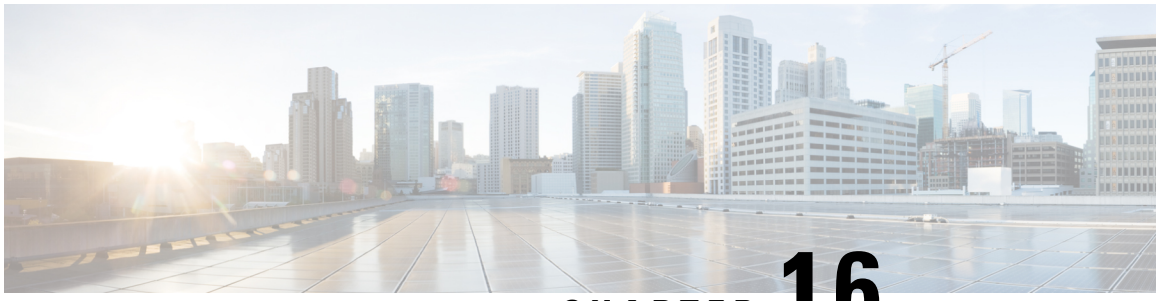
Logout Menu

To exit Unified CCXAdministration without closing your web browser, you can perform one of the following:

- Choose **System** > **Logout** from the Unified CCXAdministration menu bar.
- Click the **Logout** link displayed in the top right corner of any Cisco Unified CCX Administration web page.

The system logs you out of Unified CCX and displays the Unified CCX Authentication web page.

Note You can also exit Unified CCXAdministration by closing your web browser.



CHAPTER 16

Applications Menu

- Access Application Management Menu, on page 279
- Manage Scripts, on page 279
- Prompt Management, on page 280
- Grammar Management, on page 281
- Document Management, on page 281
- AAR Management, on page 281
- Calendar Management, on page 282

Access Application Management Menu

The Application Management menu option in the Unified CCX Administration web interface contains options for configuring and managing the applications the Unified CCX system uses to interact with contacts and perform a wide variety of functions.

To access the Application Management web pages, perform the following steps:

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Applications** > **Application Management**.

The Applications Configuration web page opens, displaying a list of applications that are currently configured on your Unified CCX server.

Step 2 Click the **Add New** icon that displays in the toolbar in the upper left corner of the window or the **Add New** button that displays at the bottom of the window to add a new application. Add a New Application web page opens.

Step 3 Select the type of application that you want to create from the Application Type drop-down list.

Manage Scripts

Use the Script Management web page to add a new script and to rename, refresh, or delete an existing script. Unified CCX applications are based on scripts created in the Unified CCX Editor.

To create a new subfolder under the `default` folder, perform the following steps:

Procedure

Step 1 To access the Script Management web page, choose **Applications** > **Script Management** from the Unified CCX Administration menu bar.

The Script Management web page opens, displaying the default directory that contains the scripts uploaded to the repository.

Step 2 Click the **Create New Folder** icon that displays in the toolbar in the upper left corner of the window or the **Create New Folder** button that displays at the bottom of the window.

The Create New Folder dialog box opens.

Step 3 Enter a name of the new subfolder in the **Folder Name** field and click **Create**.

Once the folder is successfully created, the dialog box refreshes with the following message:

`Folder successfully created`

Step 4 Click the **Return to Script Management** button to return to the **`default`** folder's updated Script Management page. You can create any number of folders within the `default` folder.

Prompt Management

Several system-level prompt files are loaded during Unified CCX installation. However, any file *you* create must be made available to the Unified CCX Engine before a Unified CCX application can use them. This is done through the Unified CCX cluster's Repository datastore, where the prompt files are created, stored, and updated.

Note You can use a custom script or the Unified CCX Administration to upload a prompt.

To access the Prompt Management page, choose **Applications** > **Prompt Management** from the Unified CCX Administration menu bar.

The Prompt Management web page contains the following icons and buttons:

- **Create Language**—Click the **Create Language** icon that displays in the toolbar in the upper left corner of the window or the **Create Language** button that displays at the bottom of the window to create a new language folder.
- **Upload Zip Files**—Click the **Upload Zip Files** icon that displays in the toolbar in the upper left corner of the window or the **Upload Zip Files** button that displays at the bottom of the window to upload a new prompt or zip file.

See **Manage Prompt Files** section to know more about the different fields in this page and how to rename, refresh, or delete existing prompts.

Grammar Management

Several system-level grammar files are loaded during Unified CCX installation. However, any file *you* create must be made available to the Unified CCX Engine before a Unified CCX application can use them. This is done through the Unified CCX cluster's Repository datastore, where the grammar files are created, stored, and updated.

To access the Grammar Management page, choose **Applications** > **Grammar Management** from the Unified CCX Administration menu bar.

The Grammar Management web page contains the following icons and buttons:

- **Create Language**—Click the **Create Language** icon that displays in the toolbar in the upper left corner of the window or the **Create Language** button that displays at the bottom of the window to create a new language folder.
- **Upload Zip Files**—Click the **Upload Zip Files** icon that displays in the toolbar in the upper left corner of the window or the **Upload Zip Files** button that displays at the bottom of the window to upload a new grammar or zip file.

Document Management

Several system-level document files are loaded during Unified CCX installation. However, any file *you* create must be made available to the Unified CCX Engine before a Unified CCX application can use them. This is done through the Unified CCX cluster's Repository datastore, where the document files are created, stored, and updated.

To access the Document Management page, choose **Applications** > **Document Management** from the Unified CCX Administration menu bar.

The Document Management web page contains the following icons and buttons:

- **Create Language**—Click the **Create Language** icon that displays in the toolbar in the upper left corner of the window or the **Create Language** button that displays at the bottom of the window to create a new language folder.
- **Upload Zip Files**—Click the **Upload Zip Files** icon that displays in the toolbar in the upper left corner of the window or the **Upload Zip Files** button that displays at the bottom of the window to upload a new document or zip file.

Note Ensure that you do not upload any .jar files that are already used by Unified CCX. For the list of .jar files that are used, refer to the specific versions of the Open Source Used In UCCX document.

AAR Management

Use the AAR Management web page to upload an AAR file to Unified CCX.

To access the AAR Management web page, choose **Applications** > **AAR Management** from the Unified CCXAdministration menu bar. The AAR Management web page appears.

Calendar Management

Use the Calendar Management section to create a new calendar. You can also configure and schedule business hours such as start and end time for business days, special days, and holidays.

To create and configure a Calendar, complete the following steps:

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Applications** > **Calendar Management**.

The **Calendar Management** web page opens and displays the information for existing calendars, if any.

Step 2 To add a new calendar, click the **Add New** icon or the **Add New** button.

The **Add New Calendar** web page opens.

Step 3 In the **Calendar Details** section, specify the following information:

Field	Description
Name	Unique name of the calendar.
Description	Calendar description.
Time Zone	Time zone for the calendar.

The following information is available to view:

Table 15:

Field	Description
Associated with	Lists the names of applications and chats that are associated with the calendar.

Step 4 In the **Business Hours** section, select one of the following options to configure the Business Days.

- 24 hours x 7 days - The service is available 24 hours a day, 7 days a week.
- Fixed Hours - Administrator can configure a fixed time range for the entire week as per the business requirements.
- Flexible Hours - Administrator can configure a flexible time range for each of the business days as per the business requirements.

Note

- The **Custom Business Hours Schedule Configuration** is based on the Unified CCX server time zone.
- During an upgrade of Unified CCX, by default the **24 hours x 7 days** is selected as the **Business Days**.

Step 5 Click **Next**.

Step 6 In the **Schedule Custom Business Days** section, specify the name, date, and configure business hours for a custom business day.

Note
Scheduling business hours for a custom business day overrides any previous schedule that was configured in **Custom Business Hours** for the same day.

a) To add more custom business days, click **Add More**. Click the delete icon to delete a custom business day.

Step 7 Click **Next**.

Step 8 In the **Schedule Holidays** section, configure holidays.

a) To add more holidays, click **Add More**. Click the delete icon to delete a configured holiday.

Step 9 Click **Finish** to save the configuration.

Note
- A maximum of 50 Calendars can be configured.
- A maximum of 40 Custom Business Days and Holidays each can be configured.

Calendar Flow

An example of the calendar step is as follows:

Procedure

Step 1 Use the **Calendar Step** of Unified CCX Editor in any of the scripts.

Step 2 Create a new variable **NewCalendar** of type **CCCalendar**.

Step 3 Save the script in an appropriate location.

Step 4 Upload the script in Unified CCX Administration.

You can also modify and save the uploaded scripts.

Step 5 Navigate to **Applications** > **Calendar Management**.

Step 6 Create a new calendar **HolidayCalendar**.

Step 7 Navigate to **Applications** > **Application Management**.

Step 8 Select an application from the list or create an application.

Step 9 Select the script that has been uploaded.

Step 10 Select the calendar variable **NewCalendar**.

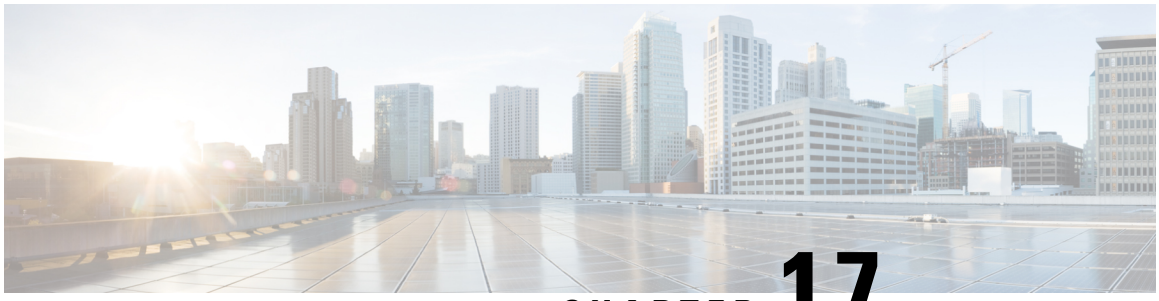
Step 11 Select **HolidayCalendar** from the list and save to associate the calendar with the application.

Step 12 Assign the **HolidayCalendar** to the appropriate supervisor.

You can assign one calendar to multiple supervisors.

The HolidayCalendar is now available in the **Calendar Management** tab of Advanced Supervisor Capabilities in Finesse Desktop, which can be edited by supervisors. If you have not associated **HolidayCalendar** in UCCX

Administration, supervisors can associate it by using the **Manage Application** from the **Application Management** tab of Advanced Supervisor Capabilities in Finesse Desktop.



CHAPTER 17

Subsystems Menu

- Unified CM Telephony Menu, on page 285
- RmCm Menu, on page 289
- Chat and Email Menu Options, on page 296
- Outbound Menu, on page 323
- Database Menu, on page 328
- HTTP Menu, on page 330
- eMail Menu, on page 330
- Cisco Media, on page 331
- MRCP ASR Menu, on page 331

Unified CM Telephony Menu

The Unified CCX system uses the Unified CM Telephony subsystem of the Unified CCX Engine to send and receive call-related messages from the Unified CM Computer Telephony Interface (CTI) Manager.

To access the Unified CM Telephony Configuration web pages, choose **Subsystems** > **Cisco Unified CM Telephony** from the Unified CCXAdministration menu bar.

The Unified CM Telephony Configuration menu contains the following submenu options:

- **Unified CM Telephony Provider**—Choose this option to enter Unified CM Telephony provider information.
- **Unified CM Telephony Call Control Group Configuration**—Choose this option to configure CTI port groups for applications.
- **Unified CM Telephony Trigger Configuration**—Choose this option to configure Unified CM Telephony triggers for applications.
- **Data Synchronization**—Choose this option to check and synchronize data components like Unified CM Telephony Users (JTAPI Application Users), Unified CCX Triggers/Route points, and Call Control Groups between Unified CCX and Unified CM.
- **Cisco JTAPI Resync**—Choose this option to resynchronize Cisco JTAPI Client versions.
- **Advanced Settings**—Choose this option to configure advanced settings for the Cisco Unified CM Telephony client.

Unified CM Telephony Provider Configuration

To access this configuration area, choose **Subsystems** > **Cisco Unified CM Telephony** > **Provider** from the Unified CCX Administration menu bar. The Cisco Unified CM Telephony Provider web page opens.

Use the Unified CM Telephony Provider Configuration web page to view and modify the primary and secondary location of your Unified CM Telephony provider, and user prefix.

Unified CM Telephony Call Control Group Configuration

Choose **Subsystems** > **Cisco Unified CM Telephony** > **Call Control Group** from the Unified CCXAdministration menu bar to access the Unified CM Telephony Call Control Group list web page. Use the Unified CM Telephony Call Control Group Configuration web pages to display, add, modify, and delete information about the call control group.

To add a new Unified CM Telephony Call Control Group, click the **Add New** icon or button on the Unified CM Telephony Call Control Group Configuration web page.

To modify an existing Unified CM Telephony Call Control Group, click any hyperlink within the Ports List table entry; the Cisco Unified CM Telephony Call Control Group Configuration web page opens.

Unified CM Telephony Triggers Configuration

Choose **Subsystems** > **Cisco Unified CM Telephony** > **Triggers** from the Cisco Unified CCX Administration menu bar to configure Unified CM Telephony Triggers.

The Cisco Unified CM Telephony Trigger Configuration web page opens where you can view, add, modify, and delete Unified CM Telephony triggers. To add a Unified CM Telephony trigger, click the **Add New** icon or button. The Cisco Unified CM Telephony Trigger Configuration web page opens.

Note Use of two(2) wildcard CTI Route Points that overlap with each other is not supported. For example, Route Point 1: 123XXXX and Route Point 2: 1234XXX overlap with one another and is not supported.

However, a wildcard CTI Route point can overlap with a full DID (best match pattern) that doesn't contain a wildcard. For example, Route Point 1: 123XXXX and Route Point 2: 1234567 is supported.

Synchronize Unified CM Telephony Data

You can configure the telephony data synchronization through a new web page called Cisco Unified CM Telephony Data Synchronization.

The data synchronization process ensures that the data components such as Unified CM Telephony Users (JTAPI Application Users), Unified CCX Triggers/Route points, Call Control Groups between Unified CCX and Unified CM, and SRTP are synchronized without any inconsistency.

The **Data Check** option displays if the selected data components are synchronized between Unified CCX and Unified CM. If you find any inconsistency, use the **Data Resync** option to rectify the issue.

To check and synchronize the JTAPI data components between Cisco Unified CM and Cisco Unified CCX, perform the following steps:

Caution It is important that you plan to perform this task during off peak hours to avoid hampering routine contact center operations.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **Cisco Unified CM Telephony** > **Data Synchronization**.

The Cisco Unified CM Telephony Data Synchronization page appears.

Step 2 Choose the desired components by selecting the corresponding check box:

- Call Control Group(s)
- Trigger(s)
- CM Telephony User(s)
- SRTP

Step 3 Click **Data Check** or **Data Resync**. When you click **Data Check** or **Data Resync**, a confirmation message dialog box appears prompting you to either proceed or cancel. Click **OK** to continue.

Note
After you click **OK** in the confirmation message for Data Check or Data Resync, you are not allowed to cancel the process.

Step 4 The Cisco Unified CM Telephony Data Synchronization web page continues to update until the Data Check or Data Resync process is complete. On completion of the Data Check or Data Resync process, the result is displayed in the same web page in a tree structure. The result for each selected component is displayed in collapsed format with a tick mark if no mismatch is found. Click the arrow that is next to each selected component to expand and view the detailed results.

If any mismatch is found in the elements of the selected component, the results for those components are displayed automatically in an expanded format.

Note

- If you had multiple device pools (for Call Control Groups) in your older versions of Unified CCX setup, performing Data Resync after an upgrade merges all multiple device pools to a single default device pool. However, you can manually assign a different device pool to the Call Control Group if the default device pool is not the intended one.
- When you select **SRTP** and click **Data Check**,
  - The status of secure JTAPI configuration for subsystems JTAPI and RmCm is displayed under sections **CM Telephony** and **RmCm** respectively.
  - In a HA setup, the status of devices and device profiles that are associated with the primary RmCm user and the system-generated RmCm user is displayed under subsections **RmCm Devices** and **RmCm Device Profiles** respectively.
- When you select **SRTP** and click **Data Resync**,
  - The secure JTAPI configuration for subsystems JTAPI and RmCm are re-synchronized as per Unified CCX SRTP configuration and the status is displayed in the respective subsections.

- In a HA setup, if devices and device profiles do not match between the primary RmCm user and system-generated RmCm user, the system-generated RmCm user is synchronized with the devices and device profiles that are configured for primary RmCm user.

Unified CM Telephony Cisco JTAPI Resync

Choose **Subsystems** > **Cisco Unified CM Telephony** > **Cisco JTAPI Resync** from the Cisco Unified CCX Administration menu bar to resynchronize the JTAPI client version on the Unified CCX with the JTAPI version on the Unified CM. You can view the status of Cisco JTAPI client resynchronization in this web page.

If the Unified CCX detects a mismatch, the system downloads and installs the compatible or JTAPI client required installer version. Restart the Unified CCX Engine to view these configuration changes.

The JTAPI client update happens only on the local node and not on the second node in case of High Availability deployment.

Unified CM Telephony Advanced Settings

Choose **Subsystems** > **Cisco Unified CM Telephony** > **Advanced Settings** from the Cisco Unified CCX Administration menu bar to configure advanced settings for the Unified CM Telephony Client.

Use the Unified CM Telephony Advanced Settings web page to update the following information:

- Periodic Wakeup Interval (seconds): Select the check box before Enable Periodic Wakeup prior to updating the existing value in this field.
- Queue Size Threshold: Select the check box before **Enable Queue Stats** prior to updating the existing value in this field.
- CTI Request Timeout (sec)
- Provider Open Request Timeout (sec)
- Provider Retry Interval (sec)
- Server Heartbeat Interval (sec)
- Route Select Timeout (ms)
- Post Condition Timeout
- Use Progress As Disconnect

Click the **Update** icon that displays in the toolbar in the upper left corner of the window or the **Update** button that displays at the bottom of the window to save the changes. Restart the Unified CCX Engine to view these configuration changes.

In case of High Availability deployment, the changes are propagated to the second node. If the second node cannot be contacted, an alert message indicating that the update has failed on the remote node is displayed.

RmCm Menu

Use the RmCm Configuration web page to configure skills groups, resources, resource groups, Contact Service Queues (CSQs), and RM (Resource Manager) Unified CM Telephony providers. To access the Unified CCX Configuration web page, choose **Subsystems** > **RmCm** from the Unified CCXAdministration menu bar.

The RmCm menu contains the following submenu options:

- **Skills**—Click this submenu to create skills. This option is available only with the Unified CCX Enhanced and Unified CCX Premium license packages.
- **Resources**—Click this submenu to assign a resource group and skills to agents.
- **Resource Groups**—Click this submenu to create resource groups.
- **Contact Services Queues (CSQs)**—Click this submenu to configure CSQs.
- **RmCm Provider**—Click this submenu to configure the RM (Resource Manager) Unified CM Telephony provider for the RmCm subsystem.
- **Assign Skills**—Click this submenu to assign skills and a resource group to agents in bulk.
- **Agent Based Routing Settings**—Click this submenu to send a call to a specific agent, rather than to any agent available in a CSQ.
- **Teams**—Click this submenu to create or associate teams with various agents, CSQs, and supervisors.

Skill Configuration

Use the Skills page to add, modify, or delete skill.

Choose **Subsystems** > **RmCm** > **Skills** from the Unified CCXAdministration menu bar to access the Skills summary web page.

Add New Skill

Use the Skill Configuration area to add a new skill name.

Procedure

Click the **Add New** icon that displays in the toolbar in the upper left corner of the window or the **Add New** button that displays at the bottom of the window to access the Skill Configuration area.

Modify Skills

Click the required skill in the Skill name column on the Skill Configuration web page to access the Skill Configuration area.

Procedure

Click the **Open Printable Report of this Skill Configuration** icon to view a list of the resources associated with that skill.

Resources Configuration

Use the Resources Configuration area to assign a resource group, to assign skills to a resource, and to assign an alias to the agent. When the agent is on chat, the alias of the agent is displayed to the customer.

To access this configuration area, choose **Subsystems** > **RmCm** > **Resources** from the Unified CCXAdministration menu bar. The main area of the Resources area of the Unified CCX Configuration web page contains a list of resources (if configured).

Click the **Open Resources Summary Report** icon to open the Resources Summary Report in a new window. For each resource, this report lists the resource groups associated with the resource, the Unified CCX extension of the resource, and the number of CSQs and team to which the resource is assigned.

Modify Resource

Use the Resource Configuration area to modify resource configuration.

To access the Resource Configuration area, click any of the required resource in the Resource area of the Unified CCX Configuration summary web page.

Procedure

Click the **Open Printable Report of this Resource Configuration** icon to open a Resource Report for the agent. The Resource Report lists each agent resource ID, resource name, Unified CCX extension, resource group, automatic available status, skills, CSQs, and team.

Resource Group Configuration

Use the Resource Group Configuration web page to display and modify the names of existing resource groups and to add new resource groups.

Choose **Subsystems** > **RmCm** > **Resource Groups** from the Unified CCXAdministration menu bar to access the Resource Groups web page.

Add New Resource Group

Use the Resource Configuration area to enter resource group name in the Resource Group Name field.

Procedure

Add a new Resource Groups by clicking **Add New** icon or button in the Resource Group area of the Unified CCX Configuration web page.

Modify Existing Resource Groups

Use the Resource Modification page to change or update the resource group name into the Resource Group Name field.

Modify an existing Resource Group by clicking the required resource group in the Resource Groups area. In the Resource Group Configuration area, change the Resource Group and update.

Procedure

Click the **Open Printable Report of this Resource Group Configuration** icon to view a list of the available resources for this resource group.

Contact Service Queues Configuration

Use the Contact Service Queues area of the Unified CCX Configuration web page to display existing CSQs, delete a CSQ, and add a new CSQ.

To access the Contact Service Queues area, choose **Subsystems** > **RmCm** > **Contact Service Queues** from the Unified CCXAdministration menu.

Note When all the CSQs assigned to the teams associated to the Supervisor are deleted, the Advanced Supervisor Capability of Queue Management is removed for the Supervisor.

Add a CSQ

Use the Contact Service Queues Configuration area to add a new CSQ.

To access the Contact Service Queues Configuration area, click the **Add New** icon or button in the Contact Service Queues area of the Unified CCX Configuration web page.

To open the Contact Service Queue Report for the required CSQ, click the **Open Printable Report of this CSQ Configuration** icon from the Contact Service Queues Configuration area.

RmCm Provider Configuration

Use the RmCm Provider area of the Unified CCX Configuration web page to identify the Unified CM Telephony user for the Resource Manager.

Choose **Subsystems** > **RmCm** > **RmCm Provider** from the Unified CCXAdministration menu bar to access the RmCm Provider web page.

Skills Configuration Assignment

Use the Assign Skills area of the Unified CCX Configuration web page to modify an existing resource group and skill configuration or to assign new resource groups and skills to all or selected agents.

Choose **Subsystems** > **RmCm** > **Assign Skills** from the Unified CCXAdministration menu bar to access this configuration area.

This web page also contains the following icons and buttons:

- **Add Skill**—to add new skills or resource groups to all or selected agents.
- **Remove Skill**—to remove skills of all or selected agents.

Add Skills

When you click the **Add Skill** button in the Assign Skills area of the Unified CCX Configuration web page, the Add Skill area opens. Use the Add Skill area to add a resource group and skills to the selected agents.

Remove Skills

When you click the **Remove Skill** button in the Assign Skills area of the Unified CCX Configuration web page, the Remove Skill area opens. Use the Remove Skill area to remove skills of all or selected agents.

Agent Based Routing Settings Configuration

Use the Agent Based Routing Settings area of the Unified CCX Configuration web page to configure Automatic Work and Wrapup Time.

Choose **Subsystems** > **RmCm** > **Agent Based Routing Settings** from the Unified CCXAdministration menu bar to access this configuration area.

Teams Configuration

Use the Teams area of the Unified CCX Configuration web page to create or associate teams with various agents, CSQs, and supervisors.

Choose **Subsystems** > **RmCm** > **Teams** from the Unified CCXAdministration menu bar to access this configuration area.

Assign Supervisor Privilege to a User

Perform the following procedure to assign supervisor privilege to a user.

Procedure

Step 1 From the Unified CCX Administration menu, choose **Tools > User Management > User View**.

The User Configuration page displays the list of all users.

Step 2 Click the user to whom you want to assign supervisor capability.

The User Configuration page displays information about that user. In the Capabilities section, the left pane displays the list of assigned capabilities and the right pane displays the list of capabilities.

Step 3 Using the left arrow, assign Supervisor capability.

Step 4 Click **Update** to save your changes.

Agents, who have logged in must logout and login again to use supervisor specific features.

For agents with chat or email skill, who have logged in, it may take maximum of 30 mins to reflect the change.

Create Teams

Use the Teams area of the RmCm Configuration web page to create or associate teams with various agents, CSQs, and supervisors.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **RmCm** > **Teams**.

Step 2 Click **Add New** icon that displays in the tool bar in the upper left corner of the window or the **Add New** button at the bottom of the window.

The Team Configuration page appears.

Step 3 Enter the **Team Name**.

Step 4 Select the **Primary Supervisor** from the drop-down list.

Step 5 (Optional) Select the secondary supervisor name from the **Available Supervisors** list and use the arrow icon to move it into the **Secondary Supervisors** list.

Step 6 (Optional) To add an agent to this team, select an agent name in the **Available Resources** list and use the arrow icon to move it into the **Assigned Resources** list.

Step 7 (Optional) Select the CSQ name in the **Available CSQs** list and use the arrow icon to move it into the **Assigned CSQs** list to add the CSQ to this team.

Step 8 In the **Team Settings** section, specify the following information:

Parameter Name	Parameter Value	Global Settings
Change Agent State to Not Ready when Agent Busy on Non ACD Line	Radio button that enables the agent state to change from the Ready state to the Not Ready state when the monitored Non ACD lines are used for Incoming or Outgoing calls. The options are: • Enable—Enables the state change of the agent in the team. • Disable (default)—Disables any state change of the agent in the team. • Allow team settings to override global settings—A check box to override the global settings. The global settings is available at **System** > **System Parameters** > **Agent Settings**. **Note** When you select the check box, a popup message reminds you that your team settings are different from the global settings. Click **OK** to proceed or **Cancel** to discard the changes. When you click OK, the team level settings override the global settings.	Displays the global settings.
Auto Answer	Enables the incoming calls to be auto answered. The options are: • Enable with Zip tone—For agents, belonging to the team, all the incoming calls to the IPCC extension is auto answered provided the agent is in the Ready state in the Cisco Finesse desktop. A zip tone plays to alert the agent. • Enable without Zip tone—For agents, belonging to the team, all the incoming calls to the IPCC extension is auto answered provided the agent is in the Ready state in the Cisco Finesse desktop. The zip tone does not play to alert the agent. • Disable (Default)—Auto answer is not enabled.	

Note

- To configure **Change Agent State to Not Ready when Agent Busy on Non ACD Line** at a team level, you must install UCCX 12.5(1) SU1 ES01.
- This functionality is applicable only for the agents and not for the supervisors of the team.

Step 9 Click **Save** to apply changes or **Cancel** to exit.

Modify Teams

Use the Teams area to modify the supervisors, agents, CSQs, or auto answer configuration on an existing Team.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **RmCm** > **Teams**.

Step 2 Click a name in the **Team Name** column.

The Team Configuration page appears.

Step 3 Select the **Primary Supervisor** from the drop-down list.

Step 4 (Optional) Select the secondary supervisor name from the **Available Supervisors** list and use the arrow icon to move it into the **Secondary Supervisors** list.

To remove the secondary supervisor name from this team, select the supervisor name in the **Secondary Supervisors** list and use the arrow icon to move it into the **Available Supervisors** list. This supervisor now belongs to the default team.

Step 5 (Optional) Select an agent name in the **Available Resources** list and use the arrow icon to move it into the **Assigned Resources** list to add an agent to this team.

To remove an agent from this team, select an agent name in the **Assigned Resources** list and use the arrow icon to move it into the **Available Resources** list. This agent now belongs to the default team.

Step 6 (Optional) Select the CSQ name in the **Available CSQs** list and use the arrow icon to move it into the **Assigned CSQs** list to add the CSQ to this team.

To remove a CSQ from this team, select a CSQ name in the **Assigned CSQs** list and use the arrow icon to move it into the **Available CSQs** list. This CSQ now belongs to the default team.

Step 7 In the **Team Settings** section, specify the following information:

Parameter Name	Parameter Value	Global Settings
Change Agent State to Not Ready when Agent Busy on Non ACD Line	Radio button that enables the agent state to change from the Ready state to the Not Ready state when the monitored Non ACD lines are used for Incoming or Outgoing calls. The options are: • Enable—Enables the state change of the agent in the team. • Disable (default)—Disables any state change of the agent in the team. • Allow team settings to override global settings—A check box to override the global settings. The global settings are available at **System** > **System Parameters** > **Agent Settings**. **Note** When you select the check box, a popup message reminds you that your team settings are different from the global settings. Click **OK** to proceed or **Cancel** to discard the changes. When you click OK, the team level settings override the global settings.	Displays the global settings.

Parameter Name	Parameter Value	Global Settings
Auto Answer	Enables the incoming calls to be automatically answered. The options are: • Enable with Zip tone—For agents, belonging to the team, all the incoming calls to the IPCC extension is auto answered provided the agent is in the Ready state in the Cisco Finesse desktop. A zip tone plays to alert the agent. • Enable without Zip tone—For agents, belonging to the team, all the incoming calls to the IPCC extension is auto answered provided the agent is in the Ready state in the Cisco Finesse desktop. The zip tone does not play to alert the agent. • Disable (Default)—Auto answer is not enabled.	

Note
To configure **Change Agent State to Not Ready when Agent Busy on Non ACD Line** at a team level, you must install UCCX 12.5(1) SU1 ES01.

Step 8 Click **Save** or **Update** to apply changes, **Cancel** to exit or **Delete** to delete this team.

Delete a Team

Use the Teams area of the RmCm Configuration web page to delete an existing Team.

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **RmCm** > **Teams**.

The Teams web page opens.

Step 2 Click the **Delete** icon beside the Team Name icon you want to delete.

The system prompts you to confirm the delete.

Step 3 Click **OK**.

Chat and Email Menu Options

Tip
- The **Chat and Email** option is available with Unified CCX Premium license package.

To access either of these menu options, choose **Subsystems** > **Chat and Email** as applicable.

The Chat and Email menu contains the following submenu options:

- **Customer Collaboration Platform Configuration**—Choose this option to configure the Customer Collaboration Platform parameters. This page also displays the overall health of Customer Collaboration Platform.
- **Mail Server Configuration**—Choose this option to configure the mail server. This page is available on the Unified CCX node with a premium license.
- **Contact Service Queues**—Choose this option to configure chat and Email CSQs. You can configure the email CSQs on the Unified CCX node with a premium license.
- **Predefined Responses**—Choose this option to define the chat and email predefined responses that are available in the Manage Chat and Email gadget on the Finesse Agent Desktop.
- **Channel Parameters**—Choose this option to configure channel parameters.
- **Chat Widget**—Choose this option to configure and manage chat widgets.
- **Teams**—Choose this option to configure teams.

Customer Collaboration Platform Configuration

Use the **CCP Configuration** web page to configure Cisco Customer Collaboration Platform. You must configure information only on this web page to enable the chat and email features.

Cisco Unified CCX does not support custom configuration changes on the chat and email campaigns or feeds from the Customer Collaboration Platform administration page.

This option is available only with the Unified CCX Premium license package. The email feature support for Unified CCX depends on the Customer Collaboration Platform version. For information about feature compatibility, see the Unified CCX Compatibility related information, located at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

Any configuration change using Customer Collaboration Platform Administration interface is not supported.

Note On a high availability setup, after the **Add to Cluster** operation is successful, the following message is displayed:

```
In case of HA, configure the CCP on secondary node after adding to cluster
in the secondary node.
```

Every time you navigate to this page, the state of feeds, campaigns, and notifications rules are validated for chat and email, the connectivity to the email server is checked, and the web page shows the appropriate status. Icons are used as visual indicators to display the status of each service. Hover the cursor over the icon to display a tool tip that explains the reason for the current state. As part of validation, Unified CCX checks the following:

- **CCP XMPP Service**

  Unified CCX checks the connectivity with the Customer Collaboration Platform XMPP service. If the XMPP service is down, the following message is displayed:

  ```
  CCP XMPP service is not accessible. Check the logs for more details.
  ```

- **CCP Runtime Service**

  Unified CCX checks the connectivity with the Customer Collaboration Platform runtime service. If the runtime service is down, the following message is displayed:

  ```
  CCP runtime service is not accessible. Check the logs for more details.
  ```

- **CCP Tomcat Service**

  Unified CCX checks the connectivity with the Customer Collaboration Platform Tomcat service. If the Tomcat service is down, the following message is displayed:

  ```
  Unable to communicate to the CCP on the IP address(Hostname) provided.
  Please verify whether CCP is running on this IP address(Hostname) or
  check the network connection and make sure that CCP is reachable from
  CCX.
  ```

- **CCP Status**

  - **Feeds**

    Unified CCX validates the status of the intended chat and email feeds in Customer Collaboration Platform.

    - —All the feeds are operating as usual in Customer Collaboration Platform.
    - —One or more feeds mismatches with Customer Collaboration Platform.
    - —All the feeds are missing in Customer Collaboration Platform.

  - **Campaigns**

    Unified CCX validates the status of the intended chat and email campaigns in Customer Collaboration Platform.

    - —All the campaigns are operating as usual in Customer Collaboration Platform.
    - —One or more campaigns mismatches with Customer Collaboration Platform.
    - —All the campaigns are missing in Customer Collaboration Platform.

  - **Notifications**

    Unified CCX validates the status of the intended chat and email notifications in Customer Collaboration Platform.

    - —All the notifications are operating as usual in Customer Collaboration Platform.
    - —One or more notifications mismatches with Customer Collaboration Platform. This status icon also appears after configuration, when no chat and email contact is injected yet. The status will change to normal after successful injection of chat and email contact.
    - —All the notifications are missing in Customer Collaboration Platform.

  - **Email Cache**

Unified CCX checks and alerts the user about the email cache.

- —Email cache is operating as usual.
- —Unable to cache emails. No new emails will be fetched.
- **Not Applicable**— Customer Collaboration Platform version is not compatible.

- **Email Server**

  Unified CCX checks the connectivity with the email server.

  - —Email server is operating as usual.
  - **Not Configured**—Channel provider is not configured.
  - **Not Applicable**—The following are the reasons for the current state:
    - Cisco Finesse is not active.
    - Email CSQ is not configured.
    - Customer Collaboration Platform version is incompatible with the Email feature.
  - —Unable to reach the email server.

- **CCP Chat Gateway**

  This indicates the status of the Customer Collaboration Platform Chat Gateway and the Channel that is integrated.

  - **CCP Chat Gateway**
    - — The gateway is operating as usual and is configured with a channel.
    - — The gateway is not in an operating state as it is either Unreachable or configurations are incorrect.
    - **Not Configured** — The gateway is not configured and no channels are configured.
    - **Not Applicable**—The following are the reasons for the current state:

      Cisco Finesse is not active.

      Customer Collaboration Platform version is incompatible or is not configured.
  - **Facebook Messenger Integration** — This indicates whether the channel is enabled. It also indicates the last failure recorded in the channel. This helps to determine any intermittent or permanent errors.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Chat and Email > CCP Configuration** as applicable.

The **Configuration** web page appears.

Note
You must perform the following actions:

- In the Unified CCX, upload Customer Collaboration Platform certificate to the Unified CCX Tomcat trust store using the Cisco Unified OS Administration interface. You can also use the `set cert import trust tomcat` CLI.
- In the Customer Collaboration Platform, upload Unified CCX certificate to the Customer Collaboration Platform Tomcat trust store using the Cisco Unified OS Administration interface.

Unified CCX and Customer Collaboration Platform servers must have DNS entries. Customer Collaboration Platform must be accessible to Unified CCX by hostname. If the entries are not valid, an error is displayed.

Step 2 Specify the following fields for Customer Collaboration Platform:

Field	Description
IP Address / Host Name	IP address or fully qualified domain name of the Customer Collaboration Platform server. For example, 192.168.1.5 or host.example.com.
User Name	Username of the Customer Collaboration Platform administrator.
Password	Password of the Customer Collaboration Platform administrator.

Note
When the Customer Collaboration Platform application password is reset, ensure that the new password is first updated in Unified CCX and then reset the password in Customer Collaboration Platform. This prevents the account getting locked due to the authentication attempts from Unified CCX with old password.

Step 3 Click **Save** to save the changes.

Note

- After saving a valid Customer Collaboration Platform configuration, you cannot change the **IP Address / Host Name** details. If you want to change the configuration, delete the existing configuration and create a new one.
- If you see an error message, click **Save** to re-create feeds, campaigns, and notifications for chat and email in Customer Collaboration Platform.
- When Unified CCX hostname is changed or when a new Unified CCX node is added, the Customer Collaboration Platform Configurations must be saved again. This enables the change to take effect to re-create all the notifications for email and chat in Customer Collaboration Platform.

Delete Customer Collaboration Platform Configuration

To delete the Customer Collaboration Platform configuration from the Unified CCX Administration interface, perform the following:

Important

- Ensure that the Customer Collaboration Platform configuration delete operation is performed during maintenance window.
- Ensure that the **Customer Collaboration Platform** configuration hostname is deleted manually from **Desktop Layout** in Cisco Finesse Administration.

Procedure

Step 1 On the **Customer Collaboration Platform Configuration** page, click **Delete**. A confirmation dialog box appears.

Step 2 Click **OK** to delete the Customer Collaboration Platform configuration.

This deletes the Customer Collaboration Platform configuration data from the Unified CCX configuration database. In addition, it deletes the configurations such as Feeds, Campaigns, Notifications, and Webhooks (that were created by Unified CCX) from the Customer Collaboration Platform application.

Note
If you select **Delete all Associated Chat and Email CSQs** check box in the confirmation dialog box, all the chat and email CSQs are also deleted from the Unified CCX configuration database.

Result: When the Customer Collaboration Platform configuration is deleted from both Unified CCX and Customer Collaboration Platform application, the following message is displayed: `CCP configuration has been deleted successfully.` However, due to connectivity issues, if the Customer Collaboration Platform configuration is deleted in Unified CCX but not deleted in Customer Collaboration Platform application, the following message is displayed: `CCP configuration has been deleted successfully from UCCX. Ensure that the related configurations are deleted manually from the the CCP application as well.`

Step 3 Restart the Unified CCX engine on both the nodes.

Step 4 Click **Cancel** to cancel this operation.

What to do next

When CCP configuration is not deleted in the Customer Collaboration Platform application.

Access Customer Collaboration Platform application: By default, access to Customer Collaboration Platform administration user interface is restricted. Administrator can provide access by using the allowed list of client's IP addresses and revoke by removing the client's IP from the allowed list. For any modification to whitelist to take effect, Cisco Tomcat must be restarted.

Whitelist administrator user interface: Use the `utils whitelist admin_ui add` command to use the allowed list the client's IP address, with which you want to access the Customer Collaboration Platform application. **For example:** `admin:utils whitelist admin_ui add 10.XXX.XX.XX`.

Delete Campaign: In the Customer Collaboration Platform application, select the **Configuration** tab. Select the checkbox to the left of one or more campaign names and click **Delete**. Click **OK** in the confirmation window to confirm the deletion of the selected campaigns.

Delete Feeds: In the Customer Collaboration Platform application, select the **Configuration** tab. Select the checkbox to the left of one or more feed names and click **Delete**. Click **OK** in the confirmation window to confirm the deletion of the selected feeds.

Delete Notifications: In the Customer Collaboration Platform application, select the **Administration** tab. Select the checkbox to the left of one or more notification names and click **Delete**. Click **OK** in the confirmation window to confirm the deletion of the selected notifications.

Reinject Email Contacts

Emails may be parked in Customer Collaboration Platform due to component failures or if the email server is down or not reachable. You can ensure that these emails are attended to when the services are restored by reinjecting the email contacts.

Note The latest 200 unread or reserved, social email contacts across the email CSQs are reinjected.

Procedure

To reinject the email contacts back to Unified CCX, click **Subsystems** > **Chat and Email CCP Configuration** > **Reinject**.

Note
The **CCP Configuration** web page is reloaded, but the configuration is not updated.

Chat Transcripts

You can search and retrieve stored chat transcripts. You can search by username (chat.agentName) and alias (chat.agentNickname). For more information on how to perform a default search or a field-specific search, see the "Search" section of the *Cisco Customer Collaboration Platform User Guide* or the Customer Collaboration Platform interface online help.

For information on how to change chat storage space and calculate the disk space that you need to store data for a specific duration, see the online help that is available for the Customer Collaboration Platform interface or see the *Cisco Customer Collaboration Platform User Guide*, located at:

https://www.cisco.com/en/US/products/sw/custcosw/ps1846/tsd_products_support_series_home.html

Mail Server Configuration

Use the **Mail Server Configuration** web page to configure the mail server.

Before you begin

- Create accounts and email addresses that must be used for CSQ creation.

- **Local Exchange Server**
  - Run the commands **set-service msExchangeIMAP4 -startuptype automatic**, and **start-service msExchangeIMAP4** on Microsoft Exchange to set the Microsoft Exchange IMAP4 service to start automatically.
  - Run the command **set-service msExchangeIMAP4BE -startuptype automatic**, and run **start-service msExchangeIMAP4BE** command (for Microsoft Exchange 2013) on Microsoft Exchange to set the Microsoft Exchange IMAP4 Back End service to start automatically.
- **Gmail**
  - Two types of authentication, **Basic** and **OAuth 2.0** are available for Gmail. **OAuth 2.0** is more secure.
  - You can select the authentication type while configuring a CSQ.
  - To use OAuth, you have to create a service account in the Google Cloud server. While creating a service account, you must download the JSON file that has the Private Key details, which must be uploaded while configuring a Contact Service Queue (CSQ). For more information on creating a service account, see https://developers.google.com/identity/protocols/oauth2/service-account.
  - To authorize a service account for accessing emails, ensure that "*https://mail.google.com/*" is entered in **API Scopes**.
- **Microsoft Office 365**
  - **OAuth 2.0** authentication is used to read emails and **Basic** authentication is used to send emails.
  - As part of COP ciscouccx.1251.su3.ES07.CSCwr61182.4.cop.sgn and ciscoccp.1251.su3.ES07.CSCwr61182.3.cop.sgn, **OAuth 2.0** authentication is used to read and send emails.
  - Create the Azure application for **OAuth 2.0** for authentication, and get the Tenant ID, Client ID, and Client secret from the Azure application. For more information on creating the Azure application see https://docs.microsoft.com/en-us/exchange/client-developer/legacy-protocols/how-to-authenticate-an-imap-pop-smtp-application-by-using-oauth#use-client-credentials-grant-flow-to-authenticate-imap-and-pop-connections.
  - Create the service principal for the Azure application. The service principal must have "FullAccess" (access rights) of the mailbox to read the email.

Note Microsoft Office 365 option is available from 12.5(1)SU2 ES03 onwards.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Chat and Email** > **Mail Server Configuration**. The **Mail Server Configuration** web page opens.

Step 2 Complete or modify the following fields for the mail server:

Field	Description
Mail Server Settings	
Mail Server	Choose the mail server that is required to be configured from the listed options: • MS Exchange Server / Office 365 • Gmail **Note** You must not perform any automatic or manual operations on the emails from the mail server. For example, create rules, move the emails manually to a different location, delete emails from the mail server, and so on. Unified CCX must be connected to a dedicated mail server. Ensure that the email account is not shared.
IMAP Folder Structure	
Sent Items Folder Name	The name of the sent items folder of the respective mail server that is configured. **Note** All the listed mail servers have the default folder names prepopulated for all the IMAP folders in English locale. These folder names can be edited and can have custom values.
Incoming (Secure IMAP)	
Host Name	Fully qualified domain name (FQDN) of the incoming (IMAP) server. Do not enter the IP address.
Port Number	Port number that is used to connect to the IMAP server. The default port number is 993.
Outgoing (Secure SMTP)	
Host Name	FQDN of the outgoing (SMTP) server. Do not enter the IP address.
Port Number	Port number that is used to connect to the SMTP server. The default port number is 587.
Proxy Settings	
HTTP	Choose the **Enable** or **Disable** radio button to use HTTP proxy for Mail Server connectivity. By default the **Disable** option is selected and **Enable** option is disabled. To enable **HTTP**, configure **Http** in **Proxy Parameters** section of **System Parameters** page. **Note** If Customer Collaboration Platform is able to access internet directly, HTTP proxy configuration is not required. Else, HTTP proxy configuration is required to invoke cloud services of mail servers (Gmail) to get the OAuth token. The OAuth token is used in SMTP/IMAP operations.

Field	Description
SOCKS	Choose the **Enable** or **Disable** radio button to use socks proxy for Mail Server connectivity. By default the **Disable** option is selected and **Enable** option is disabled. To enable **SOCKS**, configure **SOCKS Proxy** in **System Parameters** page.
Description	Description of the mail server.

Step 3 Click **Update** to save the changes.

Contact Service Queues

Before you begin

Note Microsoft Office 365 option is available from 12.5(1)SU2 ES03 onwards.

To change the Microsoft Office 365 authentication from **Basic** to **OAuth 2.0**, update the mail server selection to Microsoft Office 365, and then edit the email CSQ where the OAuth details must be filled.

As part of COP ciscouccx.1251.su3.ES07.CSCwr61182.4.cop.sgn and ciscoccp.1251.su3.ES07.CSCwr61182.3.cop.sgn, Microsoft Office 365 now supports **OAuth 2.0** authentication. To configure, select Microsoft Office 365 as the mail server and edit the email CSQ to provide the required OAuth details.

- You must create a skill before creating a CSQ. For information about creating a skill, see *Skill Configuration* section in the Cisco Unified Contact Center Express Administration and Operations Guide.
- Before creating an email CSQ, you must have configured the mail server.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Chat and Email** > **Contact Service Queues** as applicable.

The Contact Service Queues (CSQs) web page opens and displays the information for existing chat and email CSQs if any.

Step 2 To add a new chat or email CSQ, click the **Add New** icon that appears in the toolbar in the upper left corner of the window or the **Add New** button that appears at the bottom of the window.

The Contact Service Queue Configuration web page opens.

Step 3 Specify the following fields:

Field Name	Description
CSQ Name	Name for the CSQ.

Field Name	Description

Resource Selection Criteria	Resource selection criteria chosen for the chat CSQ.
	• **Longest Available**—Selects the agent who has been in the Available state for the longest amount of time.
	• **Most Skilled**—Used for expert agent chat distribution. Selects the agent with the highest total competency level. The total competency level is determined by adding the agent's competency levels for each assigned skill that is also assigned to the CSQ.
	  • Example 1: If Agent1 is assigned Skill1(5), Skill2(6), and Skill3(7) and CSQ1 specifies Skill1(min=1) and Skill3(min=1), the total competency level for Agent1 for CSQ1 is 12.
	  • Example 2: If Agent1 is assigned Skill1(5) and Skill2(6), and Skill3(7) and CSQ1 specifies Skill1(min=1), only, the total competency level for Agent1 for CSQ1 is 5.
	Note
	• To change the competence level for an already configured agent, change the agent skill level and save the CSQ.
	• If two agents score equal in the primary selection criteria, the agent who was updated first will be assigned to the incoming chat until the maximum chats threshold is reached.

Table 16: CSQ Type—Chat

Field Name	Description
CSQ Type	Choose Chat.

Table 17: CSQ Type—Email

Field Name	Description
CSQ Type	Choose Email. **Note** You can create up to 100 email CSQs. If you exceed the limit, the following error is displayed: `Cisco Unified CCX supports a maximum of 100 Email CSQs. Exceeded maximum limit for Email CSQs.`
Mail Server	Fully Qualified Domain Name (FQDN) of email server. This field displays the mail server that you configured.

Field Name	Description
Authentication Type	The type of authentication that is used to access the configured email account. **Basic** is used to access both types of email, Office 365 and Gmail by using username and password. By default, this option is selected. As part of COP ciscouccx.1251.su3.ES07.CSCwr61182.4.cop.sgn and ciscoccp.1251.su3.ES07.CSCwr61182.3.cop.sgn, Office 365 now uses OAuth instead of **Basic**. By default, this option is selected. OAuth is used to access Gmail by using the OAuth Private Key file that is downloaded from the Gmail mail server. Supports OAuth 2.0 protocol. As part of COP ciscouccx.1251.su3.ES07.CSCwr61182.4.cop.sgn and ciscoccp.1251.su3.ES07.CSCwr61182.3.cop.sgn, **OAuth 2.0** supports Microsoft Office 365. Office 365 authentication requires Tenant ID, Client ID, and Client Secret. **Note** This field is displayed only when you have configured Gmail mail server.
Email username	The email address to which emails are sent or retrieved.
Email password	Password for the email account. **Note** This field is mandatory when the email server type is Microsoft Office 365 or Microsoft Exchange. As part of COP ciscouccx.1251.su3.ES07.CSCwr61182.4.cop.sgn and ciscoccp.1251.su3.ES07.CSCwr61182.3.cop.sgn, this field is disabled for Microsoft Office 365. This field is optional when the email server type is Gmail.
Private Key	The JSON file that contains the OAuth Private Key, which is generated while creating Service Account in Google Cloud server. Click **Upload** to select the file. **Note** This field is displayed only when **Authentication Type** is **OAuth**.
Tenant ID	This is the Azure cloud tenant ID. **Note** This field is displayed when Microsoft Office 365 is selected as the email server.
Client ID	This is the Azure cloud application client ID. **Note** This field is displayed when Microsoft Office 365 is selected as the email server.
Client secret	This is the Azure cloud application client secret. **Note** This field is displayed when Microsoft Office 365 is selected as the email server.

Field Name	Description
Note Tenant ID, Client ID, and Client secret are available from 12.5(1)SU2 ES03 onwards.	
Inbox Folder Name	The folder from which emails will be fetched and queued for the Contact Service Queue. Default value = Inbox folder of the selected mail server type **Note** If you change the Inbox folder name, which is already in use, the emails that are downloaded and cached by Customer Collaboration Platform are made available to agents. The remaining emails in the folder are ignored.
Sent Items Folder Name	The folder to which Customer Collaboration Platform will move the response email to, when it is sent.
Test Configuration	This checks the following: • Connectivity from Customer Collaboration Platform to the configured mail server by using the user credentials that is specified in the Contact Service Queue (CSQ) configuration. • Presence of and permissions to the Inbox, Drafts, Outbox, and Sent Items folder for the user, that is specified in the CSQ configuration.
Poll Interval (Seconds)	Frequency in seconds to fetch emails from the server. Default value = 180, Range = 60 to 3600
Snapshot Age (Minutes)	Specify the time in minutes from when the emails are to be fetched. Default value = 120, Range = 60 to 43200 For example, if you specify 120 minutes, this field fetches the emails from the last two hours.

Step 4 Click **Next**.

The Skill Association for CSQ area opens with the newly assigned CSQ name.

Note
You can create up to 100 email CSQs. If you exceed the limit, the following error is displayed:

```
Cisco Unified CCX supports a maximum of 100 Email CSQs. Exceeded maximum limit for Email
 CSQs.
```

Step 5 From the Available Skills list, choose the skill that you want to associate with the CSQ by clicking it. To choose more than one skill, press the **Ctrl** key and click the skills that you want to associate with the CSQ.

Step 6 Click **Add**.

The chosen skill and the minimum competence level for that skill are displayed in the right pane under the heading **Selected.**

Note
To delete the skill from the Skills Required list, click the **Delete** icon next to **Minimum Competence**.

Step 7 Specify a minimum competence level for the skill assigned to the CSQ.

Step 8 To view the associated resources, click **Show Resources**.

Step 9 Click **Save** to save the changes for the CSQ.

The newly added CSQ appears in the **List of CSQs**.

Note
You can create up to 100 email CSQs. If you exceed the limit, the following error is displayed:

```
Cisco Unified CCX supports a maximum of 100 Email CSQs. Exceeded maximum limit for Email
 CSQs.
```

You can sort the CSQs by title by clicking the **CSQ Name** header and by type by clicking the **CSQ Type** header.

Step 10 To view the printable report and associated resources, click the CSQ for which you want to view the report and the associated resources and then click **Open Printable Report**.

Note
To delete a CSQ, click the CSQ that you want to delete and then click **Delete**. A warning dialog box appears, asking you to confirm the deletion. To delete, click **OK**.

Caution
Deletion of the chat CSQ affects the associated chat web forms. After deleting, modify the corresponding chat web form configurations and generate the HTML code.

Predefined Responses

To access the predefined responses, choose **Subsystems** > **Chat** > **Predefined Responses** OR **Subsystems** > **Chat and Email** > **Predefined Responses** as applicable.

Use the **Predefined Responses** page to configure and manage chat and email predefined responses. You can add a maximum of 500 chat and email predefined responses in total. These predefined responses are available in the Manage Chat and Email gadget on the Finesse Agent Desktop.

You can configure the responses to be available either to all the agents or only to the agents that are associated with specific CSQs.

Note Predefined responses are not available in the Cisco Agent Desktop. They are only available with the Finesse Agent Desktop.

Predefined Responses

Using this web page, you can add, modify, and delete predefined responses.

You can add a maximum of 500 chat and email predefined responses in total.

Note To modify an existing predefined response, click the Title header for the predefined response that you want to modify. To delete an existing predefined response, click the **Delete** icon for the predefined response that you want to delete.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Chat** > **Predefined Responses** OR **Subsystems** > **Chat and Email** > **Predefined Responses** as applicable.

The **Predefined Responses web page** opens, displaying the information for existing responses, if any.

Step 2 Click the **Add New** icon that is displayed in the toolbar in the upper left corner of the window or the **Add New** button that is displayed at the bottom of the window to create a new response.

The **Predefined Response Configuration web page** opens.

Step 3 Specify the following information:

Field	Description
Title	Unique identifier of the predefined response. **Note** The special characters angle brackets (< >), parentheses (( )), double quotation marks (" "), and pipe symbol (|) are not allowed.
Type	Types of media.
Response Description	Description for the predefined response. • Rich Text Editor is available to create an HTML-based email predefined response. Use the supported tags as provided in the Rich Text Editor for formatting purpose. • Plain Text Editor is available to create a chat predefined response. **Note** The special characters angle brackets (< >), parentheses (( )), double quotation marks (" "), and pipe symbol (|) are not allowed in Plain Text Editor for Chat Predefines Response. The maximum characters limit for predefined response for chat and email is 1500. In case of email, rich text is supported and includes the HTML tag characters for representing rich text.

Field	Description
Tags	Choose a tag for the predefined response. • **Global for all CSQs**: The predefined response is available to all the agents that are associated with all the CSQs. • **Customize (Maximum 10 CSQs)**: The predefined response is available only to the agents that are associated with the selected CSQs. If you choose this option, select the CSQs from the **Available CSQs** pane, and then click the left arrow to assign them. **Note** Predefined responses can be used only for emails sent in HTML format and not plain text.

Step 4 Click **Save**.

The newly added predefined response appears with the assigned tags in the **List of Predefined Responses**.

You can sort the predefined responses by title by clicking the Title header and by type by clicking the Type header.

Wrap-Up Reasons

To access the Wrap-Up Reasons, choose **Subsystems** > **Chat and Email** > **Wrap-Up Reasons**.

Use the **Wrap-Up Reasons** page to configure and manage Wrap-Up categories and reasons for chat and email Contact Service Queues (CSQs). Use the Ellipsis (...) to view all the Wrap-Up Reasons that are added for each Wrap-Up category.

Wrap-Up Reasons

Using this web page, you can add, modify, and delete the Wrap-Up Reasons.

You can add a maximum of 25 Wrap-Up categories. If you exceed the maximum number of categories, the **Add New** button is disabled.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Chat and Email** > **Wrap-Up Reasons**.
The **Wrap-Up Reasons** web page opens, displaying the information for existing Wrap-Up Reasons, if any.

Step 2 Click the **Add New** icon or the **Add New** button that is displayed in the toolbar in the upper left corner of the window.

The **Wrap-Up Reasons** web page opens.

Step 3 Specify the following information:

Field	Description
Category	Specify the name for the Wrap-Up category. Allows up to 40 characters.
Wrap-Up Reasons	Enter the Wrap-Up Reasons for the specified category. Allows up to 40 characters. Click the **Add** button to add up to 25 Wrap-Up Reasons for each category.
Tags	Choose a tag for the Wrap-Up category. • **Global for all CSQs**: The Wrap-Up reason is available to all the agents that are associated with all the CSQs. • **Customize** : The Wrap-Up reason is available only to the agents that are associated with the selected CSQs. If you choose this option, select the CSQs from the **Available CSQs** pane, and then click the left arrow to assign them. **Note** You can associate a maximum of 10 Wrap-Up categories to a CSQ.

Step 4 Click **Save**.

The newly added Wrap-Up category appears with the assigned tags in the **List of Wrap-Up Reasons**.

Note
When you reskill or modify a category, the logged in agents can apply Wrap-Up Reasons from the updated list of categories for the new non-voice contacts only.

Email Signatures

To access the email signatures, choose **Subsystems** > **Chat and Email** > **Email Signatures**.

Email Signature Configuration

Using this web page, you can add, modify, and delete email signatures.

Note To modify an existing email signature, click the Title header for the email signature that you want to modify. To delete an existing email signature, click the **Delete** icon for the email signature that you want to delete.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Chat and Email** > **Email Signatures**.

The **Email Signature web page** opens, displaying the list of existing email signatures that are configured, if any.

Step 2 Click the **Add New** icon that is displayed in the toolbar in the upper left corner of the window or the **Add New** button that is displayed at the bottom of the window to create a new email signature.

The **Email Signature Configuration web page** opens.

Step 3 Specify the following information:

Field	Description
Name	Unique name of the email signature. **Note** The name can have a maximum of 100 characters.
Content	The email signature content. **Note** The email signature can have a maximum of 1500 characters. You may format the text of the email signature content, add images, add URL to the email signature, and add the Agent alias information. The Agent alias variable appears by default when any new email signature is created. If it is removed from the email signature it can be reinserted at the cursor location in the email signature by clicking on the Agent alias variable icon. When there is no alias configured for an agent, the Agent ID is presented in the email signature by default.
Tags	Choose a tag for the email signature. • **Global for all CSQs**: The email signature is available to all the agents that are associated with all the CSQs. • **Customize (Maximum 10 CSQs)**: The email signature is available only to the agents that are associated with the selected CSQs. If you choose this option, select the CSQs from the **Available CSQs** pane, and then click the left arrow to assign them. **Note** Only one (1) email signature can be tagged as Global for all CSQs. A CSQ can be tagged with only one (1) email signature. When an email is responded by an agent of a particular CSQ, the system will check if there is any email signature tagged for that CSQ. The different scenarios are: • If there is an email signature tagged to a CSQ, that will be appended in the email response. • If there is no CSQ specific email signature, the global signature is appended in the email response. • If there is no global email signature and no customized email signature tagged to the CSQ then there will be no email signature appended in the email response.

Step 4 Click **Save**.

The newly added email signature appears with the assigned tags in the **List of Email Signatures**.

You can sort the email signatures by title by clicking the Title header and by type by clicking the Type header.

Channel Parameters

Use the Channel Parameters web page to configure channel parameters.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Chat** > **Channel Parameters** OR **Subsystems** > **Chat and Email** > **Channel Parameters** as applicable.

The Channel Parameters Configuration web page opens.

Step 2 Use this web page to specify or modify the following fields for channel parameters:

Field	Description
No Answer Timeout (Seconds)	The time for an agent to respond to the chat request after which, the chat request is routed back to the chat queue and for the chat toaster to fade out. This is applicable for the Group Chat request also. However when the chat is not accepted, the chat request is not routed back to the chat queue. **Note** When you use Chrome or Firefox, the browser overrides the chat toaster notification to fade out in 20 seconds, even if it is configured to a higher value.
Join Timeout (Minutes)	The time after which the customer initiates a chat and, if an agent is not joined, the customer gets a message as per the configuration in the **Chat Web Form Configuration** page. But an agent can still join the chat after this timeout. The default timeout is one minute and the maximum timeout value allowed is 60 minutes.
Inactivity Timeout (Minutes)	The customer inactivity time after which, the system ends the chat. This timeout is on the customer side only. The agent gets a message **"You are alone in the chat room. Click End to close the chat interface."**. The customer gets a message **"Warning: the server connection was lost due to an inactivity timeout or connection failure."**. Inactivity timeout may also apply to contacts in queue that have not yet been accepted by agents. This scenario occurs only when the Join Timeout value is greater than the Inactivity Timeout value. The customer then gets a message **"Sorry, the chat service is currently not available. Please try again later."**

Field	Description
Offer Chat Contact When On Voice Call	Click Yes if agents are allowed to handle a chat session during a voice call. **Note** This setting takes effect when the agent ends the current voice call. Chats are presented to agents even when they go off-hook or busy in a Non ICD call.
Offer Voice Call When On Chat	Click Yes if agents are allowed to handle a voice call during a chat session. **Note** This setting takes effect when the agent receives a new incoming chat. Direct/Consult Transfer to an IPCC extension is an exception. Even if agents are busy on a chat they would still get calls that are transferred to their extension directly.
Maximum Number Of Chat Sessions Per Agent	Number of chat sessions (ranging from 1 to 5) that an agent is allowed to handle. This includes the group chat sessions also. **Note** This option is available only if Finesse service is activated. For Cisco Agent Desktop, the value is set to 1.
Maximum Number Of Email Sessions Per Agent	Number of Email sessions (ranging from 1 to 5) that an agent is allowed to handle.
Sticky Email Timeout (Hours)	Specify the amount of time for which an email message waits in a specific agent CSQ. Sticky email routing (Last-agent email routing) is a mechanism to route an email message to the agent who handled the last leg of the email conversation. When an email message, which is part of an ongoing conversation, comes in and the agent who handled the last leg of the conversation is not available, then the email does not wait indefinitely in that agent queue. After the configured time expires, the email message is placed on the intended CSQ to be handled by any available agent. **Note** Last-agent email routing is not available if the customer changes the subject line of the email message. Default = 4 hours, Range = 1 to 120 hours.

Step 3 Click **Save** to save the changes for the channel parameters.

Note
If any of the above parameters are changed during the call center operation, the updated values are not applied to the existing contacts in the system. The changed parameters will affect only the new contacts coming into the system.

Chat Widgets

Use the **Chat Widgets** section to configure the Bubble Chat widget and generate HTML code snippet that can be hosted on the customer website.

The Bubble Chat interface supports accessibility for the visually challenged. To use this feature, users must configure Job Access With Speech (JAWS) and enable Accessibility mode in their system. When users navigate across UI elements by using the keyboard, the screen reader announces the focused elements such as fields, buttons, icons, and the incoming messages.

Note Website developers must localize the accessibility messages of Bubble Chat to ensure that the announcements are in the appropriate language.

To access the **Chat Widgets** page, choose **Subsystems** > **Chat and Email** > **Chat Widgets**.

Chat Widgets Page

The **Chat Widgets** page lists the following information and options for each chat widget:

Field	Description
Name	Name of the chat widget.
Description	A brief description.
Post Chat Rating	Whether post chat rating is available for the chat. **Note** Post chat rating can be configured for only bubble chat.
Code	Option to generate the web form code for the configured chat widget.
Delete	Option to delete the chat widget.

Chat Widget Configuration

You can add, modify, and delete chat widgets. You can select any one of the following calendars:

- 24 Hours X 7 Days
- Custom Calendar, which has been configured by using the Calendar Management in Finesse desktop.

Note

- To modify an existing chat widget, click the chat widget name.
- To delete an existing chat widget, click the delete icon. Ensure that the widget is removed from the customer website before deleting the widget.

You can configure or modify the Bubble Chat widget.

Bubble Chat Widget

To configure a Bubble Chat widget, complete the following steps:

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Chat and Email** > **Chat Widgets**.

The **Chat Widgets** web page opens, displaying the information for existing chat widgets.

Note
During the widget configuration, live preview of the widget is possible.

Step 2 Click the **Add New** icon or the **Add New** button.

The **Bubble Chat Configuration** web page opens. The administrator can configure the messages and labels in any language.

Step 3 In the **Widget Details** area, specify the following information:

Field	Description
Name	Unique name of the chat widget.
Description	Chat widget description.

Step 4 Click **Next**.
The **Attributes - Branding and Identity** area appears.

Step 5 Specify the following information:

Section	Field	Description
Font Family	Typeface	Font family used for the text in the Chat Web Form and chat window. **Note** The default font family is Helvetica. You can change the font family by either selecting from the drop-down or entering a new name. If the selected font family is not available in the system where from the AppAdmin page is accessed, it will display an alert message. When you enter a new name, ensure that the correct spelling (case sensitive) is used. The system does not indicate if you enter an invalid name. Ensure that you use commonly available fonts so as to make it easy for the customers to view the information. Before proceeding, the administrator should ensure that the selected font family is applied on the Chat Web Form preview.
Chat Title	Text	Title text displayed on the Chat Web Form and Chat Bubble.
	Text Color	Color of the title text.
Button	Text	Text displayed on the button of the Chat Web Form.
	Color	Color of the button.

Section	Field	Description
	Text Color	Color of the text displayed on the button.
Agent Message	Message Color	Background color of the agent message in the chat window.
	Text Color	Color of the agent message text.

Note
As you specify the attributes, the **Preview** area dynamically displays the preview of the Chat Web Form and chat window based on your specifications.

Step 6 Click **Next**.
The **Attributes - Post Chat Rating** areas open.

Step 7 Specify the following information:

Field	Description
Enable Post Chat Rating	If this checkbox is checked, post-chat rating will be available for the chat. The **Post Chat Rating** column in the **Chat Widgets** page indicates whether post chat rating is available for a chat.
Label	Text asking the user to rate the chat experience.
Button Text	Text displayed on the button that is used to submit the rating.

Note
The **Preview** area dynamically displays the preview of the rating window based on the information specified.

Step 8 Click **Next**.
The **User Form Fields** and **Problem Statements and CSQ Mapping** areas open.

Step 9 In the **User Form Fields** area, specify the following information:

a. From **Available Fields**, select the desired fields and move it to **Selected Fields**.

To create new fields in addition to the list of available fields, click **Add Custom Field**, enter the name of the new custom field in the pop-up window and click **OK**. The new custom field appears in the list of **Selected Fields**.

Step 10 In the **Add problem Statement CSQ mapping** area, specify the following information:

a. In **Problem Statement Caption**, enter the label for the problem statement field.

b. Enter the problem statement for the Chat Web Form and map the problem statement with an existing chat CSQ from the **CSQ List** drop-down list.

To add more problem statements and associate them with a chat CSQ, click **Add More**. Click the delete icon for a problem statement to delete that problem statement.

Step 11 Click **Next**. The **Chat Messages** area appears.

Step 12 Specify the following information:

Section	Field	Description
Initialization Messages	Widget Wait Message	Message displayed to the customer when the customer submits the chat form and waits for an agent to join.
	Join Time-out Message	Message displayed on the chat window to inform the customer that no agent is available currently.
In Progress Messages	Text for Text Typing Box	Text directing the customer to enter a message. This text appears in the text box of the chat window where the customer enters messages to be sent.
	Agent Joined Message	Message displayed on the chat window to inform the customer that an agent has joined. This message has the Agent Alias or Agent ID. Two text boxes are available to enter text to be displayed before and after the Agent Alias or Agent ID.
	Agent Left Message	Message displayed on the chat window to inform the customer that the agent has left. This message will have the Agent Alias or Agent ID. Two text boxes are available to enter text to be displayed before and after the Agent Alias or Agent ID.
End Messages	Close Chat Confirmation Pop-up message	Message displayed on the pop-up window to confirm if the customer wants to close the chat. In the **Negative Response** and **Positive Response** text boxes, enter the text to be displayed on the pop-up window buttons that allows the user to either accept or reject the chat closure.
	Close Chat and Download Transcript Confirmation Pop-up Message	Message displayed on the pop-up window to inform the customer that the chat has ended and the chat transcript is ready for download. In the **Negative Response** and **Positive Response** text boxes, enter the text appears on the pop-up window buttons that allows the user to either accept or reject the transcript download. **Note** By default, the **enableTranscriptDownload** attribute is set to True in the generated chat widget HTML code snippet.
Error Messages	System Error Message	Message displayed to the customer when the chat service is not available to handle chat requests.
	Connectivity Error Message	Message displayed to the customer when the chat is disconnected due to inactivity timeout or connection failure.

Step 13 Click **Next**. The **Service Hours** page appears.

Step 14 In **Service Hours** area, select one of the following options to configure the business hours.

- **Default (24 hours x 7 days)-** Select this option if the contact center works 24 hours and 7 days in a week.
- **Select Calendar-** Select this option to configure the business hours. Calendar drop-down is enabled for this selection.

Step 15 Select the desired calendar from the drop-down list and click the **View** link to preview the calendar details such as **Business Hours**, **Custom Business Days**, and **Holidays**.

Step 16 In the **Messages** area, specifiy the following:

Field	Description
Holiday	Message displayed on the bubble chat widget to inform the customer during a holiday.
Off Hours	Message displayed on the bubble chat widget to inform the customer during non-working hours.
Label	Heading text displayed on the bubble chat widget to inform the customer for the business hours details.

Step 17 In the **Label for Days of Week** area, specify a label for each day of the week.

Step 18 Click **Finish**.
The code for the Chat Web Form is generated and appears onscreen.

Note
The Chat Web Form that is generated uses JavaScript. You must access this Chat Web Form from a JavaScript enabled browser.

Step 19 Click **Save Code to File** to save the generated code. Click **Back to Chat Widgets** to go to the main **Chat Widgets** page.

Note
You can also generate the code from the main **Chat Widgets** page by clicking on the **Code** icon against the chat widget name. The generated code appears on a pop-up window. To save this code, click **Save Code to File**.

Integration of Chat Code into Customer Website

When you complete a chat widget configuration by clicking the **Finish** button, the code for the configured chat widget is generated. You can save this generated code by clicking **Save Code to File**. The code is saved in an HTML file. You can also generate the code from the main **Chat Widgets** page by clicking on the **Code** icon against the chat widget name.

For bubble chat, copy or download the HTML code snippet and insert it into the desired webpage of the customer's website. Use the function provided in the HTML code snippet as the event handler for an event such as “click”, etc., and use this event in an element, such as <button>, <a>, <p> etc. Invoking this event using the element will initiate the chat conversation. An example is shown in the HTML code snippet. If changes are made to the widget after deployment, there is no need to redeploy the HTML code snippet. The updated information is automatically fetched based on the widget ID and dynamically reflected for the next conversation.

Note In cases where the website is comprises more than one page, ongoing chats might get disconnected when the user navigates from one page to another.

Disable Bubble Chat Transcript Download

To disable the download option for Bubble Chat Transcript, you must set the **enableTranscriptDownload** attribute to False and then redeploy the HTML code snippet in customer website.

To change the attribute, download the generated widget code snippet, set the **enableTranscriptDownload** attribute to False, and save. Redeploy the chat widget HTML code snippet in customer website.

Localize Accessibility Messages

You can localize most of the messages by using Unified CCX Administration. However, some of the accessibility messages that are read by the screen reader on Bubble Chat interface have to be localized in the HTML code snippet. Download the generated chat widget HTML code snippet, and update the following strings:

```
//Please change the following accessibility messages to the required language:
var accesibilityMessageForCloseButton = 'close';
var accesibilityMessageForMinimizeButton = 'minimize';
var accesibilityMessageForRestoreButton = 'restore';
var accesibilityMessageToIndicateAgentTyping = 'Agent is typing';
var accesibilityMessageToIndicateMessageFromAgent = 'message from';
var accesibilityMessageToIndicateCustomerSentMessage = 'Sent message from';
var accesibilityMessageToSelectRating = 'Please press 1 to 5 key with 1 being lowest and 5
 being highest';
```

Save and redeploy the chat widget HTML code snippet in customer website.

Note Customer must have configured JAWS and enabled Accessibility mode in their system to experience the accessibility feature.

Chat - Facebook Messenger

Before you begin

To integrate Facebook Messenger with Unified CCX, you must ensure that the following conditions are met:

- Business entity must have a public Facebook page for their business.
- The endpoints like, Cisco Customer Collaboration Platform or a reverse proxy, must have valid Certificate Authority signed SSL certificates as they are exposed publicly to the Internet.
- A new Facebook App is created on the Messenger platform. For more information about creation of the Facebook App and Messenger setup see, https://developers.facebook.com/docs/messenger-platform.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Chat and Email** > **Chat - Facebook Messenger**.

Step 2 In **Configure Token from Facebook**, enter the **Facebook Page Access Token**. This access token is generated on the Facebook App page when the Facebook App is created.

Step 3 In **HTTP Proxy**, enable HTTP Proxy and provide valid values for the **HTTP Proxy**.

Step 4 Click **Validate** to ensure that the token is valid using HTTP Proxy (if provided).

Step 5 In **Problem Statements and CSQ Mapping**, enter **Problem Statement Caption**.

Step 6 Enter problem statement and select CSQ from the dropdown list. Click **Add More** to add problem statements and CSQs.

You can add a maximum number of three (3) problem statements.

Step 7 In **Chat Messages**, you can edit the existing messages as per your business requirement. The following table describes the messages that a Facebook Messenger user would see:

Section	Field	Description
Initialization Messages	Welcome Message	This message welcomes the user when a chat session is initiated. The user can select a problem statement from the list.
In Progress Messages	Wait Message	This message informs the user to wait until an agent joins the chat.
	Join Timeout Message	This message informs the user to continue to wait or try again later.
End Messages	End Message	This message informs the user that the chat session has ended.
	No Agent Available	This message informs the user that no agent is available.
Error Messages	Unsupported Content Message	This message informs the user that any attachments other than text formats are not supported.
	Unknown Error	This message informs the user about any unknown internal error.
	Inactivity Timeout Message	This message informs the user that the chat session has ended due to inactivity.

Step 8 In **Post Chat Rating**, you can enable Post Chat Rating so that customer can rate the chat experience on a scale of 1 (worst) to 5 (best). You can edit the existing messages as per your business requirement. The following table describes the messages that the Facebook Messenger user would see:

Section	Field	Description
Post Chat Rating	Rating Offer Message	This message informs the user that the chat experience can be rated. The user can select one of the ratings from 1 (worst) to 5 (best).
	Rating Completed Message	This message informs the user that the rating was sucessfully submitted.

Step 9 In **Webhooks Update in Facebook**, ensure that the Facebook Verification token and configured Callback URL are updated in the Facebook App.

Note
- If you have modified tokens, restart Customer Collaboration Platform Chat Gateway Service for the changes to take effect.

Step 10 In **Enable Integration**, check or uncheck the check box to enable or disable the integration of Facebook Messenger with Unified CCX respectively.

Step 11 Click **Save** to save settings.

Teams

Choose **Subsystems** > **Chat** > **Teams** OR **Subsystems** > **Chat and Email** > **Teams** as applicable from the Unified CCXAdministration menu bar to access this configuration area.

Note The team configuration for chat is the same as it is for voice.

Outbound Menu

Use the Outbound Configuration web page or REST API to provision outbound dialing functionality feature.

The Outbound menu option will be displayed when you upload the Cisco Unified Premium license.

General Configuration

Choose **Subsystems** > **Outbound** > **General** from the Cisco Unified CCX Administration menu bar to access the General Configuration web page.

Use this web page to add or modify Outbound dialing preferences.

Campaign Configuration

Choose **Subsystems** > **Outbound** > **Campaigns** from the Cisco Unified CCX Administration menu bar to access the Campaigns web page. You can create and schedule a campaign, modify the settings that apply to a campaign, and import a list of contacts (in bulk using a comma-separated plain text file with .txt or .csv extension) into the Unified CCX database for each campaign using this web page.

From the **Direct Preview Campaign Configuration** page, you can also create a schedule to automatically import contacts from a remote server using the **Import Contacts** option.

The Campaigns web page displays the following status in the **Automatic Import** column in the **Campaigns List** table for the listed campaigns:

- **Not Configured**—Automatic Import of contacts is not configured.
- **Enable**—Automatic Import of contacts is configured and Automatic Schedule is enabled.
- **Disable**—Automatic Import of contacts is configured but Automatic Schedule is disabled.

You can define any one of the following two types for a campaign:

- Agent-based - If you select this campaign type, all the outbound calls will be handled by the available agents.
- IVR-based - In this campaign type, the outbound calls will be handled by the IVR scripts.

Add New Campaigns

To configure the properties for direct preview, progressive and predictive agent-based campaigns, for campaign name and description, callback settings, skill group selection, time range, dialing options, retry settings, and the dial settings, click **Add New** icon or button in the Campaigns web page.

Import Contacts

To import contacts for a selected campaign, click the hyperlink for the required campaign under the Name column and click **Import Contacts**. This will open the Import Contacts window through which you can import contacts.

The **Open Printable Report for this Campaign Configuration** icon provides the information for the selected campaign in addition to call-specific information, which varies depending on the selected dialer type for outbound. Few of them are:

- Campaign Name
- Enabled - Yes or No
- Description
- Start Time of the campaign
- End Time of the campaign
- Contact Records Cache Size
- Remaining Contacts

Delete Contacts

To ensure that a contact does not get called again for subsequent campaigns, you must delete the contact from all campaigns to which it belongs.

Click **Delete All Contacts** icon or button in the Campaign Configuration web page to delete all contacts of a particular campaign. Once you click **Delete All Contacts**, you will see a dialog box with the message "This campaign will be disabled and all its contacts will be permanently deleted. Continue?" with **OK** and **Cancel** buttons.

If you click **OK**, the Outbound subsystem checks whether the contacts are used in an active Outbound campaign. If the contacts are used as part of an active Outbound campaign, you will see the following alert message in the status bar at the top of the Campaign Configuration web page: "Campaign is active. Cannot remove contacts from an active campaign. Disable the campaign and try again." In such cases, disable the campaign first and then try deleting all contacts. Click **Cancel** if you do not want to delete all contacts for the specific campaign.

Area Code Management

Use this page to manually add new area codes, update existing area codes, and to add international area codes.

Add New Area Code

The Area Codes Management page allows you to find, add, delete, and modify the mapping of area codes and time zones. The dialer uses the area code of a contact phone number to determine the time zone of the contact calling area.

Configure SIP Gateway

You can use the SIP Gateway Configuration web page to add or modify the parameters that enable the Outbound subsystem of Unified CCX to communicate with the SIP gateway. You can also update the parameters specific to Call Progress Analysis functionality of the gateway using this web page.

Call Progress Analysis is a feature of the SIP gateway by which it determines whether the outcome of a call is an answering machine, live voice, fax, or beep tone and so on. The SIP gateway performs call progressive analysis of the call and informs the outcome of the call to Unified CCX.

Note It is mandatory to configure the SIP Gateway used by the Outbound subsystem to place calls in case of IVR-based and agent-based progressive and predictive Outbound campaigns.

Follow this procedure to configure the SIP gateway parameters through Unified CCX Administration web interface:

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **Outbound** > **SIP Gateway Configuration**.

The SIP Gateway Configuration web page opens.

Step 2 Click **Update** to save the configuration changes.

The new SIP gateway configuration is added to the Unified CCX system.

Step 3 Click **Cancel** to restore the default settings.

SIP Gateway Configuration Web Page

The SIP Gateway Configuration web page.

Field	Description
Gateway Configuration	
Gateway Hostname/IP Address	The HostName or IP Address of the SIP Gateway in the Unified CCX server, which will be used by the Outbound subsystem to place calls for the predictive or progressive campaigns.
Gateway Port	Destination port used by Unified CCX to communicate with SIP gateway. The default value is 5060.

Local CCX Port	Destination port to be used by SIP gateway to communicate with Unified CCX. You cannot edit this field. Default value is as follows: • Fresh install: 5065 • Upgrade: Previously configured value. If not configured, 5065 is displayed. If you have configured a value other than 5065, you can restore to the default value by using the **Restore Default** button.
Local User Agent	This read-only field provides a description of the owner for this connection. The default value is Cisco-UCCX.
Transport(TCP/UDP)	The protocol required to send SIP messages. You can select any one of the following protocols: • TCP - Transport Control Protocol or • UDP - User Datagram Protocol The default value is UDP.
Call Progress Analysis Configuration (displays the parameter name, parameter value, and suggested value for the following fields)	
Minimum Silence Period (10-1000)	The amount of time that the signal must be silent after speech detection to declare a live voice (in milliseconds). Default = 375 milliseconds, Range = 10-1000 milliseconds
Analysis Period (1000 - 10000)	Maximum amount of time (from the moment the system first detects the speech) during which analysis will be performed on the input audio. Default = 2500 milliseconds, Range = 1000-10000 milliseconds
Maximum Time Analysis (1000-10000)	The amount of time to wait when it is difficult for the dialer to determine voice or answering machine. Default = 3000 milliseconds, Range = 1000-10000 milliseconds
Minimum Valid Speech Time (50-500)	Amount of time that the signal must be active before being declared speech. Anything less is considered as a glitch. Default = 112 milliseconds, Range = 50-500 milliseconds

Maximum Term Tone Analysis (1000-60000)	This is the amount of time the gateway will look for a terminating beep once an answering machine has been detected. Default = 15000 milliseconds, Range = 1000-60000 milliseconds

Dial Peer Configuration for Outbound

Dial peer configuration is required to transfer the outbound calls to the IVR ports and agents in case of progressive and predictive outbound campaigns. The dial peer maps to the CUCM trigger for IVR-based campaigns and to the agent extension for agent-based campaigns.

When you configure voice-network dial peers, the key commands that you must configure are the **destination-pattern** and **session-target** commands.

IVR

For IVR-based progressive and predictive campaigns, the **destination-pattern** command specifies the Unified CM Telephony Trigger associated with the IVR campaign. The **session-target** command specifies a destination address for the voice-network peer.

Agent

For agent-based progressive and predictive campaigns, the **destination-pattern** command specifies the agent extension. The **session-target** command specifies a destination address for the voice-network peer.

For Extend and Connect, the **destination-pattern** must specify the destination address of the CTI Remote Device (CTIRD). See the *Cisco Unified TAPI Developers Guide for Cisco Unified Communications Manager* at https://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_installation_guides_list.html for more information on CTIRD.

Disable Hunting for Agent-Based Outbound Calls

When the agent does not answer a live voice call within the time limit configured for Outbound Call Timeout in General Configuration web page, then the call has to be dropped. If hunting is not disabled on the gateway, the call is not dropped and is forwarded to the agent extension.

The gateway receives a 403 forbidden error message and hunts for the “preference 2 dial peer.” The gateway forwards the call to the agent extension using the “ preference 2 dial peer.” Hence, the call is seen on the agent desktop and the state of the agent is changed to Ready or Not Ready depending on the option selected for the Agent State after Ring No Answer field in System Parameters Configuration web page.

To disable hunting for the gateway, use **no voice hunt 57** command (57 maps to 403 forbidden in SIP).

Note This is a global configuration to restrict the gateway from hunting for all 403 forbidden error messages.

Translation of Phone Numbers

Unified CCX does not support the translation or modification of the phone number that it uses to dial out outbound calls. Any “voice translation rules” configured in the gateway that modifies the phone number are not supported. If the phone number is translated, then those calls are not treated as IVR or agent-based outbound

calls. Any such calls cannot have all the functionality and capabilities of a normal IVR or agent-based outbound calls.

Note You can use either of the below two supported methods to modify a dialed number in the gateway:

- To remove the initial digits of the phone number use **forward-digits** or **digit-strip** in the dial peer configuration.
- To add a prefix to the phone number use **prefix** in the dial peer configuration.

Database Menu

The Unified CCX system uses the Database subsystem of the Unified CCX Engine to communicate with database servers, to obtain information that can be relayed to callers or to make application decisions. The Database subsystem enables the Unified CCX applications to obtain information from data sources, which are databases configured to communicate with the Unified CCX system.

The Database menu contains the following options, which are explained below:

- Datasource
- Parameters
- Drivers

DataSource

Use the DataSources web page to add a new data source, display, modify, or delete existing datasources.

Choose **Subsystems** > **Database** > **DataSource** from the Cisco Unified CCX Administration menu bar to access the DataSources web page.

New DataSource

Follow this procedure from the DataSources web page to add a new DataSource:

Procedure

Click the **Add New** icon that displays in the toolbar in the upper left corner of the window or the button that displays at the bottom of the window to add a new data source.

The DataSource Configuration web page opens.

Add New Database Parameter

To add a new database parameter:

Procedure

Choose **Subsystems** > **Database** > **Parameter** from the Unified CCX Administration menu bar.

The Parameters web page displays. See **Poll Database Connectivity** to know more about how to update parameter-related fields.

Driver

Use the Driver List web page to upload new drivers, or to view and delete existing drivers.

Add New Database Driver

Follow this procedure to add a new jdbc driver:

Procedure

Step 1 From the Unified CCXAdministration menu bar, choose **Subsystems** > **Database** > **Drivers**.

The Driver List web page opens up displaying a list of uploaded driver class filenames along with a Delete icon.

Step 2 Click the **Add New** icon that displays in the toolbar in the upper left corner of the window or the **Add New** button that displays at the bottom of the window to add a new driver class name.

The Driver Management web page opens.

Step 3 Specify a valid JDBC driver jar file in the Driver File field or click **Browse** to locate the driver file.

The driver file is validated before uploading.

Step 4 Choose the supported class name for the new driver from the Driver Class Name drop-down list box.

Step 5 Click **Upload** to save the new driver to the database.

Tip

- For details on the compatible Enterprise database server version see, https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html. Ensure that a valid JDBC driver version is used that is compatible with the Enterprise database server.
- Contact your database vendor to know the appropriate JDBC driver versions that is compatible with your Enterprise database server.

- While uploading com.ibm.db2.jcc.DB2Driver, if your IBM DB2 deployment also requires a license Jar to be in the application's classpath, upload the license Jar as a Custom Jar File using the procedure detailed in **Specify Custom Classpath Entries**. Then, restart the Unified CCX Engine on all nodes through the Unified CCX Serviceability.

HTTP Menu

The Unified CCX system uses the HTTP subsystem of the Unified CCX Engine to add components to the Unified CCX Engine that allow applications to be triggered in response to requests from a variety of web clients, including computers and IP phones.

HTTP/HTTPS triggers are available if your system has a license installed for one of the following Cisco product packages: Unified IP IVR or Unified CCX Premium.

HTTP Trigger Configuration

Use the HTTP Trigger Configuration web pages to display, add, modify, and delete existing HTTP triggers.

Choose **Subsystems** > **HTTP** from the Cisco Unified CCX Administration menu bar to access the HTTP Trigger Configuration web page.

Add New HTTP Trigger

To add a new HTTP trigger:

Procedure

Click the **Add New** icon or button on the HTTP Trigger Configuration web page to access the HTTP Trigger Configuration web page.

To modify an existing trigger, click any hyperlink within the HTTP Trigger List table; the HTTP Trigger Configuration web page opens.

eMail Menu

The Unified CCX system uses the eMail subsystem of the Unified CCXEngine to communicate with your email server and enable your applications to create and send email. The email configuration identifies the default email address and server to be used for sending email (including e-pages and faxes) and for receiving acknowledgments.

Note This email subsystem is not related to agent email-based routing.

Choose **Subsystems** > **eMail** from the Cisco Unified CCX Administration menu bar to access the eMail Configuration web page. You must configure email functionality so that Unified CCX scripts created with the email steps will function correctly.

Cisco Media

Choose **Subsystems** > **Cisco Media** from the Unified CCXAdministration menu bar to access the Cisco Media Termination Dialog Group Configuration web page.

The Unified CCX system uses the Media subsystem of the Unified CCX Engine to configure Cisco Media Termination (CMT) dialog groups that can be used to handle simple Dual-Tone Multi-Frequency (DTMF) based dialog interactions with customers. A dialog group is a pool of dialog channels in which each channel is used to perform dialog interactions with a caller.

To modify an existing CMT dialog group, click any hyperlink within the trigger's summary table entry; the Cisco Media Termination Dialog Group Configuration web page opens.

To add a new CMT dialog group, click the **Add New** icon or button in the Cisco Media Termination Dialog Group Configuration web page. The Cisco Media Termination Dialog Group Configuration web page opens.

MRCP ASR Menu

The Unified CCX system uses the MRCP ASR (Automatic Speech Recognition) subsystem to allow navigation through a menu of options by speaking instead of pressing keys on a touch-tone telephone.

MRCP ASR Provider

Choose **Subsystems** > **MRCP ASR** > **MRCP ASR Provider** from the Cisco Unified CCX Administration menu bar to configure information about the vendor of your speech server, including the number of licenses, and the grammar type.

To modify an existing ASR Provider information, click any hyperlink within the provider's summary table entry; the ASR Provider Configuration web page opens.

To add a new ASR Provider information, click the **Add New** icon or button.

MRCP ASR Servers

Choose **Subsystems** > **MRCP ASR** > **MRCP ASR Servers** from the Cisco Unified CCX Administration menu bar to configure your speech server name, port location, and available languages.

Note You must have a MRCP ASR Provider defined before you can provision a MRCP ASR Server.

To modify an existing ASR Server, click any hyperlink within the server summary table entry; the ASR Server Configuration web page opens.

To add a new ASR Server, click the **Add New** icon or button.

MRCP ASR Dialog Groups

Use the MRCP ASR Dialog Group Configuration web page to display, add, modify, and delete information about MRCP ASR dialog control groups, which enable Unified CCX applications to use speech recognition.

Choose **Subsystems** > **MRCP ASR** > **MRCP ASR Dialog Groups** from the Cisco Unified CCX Administration menu bar to configure the MRCP ASR dialog control groups.

Note You must have a MRCP ASR Provider defined before you can provision a MRCP ASR Group.

To modify an existing MRCP ASR Dialog Group, click any hyperlink within the group summary table entry; the MRCP ASR Dialog Control Group Configuration web page opens.

To add a new MRCP ASR Group, click the **Add New** icon or button.

MRCP TTS Menu

The Unified CCX system uses the MRCP (Text-to-Speech) subsystem to convert plain text (UNICODE) into spoken words to provide a user with information or to prompt a user to respond to an action.

MRCP TTS Providers

Use the MRCP TTS Provider Configuration web pages to display, add, modify, and delete information about your TTS Provider.

Choose **Subsystems** > **MRCP TTS** > **MRCP TTS Provider** from the Cisco Unified CCX Administration menu bar to configure information about the vendor of your TTS system.

To modify an existing MRCP TTS Provider, click any hyperlink within the provider summary table entry; the MRCP TTS Provider Configuration web page opens.

MRCP TTS Servers

Use the MRCP TTS Server Configuration web page to display, add, modify, and delete the text-to-speech server name, port location, and available language.

To modify an existing MRCP TTS Server, click any hyperlink within the server summary table entry; the MRCP TTS Server Configuration web page opens.

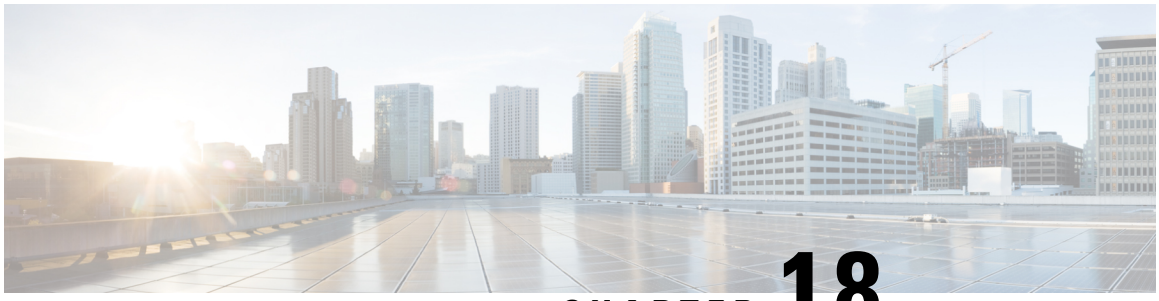
To add a new MRCP TTS Server, click **Add New** icon or button in the MRCP TTS Server Configuration web page.

Related Topic

MRCP TTS Default Genders

Use the MRCP TTS Default Genders Configuration web page to display or modify the gender setting for each Locale. You can modify the default gender setting for the Locales specified during TTS Server provisioning using this page. Click the **Update** icon or button to save the changes.

Related Topic



CHAPTER 18

Wizards Menu

The Wizards menu of the Unified CCX Administration web interface provides access to the wizards available for your Unified CCX system.

In each Wizard web page, you are provided with a list of procedures and a description for each procedure in the main pane.

Click the **Exit** icon in the toolbar in the upper left corner of the window or the **Exit** button that displays at the bottom of the window to exit the wizard at any time and to go to the main Unified CCX Administration menu bar. Click **Next** to go to the next wizard menu option.

The Unified CCX system contains the following options in the Wizards menu:

- Application Wizard, on page 333
- RmCm Wizard, on page 334

Application Wizard

Application Configuration is one of the very basic requirements in Unified CCX Administration. You must complete several steps in the following order to successfully complete Application Configuration.

To access the Application Wizard, select **Wizards** > **Application Wizard** > **Description of Steps** from the Unified CCX Administration menu bar. The Application Configuration Wizard: Description of Steps web page opens up, displaying the different steps to perform the configuration, along with a brief description of each step as shown in the following bulleted list.

Click **Next** to proceed to the subsequent steps from the main Application Configuration Wizard web page or jump directly to any step using **Wizards** > **Application Wizard** and clicking the desired submenu (see **Configure Unified CCX Applications**).

- **Scripts**—In this step, you can view a list of existing custom scripts. When you click the **Next** button from the main Application Configuration Wizard web page, you are transferred to Script Management web page, which lists the available scripts, provides links to create a folder, and uploads custom scripts. Scripts can be uploaded as either a single script file or a zip file of scripts. You can upload multiple scripts in this step (see **Script Management**).
- **Prompts**—In this step, you can view a list of existing custom prompts. The Prompt Management web page lists the available prompts, provides links to create new folders, and uploads custom prompts. Prompts can be uploaded as either a single prompt file or a zip file of prompts. You can upload multiple prompts in this step (see **Manage Prompt Files**).

- **Grammars**—In this step, you can view a list of existing custom grammar files that are used to recognize and respond to caller prompts. The Grammar Management web page lists the available grammars, provides the links to create new folders, and uploads custom grammars. Grammars can be uploaded as either a single grammar file or a zip file of grammars. You can upload multiple grammars in this step (see **Manage Grammar Files**).
- **Documents**—In this step, you can view a list of existing custom documents such as .txt, .doc, .jsp, or .html, custom classes, and Java Archive (JAR) files that allow you to customize the performance of your Unified CCX system. The Document Management web page lists the available documents, provides the links to create new folders, and uploads custom documents. Documents can be uploaded as either a single document file or a zip file of documents. You can upload multiple documents in this step (see **Manage Document Files**).
- **Application Configuration**—In this step, you can select the type of application to be configured using Add a New Application page. Click **Next** to provide configuration details for the selected application type. Each application can be any combination of the scripts, prompts, grammars, and documents on file. By default, the uploaded script, prompt, document and grammar are selected, if applicable. You can create multiple applications in this step (see **About Unified CCX Applications**).
- **Triggers**—In this step, you can create different types of triggers for the applications that were created in the previous step using the Trigger Configuration page. More than one trigger can be created for one application. By default, the application configured in the previous step is automatically selected. On providing the Directory Number, device name and language, the trigger configuration is complete. You can create multiple triggers in this step (see **Application Triggers**).

Selecting the type of the trigger concludes the Application Configuration wizard process.

RmCm Wizard

RmCm Configuration is a commonly performed procedure in the contact center environment. You must complete several steps to successfully complete RmCm Configuration. The RmCm Configuration wizard leads you through the following steps.

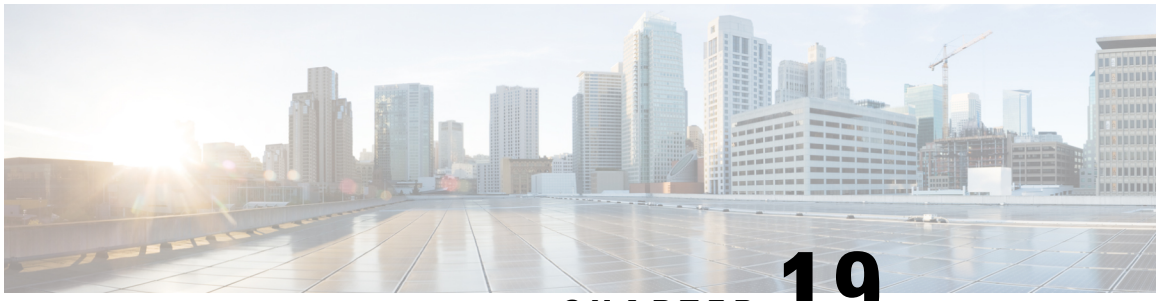
Note The RmCm Wizard option is available with all Unified CCX license packages.

To access the Application Wizard, select **Wizards** > **RmCm Wizard** > **Description of Steps** from the Unified CCXAdministration menu bar. The Application Configuration Wizard: Description of Steps web page opens up displaying the different steps in which you can perform the configuration along with a brief description of each step as shown in the bulleted list below.

Click **Next** to proceed to the subsequent steps from the main RmCm Wizard web page or jump directly to any step using **Wizards** > **RmCm Wizard** and clicking the desired submenu.

- **Add a Skill**—Choose this submenu to configure the skills to be associated with the user. In this step, you are transferred to the **RmCm** > **Skills** web page. Repeat this step to create multiple skills.
- **Add a Resource Group**—Choose this submenu to upload multiple custom scripts. In this step, you are transferred to the Resource Group Configuration web page, where you can enter the Resource Group Name.

- **Add Resources**—Choose this submenu to create resource groups that will later be assigned to resources. In this step, you are transferred to RmCm Wizard - User Configuration web page, which has a hyperlink to **Add resources in Unified CM**. This link invokes **Unified CM** automatically (see the following related topics):
  - RmCm Provider Configuration, on page 291
  -
- **Add Supervisors**—Choose this submenu to assign supervisor privileges to a user. In this step, you are transferred to the User Management web page, which allows you to search for a specific user.
- **Configure Resources**—Choose this submenu to add or remove skills that are associated with resources. In this step, you are transferred to the RmCm Configuration Resources web page, which lists the configured resources. Resources can be modified together to obtain the same skills, or they can be modified separately to be assigned different skills.
- **Modify Existing Contact Service Queues**—Choose this submenu to modify skills that are associated with a contact service queue. In this step, you are transferred to the RmCm Configuration Contact Service Queue web page, which lists the configured CSQs.
- **Add a Contact Service Queue**—Choose this submenu to add contact service queues. Skills or resource groups are associated to these contact service queues to filter out the resources. In this step, you are transferred to the RmCm Configuration Contact Service Queue Configuration web page, which allows you to add CSQs.
- **Modify Existing Teams**—Choose this submenu to modify agents in existing teams. In this step, you are transferred to the RmCm Configuration Contact Teams web page, which lists the configured teams.
- **Add a Team**—Choose this submenu to create new teams and associate those teams with new agents. In this step, you are transferred to the RmCm Configuration Team Configuration web page, which allows you to create new teams.
- **Create an Application**—On completing the RmCm configuration, you can optionally proceed to the Application Wizard configuration.



CHAPTER 19

Tools Menu

- Plug-Ins Menu, on page 337
- Real-Time Reporting Tool, on page 338
- Real-Time Snapshot Config Menu, on page 339
- Historical Reporting Menu, on page 343
- User Management Menu, on page 346
- Password Management, on page 353

Plug-Ins Menu

The Unified CCX system includes software components called *plug-ins* that you can use to enhance the Unified CCXEngine. You can download these plug-ins from the Plug-ins web page.

To access the Plug-ins web page, choose **Tools** > **Plug-ins** from the Unified CCXAdministration menu bar.

The Plug-ins web page contains one or more of the following hyperlinks (depending on the Unified CCX package you have purchased):

- **Cisco Unified CCX Editor Installer for Windows**—Click this hyperlink to install the client-side Unified CCX Editor. For more information, see the *Cisco Unified Contact Center Express Getting Started with Scripts and Cisco Unified Contact Center Express Editor Step Reference Guide.*
- **Cisco Unified CCX Editor Web Launcher**—Click Unified CCX Editor Web Launcher hyperlink to download and launch the Unified CCX Editor through JNLP file. For more information, see the *Cisco Unified Contact Center Express Getting Started with Scripts and Cisco Unified Contact Center Express Editor Step Reference Guide.*
- **Cisco Unified CCX Real-Time Monitoring Tool for Windows**—Click this hyperlink to install client-side Unified CCX Serviceability Real-Time Monitoring Tool (RTMT) for Windows. This tool monitors real-time behavior of the components in a Unified CCX cluster. RTMT uses HTTP/HTTPS and TCP to monitor device status, system performance, device discovery, and CTI applications. It also connects directly to devices by using HTTP/HTTPS for troubleshooting system problems. This plug in is available only for users with administrator capability.

Note To download on Windows, right-click **Download** hyperlink and select Save Target As option.

- **Cisco Unified CCX Real-Time Monitoring Tool for Linux**—Click this hyperlink to install client-side Unified CCX Serviceability Real-Time Monitoring Tool (RTMT) for Linux. RTMT uses HTTP/HTTPS and TCP to monitor device status, system performance, device discovery, and CTI applications. It also connects directly to devices by using HTTP/HTTPS for troubleshooting system problems. This plug in is available only for users with administrator capability.
- **Cisco Unified CCX Real-Time Reporting Tool**- Click this hyperlink to download and launch the Real-Time Reporting Tool. This provides real-time reports to monitor Unified CCX system activity. RTR client tool is a Java application and hence requires Java Runtime Environment (JRE) to be installed on the client machine. It runs outside the web browser and prompts for user authentication. **Note** : To download, right click on Download hyperlink and select Save Target As option.

Real-Time Reporting Tool

Caution While Unified CM supports Unicode characters in first and last names, those characters become corrupted in Unified CCX Administration web pages for RmCm configuration, and Real-Time Reporting.

The Real Time Reporting (RTR) client is a Java application that is used to generate various reports that provide detailed information about the status of the Unified CCX system.

You can download and access the RTR client from the Unified CCX Administration, Tools menu at the following paths:

- **Tools** > **Real Time Reporting**.
- **Tools** > **Plug-ins**.

Note Real Time Reporting (RTR) tool is downloaded as a .jnlp file. To use RTR with Java 8 and earlier, use Java Web Start. For Java 9 and later, use OpenWebStart. For more information on OpenWebstart, go to Install OpenWebStart, on page 339.

To run the Real Time Reporting client,

- In the **Security** tab of the **Java Control Panel**, add the fully qualified domain name (FQDN) of the Unified CCX server to the **Exception Site List**. For a high availability deployment, add the FQDN of both the Unified CCX servers to the **Exception Site List**.
- In the **Advanced** tab of the **Java Control Panel**, select the **Use TLS 1.2** option in the **Advanced Security Settings**.

The RTR client is a Java application. You can double-click the downloaded RTR file to run the client on the client machine. You can access the RTR client with the Unified CCX Administrator or Supervisor credentials. You must close it after you have run the reports for the Unified CCX system. The RTR client requires Java 1.7.0_80 or later to run on the client machine.

Note The Real Time Reporting (RTR) client online help requires user authentication, if the Cisco Unified CCX Administration user interface is not currently active in the web browser.

Install OpenWebStart

To install OpenWebStart, do the following:

1. Go to OpenWebStart to download the installer for your operating system.

Note We recommend you download OpenWebStart v1.5.2.

2. Follow the instructions on the setup wizard and click **Finish** to complete the installation.

   OpenWebStart is installed in your system.

What to do next

OpenWebStart allows you to add the installed Java Virtual Machines (JVMs) on your local file system. To add the locally available JVM, do the following:

1. Go to **OpenWebStart** > **itw-settings** (Windows) or **OpenWebstart** > **OpenWebStart Settings** (MacOS).

   The **Updater - OpenWebStart** dialog box appears.

2. Click **JVM Manager** in the left pane. A list of locally available JVMs appears. Do one of the following:
   a. If the installed JVM version is available in the list of JVMs, select it.
   b. If the installed JVM version is not available in the list of JVMs, do the following:
      1. Click **Add local...**.

         The **Select JVM** dialog box appears.
      2. Navigate to your Java folder and select the required JRE/JDK version. Click **Open**.

         The selected JRE/JDK version appears in the JVM Manager area.

3. Click **OK** to associate the Java version with OpenWebStart.

Note OpenWebStart supports JVMs versions 1.8 and later (1.8+) in RTR.

Real-Time Snapshot Config Menu

Many call centers use wallboards to display their real-time reporting status. Wallboards can display data such as available agents in CSQs, call volumes, talk times, wait times, and number of handled calls. You can enable

the Unified CCX system to write Unified CCX real-time information to a database that can then be displayed on a wallboard.

Note You must purchase the wallboard separately, and configure and control it with its own wallboard software. Wallboard software and hardware are supported by the third-party wallboard vendors, not by Cisco.

You must install the wallboard software on a separate machine or desktop, not on the Unified CCX server. During installation of your wallboard software, you must configure your wallboard software to access the Unified CCX database. To do this, you must assign a DSN, User ID, and password.

Use the Real-Time Snapshot Writing Configuration for Wallboard web page to enable the system to write data to the wallboard system.

To access the Real-Time Snapshot Writing Configuration for Wallboard web page, choose **Tools** > **Real Time Snapshot Config** from the Unified CCX Administration menu bar.

The following fields are displayed on the Real-Time Snapshot Writing Configuration for Wallboard web page.

Field	Description
Data Writing Enable	If checked, the system writes the data to the database. If not checked, the system does not write the data to the database. The default is disabled.
Data Writing Interval	Sets the refresh interval for the wallboard data. Valid options: 5, 10, 15, 20, 25, 30, 60, 90, 120, 150 and 180.
Cisco Unified CCX CSQs Summary	If checked, writes information about each CSQ to the RtCSQsSummary table in the Unified CCX database.
Cisco Unified CCX System Summary	If checked, writes overall Unified CCX system summary to the RtICDStatistics table in the Unified CCX database.
Wallboard System	
Server Name	IP addresses of the servers running the Wallboard software pointing to the HDS Database Server, which contains the Wallboard Real-Time Snapshot data. If you have multiple Wallboard servers, you can list their IP addresses in this field separated by commas.

Note For details about the information written to the RtCSQsSummary and RtUnified CCXStatistics database tables, see the *Cisco Unified Contact Center Express Database Schema Guide*. Only the RtCSQsSummary and RtICDStatistics statistics tables can be used in wallboard queries. Use of historical reporting tables in wallboard queries is not supported.

See the Unified CCX Compatibility related information, located at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html

Create System DSN for Wallboard

You can create a system Data Source Name (DSN) on your Windows server by performing the following procedure.

Procedure

Step 1 Install the wallboard software and IBM Informix ODBC Driver (IDS Version 3.0.0.13219 and above) on the wallboard client desktop.

Note

- You can download the Informix ODBC driver from the following URL: https://www-01.ibm.com/marketing/iwm/iwm/web/pickUrxNew.do?source=ifxdl. Download the IBM Informix Client Software Development Kit (CSDK) Version 3.00 or higher for the operating system you are installing with the wallboard client. More information about the CSDK can be found at the following URL:http://www.ibm.com/software/data/informix/tools/csdk/.
- The ODBC connections to Unified CCX do not support encryption.

Step 2 Select **Start** > **Settings** > **Control Panel**.

Step 3 From the Control Panel menu, select **Administrative Tools** > **Data Sources ODBC** to launch the OBDC Data Source Administrator.

Step 4 Click the **System DSN** tab. Then click **Add** to open the Create New Data Source dialog box.

Step 5 Scroll down to locate and select the IBM INFORMIX ODBC DRIVER.

Step 6 Click **Finish** to open the IBM Informix Setup dialog box.

Step 7 On the **General** tab, enter and apply a Data Source Name and Description.

Step 8 On the **Connection** tab, enter the values for the fields as shown in the following table:

Field	Description
Server Name	This is the instance name of the Informix database. Informix database instance name can be formed using Host Name of the Unified CCX server by following these conventions: • Convert all upper case letters to lower case. • Replace hyphens with underscore. • Add the letter “i” as a prefix to the instance name, if the hostname starts with a number. • Append the letters “_uccx” to the instance name. For example, if the hostname is “802UCCX-Ha-Node1”, enter “i802uccx_ha_node1_uccx” in the Server Name field.
Host Name	Enter the hostname of the primary Unified CCX server.

Field	Description
Service	Enter *1504*.
Protocol	Enter *onsoctcp*.
Options	Leave blank.
Database Name	Enter *db_cra*.
User ID	Enter *uccxwallboard*. This is the user id of the Unified CCX database created for wallboard.
Password	The password for the wallboard user that has been configured. You can change the password by going to **Tools** > **Password Management** submenu option from the Unified CCX Administration menu bar.

Step 9 Click **Apply**.

Step 10 Click the **Environment** tab and enter the values for the following fields:

Field	Description
Client Locale	Enter *en_US.UTF8*.
Database Locale	Enter *en_US.UTF8*.

Step 11 Click **OK**.

Step 12 Return to the **Connection** tab and click **Apply and Test Connection**.

If the phrase "Test completed successfully" is returned, click **OK**.

If the test is unsuccessful, return to the configuration sequence and fix any errors.

Wallboard Software in High Availability (HA) Deployment

If you use wallboard software in an High Availability (HA) deployment of Unified CCX and do not want any manual intervention in case of failover, you must upgrade your wallboard software.

Upgraded wallboard software should have a new service which periodically requests Unified CCX server for database mastership information using REST API (URL - *http://<Unified CCX server IP Address>/uccx/isDBMaster*). During failover, this new service in wallboard will update DSN registry to use new database primary server.

REST API can be requested only from wallboard servers configured through **Tools** > **Real Time Snapshot Config** web page from the Unified CCX Administration menu bar.

Use Upgraded Wallboard Software with New Service in HA Deployment

If you use wallboard software in a High Availability (HA) deployment of Unified CCX, you must work with your wallboard vendor to use the new API exposed by Unified CCX.

Wallboard software with the new service ensures that the wallboard server always displays data from the master database server of Unified CCX and no manual intervention is required. Follow this procedure to complete the setup:

Procedure

Step 1 Create DSN using secondary server information and modify the same DSN using primary server information. This will create sqlhost entries for both the servers in a registry at ***HKEY_LOCAL_MACHINE\SOFTWARE\Informix\SqlHosts***.

Step 2 Configure the wallboard software with new service as described in the wallboard software documentation.

Step 3 Configure information of both the Unified CCX servers with new service of wallboard as described in the wallboard software documentation.

What to do next

After you complete this procedure, no manual intervention is required in case of failover.

Use Wallboard Software (without New Service) in HA Deployment

If you use the existing wallboard software without the new service in an High Availability (HA) deployment of Unified CCX, you must complete the following actions:

Procedure

Step 1 Create DSN using secondary server information and modify the same DSN using primary server information. This will create sqlhost entries for both the servers in a registry at ***HKEY_LOCAL_MACHINE\SOFTWARE\Informix\SqlHosts***.

Step 2 Configure the wallboard software as described in the wallboard software documentation.

Step 3 Whenever there is a failover, you must manually change the DSN registry entry as follows:

a) Enter http://<Unified CCX server IP Address>/uccx/isDBMaster in a web browser from any wallboard client to know whether the requested Unified CCX IP address server has a database master or not.

b) On failover, change SERVER value to master DB instance name in registry of DSN under HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI

c) You can find the exact database instance name at ***HKEY_LOCAL_MACHINE\SOFTWARE\Informix\SqlHosts***

Historical Reporting Menu

Caution While Unified CM supports Unicode characters in first and last names, those characters become corrupted in Unified CCX Administration web pages for RmCm configuration, and Real Time Reporting.

Use the areas of the Historical Reporting Configuration web page to perform a variety of tasks, including configuring users, installing client software, and purging your database.

To access the different Historical Reporting Configuration options, choose **Tools** > **Historical Reporting** and click any of the following submenu options from the Unified CCX Administration menu bar:

- **Database Server Configuration**—to configure the database server to specify the reporting options provided to the user.
- **SMTP Configuration**—to configure the email server used to email scheduled Cisco Unified Intelligence Center (CUIC) reports.
- **Purge Schedule Configuration**—to automatically purge data as per the following configurations:
  - Timing of the purge
  - Automatic purge configuration
- **Purge Now**—to manually purge data.
- **File Restore**—to restore database records written to HR files when the database goes down.

Database Server Configuration

Use the Database Server Configuration area to specify the maximum number of client and scheduler connections that can access the database server.

SMTP Configuration

Use SMTP Server Settings area to configure the email server used to email scheduled Cisco Unified Intelligence Center (CUIC) reports.

The following fields are displayed in the SMTP Server Settings area:

Field	Description
Host/IP Address	The host name or IP address of the SMTP server
From email address	The email address that is to appear in the From field of emails sent by the Scheduler **Note** Unified CCX supports alphanumeric IDs and special characters (only hyphen "-", underscore "_", and dot ".").
Use SMTP Authentication	Check this if your SMTP server expects to receive username/password credentials
SMTP Username	If you check the Authenticate checkbox, enter the username that is to be authenticated
SMTP Password	If you check the Authenticate checkbox, enter the password that is to be authenticated

Note You will not be able to save the SMTP configuration if Cisco Unified Intelligence Center service on the publisher node is down.

Note The Unified Intelligence Center email client does not support SSL/TLS based SMTP servers to email the scheduled Unified Intelligence Center reports.

Purge Schedule Configuration Option

Use the Purge Schedule Configuration area to select a user for whom you want to choose a reporting package for the Unified CCX Historical Reports system.

Choose **Tools** > **Historical Reporting** > **Purge Schedule Configuration** from the Unified CCX Administration menu bar to access the Purge Schedule Configuration web page.

The Historical Reporting Configuration web page opens, enabling you to configure the following:

- Daily purge schedule
- Automatic purge (you can specify how long records should persist before the system purges them)

Purge Now Option

Use the Purge Now area to manually purge data.

Choose **Tools** > **Historical Reporting** > **Purge Now** from the Unified CCX Administration menu bar to access the Purge Now area.

File Restore Option

Use the File Restore area to restore the database records written to HR files when the database goes down.

In case of an High Availability setup, files from both the nodes are restored to the HR Database of the first and second node respectively. If it is unable to connect to the second node, you will see an alert message stating that the remote node is not reachable. When the second node comes up, the restored data will be replicated but you must repeat this Restore operation to restore the HR files, if any, on the second node.

Procedure

Step 1 Choose **Tools** > **Historical Reporting** > **File Restore** from the Unified CCXAdministration menu bar to access the Historical Reporting Configuration web page.

Note
Restore Now radio button is enabled by default on this page.

Step 2 Click the **Start** icon that displays in the toolbar in the upper left corner of the window or the **Start** button that displays at the bottom of the window to restore the database records.

You can view the status of the restore operation on this page.

User Management Menu

The User Management menu option allows you to assign access levels to Unified CCX system administrators and supervisors.

When you configure a Unified CCX supervisor, you are configuring users who can access the Unified CCX Supervisor web pages. You are not creating a supervisor for Unified CCX.

Attention Do not edit users, teams, and permissions in Unified Intelligence Center. The Unified CCX to Unified Intelligence Center sync runs as part of daily purge and synchronizes these settings on Unified Intelligence Center according to Unified CCX settings.

Only administrators can update the Unified CCX system. You must select at least one administrator, so that someone is available to perform updates.

Procedure

Choose **Tools** > **User Management** and click any of the following submenu options from the Unified CCXAdministration menu bar to assign administrative privileges to administrators and supervisors:

- User View Submenu, on page 346
- Name Grammar Generator Configuration, on page 347
- Spoken Name Upload Submenu, on page 348
- Administrator Capability View Menu, on page 348
- Supervisor Capability View , on page 348
- Reporting Capability View Menu, on page 351
- Agent Capability View Menu, on page 353

User View Submenu

From the Unified CCXAdministration menu bar, choose **Tools** > **User Management** > **User View** to access the User Configuration web page.

Use this page to view existing users and assign administrative privileges to administrators and Supervisors. You can provide a search string based on a user ID; for example, if you provide the search string as.

- “*Agent1”, it will display user IDs ending with Agent1.
- “Agent1*”, it will display user IDs starting with Agent1.
- “Agent1”, it will display user IDs that contain Agent1.

All the columns are hyperlinked to the user configuration page.

Note This search bar searches the users only by last name or user ID. Do not use the first name for searching.

When you unassign any Supervisor from the list of Supervisors who has one or more Advanced Supervisor Capabilities, an alert is displayed for your confirmation. Upon confirmation, the Advanced Supervisor Capabilities that are assigned and the Supervisor role are removed for that Supervisor.

Name Grammar Generator Configuration

Use the Name Grammar Generator Configuration web page to define scheduling information for the Name Grammar Generator.

From the Unified CCXAdministration menu bar, choose **Tools** > **User Management** > **Name Grammar Generator Configuration** to access Name Grammar Generator Configuration area.

Name Grammars must be generated if you wish to use the Name to User Step with ASR. The Name Grammar Generator scans the User Directory and creates a speech recognition grammar containing every user in the directory. These grammars are saved in the grammar repository.

You may use the Name Grammar Generator Configuration page to run the Name Grammar Generator or schedule it to run at some later time. The page also displays the date and time that the Name Grammar Generator was last run and the completion status of that run.

The following fields are displayed on the Name Grammar Generator web page.

Field	Description
Frequency	How often Name Grammar Generator is automatically run. Valid options: Never, Daily, and Weekly. This is a mandatory field.
Run task on (hrs of day)	Time of day to run the task. This is a mandatory field.
Run task on (day of week)	Day of week to run the task. This is a mandatory field.
Last Completed on	Date of last generation of name grammar.
Last Completion Result	The status after the last name grammar generation. (Display only.)
Grammar Variant	Select one or more grammar variants to generate from the check box next to the following three options: • OSR 3.1.x • 2003 SISR • Nuance
Current Status	Running status of the Name Grammar Generator. (Display only.)

Click the **Generate Name Grammar Now** icon or button to trigger the Name Grammar Generator.

Note Clicking **Generate Name Grammar Now** will not apply changes to the scheduling configuration; you must click **Update** to apply scheduling changes.

Spoken Name Upload Submenu

When a caller requests to be transferred to a specific extension, Unified CCX applications can playback a recording of the spoken name of the person to whom the caller has called. These spoken name recordings are stored as .wav files and managed by the Spoken Name Upload tool of the Unified CCXAdministration web interface.

To access the Spoken Name Prompt Upload web page, choose **Tools** > **User Management** > **Spoken Name Upload** from the Unified CCXAdministration menu bar.

The Spoken Name Prompt Upload web page also contains the **Click Here for Recording Information** icon and button, which displays a .htm page in your browser with more information on recording spoken name prompts.

Administrator Capability View Menu

From the Unified CCXAdministration menu bar, choose **Tools** > **User Management** > **Administrator Capability View** to access the capability view for the Administrator User Management area.

This web page contains a pane for users identified as Unified CCX Administrator and another pane with the list of Available Users. Based on your requirements, you can move users back and forth between these two panes by clicking the arrows in either direction. Click **Update** to save the changes.

Note

- You cannot assign Administrator capability to a user ID that is the same as the application administrator user ID created during the Unified CCX installation. If you assign Administrator capability to such a user ID, an error appears.
- In Single Sign-On (SSO) mode the **Application User** created during installation will not be able to access the **Cisco Unified Intelligence Center** application with administrator privileges. To enable the Cisco Unified CCX Administrator to have administrator privileges in **Cisco Unified Intelligence Center** as well, follow the steps below:
  1. Assign the reporting capability to the user.
  2. Run the CLI command, **utils cuic user make-admin**.
  3. Restart the **Cisco Unified Intelligence Center Reporting Service** for the changes to reflect.

Supervisor Capability View

From the Unified CCXAdministration menu, choose **Tools** > **User Management** > **Supervisor Capability View** menu to access the detailed view for Supervisors.

Note Assign an extension to the Supervisor so that they can access the Unified Intelligence Center Live Data reports.

Warning You cannot assign Supervisor capability to a user ID that is the same as the application administrator user ID created during the Unified CCX installation.

The **Supervisor Capability View** page displays the following information about the supervisors and their capabilities:

- The name of the supervisors.
- The teams to which the supervisors are assigned as Primary or Secondary Supervisors.
- The CSQs associated with the supervisors.
- The team level setting for **Change Agent State to Not Ready when Agent Busy on Non ACD Line** .

Note To configure **Change Agent State to Not Ready when Agent Busy on Non ACD Line** at a team level, you must install UCCX 12.5(1) SU1 ES01

The Supervisors can be assigned the following Advanced Supervisor Capabilities:

- Queue Management- Enables a Supervisor to manage resources across the assigned CSQs and teams.
- Calendar Management- Enables a Supervisor to change business hours, custom business days, and holidays.
- Outbound Campaign Management- Enables a Supervisor to schedule, enable or disable outbound campaigns, and manage import contacts.
- Application Management - Enables a Supervisor to manage Unified CCX applications.

Manage Supervisors

Procedure

Step 1 From the Unified CCXAdministration menu, choose **Tools** > **User Management** > **Supervisor Capability View** menu to access the **Supervisor Capability View** page.

Step 2 Click **Manage Supervisor**.

The **Manage Supervisor** page opens. Use this page to assign users as Supervisors from the **Available Users** field.

Note
Supervisors are listed on the **Supervisor Capability View** page.

Step 3 Click **Save**.

Note

When you unassign a Supervisor from the Supervisor role, the Supervisor capabilities and the Advanced Supervisor Capabilities are unassigned for the Supervisor.

View Supervisor Details

From the Unified CCXAdministration menu, choose **Tools** > **User Management** > **Supervisor Capability View**.

Click any Supervisor from the list of Supervisors to access the **Supervisor** page.

Use the **Supervisor** page to view the following:

- List of assigned teams
- Role details of the Supervisor
- **Contact Service Queue(s)** (CSQs)
- Team setting for **Change Agent State to Not Ready when Agent Busy on Non ACD Line**

Note To configure **Change Agent State to Not Ready when Agent Busy on Non ACD Line** at a team level, you must install UCCX 12.5(1) SU1 ES01.

- The Advanced Supervisor Capabilities that are enabled for Primary and Secondary Supervisors.

Assign an Existing Team to Secondary Supervisor

Before you begin

- Use **Manage Supervisors** to add users as Supervisors.
- Use **Teams** to add new teams.
- Use **Teams Configurations** to assign a Primary Supervisor and Secondary Supervisors to the teams.

Procedure

Step 1 From the Unified CCXAdministration menu, choose **Tools** > **User Management** > **Supervisor Capability View** menu to access the **Supervisor Capability View** page.

Note
Supervisors are listed on the **Supervisor Capability View** page.

Step 2 From the **Supervisor Name** column, click any Supervisor from the list of Supervisors.

The **Supervisor** page opens.

Step 3 Click **Assign a Team** to assign teams to the Secondary Supervisors.

The **Assign a Team** pop-up window appears.

Step 4 From the **Team Name** drop-down list, select a team and click **Assign**.

The **Assigned Teams** table lists the teams that are assigned to the Supervisor roles and the CSQs that are associated with the teams.

Assign Advanced Supervisor Capabilities

Use the **Supervisor** page to enable or disable one or more Advanced Supervisor Capabilities for Supervisors.

Note If you assign capabilities to supervisors through API, ensure that at least one calendar, one campaign, or one application is assigned accordingly. If proper assignment is not done, the supervisors will be able to view the capabilities in Finesse but none of the details will be listed.

Procedure

Step 1 From the Unified CCXAdministration menu, choose **Tools** > **User Management** > **Supervisor Capability View** menu to access the **Supervisor Capability View** page.

Note
Supervisors are listed on the **Supervisor Capability View** page.

Step 2 From the **Supervisor Name** column, click any Supervisor from the list of Supervisors.

The **Supervisor** page opens.

Step 3 Assign one or more Advanced Supervisor Capabilities to the Supervisor. From the **Advanced Supervisor Capabilities**, perform the following:

a) To enable the **Queue Management** capability for the Supervisor, check **Assign Queue Management**.

Note
A team and atleast a CSQ that is associated with the team must be assigned to the Supervisor to enable **Queue Management** capability.

b) To enable **Calendar Management** capability for the Supervisor, check the calendars from the **Calendar Name** column.

c) To enable **Outbound Campaign Management** capability, check one or more outbound campaigns from the table in the **Campaign Name** column.

d) To enable **Application Management** capability, check one or more applications from the table in the **Application Name** column.

Step 4 Click **Save**.

Reporting Capability View Menu

From the Unified CCXAdministration menu bar, choose **Tools** > **User Management** > **Reporting Capability View** to access the capability view for the Historical Report Users area.

The capability view for the Reporting Management web page contains a pane for users identified as Unified CCX Historical Report Users and another pane with the list of Available Users. Based on your requirements, you can move users back and forth between these two panes by clicking the arrows in either direction.

Note You cannot assign Reporting capability to a user ID that is the same as the application administrator user ID created during the Unified CCX installation. If you assign Reporting capability to such a user ID, an error appears.

The following users can access Unified Intelligence Center:

Roles	Access	Available reports
Application administrator	Super user	• Historical reports • Live Data reports
Reporting user	Unified CCX administrator must assign this role to a user.	• Historical reports • Live Data reports
Supervisor	Unified CCX administrator must assign this role to a user.	Live Data reports
Agent	Unified CCX administrator must assign this role to a user.	Agent-specific Live Data reports

Assign Prompts

Use this page to assign prompts to applications. The prompts must be explicitly assigned to an application when a new application is created or a new prompt is uploaded. When you upgrade to Unified CCX 12.5(1), the system behavior is as follows:

- All the prompts that were there prior to the upgrade will be assigned to all the applications.
- When you upload a new prompt to a folder that was there prior to the upgrade, the prompt will be assigned to all the applications.

Procedure

Step 1 Select **Tools** > **User Management** > **Assign Prompts**.

Note
If the system has only one application, by default, that application is selected.

Step 2 On the **Assign Prompts** page, select an **Application** from the drop-down list.

Step 3 Click **Assign/Unassign Prompts**.

Step 4 In the **Assign/Unassign Prompts** window, select the required prompt files or folders from the left navigation pane.

a) Click **Select All** to select all the folders.
b) Click **Unselect All** to clear the selection.

Note
- When you select all the files in a folder, the folder is also selected.
- When you add prompt files to a selected folder, the new prompt files are available for the respective supervisors.
- If you have selected an empty folder, add prompt files to that folder, the new prompt files are available for the respective supervisors.

Step 5 Click **Save**.

Agent Capability View Menu

From the Unified CCXAdministration menu bar, choose **Tools** > **User Management** > **Agent Capability View** to access the capability view for Unified CCX agents.

The capability view for the Agent User Management web page contains a pane for users identified as Unified CCX Agents and another pane with the list of Available Users. Based on your requirements, you can move users back and forth between these two panes by clicking the arrows in either direction.

Password Management

From the Unified CCX Administration menu bar, choose **Tools** > **Password Management**.

You can set the passwords for the following system users using this web page:

User	Username	Description
Wallboard	uccxwallboard	This user can connect to Configuration and Historical databases and has read-only access to RtICDStatistics and RtCSQsSummary tables.
Recording SFTP	uccxrecording	
Workforce Management	uccxworkforce	

User	Username	Description
Historical Reporting	uccxhruser	This user can connect to Configuration, Historical and Repository databases and has the following privileges: • read-only access to Historical, Configuration, and Repository tables • run stored procedures • create new stored procedures. This user is used by coresident Unified Intelligence Center and Standalone Unified Intelligence Center (if configured) to connect to Unified CCX Database and run historical reports. This user is also used during initialization of Live Data gadgets in Finesse and Live Data reports in Unified Intelligence Center.
System Call Tracking (part of Real Time Monitoring Tool/ Analysis Manager)	uccxsct	

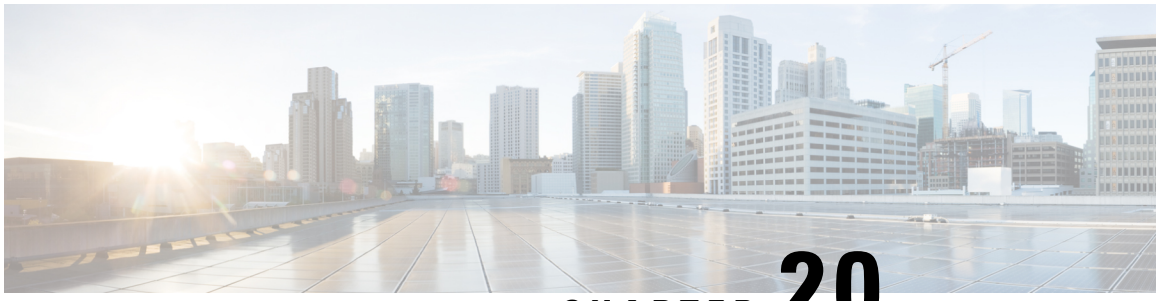
Click **Save** icon that displays in the toolbar in the upper left corner of the window or the **Save** button that displays at the bottom of the window. Click the **Clear** button to remove the data entered and to retain the existing passwords. You will see an error message if the old and new passwords are the same for any of the users. Click **Check Consistency** to confirm.

Note
- The maximum length of the password entered is limited to 80 characters.
- A new password cannot be one of the last five passwords used.
- There is no default password set. You must manually reset it for the first time.

In case of a High Availability deployment, the password change will not be propagated to the second node. You must access the AppAdmin web interface of the second node manually to change the password. In an HA setup, you will be able to see **Check Consistency** icon or button in the Password Management page. Use this button to check and confirm whether the passwords between the two nodes match or not. You will be able to see the status of the password check in the Password Management page.

Note If passwords are not same across the nodes, applications using these user credentials, such as Wallboard, Historical Reports and Live Data reports in Unified Intelligence Center and Finesse may not function. Ensure that the user passwords are same in both the nodes.

When one or more user passwords are not same across both the nodes, the following alert would be generated, **UserPasswordMismatchAcrossNodes**.



CHAPTER 20

Help Menu

- Contents and Index, on page 357
- For This Page Menu, on page 358
- Unified CCX Documentation Link, on page 358
- About Menu, on page 358

Contents and Index

To view the entire Unified CCXAdministration Guide online help system and index, choose **Help** > **Contents and Index** from the Unified CCXAdministration menu bar. The Unified CCX Administration Guide Online Help window opens.

When you click any topic in the top pane, the section of the online help that corresponds to that topic appears in the bottom pane.

The following table describes the menu options in the Unified CCX Administration Guide Online Help window.

Menu Option	Description
Back	Returns you to the previous page.
Forward	Leads you to the next page.
-	-
Print	Prints the help document.
View PDF	Opens a PDF version of the Cisco Unified CCX Administration Guide.
Contents and Index	Displays the index and contents of the Unified CCX Administrator Guide online help files in a separate web page. The index is displayed in the left pane while the contents are displayed in the right pane in the online help page.

For This Page Menu

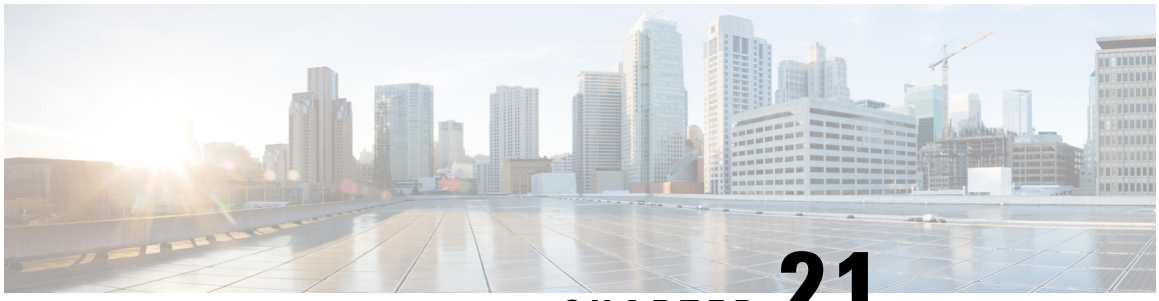
To access context-sensitive help, open the web page for which you want help and choose **Help** > **For This Page** from the Unified CCXAdministration menu bar. The Unified CCX Administration online help displays information that is specific to the open web page.

Unified CCX Documentation Link

To access the complete Unified CCX documentation set for Unified CCX, and Unified IP IVR, choose **Help** > **Cisco Unified CCX Documentation on Cisco.com** from the Unified CCX Administration menu bar. A new browser window opens to display the following documentation index page: https://www.cisco.com/en/US/products/sw/custcosw/ps1846/tsd_products_support_series_home.html.

About Menu

To access Unified CCX version information, choose **Help** > **About** from the Unified CCXAdministration menu bar. The Unified CCX Administration web page opens, displaying version information and package information.



CHAPTER 21

Cisco Finesse

- Introduction, on page 359
- Cisco Finesse Administration Console, on page 359
- Cisco Finesse Agent and Supervisor Desktop , on page 479

Introduction

Cisco Finesse is a next-generation agent and supervisor desktop designed to provide a collaborative experience for the various communities that interact with your customer service organization. It helps improve the customer experience while offering a user-centric design to enhance customer care representative satisfaction as well.

Cisco Finesse provides:

- A browser-based administration console and a browser-based desktop for agents and supervisors; no client-side installations required.
- A single, customizable "cockpit", or interface, that gives customer care providers quick and easy access to multiple assets and information sources.
- REST APIs that simplify the development and integration of value-added applications and minimize the need for detailed desktop development expertise.

Finesse configuration changes are permitted on only the primary server. Access to Finesse administration console on the secondary server is read-only.

When you attempt to save the changes in Finesse administration console on the secondary node, you receive a message that administration on the secondary node is read-only.

Cisco Finesse Administration Console

Getting Started

This chapter describes the interfaces that you use to configure, administer, and maintain Cisco Finesse and describes how to access them.

Administration Tools

Cisco Finesse Administration Console

The Cisco Finesse administration console is a web-based interface used to configure system settings in Cisco Finesse. The administration console contains tabs to click and access the various administration features. The tab names and the associated tasks are:

- **Settings:** IP Phone Agent Settings.
- **Call Variables Layout:** Manage the call and ECC variables that appear on the agent desktop call control gadget, team performance gadget, and call popover.
- **Desktop Layout:** Make changes to the default desktop layout for agents and supervisors.
- **Phone Books:** Add, edit, or delete phone books or phone book contacts.
- **Reasons:** Add, edit, or delete Not Ready reason codes, Sign Out reason codes, or Wrap-Up reasons (Reason Codes are disabled for Packaged CCE deployments).
- **Team Resources:** Assign desktop layouts, phone books, reason codes, and wrap-up reasons to specific teams.
- **Workflows:** Create and manage workflows and workflow actions.

The features you configure in the administration console are case-sensitive. For example, you can create two workflows named WORKFLOW and workflow; or two phone books named BOOK and book.

Response Caching

To reflect the changes made to system settings in Finesse desktop, the administrator must clear server cache using the CLI **utils webproxy cache clear rest**. Ensure that the agent browser is refreshed for the system settings changes to take effect.

For more information of REST API Response Caching, see *Cisco Finesse Web Services Developer Guide* at https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide.

Sign In to Cisco Finesse Administration Console

You can access the Cisco Finesse administration console only through HTTPS.

When you sign in to Cisco Finesse, always use the fully qualified domain name (FQDN) of the Cisco Finesse server in the URL.

Procedure

Step 1 Direct your browser to https://<FQDN>:8445/cfadmin, where *FQDN* is the fully qualified domain name of your primary Finesse server.

Step 2 The first time when you access the administration console using HTTPS, you are prompted to trust the self-signed certificate provided with Finesse. The following table describes the steps for each supported browser.

Note

If you are using HTTPS but have installed a CA Certificate, you can skip this step. For more information about installing a CA Certificate, see *Cisco Finesse Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html.

Option	Description
Firefox:	**a.** A page appears that states this connection is untrusted. **b.** Click **I Understand the Risks**, and then click **Add Exception**. **c.** In the Add Security Exception dialog box, ensure that the check box is**Permanently store this exception** checked. **d.** Click **Confirm Security Exception**.
Chrome and Edge Chromium (Microsoft Edge):	**a.** A page appears that states this connection is not private. **b.** In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)** **c.** In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**

Step 3 On the Sign In page, in the ID field, enter the Application User ID that was used during the installation.

Step 4 In the Password field, enter the Application User password that was used during the installation.

Step 5 Click **Sign In**.

Note
If a custom logon message is set up in Cisco Unified OS Administration, the message is displayed. Click **OK** to sign in. For more information about setting up a custom logon message, see the *Set Up Customized Logon Message* section in *Cisco Unified Operating System Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR*.

A successful sign-in launches an interface with defined administration gadgets and a Sign Out link.

Note

- If you are inactive for the configured duration (as per the time configured in webapp session timeout command), Cisco Finesse automatically signs you out of the administration console. The default session timeout is 30 minutes.
- When your administrator privileges are revoked by another Unified CCX administrator, you are automatically signed out (within 5 minutes) from the Cisco Finesse administration console. For more information on administrators privileges, see Administrator Capability View Menu, on page 348.

Sign In Using IPv6

If you sign in to the Finesse Administration Console using an IPv6-only client, include the HTTPS port in the sign in URL in Step 1 of the preceding procedure.

https://<*FQDN*>:8445/cfadmin

The remaining steps of the sign in procedure remain the same for IPv6.

If you sign in to the Finesse Administration Console using an IPv6-only client, include HTTPS port in the sign in URL in Step 1 of the preceding procedure.

- For HTTPS access, enter:

  https://<*FQDN*>:8445/cfadmin

The remaining steps of the sign in procedure remain the same for IPv6.

Account Locked after Five Failed Sign in Attempts

If an administrator tries to sign in to the Finesse administrator console (or diagnostic portal) with the wrong password five times consecutively, Finesse blocks access to that user account for 30 minutes. For security reasons, Finesse does not alert the user that their account is locked. They must wait 30 minutes and try again.

Similarly, if agents or supervisors sign in to the desktop five times consecutively with the wrong password, Finesse blocks access to that user account. However, in this case, the lockout period is 5 minutes. This restriction also applies when agents and supervisors sign in using the mobile agent or Finesse IP Phone Agent (IPPA).

Note When an agent or supervisor account is locked, subsequent attempts to sign in, even with correct credentials, reset the lockout period to 5 minutes again. For example, if a locked user tries to sign in again after only 4 minutes, the lockout period is reset and the user must wait another 5 minutes. This reset does not apply to the administrator account.

To view if a user account is locked, enter the **file get activelog desktop recurs compress** CLI command.

Extract the zipped output and search the catalina.out logs (/opt/cisco/desktop/finesse/logs/catalina.out) for the following message referring to the locked username:

```
An attempt was made to authenticate the locked user "<username>"
```

Cisco Unified Operating System Administration

This interface is web-based and is used to perform the following system administration functions:

- **Show:** View information on cluster nodes, hardware status, network configuration, installed software, system status, and IP preferences.
- **Settings:** Display and change IP settings, network time protocol (NTP) settings, SMTP settings, time, and version.
- **Security:** Manage certificates and set up and manage IPSec policies.
- **Software Upgrades:** Perform and upgrade or revert to a previous version.
- **Services:** Use the Ping and Remote Support features.

Sign In to Cisco Unified Operating System Administration

Procedure

Step 1 Direct your browser to http://*host or IP address/cmplatform*, where *host or IP address* is the hostname or IP address of your server.

Step 2 Sign in with the username and password for the Administrator User account.

Note
After you sign in, you can access other Unified Communications Solutions tools from the Navigation drop-down list.

Certificate Management

Finesse provides a self-signed certificate that use or provide a CA certificate. You can obtain a CA certificate from a third-party vendor or produce one internal to your organization.

Finesse does not support wildcard certificates. After you upload a root certificate signed by a certificate authority (CA), the self-signed certificates are overwritten.

If you use the Finesse self-signed certificate, agents must accept the security certificates the first time they sign in to the desktop. If you use a CA certificate, you can accept it for the browser on each client or deploy a root certificate using group policies.

Note If there is a mismatch between the server hostname and the certificate hostname, a certificate address mismatch warning message is displayed in IE. The certificate must be regenerated so that the hostname matches the server hostname before importing to Finesse. If there is a valid reason for the mismatch, uncheck the **Warn about certificate address mismatch** checkbox from **Tools** > **Internet Options** > **Advanced** > **Security** to allow the certificate to be accepted.

Obtain and Upload CA Certificate

Note This procedure only applies if you are using HTTPS and is optional. If you are using HTTPS, you can choose to either obtain and upload a CA certificate or 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 CA. Use the Certificate Management utility from Cisco Unified Operating System Administration.

To open Cisco Unified Operating System Administration in your browser, enter:

https://*hostname of primary UCCX server*/cmplatform

Sign in using the username and password for the Application User account created during Finesse installation.

Note You can find detailed explanations in the Security topics of the *Cisco Unified Operating System Administration Online Help*.

Procedure

Step 1 Generate a CSR.

a) Click **Security** > **Certificate Management** > **Generate CSR**.

Note
The RSA key lengths supported for the certificate signing request (CSR) generation are 1024, 2048, 3072, and 4096 bits. For Elliptic Curve Digital Signature Algorithm (ECDSA), P-384 key size is recommended, which is roughly equivalent to 7680 bits.

b) From the Certificate Name drop-down list, choose **tomcat** and click **Generate CSR**.

Step 2 Download the CSR.

a) Select **Security** > **Certificate Management** > **Download CSR**.
b) From the Certificate Name drop-down list, choose **tomcat** and click **Generate CSR**.

Step 3 Generate and download a CSR for the secondary Unified CCX server.

To open Cisco Unified Operating System Administration for the secondary server in your browser, enter:

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, you must upload the certificates in the order described in the following steps.

Step 5 When you receive the certificates, click **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, choose **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, choose **tomcat**.
b) In the **Upload File** field, click **Browse** and browse to the application certificate file.
c) Click **Upload File**.

Step 9 Restart both the Unified CCX nodes in the cluster.

Client-Side Certificate Acceptance

There are procedures that agents must perform to accept certificates the first time they sign in. The procedure type depends on the method you choose to manage certificates and the browser used by the agents.

Deploy Root Certificate

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

Note To avoid certificate warnings, each user must use the FQDN of the Finesse server to access the desktop.

Procedure

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

Step 2 Right-click Default Domain Policy and select **Edit**.

Step 3 In the Group Policy Management Console, click **Computer Configuration** > **Policies** > **Window Settings** > **Security Settings** > **Public Key Policies**.

Step 4 Right-click Trusted Root Certification Authorities and select **Import**.

Step 5 Import the *ca_name*.cer file.

Step 6 Go to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies** > **Certificate Services Client - Auto-Enrollment**.

Step 7 From the Configuration Model list, select **Enabled**.

Step 8 Sign in as a user on a computer that is part of the domain.

Step 9 If the user does not have the certificate, run the command **gpupdate.exe /target:computer /force** on the user's computer.

Set Up CA Certificate for 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 FQDN of the Unified CCX server to access the desktop.

Procedure

Step 1 From the Firefox browser menu, choose **Options**.

Step 2 Go to **Privacy and Security** tab.

Step 3 Under Certificates section, click **View Certificates**.

Step 4 Select **Authorities**.

Step 5 Click **Import** and browse to the *ca_name*.cer file.

Note
Here the *ca_name* is the name of your certificate.

Step 6 Check the **Validate Identical Certificates** check box.

Step 7 Restart the browser for the certificate to install.

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.

Note
When using Chrome, it is recommended you import your certificates to the Chrome trust store to avoid issues with the Cisco Unified CCX Administration interface. Refer to CSCwa89310 for more details.

Trust Self-Signed Certificate

Trust the self-signed certificate provided by Finesse to eliminate browser warnings each time you sign in to the administration console or agent desktop.

If you have uploaded a CA certificate, you can skip this procedure.

Procedure

In your browser, enter the URL for the administration console (https://*FQDN of primary server:portnumber*/cfadmin) or the agent desktop (https://*FQDN of primary server*).

Option	Description
If you use Internet Explorer:	**a.** A page appears that states there is a problem with the website's security certificate. Click **Continue to this website (not recommended)**. The sign in page for the administration console (or agent desktop) appears with a certificate error in the address bar if the browser. **b.** Click **Certificate Error** > **View Certificates** to open the Certificate dialog box.

Option	Description
	c. In the Certificate dialog box, click **Install Certificate** to open the Certificate Import Wizard. **d.** Click **Next**. **e.** Choose **Place all certificates in the following store** and click **Browse**. **f.** Choose **Trusted Root Certification Authorities** and click **OK**. **g.** Click **Next** > **Finish** **h.** If a Security Warning dialog box appears asking if you want to install the certificate, click **Yes**. **i.** In the Successful Certificate Import dialog box, click **OK**. **j.** Enter your credentials and click **Sign In**.
If you use Firefox:	**a.** A page appears that states this connection is untrusted. **b.** Click **I Understand the Risks Add Exception**. **c.** In the Add Security Exception dialog box, ensure the **Permanently store this exception** check box is checked. **d.** Click **Confirm Security Exception**. The page that states this connection is untrusted automatically closes and the administration console (or agent desktop) loads. **e.** Enter your credentials and click **Sign In**. **f.** For the agent desktop only, an error appears that states Finesse cannot connect to the Cisco Finesse Notification Service and prompts you to add a security exception for the certificates issued by the Finesse server. Click **OK**.

Add Certificate for HTTPS Gadget

Add a certificate for a secure HTTP (HTTPS) gadget to load the gadget on the Finesse desktop and successfully perform HTTPS requests to the Finesse server.

This process allows HTTPS communication between the Finesse gadget container and the third-party gadget site for loading the gadget and performing any API calls the gadget makes to the third-party server.

Note A gadget that loads using HTTPS may still use HTTP communication between that gadget and the application server where it resides. If all traffic must be secure, the gadget developer must ensure that HTTPS is used to make API calls to the application server.

The certificate must be signed with a common name. The gadget URL in the desktop layout must use the same name (whether it uses an IP address or an FQDN) as the name with which the certificate is signed. If

the certificate name and the name in the gadget URL don't match, the connection isn't trusted, and the gadget doesn't load.

To find the certificate name, enter the gadget URL in your browser. Click the lock icon in the address bar and then click View Details. Look for the common name field.

The Finesse host must be able to resolve this name using the DNS host entered during the installation. To verify that Finesse can resolve the name, run the CLI **utils network ping <hostname>** command.

Procedure

Step 1 Download the certificate from the third-party host running a Cisco-provided solution.

Step 2 Upload the certificate to the designated Finesse system.

a) Sign in to Cisco Unified Operating System Administration on the primary Unified CCX node (https://*FQDN*/cmplatform, where *FQDN* is the fully qualified domain name of the Unified CCX node).
b) Click **Security** > **Certificate Management**.
c) Click **Upload Certificate/Certificate Chain**.
d) From the Certificate Name drop-down list, select **tomcat-trust**.
e) Click **Browse** and navigate to the tomcat.pem file that you downloaded in the previous step.
f) Click **Upload File**.

Step 3 Restart Cisco Tomcat on the primary Unified CCX node.

Step 4 Restart Cisco Finesse Tomcat on the primary Unified CCX node.

Step 5 After synchronization is complete, restart Cisco Tomcat on the secondary Unified CCX node.

Step 6 Restart Cisco Finesse Tomcat on the secondary Unified CCX node.

Add Certificate for Multi-session Chat and Email

Add the Customer Collaboration Platform certificate to the Unified CCX servers to allow communication between Customer Collaboration Platform and Finesse. After you complete this procedure, agents must accept certificates in the Finesse desktop before they can use this gadget.

If Customer Collaboration Platform is deployed with private certificates, agents cannot join chat rooms or reply to email messages until they accept the Customer Collaboration Platform certificates. If the Manage Chat and Email gadget is deployed on the Manage Chat and Email tab of the Finesse desktop, agents may not realize that they need to accept the certificates. Have agents check the tab where the gadget appears when they sign in to Finesse to make sure that certificates are all accepted and the gadget loads correctly.

The steps to add a certificate for the Manage Chat and Email gadget are the same as the steps outlined in the procedure **Add Certificate for HTTPS Gadget**.

Note The procedure to add a certificate for an HTTPS gadget refers to the third-party gadget host. To add a certificate for chat and email, perform the applicable steps on the Customer Collaboration Platform server.

Manage System Settings

Note For information about Finesse IP Phone Agent Settings, see **Manage Finesse IP Phone Agent**.

Desktop Chat Server Settings

Desktop Chat is an XMPP browser based chat, which is powered by Cisco Instant Messaging and Presence (IM&P) service. It provides presence and chat capabilities within the Unified CM platform. For more details, see *Configuration and Administration of the IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Desktop Chat connects to Cisco IM&P servers over port 5280 from the browser hosting the agent desktop. IM&P server visibility and port accessibility needs to be ensured if clients intend to use this feature. The Desktop Chat gadget configures the IM&P host BOSH URL's used by the desktop to communicate with the IM&P server over BOSH HTTP.

IM&P has a clustered design, where users are distributed across multiple nodes in the cluster. The Desktop Chat initially discovers the IM&P nodes that a user has configured, caches this information and communicates with the actual server for subsequent login, until the browser cache is cleared. To spread the initial discovery load, it is advisable to configure the nodes in a round robin fashion if the deployment has more than one Finesse cluster. For example, if there are 5 IM&P nodes configure Finesse cluster A with node 1 & 2, Finesse cluster B with nodes 3 & 4, and so on.

Node availability should be considered while configuring the IM&P URL. The secondary node will be available for discovery in scenarios where the first node is not reachable. The secondary node will be connected for discovery only if the primary node is unreachable.

For the URL to be configured, refer Cisco Unified Presence Administration service, in *System, Service Parameters*. Choose the required IM&P server, select Cisco XCP Web Connection Manager. The URL binding path is listed against the field *HTTP Binding Path*. The full URL to be configured in Finesse is `https://<hostname>:5280/URL-binding-path`.

Use the Desktop Chat Server Settings to configure chat settings for the Finesse desktop. The following table describes the fields on the Desktop Chat Server Settings gadget.

Field	Explanation
Primary Chat Server	Enter the IM&P primary server URL of Desktop Chat.
Secondary Chat Server	Enter the IM&P secondary server URL of Desktop Chat.

Actions on the Desktop Chat Server gadget:

- **Save:** Saves your configuration changes
- **Revert:** Retrieves the most recently saved server settings

Important For Desktop Chat to work without any issues, ensure the following services are running on IM&P:

- Cisco Presence Engine
- Cisco XCP Text Conference Manager
- Cisco XCP Web Connection Manager
- Cisco XCP Connection Manager
- Cisco XCP Directory Service
- Cisco XCP Authentication Service
- Cisco XCP File Transfer Manager

Note Desktop Chat requires the Cisco IM and Presence certificates to be trusted. To start the Desktop Chat without experiencing an exception, you must add the certificate to the browser trust store, or configure IM and Presence with CA-signed certificate, or push self-signed certificate through group policies in supported browsers. For more information on accepting certificates, see the *Accept Security Certificates* section, in the *Common Tasks* chapter of *Cisco Finesse Agent and Supervisor Desktop User Guide for Cisco Unified Contact Center Express* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-user-guide-list.html.

For more information on adding certificates to the browser trust store, see the *Certificate Management* section, in the *Getting Started* chapter of *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Note Desktop Chat is not supported with the unrestricted versions of IM&P.

Configure Desktop Chat Server Settings

Procedure

Step 1 Sign in to the administration console with the Application User credentials.

Step 2 In the **Desktop Chat Server Settings** area, enter the IM&P primary and secondary server URL of the Desktop Chat.

Step 3 Click **Save**.

Note
Desktop Chat requires Cisco Unified Presence 12.5 and higher versions.

Cloud Connect Server Settings

Cloud Connect is a component that hosts services that allow customers to use cloud capabilities such as Cisco Webex Experience Management. The administrator can configure the Cloud Connect server settings in the Finesse administration console to contact the Cisco cloud services.

For more information, see the Cisco Webex Experience Management Survey section in *Cisco Unified Contact Center Express Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-feature-guides-list.html.

The following table describes the fields on the Cloud Connect server settings gadget:

Field	Explanation
Username	(mandatory) The Cloud Connect administrator username required to sign in to Cloud Connect.
Password	(mandatory) The Cloud Connect administrator password required to sign in to Cloud Connect.
Publisher Address	(mandatory) The hostname of the Cloud Connect publisher.
Subscriber Address	(optional) The hostname of the Cloud Connect subscriber.

Actions on the Cloud Connect Server Settings gadget:

- **Save:** Saves your configuration changes.
- **Revert:** Retrieves the most recently saved Cloud Connect server settings.

Configure Cloud Connect Server Settings

Procedure

Step 1 Sign in to the administration console on the primary UCCX server using the URL: https://FQDN of Unified CCX server:8445/cfadmin.

Step 2 Select **Settings** > **Cloud Connect Server Settings**.

Step 3 Enter the **Username**, **Password**, and **Publisher Address** of the Cloud Connect server.

(optional) Enter the **Subscriber Address** for multinode deployment.

Step 4 Click **Save**.

Keyboard Shortcuts

Keyboard shortcuts provide an alternate way to perform a specific action on the Finesse agent and supervisor desktop. For more information, see *Access Keyboard Shortcuts* section in the *Cisco Finesse Agent and Supervisor Desktop User Guide*.

Keyboard Shortcut Conflicts

Keyboard shortcut conflicts occur if multiple gadgets use the same keyboard shortcut. This causes a particular key combination to be disabled until the conflict is resolved.

Keyboard shortcut conflicts at the page level can be resolved only by modifying the keyboard shortcuts at the gadget level. To modify the keyboard shortcuts at the gadget level, contact developer support services.

Keyboard shortcut conflict can occur in the following scenarios:

Conflict Scenario	Resolution
Conflicts can occur between keyboard shortcuts at the page level and gadget level.	This conflict cannot be resolved by the Finesse administrator.
Conflicts can occur when two gadgets have the same keyboard shortcut, and both are in the same tab.	Move one of the gadgets to another tab.
Conflicts can occur when there are multiple instances of the same gadget and focus is on the active tab*.	Move one of the gadgets to another tab.

* - Active tab refers to the tab that is currently being used.

The administrator can use the CLI command to disable the keyboard shortcuts for the Finesse agent and supervisor desktop. For more information on CLI commands, see *Desktop Properties*.

Note

- After deploying the third-party gadgets, the administrator must sign in as an agent and a supervisor to check if there are any keyboard shortcut conflicts and resolve them.
- The third-party gadget providers can use the keyboard shortcuts JavaScript library as a guideline to provide a consistent desktop user experience.

Manage Call Variables Layouts

Call Variables Layouts

You can use the Call Variables Layouts gadget to define how call variables appear on the Finesse agent desktop. You can configure up to 200 unique Call Variables Layouts (one default and 199 custom layouts). As part of this functionality:

- Each layout has a name (required) and description (optional).
- You can change the name and description of the default Call Variables Layout.
- You cannot delete the default Call Variables Layout.
- Finesse appends *(Default)* to the name of the default Call Variables Layout.
- To display a custom Call Variables Layout, in the Unified CCX routing script, set the user.layout ECC variable to the name of a configured Call Variables Layout. In this case, if no custom layouts match the user.layout value (or no custom layouts are configured), Finesse displays the default layout.

- Finesse retains the custom layout as specified by the user.Layout ECC variable on CTI server failover. During PG failover, Finesse changes the active call layout to the default layout while retaining the call variables and time indicators.

Call Variables

Each Call Variables Layout supports one variable in the header of the call control gadget and up to a total of 20 variables in two columns below the header (up to 10 in each column). You can use call variables, Extended Call Context (ECC) variables, or the following Outbound Option ECC variables:

- BACampaign
- BAAccountNumber
- BAResponse
- BAStatus
- BADialedListID
- BATimeZone
- BABuddyName

Columns can be empty.

The administrator can include the following additional fields in the Call Variables Layout. These variables appear as a drop-down list in the call variable gadget which the admin can assign to a layout.

- queueNumber
- queueName
- callKeyCallId
- callKeyPrefix
- callKeySequenceNum
- wrapUpReason

Note The callKeyPrefix indicates the day when the call was routed.

The callKeyCallId indicates the unique number for the call routed on that day.

To uniquely locate the call in Unified CCE database records, concatenate the two variables callKeyPrefix and callKeyCallId.

To enable Outbound Option data to appear in Cisco Finesse, the administrator must edit the Default Layout to include some or all Outbound Option variables.

Edit Call Variables

Administrator can set call variables (callVariable1 to callVariable10) values and ECC variable values as editable. Amongst BA (campaign-based outbound calls) variables, only BAResponse can be edited. The agent and the supervisor can edit the call variable values during an active call or in the wrap-up state.

Note

- Cisco Finesse refers to the ECC variable length from the AWDB and this length is validated while you edit the ECC variable. Cisco Finesse server takes about 15 minutes to update these changes from AWDB. Agents must sign in again for the ECC variable configuration changes to reflect in the Cisco Finesse desktop.
- Call variables edit operation updates the values of the variables within the particular call. All entities listening to dialog events receive the updated call variables through the Cisco Finesse notifications. If any CTI clients are connected to the same Agent PG, they also receive notifications of the changed call data though CTI call events. However, application scripts or databases that are used to populate the call variables are not directly affected by this edit.

Note Call variables edit operation updates the values of the variables within the particular call. All entities listening to dialog events receive the updated call variables through the Cisco Finesse notifications. If any CTI clients are connected to the same Agent PG, they also receive notifications of the changed call data though CTI call events. However, application scripts or databases that are used to populate the call variables are not directly affected by this edit.

Configure Call Variables Layouts

Procedure

Step 1 From the Manage Call Variables Layouts gadget:

- Click **New** to create a new Call Variables Layout.
- Choose a layout from the list and click **Edit** to modify an existing Call Variables Layout (or click **Delete** to remove it).

Step 2 Under **Create New Layout** (or under Edit <layout name> when editing an existing layout):

- Enter a name for the Call Variables Layout (maximum 40 characters).
- Enter a description of the Call Variables Layout (maximum 128 characters).

Step 3 Under Call Header Layout:

- Enter the display name that you want to appear in the header of the Call Control gadget on the Finesse desktop. For example, Customer Name (maximum 50 characters).
- From the drop-down list, choose the call variable or Outbound Option ECC variable that you want to appear in the header. For example, callVariable3 (maximum 32 characters).

Step 4 In the Call Body Left-Hand Layout and Call Body Right-Hand Layout areas:

a) Click **Add Row** to add a new row (or click the "X" to delete a row).
b) For each row:

- Enter the display name that you want to appear on the desktop. For example, Customer Name (maximum 50 characters).
- Enter the corresponding call variable or Outbound Option ECC variable from the drop-down list (maximum 32 characters).

Step 5 Select up to five call variables using the check box. The selected call variables are displayed in agent call popover and supervisor active call details.

Note
If you do not select any call variables, the first two call variables from the Call Body Left-Hand layout area will be displayed in the agent call popover and supervisor active call details. If there are no call variables in the Left-hand layout area, then the call variables in the Right-Hand Layout will be selected.

Step 6 Turn on the toggle switch to enable the edit option for a specific call variable. By default, this option is turned off.

Note
- Call variable (callVariable1 to callVariable10) values are editable.
- ECC variable values are editable.
- Amongst BA variables (campaign-based outbound calls), only BAResponse value is editable.

Step 7 Click **Save** to save the changes, or **Cancel** to discard the changes.

Note
When you modify the Call Variables Layout of the agent desktop, the changes you make take effect after three seconds. However, agents or supervisors who are signed in when the changes are made must sign out and sign back in to see those changes reflected on their desktops.

Step 8 To view the latest configured Call Variables Layout, click **Refresh** from the Manage Call Variables Layouts gadget.

Add ECC Variables to Call Variables Layout

Procedure

Step 1 In the header or the row where you want the ECC variable to appear, from the Variable drop-down list, choose **Custom**.

Step 2 In the Custom/ECC Variable Name field, enter the name of the ECC variable you want to appear on the agent desktop.

Step 3 Click **Set**.

The ECC variable now appears in the Variable drop-down list for selection.

Assign Call Variables Layouts

Procedure

Step 1 In Cisco Unified CCX Editor, open the script for which you want to assign ECC call variables.

Step 2 Select **Expanded Call Variables** from **Settings**.

Step 3 Click **New Variable** icon.

Step 4 Create a variable with "user" as prefix.

For example: userSSN

Step 5 In **Set Enterprise Call Info** step of the script, add or modify the **Expanded Call Variables**.

Manipulate Call Variables Layouts with a Workflow

You can manipulate the call variables layout that an agent sees when a call is answered by using a workflow. To do so, configure an HTTP Request workflow action and set the value of the ECC variable user. Layout to the name of the custom layout to display.

For information about how and when workflows are run, see **Workflows and Workflow Actions**.

For more details, see the section, "Adding an HTTP Request Workflow Action" in the technical paper *Cisco Finesse: How to Create a Screen-Pop Workflow*.

Manage Desktop Layout

You can define the layout of the Finesse desktop on the Desktop Layout tab.

Important Requirements, such as processor speed and RAM, for clients that access the Finesse desktop can vary. Desktops that receive events for more than one agent (such as agent and supervisor desktops running Live Data reports that contain information about other agents and skill groups) require more processing power than desktops that receive events for a single agent.

Factors that determine how much power is required for the client include, but are not limited to, the following:

- Contact center traffic
- Additional integrated gadgets in the desktop (such as Live Data reports or third-party gadgets)
- Other applications that run on the client and share resources with the Finesse desktop

Gadgets and Components

Gadgets

Cisco Finesse is an OpenSocial gadget, which is an XML document that defines metadata for an OpenSocial Gadget container. The gadgets are applications that are placed within the Cisco Finesse desktop. This helps

administrator to provide access to the contact center agents for all the applications that is required to service calls inside a single application.

Cisco Finesse comes with default gadgets such as, the team performance gadget, call control gadget, and call popover. JavaScript library is available for any customers with specific requirements that are not available out of the box.

Gadgets are listed in the desktop layout using the <gadget> tag.

Note Finesse Desktop is tested to perform well with an average of 20 gadgets per Desktop (across all tabs), over a sign in period of 8 minutes for 2000 users (agents and supervisors). When you increase the total number of gadgets that are configured on the Desktop, the CPU consumption marginally increases during users sign in. When all the configured gadgets are enabled for all the users, it impacts the Finesse server. Higher number of gadgets will also need more browser memory and network bandwidth.

If considerably larger number of gadgets are configured or if more users sign in (more than the tested number of users) in a short time frame, you must monitor the CPU consumption and network bandwidth during users sign in and ensure that the end-point devices have enough memory.

Failover uses optimization to sign in the users quickly and is not considered the same as a new browser sign in.

Third-party gadgets are hosted on the Cisco Finesse server using the `3rdpartygadget` web application or on an external web server. Gadgets can make REST requests to services hosted on external servers using the Cisco Finesse JavaScript Library API. To avoid browser cross-origin issues, REST requests are proxied through the backend Shindig web application. Third-party gadgets must implement their own authentication mechanisms for third-party REST services.

For more information about gadgets, see https://developer.cisco.com/docs/finesse/.

Components

Components are simple scripts that are loaded into the desktop directly at predefined positions as directed by the layout, without an enclosing frame and its document.

Components are introduced in the desktop to overcome a few rendering limitations and performance considerations inherent to gadgets.

The <component> tag lists the components in the desktop layout. Currently, the layout validations prevent creating custom components. Hence, default components are allowed in the desktop layouts. The default desktop functionalities are currently registered as components to provide flexibility and to reduce the load on the server.

Finesse Desktop Layout XML

The Finesse Layout XML defines the layout of the Finesse desktop, and the gadgets and components displayed on the desktop.

Use the Manage Desktop Layout gadget to upload an XML layout file to define the layout of the Finesse desktop for agents and supervisors.

Actions on the **Manage Desktop Layout** gadget are as follows.

- Edit the code using any of the following editors:

- **Text Editor**
- **XML Editor**

- **View Default Layout** - Displays the Cisco Finesse default layout.
- **Restore Default Layout** - Restores the Cisco Finesse desktop to the default layout.
- **Save** - Saves your configuration changes.
- **Revert** - Retrieves and applies the most recently saved desktop layout.

Default Layout XML

The Finesse default desktop layout XML for Unified CCX contains optional tabs and gadgets for Web Chat and Email, Advanced Supervisor Capabilities, and notes that describe how to modify the layout for your deployment type.

Remove the comments from the optional gadgets and tabs that you want to appear on the Finesse desktop.

Remove any gadgets or tabs that you do not want to use.

The **Manage Desktop Layout** supports the following types of editors:

- **Text Editor**—A plain text editor. It is the default editor. You can use the **Expand All** option to see all the code details and Search text box to refine your search results.
- **XML Editor**—An XML editor.

Note

- You cannot add or edit comments (<!-- and -->) in the **XML Editor**.
- In this document, all the examples that are related to desktop layout are applicable for text editor.

Both the editors support the following features:

- Expand and collapse option
- Syntax highlights and color code for the visual indication
- Auto-complete suggestions and hints for valid elements in the tags

Following are the updates available in the default layout XML in Unified CCX 12.5(1) release:

- Sample configurations for customizing desktop properties are added to the default layout (**Desktop Layout**) and team-specific layout (**Team Resources** > **Desktop Layout**).

  For upgraded layouts, sample configurations for customizing desktop properties do not appear by default. The administrator must copy the XML from the **View Default Layout** and add to the respective custom layouts.

- Horizontal Header is available in the layout configuration and the Header can be customised.
- Title and Logo of Finesse desktop can be customised.

- Desktop Chat, TeamMessage, Dialer, Agent Identity, and Non-Voice State Control are added as part of the header component.
- Vertical tabs in Finesse desktop are moved to collapsable left navigation bar for which the icons can be customised.
- Support for inbuilt java script components has been added.
- The **ID** attribute (optional) is the ID of the HTML DOM element used to display the gadget or component. The ID should start with an alphabet and can contain alpha numeric characters along with hyphen(-) and underscore(_).It can be set through the Finesse Administrative portal and has to be unique across components and gadgets.
- The **managedBy** attribute (optional) for Live Data gadgets defines the gadgets which manage these Live Data gadgets. The value of **managedBy** attribute for Live Data gadgets is **team-performance**. This means that the rendering of the gadget is managed by the Team Performance gadget. These gadgets are not rendered by default, but will be rendered when the options Show State History and Show Call History are selected in the Team Performance gadget.

  For upgraded layouts, the **managedBy** attribute will be introduced, and will have the value of the **ID** of the Team Performance gadget in the same tab. If there are multiple instances of Team Performance gadgets and Live Data gadget pairs, they will be associated in that order. If the **ID** of the Team Performance gadget is changed, the value of the **managedBy** attribute should also be updated to reflect the same **ID** for the Live Data gadgets. Otherwise, the Team Performance gadget instance will not show its respective Live Data gadgets.
- The **Hidden** attribute (optional) is used to support headless gadgets. When an attribute is set to "hidden=true", then the gadget is loaded by the container, but will not be displayed. The default value set for the attribute is "false".
- The **maxRow** attribute (optional) is used to adjust the height of the Team Performance gadget. If there are multiple instances of the Team Performance gadget, each instance height can be set by using this attribute. By default the **maxRow** attribute value is set to 10 rows.
- Agents can view Recent Call History and Recent State History gadgets in the My History tab.
- Supervisors can view Recent Call History and Recent State History gadgets in the My History tab.

Important After a system upgrade, the old desktop layout is retained. If you had a modified desktop layout before upgrade, perform the following steps to ensure you obtain the latest changes:

- Sign in to the Finesse administration console and click the **Desktop Layout** tab.
- Copy the desktop layout to a text file.
- On the Manage Desktop Layout gadget, click **Restore Default Layout**.
- Click **Save**.
- Using the text file of the desktop layout that you saved before the upgrade as a reference, modify the layout to include the changes that you made to the previous layout.
- Click **Save** to save your changes.

If any changes are made to the component IDs or URLs in the default XML layout, the following features may not work as expected.

Note The components can be rearranged in any order to show on the Finesse desktop.

Feature	Component ID	URL
Title and Logo	cd-logo	<url>/desktop/scripts/js/logo.js</url>
Voice State control	agent-voice-state	<url>/desktop/scripts/js/agentvoicestate.component.js</url>
Non-voice state control	nonvoice-state-menu	<url>/desktop/scripts/js/nonvoice-state-menu.component.js</url>
Team Message	broadcastmessagepopover	<url>/desktop/scripts/js/teammessage.component.js</url>
Desktop Chat	chat	<url>/desktop/scripts/js/chat.component.js</url>
Dialer	make-new-call-component	<url>/desktop/scripts/js/makenewcall.component.js</url>
Agent identity	identity-component	<url>/desktop/scripts/js/identity-component.js</url>

Update Default Desktop Layout

When you modify the layout of the Finesse desktop, the changes you make take effect on the desktop after 3 seconds. However, agents who are signed in when the changes are made must sign out and sign in again to see those changes reflect on the desktop.

Note The call control gadget is only supported at the page level. You must ensure that the call control gadget (<gadget>/desktop/scripts/js/callcontrol.js</gadget>) is placed within the <page></page> tag for it to work correctly. Don't place this gadget within a <tab></tab> tag.

The version tag of Desktop Layout XML can’t be edited.

For the changes to take effect, refresh the page, or sign out and sign in again into Cisco Finesse.

Procedure

Step 1 Click **Desktop Layout**.

Step 2 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 3 Make changes to the XML as required.

Example:

If you want to add a new tab called Reports, add the following XML within the tabs tags under the <role>Agent</role> tag:

```
<tab>
   <id>reports</id>
   <icon>Reports</icon>
   <label>Reports</label>
</tab>
```

If you want to add this tab to the supervisor desktop, add the XML within the tabs tags under the <role>Supervisor</role> tag.

To add a gadget to a tab, add the XML for the gadget within the gadgets tag for that tab.

```
<gadgets>
<gadget>https://<ipAddress>/gadgets/<gadgetname>.xml</gadget>
</gadgets>
```

Replace <ipAddress> with the IP address of the server where the gadget resides.

If you want to add multiple columns to a tab on the Finesse desktop, add the gadgets for each column within the columns tags for that tab. You can have up to four columns on a tab.

```
<tabs>
    <tab>
        <id>home</id>
        <icon>home</icon>
        <label>finesse.container.tabs.agent.homeLabel</label>
        <columns>
            <column>
                <gadgets>
                    <gadget>/desktop/scripts/js/queueStatistics.js</gadget>
                </gadgets>
            </column>
        </columns>
    </tab>
    <tab>
        <id>myHistory</id>
        <icon>history</icon>
        <label>finesse.container.tabs.agent.myHistoryLabel</label>
        <columns>
            <column>
                <!-- The following gadgets are used for viewing the call history
and state history of an agent. -->
            </column>
        </columns>
    </tab>
```

Step 4 Click **Save**.

Finesse validates the XML file to ensure that it's valid XML syntax and conforms to the Finesse schema.

Step 5 After you save your changes, if you want to revert to the last saved desktop layout, click **Revert**. If you want to revert to the default desktop layout, click **Restore Default Layout**.

Note
During upgrade, any changes made to the Cisco Finesse Default Layout won't be updated. Click on **Restore Default Layout** to get the latest changes.

The Finesse default XML layout is as follows:

```
<finesseLayout xmlns="http://www.cisco.com/vtg/finesse">
    <!--  DO NOT EDIT. The version number for the layout XML. -->
    <version>1250.03</version>
    <configs>
        <!-- The Title for the application which can be customized. -->
        <config key="title" value="Cisco Finesse"/>
       <!-- The following entries are examples of changing defaults for desktop properties.

       To change any property, uncomment the respective line and set the appropriate value.

      For more details on the properties that can be customized, refer to the Cisco Finesse
 Administration Guide.
       Note: The customized properties can only be set in the configs section and are not
 role-specific. -->
        <!-- <config key="enableDragDropAndResizeGadget" value="false"/> -->
        <!-- <config key="wrapUpCountDown" value="true"/> -->
        <!-- <config key="desktopChatAttachmentEnabled" value="true"/> -->
        <!-- <config key="forceWrapUp" value="true"/> -->
        <!-- Possible Values: supervisor_only, conference_controller_and_supervisor, all
-->
        <!-- <config key="enableDropParticipantFor" value="supervisor_only"/> -->
        <!-- Possible Values: agents, all -->
        <!-- <config key="dropParticipant" value="agents"/> -->
        <!-- The logo file for the application -->
        <!-- For detailed instructions on using custom icons for logos and tabs,
        please refer to the section "Customize Title and Logo in the Header"
        in the Finesse Administration Guide. -->
        <!-- <config key="logo" value="/3rdpartygadget/files/cisco_finext_logo.png"/>  -->
    </configs>
    <header>
        <!--  Please ensure that at least one gadget/component is present within every
headercolumn tag -->
  <leftAlignedColumns>
   <headercolumn width="300px">
    <component id="cd-logo">
     <url>/desktop/scripts/js/logo.js</url>
    </component>
   </headercolumn>
   <headercolumn width="230px">
    <component id="agent-voice-state">
     <url>/desktop/scripts/js/agentvoicestate.component.js</url>
    </component>
   </headercolumn>
   <headercolumn width="251px">
    <component id="nonvoice-state-menu">
     <url>/desktop/scripts/js/nonvoice-state-menu.component.js</url>
    </component>
   </headercolumn>

  </leftAlignedColumns>
  <rightAlignedColumns>
   <headercolumn width="50px">
               <component id="broadcastmessagepopover">
                   <url>/desktop/scripts/js/teammessage.component.js</url>
               </component>
           </headercolumn>
   <headercolumn width="50px">
               <component id="chat">
                   <url>/desktop/scripts/js/chat.component.js</url>
               </component>
           </headercolumn>
```

```
  <headercolumn width="50px">
   <component id="make-new-call-component">
    <url>/desktop/scripts/js/makenewcall.component.js</url>
   </component>
  </headercolumn>
  <headercolumn width="72px">
   <component id="identity-component">
    <url>/desktop/scripts/js/identity-component.js</url>
   </component>
  </headercolumn>
 </rightAlignedColumns>
</header>
   <layout>
       <role>Agent</role>
       <page>
           <gadget>/desktop/scripts/js/callcontrol.js</gadget>

           <!-- The following gadget is for WXM Customer Experience Journey.
           If WXM is onboarded successfully with all configurations, then replace the url

          with the actual url obtained by exporting the Cisco Finesse gadget from WXM -->

           <!-- <gadget>/3rdpartygadget/files/CXService/CiscoCXJourneyGadget.xml</gadget>
 -->
       </page>
       <tabs>
           <tab>
               <id>home</id>
               <icon>home</icon>
               <label>finesse.container.tabs.agent.homeLabel</label>
               <columns>
                   <column>
                       <gadgets>
                           <!-- The following gadget is for recording and displaying Call
 Transcripts.
                           If Voicea is onboarded successfully and all configuration done
 correctly then uncomment this gadget-->
                           <!--
<gadget>/3rdpartygadget/files/calltranscript/CallTranscriptGadget.xml</gadget> -->

                           <!-- The following gadget is for WXM Customer Experience
Analytics.
                           If WXM is onboarded successfully with all configurations, then
 replace the url
                           with the actual url obtained by exporting the Cisco Finesse
gadget from WXM -->
                           <!--
<gadget>/3rdpartygadget/files/CXService/CiscoCXAnalyticsGadget.xml</gadget> -->

                           <gadget>/desktop/scripts/js/queueStatistics.js</gadget>

                           <!--
               The following Gadgets are for LiveData.
               If you wish to show LiveData Reports, then do the following:
                   1) Uncomment each Gadget you wish to show.
                 2) Replace all instances of "my-cuic-server.com" with the Fully Qualified
 Domain Name of your Intelligence Center Server.
                   3) [OPTIONAL] Adjust the height of the gadget by changing the
"gadgetHeight" parameter.
               IMPORTANT NOTES:
                   - In order for these Gadgets to work, you must have performed all
documented pre-requisite steps.
                 - Do *NOT* change the viewId (unless you have built a custom report and
 know what you are doing).
```

```
                    - The "teamName" will be automatically replaced with the Team Name of
the User logged into Finesse (for Team-specific layouts).
-->
                            <!-- HTTPS Version of LiveData Gadgets -->
                            <!-- TEAM STATUS REPORTS: 1. Agent Default view (default), 2.
Agent Skill Group Default view -->
                            <!--
<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;


viewId_1=99E6C8E2100001410000000D80A0006C4&amp;filterId_1=agent.id=CL%20teamName&amp;viewId_2=9AB7848B10000141000001C50A0006C4&amp;

                           filterId_2=agent.id=CL%20teamName</gadget> -->
                          <!-- QUEUE STATUS REPORTS: 1. Skill Group Default view (default),
 2. Skill Group Utilization view, 3. Precision Queue Default view, 4. Precision Queue
Utilization view -->
                            <!--
<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;


viewId_1=B7371BE210000144000002870A0007C5&amp;filterId_1=skillGroup.id=CL%20teamName&amp;

viewId_2=9E760C8B1000014B0000005A0A0006C4&amp;filterId_2=skillGroup.id=CL%20teamName&amp;

viewId_3=B71A630C10000144000002480A0007C5&amp;filterId_3=precisionQueue.id=CL%20teamName&amp;


viewId_4=286B86F01000014C000005330A0006C4&amp;filterId_4=precisionQueue.id=CL%20teamName</gadget>
 -->
                        </gadgets>
                    </column>
                </columns>
            </tab>
            <tab>
                <id>myStatistics</id>
                <icon>column-chart</icon>
                <label>finesse.container.tabs.agent.myStatisticsLabel</label>
                <columns>
                    <column>
                        <gadgets>

<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=150&amp;


viewId=0B8D11317ED54A80B64F3AE28C5139E5&amp;filterId=agentStats.id=CL%20teamName</gadget>
                        </gadgets>
                    </column>
                </columns>
            </tab>
            <tab>
                <id>myHistory</id>
                <icon>history</icon>
                <label>finesse.container.tabs.agent.myHistoryLabel</label>
                <columns>
                    <column>
                        <!-- The following gadgets are used for viewing the call history
and state history of an agent. -->
                        <gadgets>

<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=280&amp;


viewId=5FA44C6F930C4A64A6775B21A17EED6A&amp;filterId=agentTaskLog.id=CL%20teamName</gadget>
```

```
<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=280&amp;

viewId=56BC5CCE8C37467EA4D4EFA8371258BC&amp;filterId=agentStateLog.id=CL%20teamName</gadget>

                        </gadgets>
                    </column>
                </columns>
            </tab>
            <!--
The following Gadgets are for LiveData.
If you wish to show More LiveData Reports, then do the following:
    1) Uncomment each Gadget you wish to show.
    2) Replace all instances of "my-cuic-server.com" with the Fully Qualified Domain Name
of your Intelligence Center Server.
    3) [OPTIONAL] Adjust the height of the gadget by changing the "gadgetHeight" parameter.
IMPORTANT NOTES:
   - In order for these Gadgets to work, you must have performed all documented pre-requisite
 steps.
    - Do *NOT* change the viewId (unless you have built a custom report and know what you
are doing).
    - The "teamName" will be automatically replaced with the Team Name of the User logged
into Finesse (for Team-specific layouts).
-->
            <!-- If you are showing the "More Live Data Reports" tab, then also uncomment
this section.
            <tab>
                <id>moreLiveDataReports</id>
                <icon>reports-more</icon>
                <label>finesse.container.tabs.agent.moreLiveDataReportsLabel</label>
                <gadgets>
-->
            <!-- HTTPS Version of LiveData Gadgets -->
            <!-- AGENT REPORTS: 1. Agent Default view (default) -->
            <!--
<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;

viewId_1=99E6C8E210000141000000D80A0006C4&amp;filterId_1=agent.id=CL%20teamName</gadget>-->

           <!-- AGENT SKILL GROUP REPORTS: 1. Agent Skill Group Default view (default) -->

            <!--
<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;

viewId_1=9AB7848B10000141000001C50A0006C4&amp;filterId_1=agent.id=CL%20teamName</gadget>-->

            <!-- QUEUE STATUS SKILL GROUP REPORTS: 1. Skill Group Default view (default),
2. Skill Group Utilization view -->
            <!--
<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;

viewId_1=B7371BE2100001440000002870A0007C5&amp;filterId_1=skillGroup.id=CL%20teamName&amp;

viewId_2=9E760C8B1000014B0000005A0A0006C4&amp;filterId_2=skillGroup.id=CL%20teamName</gadget>-->

            <!-- QUEUE STATUS PRECISION QUEUE REPORTS: 1. Precision Queue Default view
(default), 2. Precision Queue Utilization view -->
            <!--
<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;
```

```
viewId_1=B71A630C10000144000002480A0007C5&amp;filterId_1=precisionQueue.id=CL%20teamName&amp;

viewId_2=286B86F01000014C000005330A0006C4&amp;filterId_2=precisionQueue.id=CL%20teamName</gadget>-->

            <!-- If you are showing the "more reports" tab, then uncomment this section
too.
                </gadgets>
            </tab>
            -->
        </tabs>
    </layout>
    <layout>
        <role>Supervisor</role>
        <page>
            <gadget>/desktop/scripts/js/callcontrol.js</gadget>

            <!-- The following gadget is for WXM Customer Experience Journey.
            If WXM is onboarded successfully with all configurations, then replace the url

           with the actual url obtained by exporting the Cisco Finesse gadget from WXM -->

            <!-- <gadget>/3rdpartygadget/files/CXService/CiscoCXJourneyGadget.xml</gadget>
 -->
        </page>
        <tabs>
            <tab>
                <id>home</id>
                <icon>home</icon>
                <label>finesse.container.tabs.supervisor.homeLabel</label>
                <columns>
                    <column>
                        <gadgets>
                           <!-- The following gadget is for recording and displaying Call
Transcripts.
                            If Voicea is onboarded successfully and all configuration done
 correctly then uncomment this gadget-->
                            <!--
<gadget>/3rdpartygadget/files/calltranscript/CallTranscriptGadget.xml</gadget> -->

                            <!-- The following gadget is for WXM Customer Experience
Analytics.
                            If WXM is onboarded successfully with all configurations, then
 replace the url
                            with the actual url obtained by exporting the Cisco Finesse
gadget from WXM -->
                            <!--
<gadget>/3rdpartygadget/files/CXService/CiscoCXAnalyticsGadget.xml</gadget> -->

                            <gadget
id="team-performance">/desktop/scripts/js/teamPerformance.js</gadget>
                          <!-- The following gadgets are used for viewing the call history
 and state history of an agent selected in the Team Performance Gadget. -->
                            <!-- The following gadgets are managed(loaded and displayed)
by the team performance gadget (associated with id "team-performance").
                                 This association is done using the mapping of managedBy
attribute of the managed gadgets, to the id of managing gadget.
                                 If the id for team performance gadget is changed, the
values for the associated managedBy attribute
                                 for the managed gadgets, also need to be updated with the
 new id.
                                 These managed gadgets are not displayed by default, but
would be displayed when the option
```

```
                                    "view history" is selected, for an agent, in the team
performance gadget.
                                    Note: As managed gadgets are not displayed by default,
placing managed gadgets alone on
                                    separate columns of their own, would display blank space
in that area.
                                For more details on managed gadgets and managedBy attribute,
 please refer to Finesse Administration Guide.
                                -->
                                <gadget
managedBy="team-performance">https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=275&amp;

viewId=630CB4C96B0045D9BFF295A49A0BA45E&amp;filterId=agentTaskLog.id=AgentEvent:Id&amp;type=dynamic&amp;maxRows=20</gadget>

                                <gadget
managedBy="team-performance">https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=275&amp;

viewId=56BC5CCE8C37467EA4D4EFA8371258BC&amp;filterId=agentStateLog.id=AgentEvent:Id&amp;type=dynamic&amp;maxRows=20</gadget>

                        </gadgets>
                    </column>
                </columns>
            </tab>
            <tab>
                <id>myHistory</id>
                <icon>history</icon>
                <label>finesse.container.tabs.agent.myHistoryLabel</label>
                <columns>
                    <column>
                        <!-- The following gadgets are used for viewing the call history
and state history of a logged in supervisor. -->
                        <gadgets>

<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=280&amp;

viewId=5FA44C6F930C4A64A6775B21A17EED6A&amp;filterId=agentTaskLog.id=CL%20teamName</gadget>

<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=280&amp;

viewId=56BC5CCE8C37467EA4D4EFA8371258BC&amp;filterId=agentStateLog.id=CL%20teamName</gadget>

                        </gadgets>
                    </column>
                </columns>
            </tab>
            <tab>
                <id>teamData</id>
                <icon>team-data</icon>
                <label>finesse.container.tabs.supervisor.teamDataLabel</label>
                <columns>
                    <column>
                        <!-- The following gadget is used by the supervisor to view an
agent's queue interval details. -->
                        <gadgets>

<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;

viewId=0B8D11317ED54A80B64F3AE28C5139E5&amp;filterId=agentStats.id=CL%20teamName</gadget>
```

```
<gadget>https://my-cuic-server.com:8444/cuic/gadget/Historical/HistoricalGadget.jsp?viewId=BD9A8B7DBE714E7EB758A9D472F0E7DC&amp;

linkType=htmlType&amp;viewType=Grid&amp;refreshRate=900&amp;@start_date=RELDATE%20THISWEEK&amp;

@end_date=RELDATE%20THISWEEK&amp;@agent_list=CL%20~teams~&amp;gadgetHeight=360</gadget>
                        </gadgets>
                    </column>
                </columns>
            </tab>
            <tab>
                <id>queueData</id>
                <icon>storage</icon>
                <label>finesse.container.tabs.supervisor.queueDataLabel</label>
                <columns>
                    <column>
                        <gadgets>
                            <gadget>/desktop/scripts/js/queueStatistics.js</gadget>
                        </gadgets>
                    </column>
                </columns>
            </tab>

        </tabs>
    </layout>
</finesseLayout>
```

Drag-and-Drop and Resize Gadget or Component

The administrator can configure the drag-and-drop and resize gadget or component features for agents and supervisors to customize their Finesse desktop.

- The drag-and-drop feature allows agents and supervisors to drag (and drop) the gadget or the component to the required position on the desktop layout.
- The resize feature allows the agents and supervisors to shrink or expand the gadget or the component to a custom size on the desktop layout.

Note By default, the drag-and-drop and resize features are disabled. The administrator must set the `enableDragDropAndResizeGadget` desktop property value as *true* to enable these features.

The administrator can customize the desktop property value of these features through the desktop layout:

- Default layout (**Desktop Layout**)—In the **Text Editor**, remove the comment (<!—and -->) from the `enableDragDropAndResizeGadget` code snippet and enter the value as *true* to add these features to the desktop layout. For more information, see Customize Desktop Properties, on page 389.

  The following is the sample code snippet, as displayed in the default **Desktop Layout**.

  ```
  <!-- <config key="enableDragDropAndResizeGadget" value="false"/> -->
  ```

- Team-specific layouts (**Manage Team Resources** > **Desktop Layout**)—Select a specific team and then in the **Text Editor**, remove the comment (<!—and -->) from the `enableDragDropAndResizeGadget` code snippet and enter the value as *true* to add these features to the team desktop layout. For more information, see Customize Desktop Properties at Team Level, on page 447.

The following is the sample code snippet, as displayed in the team **Desktop Layout**.

```
<!-- <config key="enableDragDropAndResizeGadget" value="false"/> -->
```

Note

- For upgraded layouts, the sample configuration for customizing desktop property (`enableDragDropAndResizeGadget`) doesn't appear by default in the **Desktop Layout**. Administrators must copy the XML from the **View Default Layout** and add to the respective custom layouts.
- For new layouts, the sample configuration for customizing desktop property (`enableDragDropAndResizeGadget`) appears by default in the **Desktop Layout**.
- The administrator can also use the CLI and set the **utils finesse set_propertydesktop enableDragDropAndResizeGadget** to *true* to enable these features. For more information see *Desktop Properties*.
-
- If the property value is defined in the team-specific desktop layout (**Manage Team Resources** > **Desktop Layout**), the team-specific desktop layout takes precedence over the property value defined in the **Desktop Layout** and CLI.
- These features aren't applicable for gadgets that don't have a defined title. For more information, see the *Gadget Limitations* section in the *Cisco Finesse Web Services Developer Guide* at https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide.

Customize Desktop Properties

You can customize the Finesse desktop properties.

Procedure

Step 1 Click **Desktop Layout**.

Step 2 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 3 Enter the desktop property name in the config key tag.

Step 4 Enter the possible value of the desktop property in the value tag.

The following are the sample desktop property entries, as displayed in the default **Desktop Layout**. To change these desktop property entries in **Text Editor**, remove the comment (<!-- and -->) and set appropriate values.

Note
If the property value is defined in the **Desktop Layout**, then the **Desktop Layout** value takes precedence over the property value defined using the CLI. For more information on Finesse CLIs, see *Desktop Properties*.

The following table lists the supported desktop properties:

Config Key	Value	Default Value
enableDragDropAndResizeGadget	true|false	false
enableShortCutKeys	true|false	true
forceWrapUp	true|false	true
wrapUpCountDown	true|false	true
showWrapUpTimer	true|false	true
desktopChatAttachmentEnabled	true|false	true
desktopChatMaxAttachmentSize	Range: 1—10 (MB)	5
desktopChatUnsupportedFileTypes	Unsupported file formats include comma-separated valid file extensions. For example: .exe, .sh	.exe, .msi, .sh, .bat
showAgentHistoryGadgets	true|false	true
showActiveCallDetails (for Supervisor Only)	true|false	true
pendingDTMFThresholdCount	Range: 1—20	20
dtmfRequestTimeoutInMs	Range: 1000—200000 (1 to 200 seconds)	5000 (5 seconds)
enableDropParticipantFor	supervisor_only|conference_controller_ and_supervisor|all	supervisor_only
dropParticipant	agents|all	agents

Note

- To enable the following Finesse desktop properties in Cisco Finesse, install Cisco Finesse Release 12.5(1) ES1 COP or higher.
  - pendingDTMFThresholdCount
  - dtmfRequestTimeoutInMs
- To enable the following Finesse desktop properties in Cisco Finesse, install Cisco Finesse Release 12.5(1) ES4 COP or higher.
  - enableDropParticipantFor
  - dropParticipant

For more information on Finesse desktop properties, see *Desktop Properties*.

Step 5 Click **Save**.

The change takes effect when the agent or supervisor refreshes the Finesse desktop or sign out and sign in again.

Note
If you clear the **Override System Default** check box and click **Save**. The changes are overwritten, and the editing pane reverts to the default desktop layout XML.

Horizontal Header

The Horizontal Header on the Finesse desktop has the following components from left to right. All these components can be removed and replaced with custom gadgets as required.

- **Logo:** Default is Cisco logo. Can be customized.
- **Product Name:** Default is Cisco Finesse. Can be customized.
- **Agent State for Voice:** Displays agent state for voice call.
- **Agent State for Digital Channels:** Displays agent state for digital channels.
- **Dialer Component:** Agent can make a new call.
- **Identity Component:** Displays agent name and signout functionality with reason codes.

Note The sum of widths set for all gadgets and components in the header (inside right aligned columns and left aligned colums) should not exceed the total header width. If it exceeds the header width, some of the gadgets/components will not be visible.

Customize Title and Logo in the Header

You can customize the title and logo displayed on the Finesse desktop:

Procedure

Step 1 Click **Desktop Layout**.

Step 2 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 3 Enter the product name in the config value tag with title key.

Step 4 Upload the logo file just like any third-party gadget.

For more information, see section *Upload Third-Party Gadgets* in *Cisco Finesse Admin Guide*.

Step 5 Enter the URL of the logo file in the config value tag with logo key.

Example:

```
<configs>
        <!-- The Title for the application which can be customised.-->
<config value="product.full-name" Key="title"/>
     <!-- The logo file for the application-->
```

```
    <!--<config key="logo" value="/3rdpartygadgets/<some_sample_image>"/-->
</configs>
```

The customized logo and product name is displayed on the Finesse desktop.

Note The file size that can be uploaded for the logo must be kept within 40 pixels. The file types supported are .svg, .png, .gif, and .jpeg/jpg.

alternateHosts Configuration

The <gadget> element in the Finesse Layout XML provides an attribute to specify alternate hosts from which the gadget can be loaded. This allows the Cisco Finesse desktop to load the gadget using a different host if the primary server is unavailable.

The **alternateHosts** attribute contains a comma-separated list of FQDNs that will be used if the primary-host-FQDN is unavailable.

```
<gadget alternateHosts="host1,host2,host3,...">
        https://<primary-host-FQDN>/<gadget-URL>
    </gadget>
```

The **alternateHosts** attribute is only applicable for gadgets with an absolute URL. That is URLs containing the FQDN of a host, an optional port, and the complete URL path to the gadget. For example: <gadget alternateHosts="host1,host2">*https://primary host/relative_path*</gadget>

If loading the gadget from the primary-host fails, the Cisco Finesse container attempts to load the gadget from the alternate hosts in the order specified in the **alternateHosts** attribute.

The Cisco Finesse desktop may fail to load the gadget even if some of the hosts are reachable. In such cases, refresh the Cisco Finesse desktop.

When the gadget is specified with a relative URL, for example: <*gadget*>*/3rdpartygadgets/relative_path*</*gadget*>, the **alternateHosts** attribute does not apply and is ignored by the Cisco Finesse desktop.

Note If the host serving the gadget fails after the Cisco Finesse desktop was successfully loaded, the desktop must be refreshed in order to load the gadget from an alternate host. The gadget does not implement its own failover mechanism.

Headless Gadget Configuration

Headless gadgets are gadgets which do not need a display space, but can be loaded and run like a background task in the browser. The **Hidden** attribute (optional) is used to support headless gadgets in the layout XML. When an attribute is set to "hidden=true", then the gadget is loaded by the container, but will not be displayed. The default value set for the attribute is "false".

Customize Icons in Left Navigation Bar

You can add icons (both custom and inbuilt) to the collapsible left navigation bar of the Finesse desktop:

Procedure

Step 1 Click **Desktop Layout**.

Step 2 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 3 Enter name of the gadget or component in the id tag.

Step 4 Enter the value of the icon in the icon tag.

Step 5 Upload the icon file just like any third-party gadget.

For more information, see section *Upload Third-Party Gadgets* in *Cisco Finesse Admin Guide*.

Note
When adding a custom icon, provide the path in the icon tag and if you are adding an inbuilt icon, provide the icon value in the icon tag

Example:

Note
The file size that can be uploaded in the left navigation bar as custom icons is 25 pixels by 25 pixels. The maximum width of the tab title in the left navigation bar must be 80 pixels or less. The file types supported are .svg, .png, .gif, and .jpeg/jpg.

Customize Icons for Gadgets

As part of the Cisco Finesse container, various standard icons are available. Use the following procedure to customize the icons for the gadgets hosted in Finesse desktop.

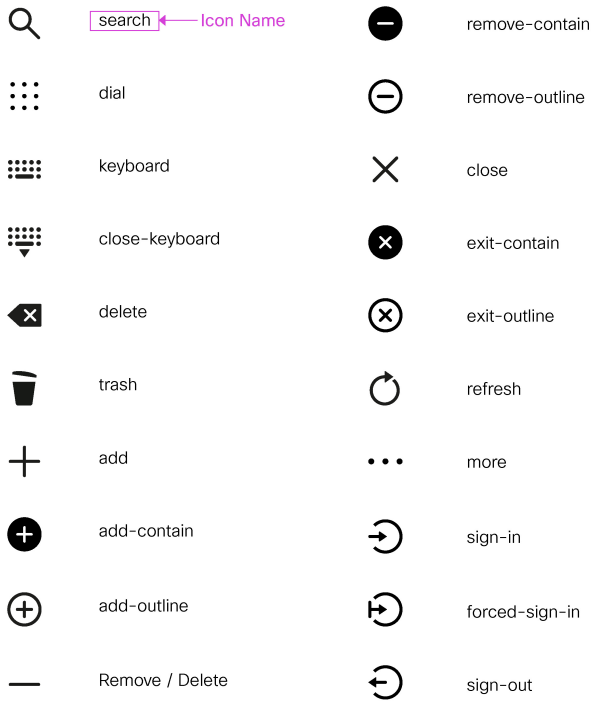
Procedure

Step 1 Click **Desktop Layout**.

Step 2 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 3 Enter the value of the icon in the icon tag. Get the icon name from the List of Icons, on page 395. The icon name is located on the right of the icon image. For example, search.



Note
Icon name is case sensitive. Enter the icon name exactly as displayed in the List of Icons, on page 395.

Example

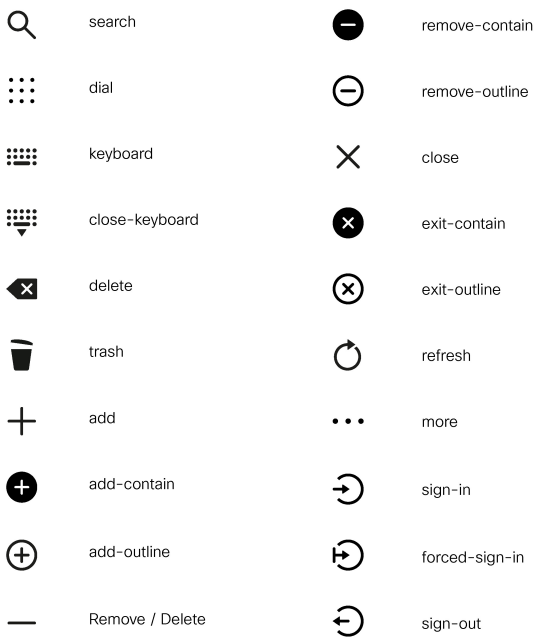
An example of the desktop layout using the *Search* and *Close-Keyboard* icons.

```
<tab>
    <id>home</id>
    <icon>search</icon>
    <label>finesse.container.tabs.agent.homeLabel</label>
    <columns>
        <column>
            <gadgets>
                <gadget>/desktop/scripts/js/queueStatistics.js</gadget>
            </gadgets>
        </column>
    </columns>
</tab>
<tab>
    <id>sample</id>
    <icon>close-keyboard</icon>
    <label>finesse.container.tabs.agent.homeLabel2</label>
    <columns>
        <column>
            <gadgets>
                <gadget>/desktop/scripts/js/samplequeue.js</gadget>
            </gadgets>
        </column>
```

```
    </columns>
</tab>
```

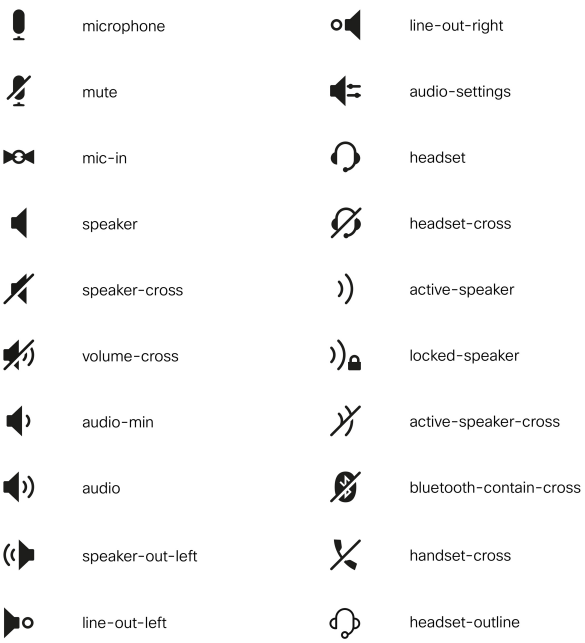
List of Icons

The following are the icons for Actions.



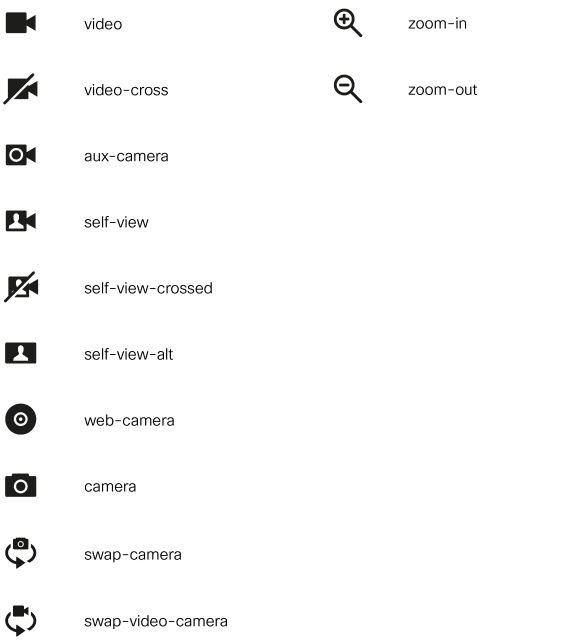
510879

The following are the icons for Audio.



510880

The following are the icons for Camera.

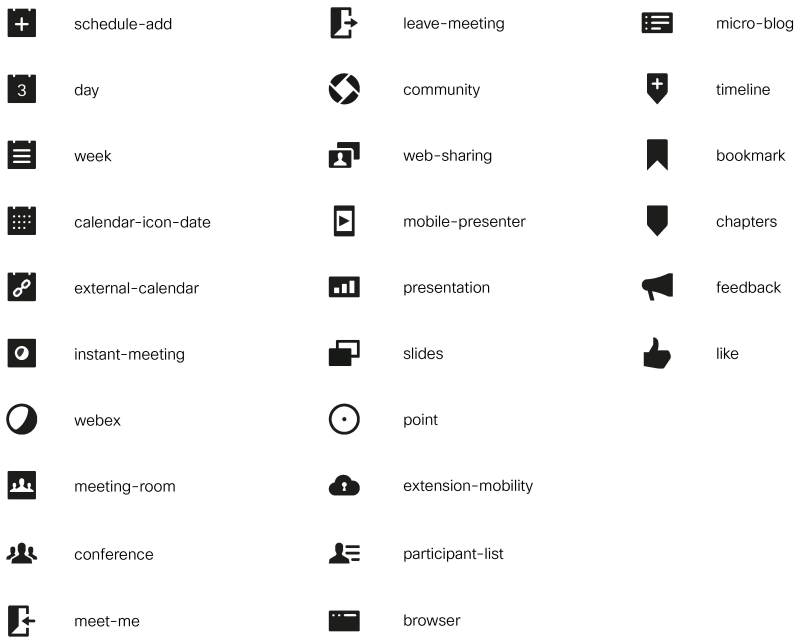


510881

The following are the icons for Chat.

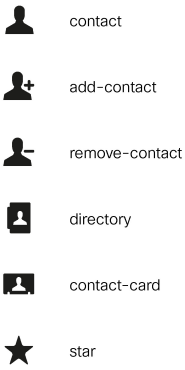
510882

The following are the icons for Collaboration.



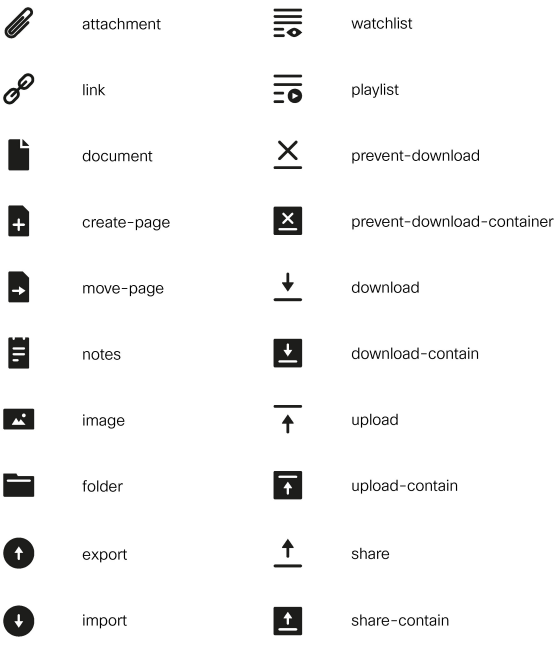
510883

The following are the icons for Contacts.



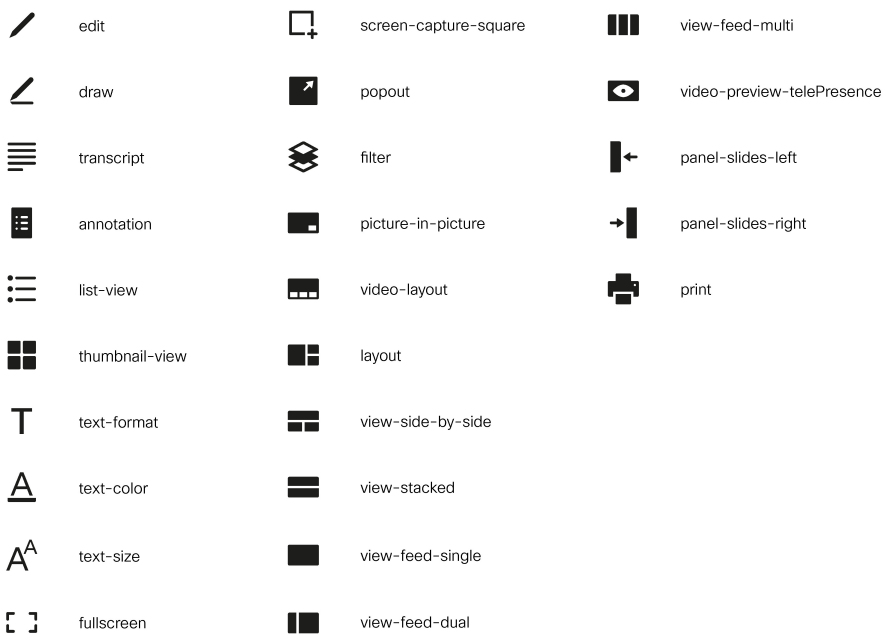
510884

The following are the icons for Content.



510885

The following are the icons for Editor.



510886

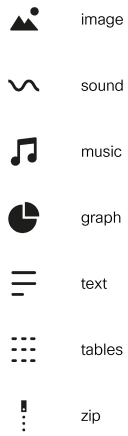
The following are the icons for Email.

510887

The following are the icons for Hardware.

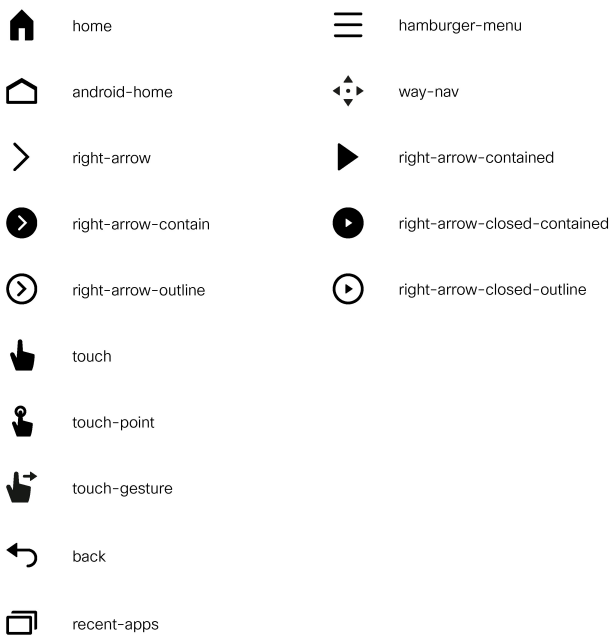
510888

The following are the icons for Media.



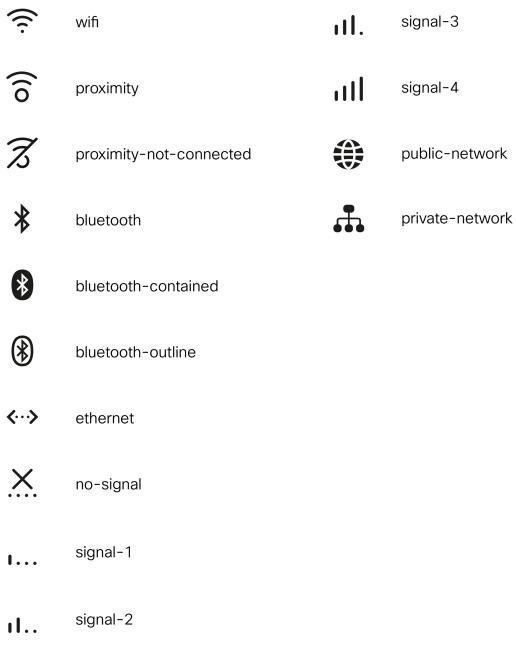
510889

The following are the icons for Navigation.



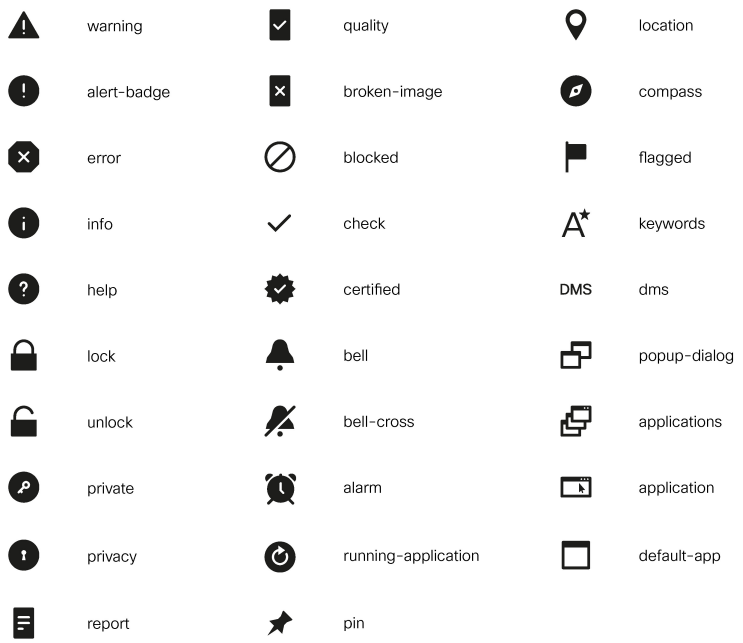
510890

The following are the icons for Network.



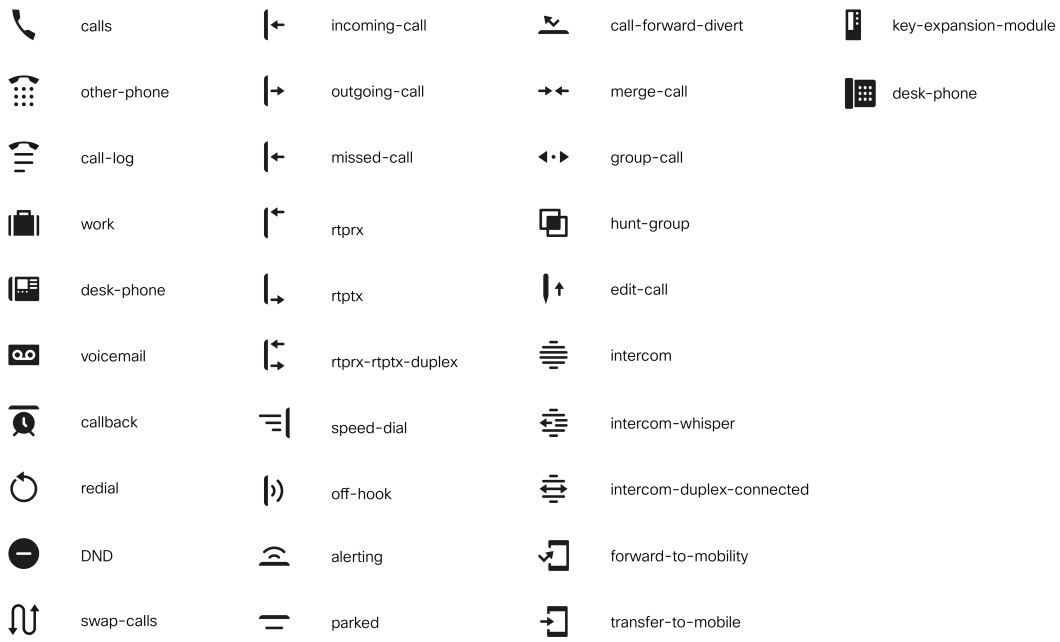
510891

The following are the icons for Notifications and Alerts.



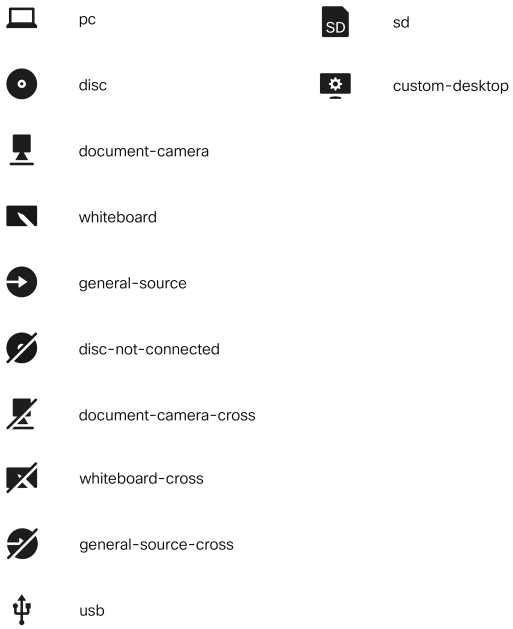
510892

The following are the icons for Phone.



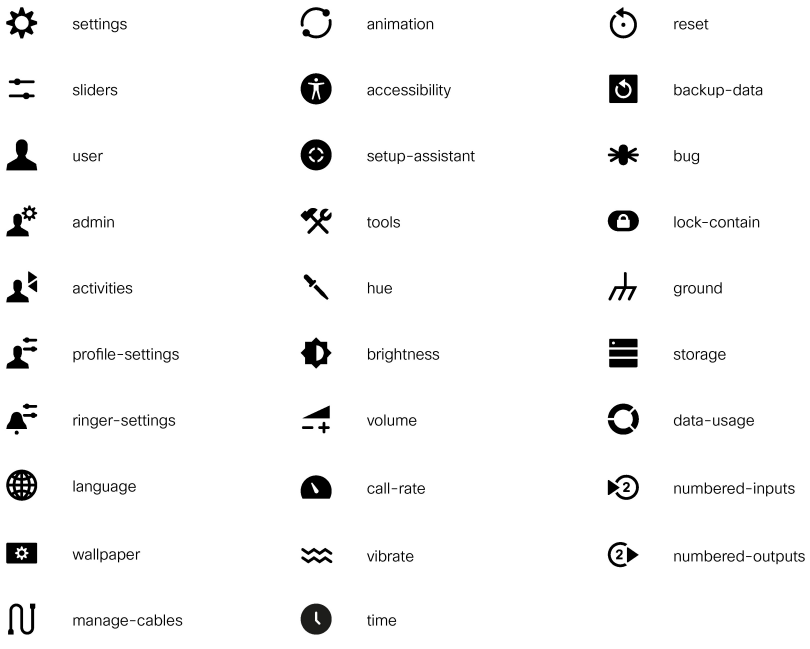
510893

The following are the icons for Sources.



510894

The following are the icons for Settings.

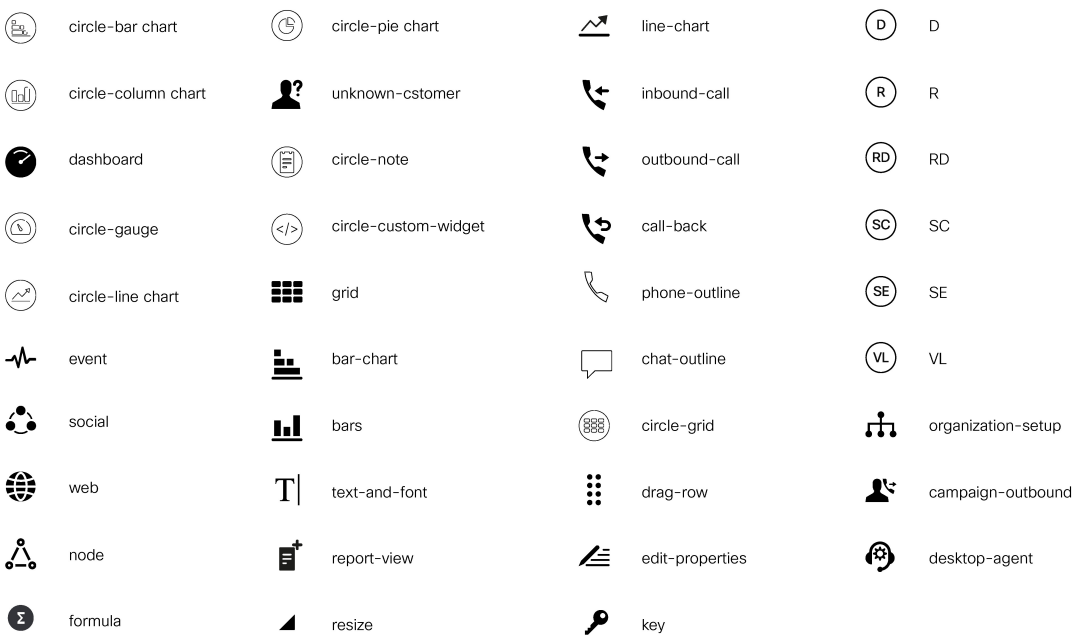


510895

The following are the icons for Video Controls.

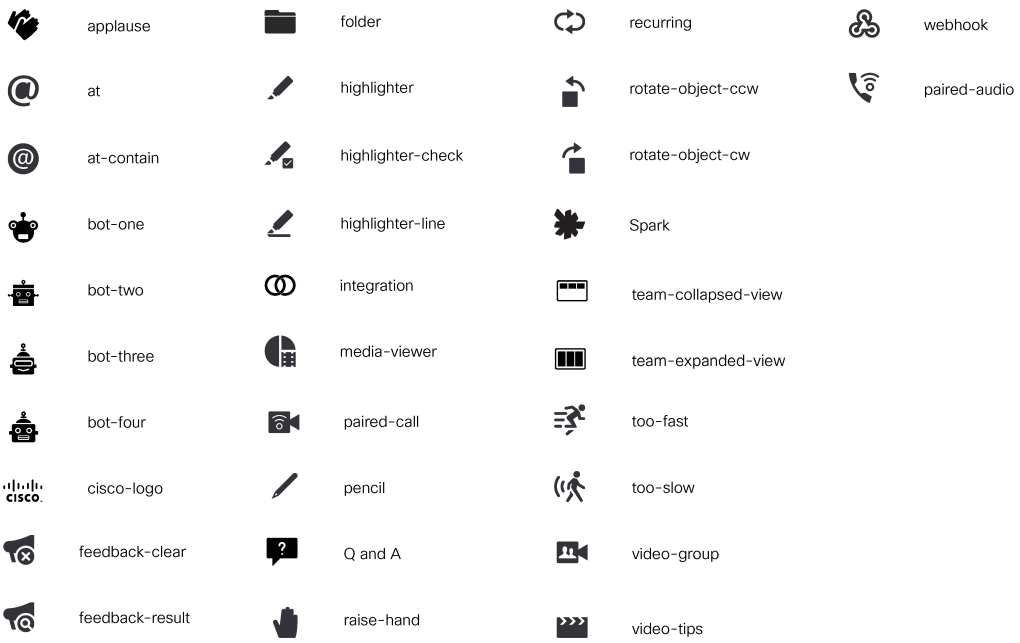
510896

The following are the icons for Miscellaneous Icons.

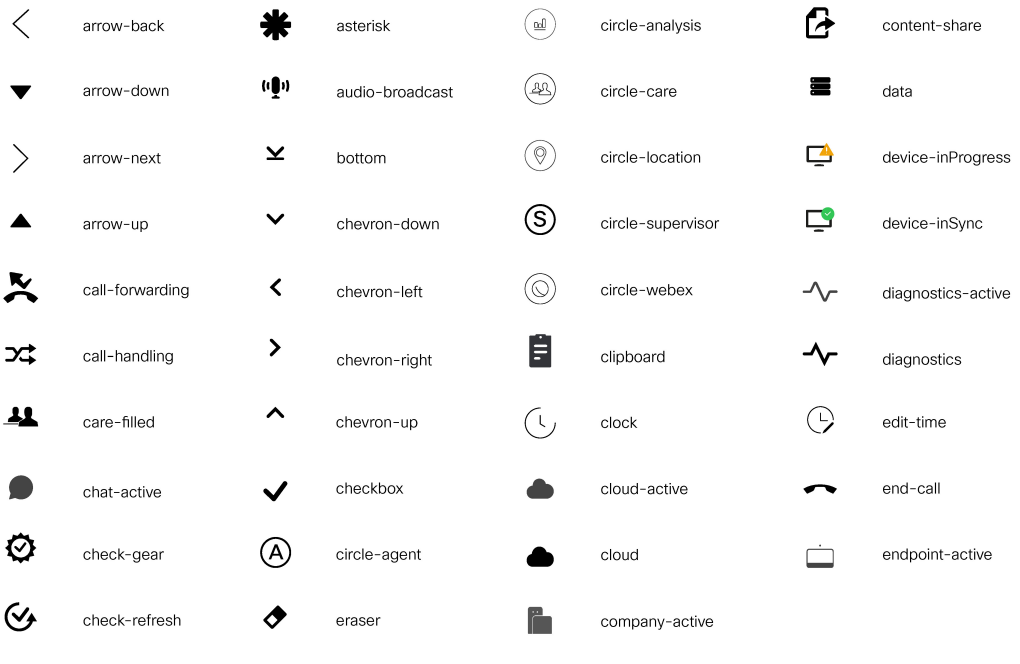


510898

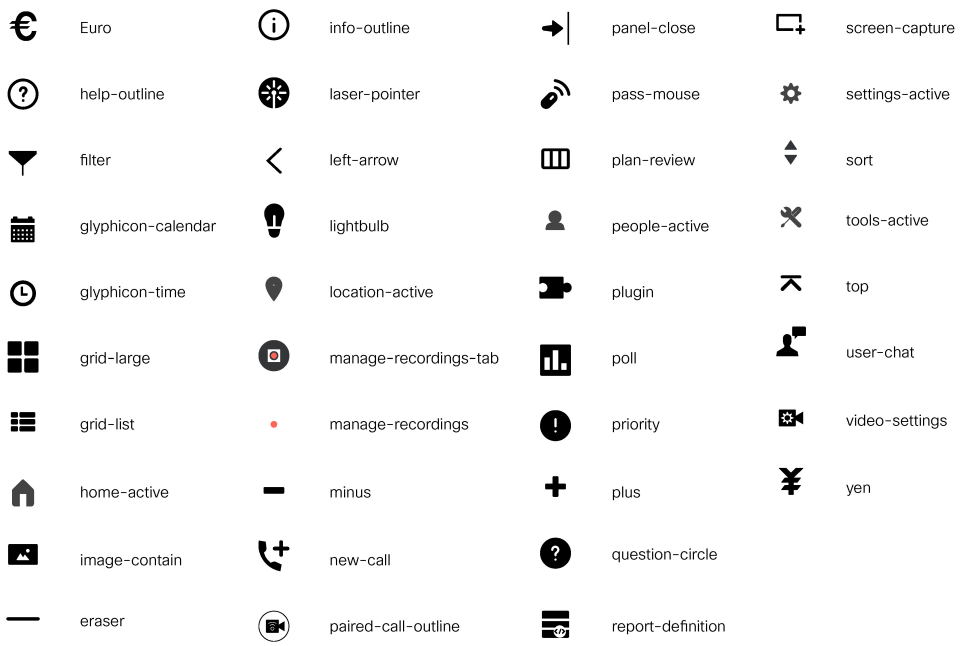
510899



510900



510901



For more information on customizing the visual experience, see *Visual Design Kit* at https://developer.cisco.com/docs/finesse/#!visual-design-guide.

XML Schema Definition

You must ensure that the XML uploaded conforms to the XML schema definition for Finesse. The XML schema definition for Finesse is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://www.cisco.com/vtg/finesse" targetNamespace="http://www.cisco.com/vtg/finesse"
 elementFormDefault="qualified">
   <!-- definition of version element -->
   <xs:element name="version">
      <xs:simpleType>
         <xs:restriction base="xs:double">
            <xs:pattern value="[0-9\.]+" />
         </xs:restriction>
      </xs:simpleType>
   </xs:element>
   <!--  The below elements are for common desktop header and configs -->
   <!--  Copied from:
https://github5.cisco.com/cdbu-shared/common-desktop/blob/master/java/layout-manager/src/main/resources/layoutSchema.xsd
 -->
   <!--  If the common-desktop XSD changes, this too needs to be updated -->
   <!--  Only difference is that, column has been renamed to headercolumn, since column is
 alredy there in finesse desktop layout -->
   <xs:complexType name="configs">
      <xs:sequence>
         <xs:element name="config" type="config" minOccurs="0" maxOccurs="unbounded" />
      </xs:sequence>
   </xs:complexType>
   <xs:complexType name="config">
      <xs:attribute name="key">
```

```
            <xs:simpleType>
               <xs:restriction base="xs:string">
                  <xs:pattern value="[a-zA-Z]*" />
               </xs:restriction>
            </xs:simpleType>
         </xs:attribute>
         <xs:attribute name="value" type="xs:string" />
      </xs:complexType>
      <xs:complexType name="header">
         <xs:choice>
            <xs:sequence>
               <xs:element name="leftAlignedColumns" type="listOfColumns" minOccurs="1"
maxOccurs="1" />
               <xs:element name="rightAlignedColumns" type="listOfColumns" minOccurs="0"
maxOccurs="1" />
            </xs:sequence>
            <xs:sequence>
               <xs:element name="rightAlignedColumns" type="listOfColumns" minOccurs="1"
maxOccurs="1" />
            </xs:sequence>
         </xs:choice>
      </xs:complexType>
      <xs:complexType name="component">
         <xs:sequence>
            <xs:element name="url" type="xs:string" minOccurs="1" maxOccurs="1" />
            <xs:element name="stylesheet" type="xs:string" minOccurs="0" maxOccurs="1" />
         </xs:sequence>
         <xs:attribute name="id" use="required">
            <xs:simpleType>
               <xs:restriction base="xs:string">
                  <xs:pattern value=".+" />
               </xs:restriction>
            </xs:simpleType>
         </xs:attribute>
         <xs:attribute name="order">
            <xs:simpleType>
               <xs:restriction base="xs:string">
                  <xs:pattern value="[0-9]{0,10}" />
               </xs:restriction>
            </xs:simpleType>
         </xs:attribute>
      </xs:complexType>
      <xs:complexType name="listOfColumns">
         <xs:sequence>
            <xs:element name="headercolumn" type="headercolumn" minOccurs="1"
maxOccurs="unbounded" />
         </xs:sequence>
      </xs:complexType>
      <xs:complexType name="headercolumn">
         <xs:choice minOccurs="0" maxOccurs="1">
            <xs:element ref="gadget" />
            <xs:element name="component" type="component" />
         </xs:choice>
         <xs:attribute name="width">
            <xs:simpleType>
               <xs:restriction base="xs:string">
                  <xs:pattern value="[0-9]+(px|%)" />
               </xs:restriction>
            </xs:simpleType>
         </xs:attribute>
      </xs:complexType>
      <!--  The above elements are for common desktop header and configs -->
      <!-- definition of role type -->
      <xs:simpleType name="role">
```

```
      <xs:restriction base="xs:string">
         <xs:enumeration value="Agent" />
         <xs:enumeration value="Supervisor" />
         <xs:enumeration value="Admin" />
      </xs:restriction>
   </xs:simpleType>
   <!-- definition of simple elements -->
   <xs:element name="id">
      <xs:simpleType>
         <xs:restriction base="xs:string">
            <xs:pattern value="[a-zA-Z]([-_:\.a-zA-Z0-9])*" />
         </xs:restriction>
      </xs:simpleType>
   </xs:element>
   <xs:element name="label">
      <xs:simpleType>
         <xs:restriction base="xs:string">
            <xs:minLength value="1" />
            <xs:pattern value="[^\r\n]+" />
            <!-- This regex restricts the label string from carriage returns or newline
characters -->
         </xs:restriction>
      </xs:simpleType>
   </xs:element>
   <xs:element name="icon" type="xs:anyURI" />
   <xs:element name="gadget">
      <xs:complexType>
         <xs:simpleContent>
            <xs:extension base="restrictWhiteSpaces">
               <!-- <xs:attribute name="staticMessage" type="xs:string"/> -->
               <xs:attribute name="id">
                  <xs:simpleType>
                     <xs:restriction base="xs:string">
                        <xs:pattern value="[a-zA-Z]([-_a-zA-Z0-9])*" />
                     </xs:restriction>
                  </xs:simpleType>
               </xs:attribute>
               <xs:attribute name="alternateHosts" type="xs:string" />
               <xs:attribute name="managedBy" type="xs:string" />
               <xs:attribute name="hidden" type="xs:boolean" />
            </xs:extension>
         </xs:simpleContent>
      </xs:complexType>
   </xs:element>
   <xs:element name="role" type="role" />
   <xs:element name="gadgets">
      <!-- Grouping of a set of gadgets -->
      <xs:complexType>
         <xs:sequence minOccurs="0" maxOccurs="unbounded">
            <!-- No limit to number of gadget URIs for now -->
            <xs:element ref="gadget" />
            <!-- URI of the gadget xml -->
         </xs:sequence>
      </xs:complexType>
   </xs:element>
   <xs:simpleType name="restrictWhiteSpaces">
      <xs:restriction base="xs:anyURI">
         <xs:minLength value="1" />
         <xs:pattern value="\S+" />
         <!-- This regex restricts anyURI from containing whitespace within -->
      </xs:restriction>
   </xs:simpleType>
   <xs:element name="column">
      <!-- Grouping of a set of gadgets within a column -->
```

```
   <xs:complexType>
      <xs:sequence minOccurs="0" maxOccurs="unbounded">
         <!-- No limit to number of gadget URIs for now -->
         <xs:element ref="gadgets" />
         <!-- URI of the gadget xml -->
      </xs:sequence>
   </xs:complexType>
</xs:element>
<xs:element name="columns">
   <!-- Grouping of a set of columns -->
   <xs:complexType>
      <xs:sequence>
         <xs:element ref="column" minOccurs="0" maxOccurs="unbounded" />
      </xs:sequence>
   </xs:complexType>
</xs:element>
<xs:element name="page">
   <!-- Grouping of a set of persistent gadgets -->
   <xs:complexType>
      <xs:sequence minOccurs="0" maxOccurs="unbounded">
         <!-- No limit to number of gadget URIs for now -->
         <xs:element ref="gadget" />
         <!-- URI of the gadget xml -->
      </xs:sequence>
   </xs:complexType>
</xs:element>
<xs:element name="tab">
   <xs:complexType>
      <xs:sequence>
         <xs:element ref="id" />
         <!-- Id of the tab selector in the desktop -->
         <xs:element ref="icon" minOccurs="0" maxOccurs="1" />
         <xs:element ref="label" />
         <!-- Label of the tab selector -->
         <xs:choice>
            <xs:element ref="gadgets" minOccurs="0" maxOccurs="1" />
            <xs:element ref="columns" minOccurs="0" maxOccurs="1" />
         </xs:choice>
      </xs:sequence>
   </xs:complexType>
</xs:element>
<xs:element name="tabs">
   <!-- Grouping of tabs -->
   <xs:complexType>
      <xs:sequence maxOccurs="unbounded">
         <!-- No limit to number of tabs for now -->
         <xs:element ref="tab" />
      </xs:sequence>
   </xs:complexType>
</xs:element>
<xs:element name="layout">
   <xs:complexType>
      <xs:sequence>
         <xs:element ref="role" />
         <!-- Type of the role -->
         <xs:element ref="page" />
         <!-- List of page gadgets -->
         <xs:element ref="tabs" />
         <!-- Grouping of tabs for this particular role -->
      </xs:sequence>
   </xs:complexType>
</xs:element>
<xs:element name="finesseLayout">
   <!-- Layout of the desktop -->
```

```
      <xs:complexType>
         <xs:sequence>
            <xs:element ref="version" />
            <xs:element name="configs" type="configs" minOccurs="0" maxOccurs="1" />
            <xs:element name="header" type="header" minOccurs="1" maxOccurs="1" />
            <xs:sequence maxOccurs="3">
               <!-- only support 3 roles for now -->
               <xs:element ref="layout" />
            </xs:sequence>
         </xs:sequence>
      </xs:complexType>
   </xs:element>
</xs:schema>
```

Add Webchat and Email to Finesse

The Cisco Finesse default layout XML contains commented XML code for Web Chat and Email gadgets available for the Finesse desktop. Each gadget or tab is surrounded by comment characters (<!-- and -->) and comments that describe what the tab or gadget is for and how to add it to the desktop.

Note The Chat and Email Control gadget is only supported at the page level. You must ensure that the Chat and Email Control gadget (<gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>) is placed within the <page></page> tag. Placing this gadget within a <tab></tab> tag is not supported.

The procedure that you follow depends on your deployment. The following table describes when to use each procedure.

Procedure	When to use
Add Web Chat and Email to the default desktop layout.	Follow this procedure if you want to add Web Chat and Email to the Finesse desktop after a fresh installation or after an upgrade if you have not customized the default desktop layout.
Add Web Chat and Email to a custom desktop layout.	Follow this procedure if you want to add Web Chat and Email and have customized the desktop layout.
Add Web Chat and Email to a team layout.	Follow this procedure if you want to add Web Chat and Email to the desktop only for specific teams.

Note After you add the Web Chat and Email gadgets, sign in to the Finesse desktop and make sure they appear the way you want. Agents who are signed in to Finesse when you change the desktop layout must sign out and sign back in to see the change on their desktops.

Add Web Chat and Email to the Default Desktop Layout

Note If you upgraded from a previous release 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.

Procedure

Step 1 In the Finesse administration console, click the **Desktop Layout** tab.

Step 2 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 3 To add the Chat and Email Control gadget to the agent desktop, look for the following under the <role>Agent</role> tag and within the <page></page> tag:

```
<gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>
```

Step 4 Remove the comments and comment characters (<!-- and -->) that surround the gadget, leaving only the gadget (<gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>).

Step 5 To add the Manage Chat and Email tab and gadget to the agent desktop, look for the following within the <tabs></tabs> tag:

```
<tab>
    <id>manageNonVoiceMedia</id>
    <label>finesse.container.tabs.agent.manageNonVoiceMediaLabel</label>
    <columns>
        <column>
            <gadgets>
                <gadget>https://my-CCP-server/multisession/ui/gadgets/
                 multisession-reply-gadget.xml?gadgetHeight=590</gadget>
            </gadgets>
        </column>
    </columns>
</tab>
```

Step 6 Remove the comments and comment characters (<!-- and -->) that surround the tab.

Step 7 Replace my-CCP-server in the gadget URL with the fully-qualified domain name (FQDN) of your Customer Collaboration Platform server.

Step 8 Optionally, change the height of the Manage Chat and Email gadget.

Example:

The height specified in the gadget URL is 590 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 600 pixels, change the code as follows:

```
<gadget>https://my-CCP-server/multisession/ui/gadgets/
         multisession-reply-gadget.xml?gadgetHeight=600</gadget>
```

The default and minimum height of the Manage Chat and Email gadget is 590 pixels. If you do not specify a value for the gadgetHeight parameter or if you specify a value that is less than 590, the gadget defaults to 590 pixels.

Note
An agent can be configured to handle up to five chat contacts and five email contacts at a time. If the agent has the maximum number of contacts on the desktop, not all contacts are visible. If your agents are configured to handle the maximum number of contacts, you must increase the height of this gadget to a minimum of 570 pixels to ensure there is enough space for all of the contacts to appear.

Step 9 To add the Chat and Email Control gadget to the supervisor desktop, look for the following under the <role>Supervisor</role> tag and within the <page></page> tag:

```
<gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>
```

Step 10 Remove the comments and comment characters (<!-- and -->), leaving only the gadget (<gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>).

Step 11 To add the Live Data report for Agent Chat Statistics to the supervisor desktop, look for the following:

```
<gadget>https://localhost:8444/cuic/gadget/LiveData/
 LiveDataGadget.xml?gadgetHeight=310&
 viewId=F2F1FC17100001440000014E0A4E5D48&
 filterId=ChatAgentStats.agentId=CL</gadget>
```

Step 12 Remove the comments and comment characters (<!-- and -->), leaving only the gadget.

Step 13 To add the Live Data report for Chat Queue Statistics to the supervisor desktop, look for the following:

```
<gadget>https://localhost:8444/cuic/gadget/LiveData/
 LiveDataGadget.xml?gadgetHeight=310&
 viewId=E42ED7881000014400000007B0A4E5CA1&
 filterId=ChatQueueStatistics.queueName=CL</gadget>
```

Step 14 Remove the comments and comment characters (<!-- and -->), leaving only the gadget.

Step 15 To add the Manage Chat and Email tab and gadget to the supervisor desktop, look for the following within the <tabs></tabs> tag:

```
<tab>
    <id>manageNonVoiceMedia</id>
    <label>finesse.container.tabs.supervisor.manageNonVoiceMediaLabel</label>
    <columns>
        <column>
            <gadgets>
                <gadget>https://my-CCP-server/multisession/ui/gadgets/
                 multisession-reply-gadget.xml?gadgetHeight=590</gadget>
            </gadgets>
        </column>
    </columns>
</tab>
```

Step 16 Remove the comments and comment characters (<!-- and -->) that surround the tab.

Step 17 Replace my-CCP-server in the gadget URL with the fully-qualified domain name (FQDN) of your Customer Collaboration Platform server.

Step 18 Optionally, change the height of the Manage Chat and Email gadget.

Step 19 Click **Save**.

Add Webchat and Email to a Custom Desktop Layout

Procedure

Step 1 In the Finesse administration console, click the **Desktop Layout** tab.

Step 2 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 3 Copy the XML code for the Chat and Email Control gadget for the agent desktop.

```
<gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>
```

Step 4 To add the gadget to the agent desktop, paste the code within the <page></page> tags under the Call Control gadget as follows:

```
<role>Agent</role>
<page>
   <gadget>/desktop/gadgets/CallControl.xml</gadget>
   <gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>
</page>
```

Step 5 To add the gadget to the supervisor desktop, paste the code within the <page></page> tags under the Call Control gadget as follows:

```
<role>Supervisor</role>
<page>
   <gadget>/desktop/gadgets/CallControl.xml</gadget>
   <gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>
</page>
```

Step 6 Copy the code for the agent Manage Chat and Email tab and gadget from the default layout XML.

```
<tab>
    <id>manageNonVoiceMedia</id>
    <label>finesse.container.tabs.agent.manageNonVoiceMediaLabel</label>
    <columns>
        <column>
            <gadgets>
                <gadget>https://my-CCP-server/multisession/ui/gadgets/
                 multisession-reply-gadget.xml?gadgetHeight=430</gadget>
            </gadgets>
        </column>
    </columns>
</tab>
```

Step 7 Paste the code within the <tabs></tabs> tag for the agent role after the Manage Call tab:

```
<tab>
    <id>manageCall</id>
    <label>finesse.container.tabs.agent.manageCallLabel</label>
</tab>
<tab>
    <id>manageNonVoiceMedia</id>
    <label>finesse.container.tabs.agent.manageNonVoiceMediaLabel</label>
    <columns>
        <column>
            <gadgets>
                <gadget>https://my-CCP-server/multisession/ui/gadgets/
                 multisession-reply-gadget.xml?gadgetHeight=430</gadget>
            </gadgets>
        </column>
    </columns>
</tab>
```

Step 8 Replace my-social-miner-server with the FQDN of your Customer Collaboration Platform server.

Step 9 Optionally, change the height of the Manage Chat and Email gadget.

Example:

The height specified in the gadget URL is 430 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 600 pixels, change the code as follows:

```
<gadget>https://my-CCP-server/multisession/ui/gadgets/
         multisession-reply-gadget.xml?gadgetHeight=600</gadget>
```

The default and minimum height of the Manage Chat and Email gadget is 430 pixels. If you do not specify a value for the gadgetHeight parameter or if you specify a value that is less than 430, the gadget defaults to 430 pixels.

Note
An agent can be configured to handle up to five chat contacts and five email contacts at a time. If the agent has the maximum number of contacts on the desktop, not all contacts are visible. If your agents are configured to handle the maximum number of contacts, you must increase the height of this gadget to a minimum of 570 pixels to ensure there is enough space for all of the contacts to appear.

Step 10 Copy the code for the Live Data gadgets for Agent Chat Statistics and Chat Queue Statistics from the default layout XML.

```
<gadget>https://localhost:8444/cuic/gadget/LiveData/
 LiveDataGadget.xml?gadgetHeight=310&
 viewId=F2F1FC17100001440000014E0A4E5D48&
 filterId=ChatAgentStats.agentId=CL</gadget>

<gadget>https://localhost:8444/cuic/gadget/LiveData/
 LiveDataGadget.xml?gadgetHeight=310&
 viewId=E42ED7881000014400000007B0A4E5CA1&
 filterId=ChatQueueStatistics.queueName=CL</gadget>
```

Step 11 Paste the code for these gadgets within the <gadgets></gadgets> tags for the tabs on which you want them to appear.

Step 12 Copy the code for the supervisor Manage Chat and Email tab and gadget from the default layout XML.

```
<tab>
    <id>manageNonVoiceMedia</id>
    <label>finesse.container.tabs.supervisor.manageNonVoiceMediaLabel</label>
    <columns>
        <column>
            <gadgets>
                <gadget>https://my-CCP-server/multisession/ui/gadgets/
                 multisession-reply-gadget.xml?gadgetHeight=430</gadget>
            </gadgets>
        </column>
    </columns>
</tab>
```

Step 13 Paste the code within the <tabs></tabs> tag for the supervisor role after the Manage Call tab:

```
<tab>
    <id>manageCall</id>
    <label>finesse.container.tabs.supervisor.manageCallLabel</label>
</tab>
<tab>
    <id>manageNonVoiceMedia</id>
    <label>finesse.container.tabs.supervisor.manageNonVoiceMediaLabel</label>
    <columns>
        <column>
            <gadgets>
                <gadget>https://my-CCP-server/multisession/ui/gadgets/
                 multisession-reply-gadget.xml?gadgetHeight=430</gadget>
            </gadgets>
        </column>
    </columns>
</tab>
```

Step 14 Replace my-social-miner-server with the FQDN of your Customer Collaboration Platform server.

Step 15 Optionally, change the height of the gadget.

Step 16 Click **Save**.

Add Web Chat and Email to a Team Layout

Procedure

Step 1 In the Finesse administration console, click the **Desktop Layout** tab.

Step 2 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 3 Copy the XML code for the Chat and Email Control gadget for the agent desktop and paste it into a text file.

```
<gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>
```

Step 4 Copy the code for the agent Manage Chat and Email tab and gadget and paste it into your text file.

```
<tab>
    <id>manageNonVoiceMedia</id>
    <label>finesse.container.tabs.agent.manageNonVoiceMediaLabel</label>
    <columns>
        <column>
            <gadgets>
                <gadget>https://my-CCP-server/multisession/ui/gadgets/
                 multisession-reply-gadget.xml?gadgetHeight=430</gadget>
            </gadgets>
        </column>
    </columns>
</tab>
```

Step 5 Copy the code for the Live Data gadgets for Agent Chat Statistics and Chat Queue Statistics and paste it into your text file.

```
<gadget>https://localhost:8444/cuic/gadget/LiveData/
 LiveDataGadget.xml?gadgetHeight=310&
 viewId=F2F1FC17100001440000014E0A4E5D48&
 filterId=ChatAgentStats.agentId=CL</gadget>

<gadget>https://localhost:8444/cuic/gadget/LiveData/
 LiveDataGadget.xml?gadgetHeight=310&
 viewId=E42ED788100001440000007B0A4E5CA1&
 filterId=ChatQueueStatistics.queueName=CL</gadget>
```

Step 6 Copy the code for the supervisor Manage Chat and Email tab and gadget and paste it into your text file.

```
<tab>
    <id>manageNonVoiceMedia</id>
    <label>finesse.container.tabs.supervisor.manageNonVoiceMediaLabel</label>
    <columns>
        <column>
            <gadgets>
                <gadget>https://my-CCP-server/multisession/ui/gadgets/
                 multisession-reply-gadget.xml?gadgetHeight=430</gadget>
            </gadgets>
        </column>
    </columns>
</tab>
```

Step 7 Click the **Team Resources** tab.

Step 8 Select the team from the list of teams for which you want to add Web Chat and Email.

Step 9 Check the **Override System Default** check box.

Step 10 In the Resources for <team name> area, click the **Desktop Layout** tab.

Step 11 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 12 To add the Chat and Email Control gadget to the agent desktop, copy the code for the gadget from your text file and paste it within the <page></page> tags under the Call Control gadget as follows:

```
<role>Agent</role>
<page>
   <gadget>/desktop/gadgets/CallControl.xml</gadget>
   <gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>
</page>
```

Step 13 To add the gadget to the supervisor desktop, paste the code within the <page></page> tags under the Call Control gadget as follows:

Step 14 To add the Manage Chat and Email tab and gadget to the agent desktop, copy the code from your text file and paste it within the <tabs></tabs> tag for the agent role after the Manage Call tab:

```
<tab>
    <id>manageCall</id>
    <label>finesse.container.tabs.agent.manageCallLabel</label>
</tab>
<tab>
    <id>manageNonVoiceMedia</id>
    <label>finesse.container.tabs.agent.manageNonVoiceMediaLabel</label>
    <columns>
        <column>
            <gadgets>
                <gadget>https://my-CCP-server/multisession/ui/gadgets/
                 multisession-reply-gadget.xml?gadgetHeight=430</gadget>
            </gadgets>
        </column>
    </columns>
</tab>
```

Step 15 Replace my-social-miner-server with the FQDN of your Customer Collaboration Platform server.

Step 16 Optionally, change the height of the Manage Chat and Email gadget.

Example:

The height specified in the gadget URL is 430 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 600 pixels, change the code as follows:

```
<gadget>https://my-CCP-server/multisession/ui/gadgets/
         multisession-reply-gadget.xml?gadgetHeight=600</gadget>
```

The default and minimum height of the Manage Chat and Email gadget is 430 pixels. If you do not specify a value for the gadgetHeight parameter or if you specify a value that is less than 430, the gadget defaults to 430 pixels.

Note
An agent can be configured to handle up to five chat contacts and five email contacts at a time. If the agent has the maximum number of contacts on the desktop, not all contacts are visible. If your agents are configured to handle the

maximum number of contacts, you must increase the height of this gadget to a minimum of 570 pixels to ensure there is enough space for all of the contacts to appear.

Step 17 To add the Live Data gadgets for Web Chat and Email to the supervisor desktop:

a) Copy the code for the Agent Chat Statistics Live Data gadget from your text file and paste it within the <gadgets></gadgets> tags for the tab on which you want it to appear.

b) Copy the code for the Chat Queue Statistics Live Data gadget from your text file and paste it within the <gadgets></gadgets> tags for the tab on which you want it to appear.

Step 18 To add the Manage Chat and Email tab gadget to the supervisor desktop, copy the code from your text file and paste it within the <tabs></tabs> tag for the supervisor role after the Manage Call tab:

```
<tab>
    <id>manageCall</id>
    <label>finesse.container.tabs.supervisor.manageCallLabel</label>
</tab>
<tab>
    <id>manageNonVoiceMedia</id>
    <label>finesse.container.tabs.supervisor.manageNonVoiceMediaLabel</label>
    <columns>
        <column>
            <gadgets>
                <gadget>https://my-CCP-server/multisession/ui/gadgets/
                 multisession-reply-gadget.xml?gadgetHeight=430</gadget>
            </gadgets>
        </column>
    </columns>
</tab>
```

Step 19 Replace my-social-miner-server with the FQDN of your Customer Collaboration Platform server.

Step 20 Optionally, change the height of the gadget.

Step 21 Click **Save**.

Enable Advanced Supervisor Capabilities in Finesse

The Cisco Finesse default layout XML contains commented XML code of Advanced Supervisor Capabilities gadget for the Finesse desktop. Each gadget or tab is surrounded by comment characters (<!-- and -->) and comments that describe what the tab or gadget is for and how to add it to the desktop.

Note The Advanced Supervisor Capability is designed for only supervisors.

The procedure that you must follow to enable the gadget depends on your deployment. The following table describes when to use each procedure.

Procedure	When to use
Enable Advanced Supervisor Capabilities for Default Desktop Layout	Follow this procedure if you want to enable Advanced Supervisor Capabilities in the Finesse desktop after a fresh installation or after an upgrade if you have not customized the default desktop layout.

Procedure	When to use
Add Advanced Supervisor Capabilities in Custom Desktop Layout	Follow this procedure if you want to add Advanced Supervisor Capabilities and have customized the desktop layout.
Add Advanced Supervisor Capabilities to a team layout.	Follow this procedure if you want to add Advanced Supervisor Capabilities to the desktop for specific teams.

Note After you enable the Advanced Supervisor Capabilities gadget, sign in to the Finesse desktop as a supervisor and ensure that they appear the way you want. When you change the desktop layout, supervisors who are signed in to Finesse must sign out and sign in again to see the change on their desktops.

Enable Advanced Supervisor Capabilities in Default Desktop Layout

If you upgraded from a previous release 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 Perform this task only once at the beginning of Default Desktop Layout modification. If you do it later, the previous changes will be lost.

Procedure

Step 1 In the Finesse administration console, click the **Desktop Layout** in the left pane.
Manage Desktop Layout page is displayed with **Desktop Layout** XML.

Step 2 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 3 To enable Advanced Supervisor Capabilities gadget in the supervisor desktop, look for the following under the `<role>Supervisor</role>` tag:

```
<id>ASCGadget</id>
```

Step 4 Remove the comments and comment characters (`<!--` and `-->`) that surround the gadget, leaving only the gadget `<gadget>https://localhost/ascgadget/gadgets/ascgadget.xml</gadget>`.

Step 5 Click **Save**.

Add Advanced Supervisor Capabilities in Custom Desktop Layout

Procedure

Step 1 In the Finesse administration console, click the **Desktop Layout** in the left pane.
Manage Desktop Layout page is displayed with **Desktop Layout** XML.

Step 2 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 3 Copy the XML code of Advanced Supervisor Capabilities gadget.

```
<gadget>https://localhost/ascgadget/gadgets/ascgadget.xml</gadget>
```

Step 4 In the **Desktop Layout** XML, look for the `<role>Supervisor</role>` tag.

Step 5 Paste the copied code within the `<tab> </tab>` tags in the Desktop Layout XML, below the WebChat and Email gadget as follows:

```
<tab>
    <id>ASCGadget</id>
    <icon>admin</icon>
    <label>finesse.container.tabs.supervisor.advancedcapabilities</label>
    <columns>
        <column>
            <gadgets>
                <gadget>https://localhost/ascgadget/gadgets/ascgadget.xml</gadget>
            </gadgets>
        </column>
    </columns>
</tab>
```

Note
Ensure that the gadget is available only for supervisors.

Step 6 Click **Save**.

Add Advanced Supervisor Capabilities in Team Layout

Procedure

Step 1 In the Finesse administration console, click the **Desktop Layout** in the left pane.
Manage Desktop Layout page is displayed with **Desktop Layout** XML.

Step 2 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 3 Copy the XML code of Advanced Supervisor Capabilities gadget.

```
<gadget>https://localhost/ascgadget/gadgets/ascgadget.xml</gadget>
```

Step 4 Click the **Team Resources** in the left pane.

Step 5 Select the team from the list of teams for which you want to add Advanced Supervisor Capabilities.

Step 6 Check the **Override System Default** check box.

Step 7 In the Resources for <team name> area, click the **Desktop Layout** tab.

Step 8 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 9 In the XML, look for the `<role>Supervisor</role>` tag.

Step 10 Paste the copied code within the `<tab> </tab>` tags in the XML, below the WeChat and Email gadget as follows:

```
<tab>
    <id>ASCGadget</id>
    <icon>admin</icon>
    <label>finesse.container.tabs.supervisor.advancedcapabilities</label>
    <columns>
        <column>
            <gadgets>
                <gadget>https://localhost/ascgadget/gadgets/ascgadget.xml</gadget>
            </gadgets>
        </column>
    </columns>
</tab>
```

Note
Ensure that the gadget is available only for supervisors.

Step 11 Click **Save**.

Add Team Message in Custom Desktop Layout

Procedure

Step 1 In the Finesse administration console, click the **Desktop Layout** in the left pane.
Manage Desktop Layout page is displayed with **Desktop Layout** XML.

Step 2 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 3 Copy the XML code where `component id="broadcastmessagepopover"`.

```
<component id="broadcastmessagepopover">
            <url>/desktop/scripts/js/teammessage.component.js</url>
        </component>
```

Step 4 Click the **Team Resources** in the left pane.

Step 5 Check the **Override System Default** check box.

Step 6 In the Resources for <team name> area, click the **Desktop Layout** tab.

Step 7 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 8 In the XML, look for the `</headercolumn>` tag in the XML.

Step 9 Paste the copied code below the `</headercolumn>` tag as follows:

```
<headercolumn width="50px">
    <component id="broadcastmessagepopover">
        <url>/desktop/scripts/js/teammessage.component.js</url>
    </component>
</headercolumn>
```

Step 10 Click **Save**.

Add Desktop Chat in Custom Desktop Layout

Procedure

Step 1 In the Finesse administration console, click the **Desktop Layout** in the left pane.
Manage Desktop Layout page is displayed with **Desktop Layout** XML.

Step 2 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 3 Copy the XML code where `component id="chat"`.

```
<component id="chat">
            <url>/desktop/scripts/js/chat.component.js</url>
        </component>
```

Step 4 Click the **Team Resources** in the left pane.

Step 5 Check the **Override System Default** check box.

Step 6 In the Resources for <team name> area, click the **Desktop Layout** tab.

Step 7 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 8 In the XML, look for the `</headercolumn>` tag in the XML.

Step 9 Paste the copied code below the `</headercolumn>` tag as follows:

```
<headercolumn width="50px">
    <component id="chat">
        <url>/desktop/scripts/js/chat.component.js</url>
    </component>
</headercolumn>
```

Step 10 Click **Save**.

Live Data Gadgets

Cisco Finesse for Unified CCX supports Live Data gadgets. Live Data gadgets display information about the current state of the contact center. The gadgets receive data from the real-time data source at frequent intervals and display reports in grid format only.

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

This feature provides the following access:

- Agents can access the Live Data agent reports.
- Supervisors can access the Live Data supervisor reports.

Gadgets URLs for Reports

The following table displays gadgets URLs for reports.

Users	Reports	Report View	Is the Report Available in Default Layout ?	Tab	Gadget URLs
Agent	Agent CSQ Statistics Report	Agent CSQ Statistics Report	Yes	Home	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=76D964AD10000140000000830A4E5E6F&filterId=AgentCSQStats.csqName=CL&compositeFilterId=AgentCSQStats.AgentIds.agentId=loginId</gadget>
Agent	Agent State Log Report	Agent State Log Report	Yes	My Statistics	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=420&viewId=5D411E8A10000140000000230A4E5E6B&filterId=AgentStateDetailStats.agentID=loginId</gadget>
Agent	Agent Statistics Report	Agent Statistics Report	Yes	My Statistics	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=150&viewId=67D43711100001400000001080A4E5E6B&filterId=ResourceIAQStats.resourceId=loginId</gadget>
Agent	Agent Team Summary Report	Agent Team Summary Report	Yes	Home	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=5C626F9C10000140000000600A4E5B33&filterId=ResourceIAQStats.resourceId=CL</gadget>

Users	Reports	Report View	Is the Report Available in Default Layout ?	Tab	Gadget URLs
Supervisor	Agent Outbound Team Summary Report	Report since midnight	No	Team Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=FD919FB9100001440000005D0A4E5B29&filterId=ResourceIAQStats.resourceId=CL</gadget>
Supervisor	Agent Outbound Team Summary Report	Short and long term average	No	Team Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=FD919FB510000144000000470A4E5B29&filterId=ResourceIAQStats.resourceId=CL</gadget>
Supervisor	Chat Agent Statistics Report	Chat Agent Statistics Report	No	Team Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=120&viewId=F2F1FC17100001440000014E0A4E5D48&filterId=ChatAgentStats.agentId=CL</gadget>
Supervisor	Chat CSQ Summary Report	Chat CSQ Summary Report	No	Queue Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=120&viewId=E42ED7881000014400000007B0A4E5CA1&filterId=ChatQueueStatistics.queueName=CL</gadget>
Supervisor	Email Agent Statistics Report	Email Agent Statistics Report	No	Team Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=BCC5767B1000014F000000580A4D3FA7&filterId=EmailAgentStats.agentId=CL</gadget>
Supervisor	Email CSQ Summary Report	Email CSQ Summary Report	No	Queue Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=13970B4E100001500000021C0A4D3FA7&filterId=EmailQueueStatistics.queueName=CL</gadget>
Supervisor	Team State Report	Team State Report	No	—	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=5C90012F10000140000000830A4E5B33&filterId=ResourceIAQStats.resourceId=CL</gadget>
Supervisor	Team Summary Report	Report since midnight	Yes	Team Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=728283C210000140000000530A4E5B33&filterId=ResourceIAQStats.resourceId=CL</gadget>

Users	Reports	Report View	Is the Report Available in Default Layout ?	Tab	Gadget URLs
Supervisor	Team Summary Report	Short and long term average	Yes	Team Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=7291DCB410000140000000890A4E5B33&filterId=ResourceIAQStats.resourceId=CL</gadget>
Supervisor	Voice CSQ Agent Detail Report	Voice CSQ Agent Detail Report	Yes	Queue Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=9A7A14CE10000140000000ED0A4E5E6B&filterId=VoiceCSQDetailsStats.agentId=CL&compositeFilterId=VoiceCSQDetailsStats.AgentVoiceCSQNames.agentVoiceCSQName=CL</gadget>
Supervisor	Voice CSQ Summary	Snapshot	Yes	Queue Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=C8E2DB16100001400000000A60A4E5E6B&filterId=VoiceIAQStats.esdName=CL</gadget>
Supervisor	Voice CSQ Summary	Short and long term average	Yes	Queue Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=C8EE241910000140000000C30A4E5E6B&filterId=VoiceIAQStats.esdName=CL</gadget>
Supervisor	Voice CSQ Summary	Report since midnight	No	Queue Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=C8EF5108100001400000000EB0A4E5E6B&filterId=VoiceIAQStats.esdName=CL</gadget>

Gadgets Customization

You can use optional query parameter to adjust height of the gadgets.

Query Parameter

```
<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?
gadgetHeight=200&viewId=5C626F9C10000140000000600A4E5B33&filterId=ResourceIAQStats.resourceId=CL</gadget>
```

Add Live Data Gadgets to Desktop Layout

The Cisco Finesse default layout XML contains commented XML code for the Live Data gadgets available for Cisco Finesse desktop. Perform the following steps to add Live Data gadgets to desktop layout:

Procedure

Step 1 Sign in to Cisco Finesse administration console.
Cisco Finesse home page appears.

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

Step 3 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 4 Copy the gadget URL for the report you want to add from **Live Data Gadgets**.

Example:

To add the Agent Report, copy the following:

```
<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight
=150&viewId=67D43711100001400000001080A4E5E6B&filterId=ResourceIAQStats.resourceId=loginId</gadget>
```

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

Example:

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

```
<finesseLayout xmlns="http://www.cisco.com/vtg/finesse">
 <layout>
  <role>Agent</role>
  <page>
   <gadget>/desktop/gadgets/CallControl.xml</gadget>
  </page>
  <tabs>
   <tab>
    <id>home</id>
    <label>finesse.container.tabs.agent.homeLabel</label>
    <gadgets>
     <gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight
      =310&viewId=76D964AD10000140000000830A4E5E6F&filterId=AgentCSQStats.csqName
      =CL&compositeFilterId=AgentCSQStats.AgentIds.agentId=loginId</gadget>
     <gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight
      =310&viewId=5C626F9C10000140000000600A4E5B33&filterId
      =ResourceIAQStats.resourceId=CL</gadget>
    </gadgets>
    <gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight
     =150&viewId=67D43711100001400000001080A4E5E6B&filterId=ResourceIAQStats.resourceId
     =loginId</gadget>
   </tab>
   <tab>
    <id>myStatistics</id>
    <label>finesse.container.tabs.agent.myStatisticsLabel</label>
    <gadgets>
     <gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight
    =600&viewId=5D411E8A10000140000000230A4E5E6B&filterId=AgentStateDetailStats.agentID
    =loginId</gadget>
    </gadgets>
   </tab>
   <tab>
    <id>manageCall</id>
    <label>finesse.container.tabs.agent.manageCallLabel</label>
   </tab>
```

```
  </tabs>
 </layout>
 <layout>
  <role>Supervisor</role>
  <page>
   <gadget>/desktop/gadgets/CallControl.xml</gadget>
  </page>
```

Step 6 Click **Save**. Cisco Finesse validates the XML file to ensure that it is valid XML syntax and conforms to the Cisco Finesse schema.

Step 7 To verify, log in to Cisco Finesse agent desktop as agent/Cisco Finesse supervisor desktop as supervisor and check the reports.

Add Customized Live Data Gadgets to Desktop Layout

This procedure explains how to create gadget URLs for customized Live Data reports, which are copied from stock reports, and add them to desktop layout.

Note The new gadget renders the report only when the appropriate permission on that report is given in Cisco Unified Intelligence Center.

Procedure

Step 1 Copy the gadget URL of the stock report that you want to customize from **Live Data Gadgets** and paste it in a text editor.

Example:

Consider the URL shown here as the gadget URL. Copy and paste it in a text editor. The underlined ID is the value of viewID.

```
<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310
&viewId=5C626F9C10000140000000600A4E5B33&filterId=ResourceIAQStats.resourceId=CL</gadget>
```

Step 2 In Cisco Unified Intelligence Center, in the Edit view of the customized report, select the view for which you want to create the gadget URL and then click **Links**.

The HTML Link field displays the permalink of the customized report.

Step 3 Copy the permalink of the customized report from the **HTML Link** field and paste it in a text editor, then copy the viewID value from this link.

Example:

Copy the underlined viewID value from the permalink of the customized report.

```
https://<Server Name>:8444/cuic/permalink/PermalinkViewer.htmx?
viewId=5C90012F10000140000000830A4E5B33&linkType=htmlType&viewType=Grid
```

Step 4 Replace the viewID value in the gadget URL with the viewID value from the permalink of the customized report.

Example:

The customized gadget URL appears as shown here after replacing the viewID value with the viewID value of the customized report.

```
<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310
&viewId=5C90012F10000140000000830A4E5B33&filterId=ResourceIAQStats.resourceId=CL</gadget>
```

Step 5 Add the customized gadget URL to Desktop Layout in the Finesse administration console and save.

Step 6 Log in to Finesse desktop and check the report.

Configure Live Data Reports with Multiple Views

Cisco Finesse allows you to display multiple Live Data reports or views on a single gadget. Supervisors can select the desired view to display from a drop-down list on the gadget toolbar, which lists up to five report views in *Report Name - View Name* format.

This procedure describes how to add multiple Live Data views to the Finesse desktop layout using the viewId_n and filterId_n keys. You can specify up to five report views to appear in your gadget. The first view among the five is the default view. There is no defined order for how the remaining views are displayed.

Finesse still supports the display of a single gadget using a single viewId. However, if you specify the single viewId along with multiple viewId_n keys, the multiple views are used and the single viewId is ignored.

Note To make sure the modified gadget renders in the Finesse desktop, you must give the appropriate permission for that report in Unified Intelligence Center.

Procedure

Step 1 For each report or view that you want to include in the gadget, obtain the associated viewId from the permalink for the view:

a) In Unified Intelligence Center, in Edit view of the report, select the desired view then click **Links**.

The HTML Link field displays the permalink of the customized report.

b) Copy the permalink of the customized report from the **HTML Link** field, and paste it in a text editor, and then copy the viewID value from the permalink and save it.

Example:

Copy the viewId, which is underlined in this example, from the permalink for the report.

```
https://<Server Name>:8444/cuic/permalink/PermalinkViewer.htmx?
viewId=5C90012F10000140000000830A4E5B33&linkType=htmlType&viewType=Grid
```

Step 2 From the Finesse default layout XML, copy the gadget URL for one of the Live Data reports and paste it into a text editor.

Example:

Copy the URL for the Agent Skill Group for HTTPS from the default layout XML and paste it into a text editor:

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

Step 3 To update the URL to refer to a different report view, populate the viewId_1 value (after the equal sign) with the desired viewId obtained in step 1.

Example:

The following shows the URL updated with the example viewId copied from step 1.

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName</gadget>
```

Step 4 For each additional view you want to include:

a) At the end of the URL, copy and paste the viewId_1 and agentId_1 strings with a leading ampersand.

Example:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName</gadget>
```

b) Update the copied viewId_1 and filterId_1 in the URL to the next available integer (in this example, viewId_2 and filterId_2).

Example:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName&
viewId_2=5C90012F10000140000000830A4E5B33&filterId_2=agent.id=CL%20teamName</gadget>
```

c) Populate the copied viewId value (after the equal sign) with the value defined in the permalink for the desired report (in this example, `99E6C8E210000141000000D80A0006C4`).

Example:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName&
viewId_2=99E6C8E210000141000000D80A0006C4&filterId_2=agent.id=CL%20teamName</gadget>
```

d) Make sure that the filterId value matches the type required by the report type, as follows:

- Agent Reports: filterId_*N*=agent.id=CL%20teamName
- Agent Skill Group Reports: filterId_*N*=agent.id=CL%20teamName
- Skill Group Reports: filterId_*N*=skillGroup.id=CL%20teamName
- Precision Queue Reports: filterId_*N*=precisionQueue.id=CL%20teamName

Step 5 Replace my-cuic-server with the FQDN of your Cisco Unified Intelligence Center Server.

Step 6 Add the customized gadget URL to the desktop layout XML in the Manage Desktop Layout gadget and click **Save**.

Manage Phone Books

On the Phone Books tab of the Cisco Finesse administration console, you can create and manage global and team phone books and phone book contacts. Global phone books are available to all agents; team phone books are available to agents in that specific team.

Phone Books and Contacts

Finesse supports the following number of phone books:

- 10 global phone books
- 300 team phone books

The system supports a total of 50,000 contacts. The total number of contacts per agent across all phone books is limited to 6000.

Use the Manage Phone Books gadget to view, add, edit, or delete phone books and phone book contacts. Click the Name or Assign To headers to sort the phone books in ascending or descending order. Click the last Name, First Name, Number, or Note headers to sort the contacts in ascending or descending order.

The following table describes the fields on the Manage Phone Books gadget:

Field	Explanation
Name	The name of the phone book. It must be unique, and can be a maximum of 64 alphanumeric characters.
Assign To	Indicates if the phone book is global (All Users) or team (Teams).
Last Name	The last name of a contact. The last name can be a maximum of 128 characters. This field is optional.
First Name	The first name of a contact. The first name can be a maximum of 128 characters. This field is optional.
Number	The phone number for the contact. The phone number can be 1-32 characters long and cannot be blank.
Note	Optional text that describes the contact. The note can be a maximum of 128 characters.

Actions on the Manage Phone Books gadget:

- **New:** Add a new phone book or contact
- **Edit:** Edit an existing phone book or contact
- **Delete:** Delete a phone book or contact
- **Refresh:** Reload the list of phone books or contacts from the server
- **Import:** Import a list of contacts to the phone book
- **Export:** Export a list of contacts from the phone book

Add Phone Book

Procedure

Step 1 In the Manage Phone Books gadget, click **New**.

Step 2 In the **Name** field, enter a name for the phone book.

Note
Phone book names can be a maximum of 64 characters.

Step 3 From the **Assign To** drop-down, select **All Users** if the phone book is global or **Teams** if the phone book is available to specified teams.

Step 4 Click **Save**.

Edit Phone Book

Procedure

Step 1 In the Manage Phone Books gadget, select the phone book you want to edit.

Step 2 Click **Edit**.

Step 3 In the **Name** field, enter the new name for the phone book. If you want to change who can access the phone book, in the **Assign To** drop-down, choose **All Users** or **Teams**.

Step 4 Click **Save**.

If you change the Assign To field from Teams to All Users, click **`Yes`** to confirm the change.

Delete Phone Book

Procedure

Step 1 In the Manage Phone Books gadget, select the phone book that you want to delete.

Step 2 Click **Delete**.

Step 3 Click **Yes** to confirm the deletion of the selected phone book.

Import Contacts

The Import function allows you to replace all the contacts in a phone book with a new list of contacts, or to populate a new phone book with contacts.

The import list must be in the specified comma separated values (CSV) format, and can contain a maximum of 6000 contacts. Import lists that contain more than 6000 contacts are rejected with an error message.

The CSV file contains the fields described in the following table:

Field	Max Length	Can Be Blank?	Permitted Characters
First Name	128	Yes	Alphanumeric characters **Note** The CSV file that contains the contacts to import must use Latin encoding.
Last Name	128	Yes	
Phone Number	32	No	
Notes	128	Yes	

The following is an example of a phone book CSV file:

```
"First Name","Last Name","Phone Number","Notes"
"Amanda","Cohen","6511234",""
"Nicholas","Knight","612-555-1228","Sales"
"Natalie","Lambert","952-555-9876","Benefits"
"Joseph","Stonetree","651-555-7612","Manager"
```

A phone book CSV file must conform to this format and include the headers in the first line. During import, the file is scanned for illegal characters. If any are found, they are replaced with question marks.

Note Exported CSV files always show each field enclosed in double quotes to ensure that any commas or double quotes that are part of the actual filed data are not mistaken for field delimiters. If your data does not include these characters, you can omit the double quotes in files you prepare for importing.

Procedure

Step 1 In the Manage Phone Books gadget, select the phone book into which you want to import a list of contacts.

Step 2 Click **Import**.

Step 3 Click **Browse** and navigate to the location of the CSV file containing the contacts you want to import.

Note
The CSV file must use Latin encoding.

Step 4 Click **OK**.

Export Contacts

The Export function allows you to extract a list of contacts from an existing phone book. The exported list is saved in CSV format.

Procedure

Step 1 In the Manage Phone Books gadget, select the phone book that contains the contacts you want to export.

Step 2 Click **Export**.

Step 3 Click **Open** to open the CSV file in Excel, or click the **Save** drop-down list and choose **Save**, **Save as**, or **Save and open**.

Add Contact

Procedure

Step 1 In the Manage Phone Books gadget, select the phone book to which you want to add a contact.

The List of Contacts for <phone book name> area appears.

Step 2 Click **New**.

Step 3 Complete the fields. The First Name, Last Name, and Note fields are optional and have a maximum length of 128 characters. The Number field is required and has a maximum length of 32 characters.

Step 4 Click **Save**.

Edit Contact

Procedure

Step 1 In the Manage Phone Books gadget, select the phone book that contains the contact you want to edit.

The List of Contacts for <phone book name> area appears.

Step 2 Select the contact you want to edit.

Step 3 Click **Edit**.

Step 4 Edit the fields that you want to change. The First Name, Last Name, and Note fields are optional and have a maximum of 128 characters. The Number field is required and has a maximum of 32 characters.

Step 5 Click **Save**.

Delete Contact

Procedure

Step 1 In the Manage Phone Books gadget, select the phone book that contains the contact you want to delete.

The List of Contacts for <phone book name> area appears.

Step 2 Select the contact that you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Yes** to confirm the deletion of the selected contact.

Manage Reasons

The Reasons tab on the Cisco Finesse administration console allows you to view, add, edit, and delete Not Ready reason codes, Sign Out reason codes, and Wrap-Up reasons.

Note Certain reason codes are reserved and cannot be used.

For Unified CCX systems, these reserved reason codes are as follows: 0, 22, and 33.

Not Ready Reason Codes

Not Ready reason codes represent reasons that agents can select when they change their state to Not Ready.

Use the Manage Reason Codes (Not Ready) gadget to view, add, edit, or delete Not Ready reason codes.

1. Click the Reason Label or Reason Code headers to sort the Not Ready reason codes by label or reason code in ascending or descending order.
2. Click the Type header to sort and display system or custom reason codes.
3. Click the Global header to sort reason codes by whether they are global (Yes) or not (No).

Not Ready reason codes can be global (visible to all agents) or team (visible only to agents on specified teams).

Note Finesse supports a total of 200 Not Ready reason codes. This includes a maximum of 100 global Not Ready reason codes, and 100 team Not Ready reason codes. The team reason codes can be mapped to any team, and the same reason code can be mapped to multiple teams.

The following table describes the fields on the Manage Reason Codes (Not Ready) gadget:

Field	Explanation
Reason Label	The label for the Not Ready reason code. The label has a maximum length of 40 characters and should be unique for each Not Ready reason code. Alphanumeric and special characters are supported.
Type	The type of reason code (System or Custom). The column is default and can be sorted to display both System reason codes and Custom reason codes.
Reason Code	A code for the Not Ready reason. The value of the code must be between 1 and 999 and must be unique.
Global?	Yes/No. Indicates if the reason code is available globally to all agents (Yes) or to specific teams of agents (No).

Actions on the Manage Reason Codes (Not Ready) gadget:

- **New:** Add a new Not Ready reason code
- **Edit:** Edit an existing Not Ready reason code
- **Delete:** Delete a Not Ready reason code
- **Refresh:** Reload the list of Not Ready reason codes from the server

Note When you add, edit, or delete a Not Ready reason code, the changes you make take effect on the Finesse desktop after three seconds. However, agents who are signed in when the changes are made must sign out and sign back in to see those changes reflected on their desktops.

When an agent signs in to the Finesse desktop, the agent state is set to Not Ready. The agent can then choose to go to Ready status or choose from one of the configured Not Ready reason codes from the agent state drop-down list.

If an agent wants to change from Ready to Not Ready status, that agent can choose the appropriate Not Ready reason code from the list of configured codes.

An agent who is on a call can select a state to be applied when the call is complete. For example, if an agent wants to be in Not Ready state when the call ends, that agent can choose Not Ready from the drop-down list while still on the call. The Finesse desktop shows the agent in Talking state and a pending state of Not Ready.

Pending state changes appear on the desktop while the agent's state is Talking (for example, on hold, in a consult call, conference, or silent monitor call).

Note During a PG or CTI server failover, the pending state of an agent is not retained.

Add Not Ready Reason Code

Procedure

Step 1 In the Manage Reason Codes (Not Ready) gadget, click **New**.

Step 2 In the Reason Label box, enter a label for the reason code.

Note
Not Ready reason code labels are limited to 40 characters.

Step 3 In the Reason Code box, an auto populated reason code is displayed. If you choose not to save the prepopulated reason code, you can enter your own reason code.

Note
The code must be between 1 and 999 and must be unique.

Ensure there are no leading or trailing spaces.

Step 4 If the reason code is global, select the Global? check box. If the reason code is specific to a team, clear the Global? check box.

Note
By default, the Global? check box is selected.

Step 5 Click **Save**.

Note
The Finesse server removes leading or trailing spaces before saving the Reason Label in the database.

Edit Not Ready Reason Code

Procedure

Step 1 In the Manage Reason Codes (Not Ready) gadget, select the reason code that you want to edit.

Step 2 Click **Edit**.

Step 3 If you want to change the label for the Not Ready reason code, in the Reason Label field, enter a new label for the reason code. If you want to change the code, in the Reason Code field, enter the new code. If you want to change who has access to the code, select or clear the Global? check box.

Step 4 Click **Save**.

Delete Not Ready Reason Code

Note An error may occur if an agent selects a Not Ready reason code after it has been deleted. Agents who are signed in when you make changes to Not Ready reason codes must sign out and sign back in to see those changes reflected on their desktops.

Procedure

Step 1 In the Manage Reason Codes (Not Ready) gadget, select the Not Ready reason code that you want to delete.

Step 2 Click **Delete**.

Step 3 Click **Yes** to confirm the deletion of the selected reason code.

Sign Out Reason Codes

Sign Out reason codes represent reasons that agents can select when they sign out of the Finesse desktop.

Use the Manage Reason Codes (Sign Out) gadget to view, add, edit, or delete Sign Out reason codes. Click the Reason Label or Reason Code headers to sort the Sign Out reason codes by label or by reason code, in

ascending or descending order. Click the Type header to sort and display system or custom reason codes. Click the Global header to sort the reason codes by whether they are global (Yes) or not (No).

Sign Out reason codes can be global (visible to all agents) or team (visible only to agents on specified teams).

Note Finesse supports 200 Sign Out reason codes. These include 100 global Sign Out reason codes, and 100 Sign Out team reason codes. The team reason codes can be mapped to any team, and the same reason code can be mapped to multiple teams.

The following table describes the fields on the Manage Reason Codes (Sign Out) gadget:

Field	Explanation
Reason Label	The label for the Sign Out reason code. The label has a maximum length of 40 characters and should be unique for each Sign Out reason code. Alphanumeric and special characters are supported.
Type	The type of reason code (System or Custom). The column is default and can be sorted to display both System reason codes and Custom reason codes.
Reason Code	A code for the Sign Out reason. The code must be between 1 and 999 and must be unique.
Global?	Yes/No. Indicates if the reason code is available globally to all agents (Yes) or to specific teams of agents (No).

Actions on the Manage Reason Codes (Sign Out) gadget:

- **New:** Add a new Sign Out reason code
- **Edit:** Edit an existing Sign Out reason code
- **Delete:** Delete a Sign Out reason code
- **Refresh:** Reload the list of Sign Out reason codes from the server

Note When you add, edit, or delete a Sign Out reason code, the changes you make take effect on the Finesse desktop after three seconds. However, agents who are signed in when the changes are made must sign out and sign in again to see those changes reflected on their desktops.

When an agent clicks Sign Out on the desktop, any configured Sign Out codes appear in a drop-down list. The agent can select the code that represents why that agent is signing out.

Add Sign Out Reason Code

Procedure

Step 1 In the Manage Reason Codes (Sign Out) gadget, click **New**.

Step 2 In the Reason Label box, enter a label for the reason code.

Note
Sign Out reason code labels are limited to 40 characters.

Step 3 In the Reason Code box, an auto populated reason code is displayed. If you choose not to save the prepopulated reason, you can enter your own reason code.

Note
The code must be between 1 and 999 and must be unique.

Ensure there are no leading or trailing spaces.

Step 4 If the reason code is global, select the Global? check box. If the reason code is specific to a team, clear the Global? check box.

Note
By default, the Global? check box is selected.

Step 5 Click **Save**.

Edit Sign Out Reason Code

Procedure

Step 1 In the Manage Reason Codes (Sign Out) gadget, select the reason code that you want to edit.

Step 2 Click **Edit**.

Step 3 If you want to change the label of the Sign Out reason code, in the Reason Label field, enter a new label for the reason code. If you want to change the code, in the Reason Code field, enter the new code. If you want to change who has access to the code, select or clear the Global? check box.

Step 4 Click **Save**.

Delete Sign Out Reason Code

Note An error may occur if an agent selects a Sign Out reason code after it has been deleted. Agents who are signed in when you make changes to Sign Out reason codes must sign out and sign back in to see those changes reflected on their desktops.

Procedure

Step 1 In the Manage Reason Codes (Sign Out) gadget, select the Sign Out reason code that you want to delete.

Step 2 Click **Delete**.

Step 3 Click **Yes** to confirm the deletion of the selected Sign Out reason code.

Predefined System Reason Codes

For Not Ready system reason codes and Sign Out system reason codes, only the reason code label can be edited and saved. The Global attribute and system code cannot be modified. In case the system reason code label is modified and you wish to revert to the default label, refer to the following list of predefined system reason codes:

System Reason Code	Reason Label	Reason Label Description
32767	Logged Out - Device Conflict	The system issues this reason code when an agent is already logged in to one device (computer or phone) and then tries to re-login to a second device.
32765	Logged Out - System Disconnect	The system issues this reason code when a Cisco Finesse IP Phone Agent or Cisco Finesse desktop crashes due to any reason or if the connection is disrupted.
32764	Logged Out - System Standby	The system issues this reason code when the active server becomes the standby server and the agent loses connection to the Unified CCX Platform.
32763	Not Ready - Call Not Answered	The system issues this reason code when the agent fails to answer a Unified CCX call within the specified timeout period.
32762	Not Ready - Offhook	The system issues this reason code when the agent goes off the hook to place a call. If the agent remembers to do this task the corresponding agent-triggered reason code is displayed. If the agent does not remember to do this task, the system issues this reason code.
32761	Not Ready - Non ACD Busy	The system issues this reason code when the agent is logged on to the Cisco Finesse desktop or Cisco Finesse IP phone and then receives a call that is not queued on the Unified CCX Platform.
32760	Not Ready - Log On	The system issues this reason code when an agent logs in and is automatically placed in the Not Ready state.
32759	Not Ready - Phone Failure	The system issues this reason code if the agent’s phone crashes and that agent is placed in the unavailable state.

32758	Not Ready - Wrap Up Timer Expiry	The system issues this reason code when an agent's state is changed from WORK to Not Ready. This change occurs if the WORK state for that agent's CSQ is associated with an expired wrap-up timer.
32757	Not Ready - CUCM Failover	The system issues this reason code when the Unified CM fails over and the agent is moved to the Not Ready state.
32756	Not Ready - Phone Working	The system issues this reason code when the agent's phone comes up after it has been through a Phone Down state.
32755	Not Ready - Call Ended	The system issues this reason code when an agent is moved to the Not Ready state after handling a Unified CCX call. This situation occurs in one of two cases: **1.** If an agent (Agent 1) is in the Not Ready state and gets a consult Unified CCX call from another agent (Agent 2). In this case, after handling the call, Agent 1 moves back to the Not Ready state. **2.** If an agent's Automatic Available option is disabled and this agent gets a Unified CCX call, then this agent goes to the Not Ready state after handling the call.
32749	Not Ready - Call Cancel	The system issues this reason code when an agent's state is changed from TALKING to Not Ready because of the Cancel feature. The feature is triggered during an ICD consult call between two agents. When the consulting agent presses the Cancel softkey on the phone, the consulted agent is no longer associated with an ICD call and their state changes to Not Ready. This feature is only available on some newer phone models.
32754	Not Ready - Restricted Device	The system issues this reason code if the agent device is flagged as a restricted device by the Unified CM Administrator.
32753	Not Ready - Restricted Line	The system issues this reason code if the agent's phone line is flagged as a restricted device by the Unified CM Administrator.
32752	Not Ready - Cancel Reservation Preview Call	The system issues this reason code when an agent receives a preview outbound call and decides to cancel the reservation by pressing "Decline" button on Cisco Finesse desktop.
32751	Not Ready - Skip Preview Call	The system issues this reason code when an agent receives a preview outbound call and skips the call.
32748	Log Out - Agent Deleted	Agent is logged out from Unified CCX as the agent is deleted from Unified Communications Manager. This event is triggered when Unified CCX synchronizes the agent information with Unified Communications Manager.
32750	Not Ready - Extension Modified	The system issues this reason code when an agent is logged out from CCX because the agent's IPCC extension was changed in Unified Communications Manager.

32742	Not Ready - Non ACD Offhook	Agent's state is changed from Ready state to Not Ready state when the monitored Non ICD lines are used for Incoming or Outgoing calls.
32741	Logged Out - Extension Conflict	The system issues this reason code when an agent logs in to Cisco Finesse using an extension number that has already been used by another agent to log in, the first agent is logged out forcibly with this reason code.
32740	Logout - System Initiated Relogin	The system logs out the agent from one session when the agent tries to log in with the same credentials in another session.
33	Not Ready - Supervisor Initiated	The system issues this reason code when the Supervisor changes an agent’s state to Not Ready state.
22	Logged Out - Supervisor Initiated	The system issues this reason code when the Supervisor changes an agent’s state to log out.
255	Logged Out - Connection Failure	The system issues this reason code when the agent is forcibly logged out when there is a connection failure between the Cisco Finesse Desktop and the Cisco Finesse Server.

Manage Reason Code Conflicts During Upgrade

System Reason Codes are auto-generated reason codes that may conflict with custom reason codes when upgrading from an older version to Cisco Finesse 11.6(1). If there is a reason code conflict then the following message appears when you sign in to the administration console:

Custom reason codes conflict with system reason codes. Resolve to avoid reporting inconsistency.

Note Clear your browser cache to ensure that you are allowed to view and resolve system reason code conflicts.

All conflicting reason codes are highlighted. To edit, select each conflicting reason code and click **Edit**. The **Edit Reason Code** area appears. Select the reason code from the available options listed or enter any other code you wish. The code must be unique to the particular category (Not Ready or Sign Out).

Once resolved, the reason code gets sorted based on the reason code number and placed in the table accordingly.

Wrap-Up Reasons

Wrap-Up reasons represent the reasons that agents can apply to calls. A Wrap-Up reason indicates why a customer called the contact center. For example, you may have one Wrap-Up reason for sales calls and another for support calls.

You can configure Wrap-Up reasons to be available globally to all agents or only to specific teams.

Use the Manage Wrap-Up Reasons gadget to view, add, edit, or delete Wrap-Up reasons. Click the Reason Label header to sort the Wrap-Up reasons in ascending or descending order.

Note Cisco Finesse supports a maximum of 100 global and 1500 team Wrap-Up reasons. No more than 100 Wrap-Up reasons can be assigned to any one team.

Cisco Finesse supports the wrap-up functionality for all types of inbound and outbound calls.

- Set the Work mode on incoming attribute to either *Optional* or *Required*.
- Set the Work mode on outgoing attribute to either *Optional* or *Not Allowed*.

If the Work mode on incoming attribute is set to Required, agents automatically transition to wrap-up state after an incoming or Outbound Option call ends. If the Work mode on incoming attribute is set to Optional, agents must select Wrap-Up from the agent state drop-down list while on a call to transition to wrap-up state when the call ends. If the agent does not select Wrap-Up during the call, the agent does not transition to wrap-up state when the call ends.

Note The showWrapUpTimer property can be used to show or hide timer in wrap-up state.

If showWrapUpTimer is set to true then timer is displayed.

If showWrapUpTimer is set to false then timer is hidden.

Note Wrap-Up timer is configurable. By default wrapUpCountDown property is set to true. The timer counts down by default when the agent is in wrap-up state. For more information, see *Desktop Properties*.

For Example, if you set the timer to 30 seconds, by default the timer starts from 30 and ends at zero.

The default behavior can be changed by setting the wrapUpCountDown property to false.

If an agent is configured for wrap-up and selects a pending state during a call, when the call finishes that agent goes into the pending state selected during the call.

The following table describes the fields on the Manage Wrap-Up Reasons gadget:

Field	Explanation
Reason Label	The label for the Wrap-Up reason. This label must be unique for each Wrap-Up reason and has a maximum length of 39 bytes (which equals 39 US English characters). Both alphanumeric and special characters are supported.
Global?	Yes/No. Indicates if the Wrap-Up reason is available globally to all agents (Yes) or to specific teams of agents (No).

Actions on the Manage Wrap-Up Reasons gadget:

- **New:** Add a new Wrap-Up reason
- **Edit:** Edit an existing Wrap-Up reason

- **Delete:** Delete a Wrap-Up reason
- **Refresh:** Reload the list of Wrap-Up reasons from the server

Note When you add, edit, or delete a Wrap-Up reason, the changes you make take effect on the agent or supervisor desktop after three seconds. However, agents who are signed in when the changes are made must sign out and sign in again to see those changes reflected on their desktops.

Add Wrap-Up Reason

Procedure

Step 1 In the Manage Wrap-Up Reasons gadget, click **New**.

Step 2 In the Reason Label field, add a label for the Wrap-Up reason.

Note
Wrap-Up reason labels are limited to 39 bytes.

Step 3 If the Wrap-Up reason is global, select the Global? check box. If the Wrap-Up reason is specific to a team, clear the Global? check box.

Note
By default, the Global? check box is selected.

Step 4 Click **Save**.

Edit Wrap-Up Reason

Procedure

Step 1 In the Manage Wrap-Up Reasons gadget, select the Wrap-Up reason that you want to edit.

Step 2 Click **Edit**.

The Edit Wrap-Up Reason area appears.

Step 3 In the Wrap-Up Reason Label field, enter the new label for the Wrap-Up reason. If you want to change who has access to the Wrap-Up reason, select or clear the Global? check box.

Step 4 Click **Save**.

Delete Wrap-Up Reason

Procedure

Step 1 In the Manage Wrap-Up Reasons gadget, select the Wrap-Up reason that you want to delete.

Step 2 Click **Delete**.

A question appears asking you to confirm that you want to delete the selected Wrap-Up reason.

Step 3 Click **Yes** to confirm the deletion of the selected Wrap-Up reason.

Force Wrap-Up Reason

For voice channel-If the Force Wrap-Up reason is configured, agents must select a Wrap-Up reason before changing the state after the call ends. The agent cannot change the state until the Wrap-up reason is applied. The Wrap-Up reason can be selected during the call or after the call ends.

For digital channels-If the Force Wrap-Up reason is configured, agents must select a Wrap-Up reason before transfering or ending an interaction.

Note The Force Wrap-Up reason is disabled by default. Use the CLI commands to enable and disable this feature. For more information, see *Desktop Properties* in Cisco Finesse Administration Guide.

Manage Team Resources

You can assign phone books, reason codes, wrap-up reasons, custom desktop layouts, and workflows to teams on the Team Resources tab of the administration console.

Team Resources

Use the Manage Team Resources gadget on the Team Resources tab to assign and unassign phone books, reasons, custom desktop layouts, and workflows to teams. Click the Name or ID header to sort the teams in ascending or descending order.

The Manage Team Resources gadget contains six tabs, each enabling you to assign or unassign resources to a team. The tabs are defined in the following table:

Tab Name	Description
Desktop Layout	Use this tab to customize the desktop layout for the team. The default layout is defined in the Manage Desktop Layout gadget. You can define one custom layout for the team.
Phone Books	Use this tab to assign and unassign phone books to the team. Only phone books that are defined in the Manage Phone Books gadget as available to teams are available for assignment.

Tab Name	Description
Reason Codes (Not Ready)	Use this tab to assign and unassign Not Ready reason codes to the team. Only Not Ready reason codes that are defined in the Manage Reason Codes (Not Ready) gadget as available to teams (not global) are available for assignment.
Reason Codes (Sign Out)	Use this tab to assign and unassign Sign Out reason codes to the team. Only Sign Out reason codes that are defined in the Manage Reason Codes (Sign Out) gadget as available to teams (not global) are available for assignment.
Wrap-Up Reasons	Use this tab to assign and unassign Wrap-Up reasons to the team. Only Wrap-Up reasons that are defined in the Manage Wrap-Up Reasons gadget as available to teams (not global) are available for assignment.
Workflows	Use this tab to assign and unassign workflows to the team. Only workflows that are defined in the Manage Workflows gadget are available for assignment.

Actions on the Manage Team Resources Gadget

- **Add**: Assign a phone book, reason, or workflow to the team
- **Save**: Save the phone book, reason, desktop layout assignment, or workflow to the team
- **Revert**: Cancel any changes made before they are saved
- **Refresh**: Refresh the list of teams

Note If you select a team and then click Refresh, the team is deselected and the Resources area for that team disappears. The list of teams is refreshed and you must select a team again.

Add or Delete a Team When Database is Not Accessible

If you add or delete a team when Finesse cannot access the Finesse database, those changes do not appear in the Finesse administration console unless you restart Cisco Finesse Tomcat or the Cisco Unified CCX Engine.

Assign Phone Books and Reasons to Team

Procedure

Step 1 In the Manage Team Resources gadget, select a team.

Step 2 Click the tab for the resource you want to assign for the selected team.

Step 3 Click **Add**.

Step 4 Select one or more resources from the list to assign them to the team.

Resources you assign are highlighted in blue in the Add <resources> popup and added to the List of <resources> area.

Step 5 When you finish assigning resources, click **Save**.

Note
You can make changes on all resource tabs and then save them at the same time. If there is an error on one resource tab but not others, the changes on the tabs with no errors are saved while the changes on the tab with errors are not saved.

Unassign Phone Books and Reasons from Team

Procedure

Step 1 In the Manage Team Resources gadget, select a team.
Step 2 Click the tab for the resource you want to unassign from the selected team.
Step 3 Click the red X next to the resource you want to unassign.
Step 4 Click **Save**.

Assign Custom Desktop Layout to Team

Procedure

Step 1 In the **Manage Team Resources** gadget, select a team.
Step 2 Click **Desktop Layout**.

The Desktop Layout XML area appears. The area contains the default desktop layout XML.

Step 3 Select the **Override System Default** check box.

The XML becomes editable.

Step 4 Select from the following editors:

- **Text Editor**
- **XML Editor**

For more information, see *Default Layout XML*.

Step 5 Edit the XML.
Step 6 Click **Save**.

The custom desktop layout replaces the default desktop layout for the team after 10 seconds. If a supervisor or agent is signed in when the change is saved, the change does not take effect on their desktop until the supervisor or agent signs out and signs in again.

Note
If you clear the Override System Default check box, any changes you made to the XML are lost and the XML in the editing pane reverts to the default desktop layout XML.

Note If the Supervisor is managing single / multiple teams, the custom layout of the team for which the supervisor is a resource/agent is displayed. However, if the supervisor is not the resource/agent of a team, the layout of the default team is displayed.

Customize Desktop Properties at Team Level

You can customize the Finesse desktop properties for a specific team.

Procedure

Step 1 In the **Manage Team Resources** gadget, select a team.

Step 2 Click **Desktop Layout**.

Step 3 Select the **Override System Default** check box.

Step 4 Select from the following editors:

- **Text Editor**
- **XML Editor**

Step 5 Enter the desktop property name in the config key tag.

Step 6 Enter the possible value of the desktop property in the value tag.

The following are the sample desktop property entries, as displayed in the default **Desktop Layout**. To change these desktop property entries in **Text Editor**, remove the comment (<!-- and -->) and set appropriate values.

Note
If the property value is defined in the team-specific desktop layout (**Manage Team Resources** > **Desktop Layout**), then the team-specific desktop layout takes precedence over the property value defined in the **Desktop Layout** and CLI.

For more information on customizing desktop properties at **Desktop Layout**, see *Customize Desktop Properties*.

For more information on Finesse CLIs, see *Desktop Properties*.

The following table lists the desktop properties that support team-level updates:

Config Key	Value	Default Value
enableDragDropAndResizeGadget	true|false	false
enableShortCutKeys	true|false	true
forceWrapUp	true|false	true
wrapUpCountDown	true|false	true
showWrapUpTimer	true|false	true
desktopChatAttachmentEnabled	true|false	true
desktopChatMaxAttachmentSize	Range: 1—10 (MB)	5

Config Key	Value	Default Value
desktopChatUnsupportedFileTypes	Unsupported file formats include comma-separated valid file extensions. For example: .exe, .sh	.exe, .msi, .sh, .bat
showAgentHistoryGadgets	true|false	true
showActiveCallDetails (for Supervisor Only)	true|false	true
pendingDTMFThresholdCount	Range: 1—20	20
dtmfRequestTimeoutInMs	Range: 1000—200000 (1 to 200 seconds)	5000 (5 seconds)
enableDropParticipantFor	supervisor_only|conference_controller_ and_supervisor|all	supervisor_only
dropParticipant	agents|all	agents

Note

- To enable the following Finesse desktop properties in Cisco Finesse, install Cisco Finesse Release 12.5(1) ES1 COP or higher.
  - pendingDTMFThresholdCount
  - dtmfRequestTimeoutInMs
- To enable the following Finesse desktop properties in Cisco Finesse, install Cisco Finesse Release 12.5(1) ES4 COP or higher.
  - enableDropParticipantFor
  - dropParticipant

For more information on Finesse desktop properties, see *Desktop Properties*.

Step 7 Click **Save**.

The change takes effect when the agent or supervisor refreshes the Finesse desktop or sign out and sign in again.

Note
If you clear the **Override System Default** check box and click **Save**. The changes are overwritten, and the editing pane reverts to the default desktop layout XML.

Assign Workflows to Team

Procedure

Step 1 In the Manage Team Resources gadget, select a team.

Step 2 Click the Workflows tab.

Step 3 Click **Add**.

Step 4 Select one or more workflows from the list to assign them to the team.

Workflows you assign are highlighted in blue in the Add Workflows popup and added to the List of Workflows area.

Step 5 Workflows are run in the order they are listed. Use the up and down arrows to move a selected workflow to the desired position in the list.

Step 6 When you has finished assigning workflows, click **Save**.

Note
You can make changes on all resource tabs and then save them at the same time. If there is an error on one resource tab but not on others, the changes on the tabs with no errors are saved while the changes on the tab with errors are not saved.

Unassign Workflows from Team

Procedure

Step 1 In the Manage Team Resources gadget, select a team.

Step 2 Click the Workflows tab.

Step 3 Click the red X next to the workflow to unassign.

Step 4 Click **Save**.

Manage Workflows

On the Workflows tab of the Cisco Finesse administration console, you can create and manage workflows and workflow actions.

Workflows and Workflow Actions

You can use workflows to automate common repetitive agent tasks. A workflow has a unique name and a helpful description. Use the Manage Workflows and Manage Workflow Actions gadgets to view, add, edit, or delete workflows and workflow actions.

All workflows are team-level workflows. You cannot create a global workflow. If you need a global workflow, create a team workflow and assign it to all teams.

Cisco Finesse supports the following number of workflows and workflow actions:

- 100 workflows per Cisco Finesse system
- 100 actions per Cisco Finesse system
- 20 workflows per team
- Five conditions per workflow
- Five actions per workflow
- Five variables per action
- For Voice - Call variables, Outbound Option variables, queue details, wrap-up reasons, agent details, or team details.
- For Email - Queue name and email attributes like From, To, Cc, Bcc, or Subject.
- For Chat - Queue name, chat type, or system defined customer details as available from the web chat form.

Click the column headers to sort workflows and workflow actions in ascending or descending order.

The following table describes the fields on the Manage Workflows gadget:

The following table describes the fields on the Manage Workflow Actions gadget:

Field	Explanation
Name	The name of the workflow action must be unique and can have a maximum length of 64 characters.
Type	The type of workflow. Possible values are Browser Pop and HTTP Request.

Actions on the Manage Workflows and Manage Workflow Actions gadgets:

- **New:** Add a new workflow or workflow action
- **Edit:** Edit a workflow or workflow action
- **Delete:** Delete a workflow or workflow action
- **Refresh:** Reload the list of workflows or workflow actions from the server.

You can configure workflow actions to be handled by the Cisco Finesse desktop or in a third-party gadget. A third-party gadget can be designed to handle the action differently than Cisco Finesse does.

Each workflow must contain only one trigger. Triggers are based on Cisco Finesse dialog events.

Note You can configure the trigger only after you select the media.

- Voice dialog events include the following:
  - When a Call arrives
  - When a Call is answered
  - When a Call ends

- When making a Call

Note The call variable workflow responds as expected only when you add both the conditions **Is not equal** and **Is not empty**.

- While previewing an Outbound Option call.

The workflow engine uses the following simple logic to determine whether to run a workflow:

Note The workflow logic and examples are similar for all media.

- Its trigger set and conditions are evaluated against each dialog event received.
- The workflow engine processes workflow events for the first call that matches any configured workflow's trigger set and conditions. No other workflows run until this call has ended. If the agent accepts a second call while still on the first call, workflows do not run on the second call even after the first call has ended.
- After a workflow for a particular trigger type (for example, Call Arrives) runs, it never triggers again for the same dialog ID.

The workflow engine caches workflows for an agent when the agent signs in. Workflows do not change for the agent until the agent signs out and signs in again or refreshes the browser.

Note Whenever the browser is refreshed, the workflows that trigger the following events run:

- when a call arrives
- when a call is answered
- when making a call

When an agent refreshes the browser, the workflow engine considers the call as newly arrived or newly made. If an HTTP request action is part of the workflow, the HTTP request is sent when the agent refreshes the browser. Applications that receive the HTTP requests must account for this scenario.

An example of a workflow is a Call Arrival event that triggers an action that collects information from the dialog event (for example, the ANI or customer information) and displays a web page containing customer information.

You can filter trigger events by the value of the data that comes in the event. You can configure a workflow to run if any of the conditions are met or if all the conditions are met.

Individual conditions comprise of the following:

- A piece of event data to be examined. For example, **DNIS** or call variables.
- A comparison between the event data and the values entered (for example **contains**, **is equal to**, **is not equal to**, **begins with**, **ends with**, **is empty**, **is not empty**, and **is in list**).

When the trigger and its conditions are satisfied, a list of actions assigned to the workflow are run. The actions are run in the listed order.

Workflows run only for agents and supervisors who are Cisco Finesse users. The Workflow Engine is a JavaScript library that runs client-side on a per-user basis within the Cisco Finesse desktop application. The desktop retrieves the workflows that are to be run for a user from the server when the user signs in or when the browser is refreshed.

Note Changes made to a workflow or its actions while a user is signed in are not automatically pushed to that user.

It is possible to set workflows, conditions, and actions that are contradictory so that a workflow or action cannot function. Workflows are not validated.

If multiple workflows are configured for a team, the Workflow Engine evaluates them in the configured order. The Workflow Engine ignores workflows with no actions. When the Workflow Engine finds a workflow with a matching trigger for an event and the workflow conditions evaluate to true, that workflow is used, and the subsequent workflows in the list are not evaluated. Workflows with no conditions evaluate to true if the event matches the workflow trigger. All workflows are enabled by default. Only one workflow for a specific user can run at a time.

The Workflow Engine retrieves dialog-based variables that are used in workflow conditions from the dialog that triggered the workflow. If a variable is not found in the dialog, it's value is considered to be empty.

The Workflow Engine runs the actions that are associated with the matched workflow in the order in which they are listed. The Workflow Engine runs actions in a workflow even if the previously run action fails. Failed actions are logged.

The Cisco Finesse server controls the calls that are displayed to the Cisco Finesse user. If the user has multiple calls, the workflow applies only to the first call that matches a trigger. If the first call displayed does not match any triggers but the second call does match a trigger, the Workflow Engine evaluates and processes the triggers for the second call.

A call is considered to be the first displayed call if it is the only call on the Cisco Finesse desktop when it appears. If two calls on a phone are merged (as they are in a conference call), then the first displayed call flag value of the surviving call is used.

If a user has a call and the user refreshes the browser, the Workflow Engine evaluates the call as it is. If the dialog data (call variable values) change, the data may not match the trigger and conditions of the original workflow. The data may match a different workflow or no workflows at all.

If a user has multiple calls and the user refreshes the browser, the Workflow Engine treats the first dialog received from the Cisco Finesse server as the first displayed call. This call may not be the same call that was first displayed before the refreshing the browser. Dialogs received for any other call are ignored because they are not considered as first displayed calls. After refreshing the browser, if dialogs for more than one call are received before the Workflow Engine is loaded, none of the dialogs are evaluated because they are not considered as first displayed calls.

Workflows that are run for both Cisco Finesse agents and supervisors. The team to which the supervisor belongs (as distinguished from the team that the supervisor manages) determines which workflows run for the supervisor. Put the supervisors in their own team to keep agent workflows from being run for them.

Workflow Triggers and Outbound Calls

Note When you create a workflow specifically for Outbound Option calls, add a condition of BAStatus is not empty (except for the Workflow Trigger 'When a call arrives' as BAStatus will be empty at that point of time). This condition ensures that the workflow can distinguish Outbound Option calls from agent-initiated outbound calls.

The following table illustrates when workflows trigger in outbound call scenarios:

Workflow Trigger	Direct Preview Outbound Call	Preview Outbound Call	Progressive/Predictive Outbound Call
While previewing a call	When the agent previews the call (before accepting or rejecting it)	When the agent previews the call (before accepting or rejecting it)	Does not trigger
When a call arrives	Does not trigger	When the agent accepts the call	When the call arrives on the agent desktop
When a call is answered	When the customer answers the call and during failover	When the customer answers the call and during failover	When the customer answers the call
When a call is made	When the customer call is initiated	When the customer call is initiated	When the customer call is initiated, and during failover
When a call ends	When the customer call ends	When the customer call ends	When the customer call ends

Add Browser Pop Workflow Action

The Browser Pop workflow action opens a browser window or tab on the user's desktop when workflow conditions are met.

Note Whether the action opens a new window or tab on the desktop depends on the target user's browser settings.

Procedure

Step 1 In the Manage Workflow Actions gadget, click **New**.

Step 2 In the Name box, enter a name for the action.

Note
Workflow action names are limited to 64 characters.

Step 3 From the Type drop-down list, choose **Browser Pop**.

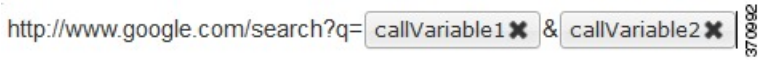
Step 4 From the Handled By drop-down list, choose what will run the action, either the Finesse Desktop or Other (a third-party gadget).

Step 5 In the Window Name box, enter the ID name of the window that is opened. Any action that uses this window name reuses that specific window.

Note
Window names are limited to 40 characters, and can be blank. If you leave the window name blank, a new window opens every time the action runs.

Step 6 Enter the URL of the browser window and click the tag icon at the right of the box and select one or more variables from the drop-down list to add tags.

Example:



For every variable you select, you can enter test data in the Sample Data box. A sample URL is automatically built in the Browser URL box below the Sample Data area. To test the URL, click Open to open the URL in your browser.

Note
Finesse does not validate the URL you enter.

Step 7 Click **Save**.

Add HTTP Request Workflow Action

The HTTP Request workflow action makes an HTTP request to an API on behalf of the desktop user.

Procedure

Step 1 In the Manage Workflow Actions area, click **New**.

Step 2 In the Name box, enter a name for the action.

A workflow action name can contain a maximum of 64 characters.

Step 3 From the Type drop-down list, select **HTTP Request**.

Step 4 From the Handled By drop-down list, select what will run the action, the Finesse desktop or Other (a third-party gadget).

Step 5 From the Method drop-down list, select the method to use.

You can select either PUT or POST.

Step 6 From the Location drop-down list, select the location.

If you are making the HTTP request to a Finesse API, select **Finesse**. If you are making a request to any other API, select **Other**.

Step 7 In the Content Type box, enter the content type.

The default content type is application/xml, which is the content type for Finesse APIs. If you are using a different API, enter the content types for that API (for example, application/JSON).

Step 8 In the URL box, enter the URL to which to make the request. To add variables to the URL, click the tag icon at the right of the box and select one or more variables from the drop-down list.

Example:

The following is the URL example for a Finesse API:

Note
When the location is FINESSE, do not specify the protocol, host, and port information. Finesse automatically fetches these details when the REST request is run.

If you want to make a request to another API, you must enter the entire URL (for example, http://googleapis.com).

You can click the tag icon at the right of the box and select one or more variables from the drop-down list to add tags to the URL. In the preceding example, to add the dialogId, click the tag icon and select dialogId from the list.

Step 9 In the Body box, enter the text for the request. The body must match the content type (for example, if the content types is application/xml, the body must contain XML). To add variables to the body, click the tag icon at the right of the box and select one or more variables from the drop-down list.

Example:

To make an HTTP request to the Dialog - Start a recording API, enter the following into the Body box:

To add the extension, click the tag icon and select extension.

For every variable you add, you can enter test data in the Sample Data box.

Step 10 Click **Save**.

Edit Workflow Action

Procedure

Step 1 In the Manage Workflow Actions gadget, select the action that you want to edit.

Step 2 Click **Edit**.

Step 3 Edit the fields that you want to change.

Step 4 Click **Save**.

Delete Workflow Action

Procedure

Step 1 In the Workflow Actions gadget, select the action that you want to delete.

Step 2 Click **Delete**.

Step 3 Click **Yes** to confirm the deletion of the selected action.

Add Workflow

Procedure

Step 1 In the Manage Workflows gadget, click **New**.

Step 2 From the **Choose Media** drop-down, select the media.

Note
In case of a voice only configuration, the **Choose Media** drop-down will display only Voice.

Step 3 In the **Name** box, enter the name of the workflow.

Note
The name is limited to 40 characters.

Step 4 In the **Description** box, enter a description of the workflow.

Note
The description is limited to 128 characters.

Step 5 In the **When to perform Actions** drop-down list, select the event that triggers the workflow.

Note
The drop-down actions change depending on the selected media.

Step 6 In the **How to apply Conditions** box, select if all conditions are met, or if any conditions are met, and then click **Add Condition** to add up to five conditions.

Note
Variables in the drop-down for conditions are grouped depending on the selected media.

The fields **To**, **Cc**, and **Bcc** support comma seperated values, so that, agents can enter multiple email IDs.

Example:

For example, you can specify that the action is taken when CallVariable 1 equals 123 and CallVariable 2 begins with 2.

Step 7 In the Ordered List of Actions area, click **Add** to open the Add Actions area. Click an action in this area to add it to the Ordered List of Actions.

Step 8 Use the up and down arrows next to the Ordered List of Actions to move actions into the performance order.

Step 9 Click **Save**.

Step 10 Assign the workflow to one or more teams.

Note
A workflow does not run until it is assigned to a team.

Edit Workflow

Procedure

Step 1 In the Manage Workflows gadget, select the workflow you want to edit.

Step 2 Click **Edit**.

Note
The media for an existing workflow can be changed by editing the workflow.

Step 3 Edit the fields that you want to change.

Step 4 Click **Save**.

Delete Workflow

Procedure

Step 1 In the Manage Workflows gadget, select the workflow that you want to delete.

Step 2 Click **Delete**.

Step 3 Click **Yes** to confirm the deletion of the selected workflow.

Manage Connected Agents

Connected Agents

Use the Connected Agents gadget on the Connected Agents tab to view the list of agents currently signed in to Cisco Finesse

You can use this gadget to determine which agents are signed in to the Publisher Side or the Subscriber Side. You can use this gadget also to filter the client types and identify the client type through which an agent has logged in. The client types can be Finesse Desktop, Finesse IP Phone, and Custom Desktop.

The list of signed-in agents is displayed in the form of a table, the Connected Agents table.

You can search the Connected Agents table for certain entries, sort the table, or refresh the table to view the latest data. The number of agents signed in to the Publisher Side and the Subscriber Side are displayed in the gadget (above the table).

The columns of the Connected Agents table are displayed below:

Column	Explanation
Agent Name	The first and last name of an agent.
Username	The Agent ID or username required to sign in to Cisco Finesse.
Extension	The extension number of the agent.
Team	The team the agent belongs to.
Connected Time	The total duration (in hh:mm:ss) for which the agent has been logged in.
Connected Side	Publisher/Subscriber/Both Sides.
Finesse Host	The Finesse host through which the agent is connected.

Actions on the Connected Agents Gadget

- **Search**: Searches for the entered text across all columns of the Connected Agents table.
- **Sort**: Sorts the column values of the Connected Agents table in ascending or descending order.
- **Filter**: Filters agents connected to Both Sides, the Publisher side, or the Subscriber side.

  The default selection for this drop-down box is Both Sides.
- **Refresh**: Refreshes the Connected Agents table. When the Refresh button is clicked, a new REST API call is made to both the publisher and subscriber servers to get the latest information about the signed-in agents.

  The time at which the agent information was last fetched from the server is displayed beside the Refresh button (For example, Updated 45 minutes ago).

Manage Security

The Cisco Finesse administration console and agent desktop support secure HTTP (HTTPS). To access the administration console, enter the following URL in your browser (where *FQDN* is the fully qualified domain name of your primary server):

https://*FQDN*:8445/cfadmin

Similarly, agents and supervisors can access their desktops as follows:

https://*FQDN*:8445/

For HTTPS access, you can eliminate browser security warnings by choosing to trust the self-signed certificate provided with Finesse or uploading a CA certificate.

If you add custom gadgets that perform HTTPS requests to Finesse, you must add a certificate to the Finesse server for that gadget.

Note Wildcard Certificates are not supported in Unified CCX.

HTTPS Support

The Cisco Finesse administration console and agent desktop supports only HTTPS. To access the administration console using HTTPS, enter the following URL in your browser:

https://*FQDN: 8445*/cfadmin

Where *FQDN* is the name of your primary Finesse server and 8445 is the port number.

Similarly, agents and supervisors can access their desktops using HTTPS as follows:

- https://*FQDN:8445*/desktop

For HTTPS access, you can eliminate browser security warnings by choosing to trust the self-signed certificate provided with Finesse or uploading a CA certificate.

If you add custom gadgets that perform HTTPS requests to Finesse, you must add a certificate to the Finesse server for that gadget.

HSTS

Finesse supports HTTP Strict Transport Security (HSTS) for increased security. HSTS is automatically enabled, in which case the Finesse server sends HTTPS responses indicating to browsers that Finesse can only be accessed using HTTPS. If users then try to access Finesse using HTTP instead of HTTPS, the browser changes the connection to HTTPS before generating any network traffic. This functionality prevents browsers from sending requests to Finesse using unencrypted HTTP before the server can redirect them.

Cross-Origin Resource Sharing (CORS)

Finesse supports CORS requests and allows the customization of the domains which are allowed to make CORS requests to the Finesse desktop. Once CORS is enabled via the CLI **utils finesse cors enable**, the CORS origin request from external domains is blocked by the browser. To enable specific domains to access Finesse desktop via CORS, the domains need to be added to the CORS origin allowed list using the CLI **utils finesse cors allowed_origin add**. For more information on the CORS CLIs, see *Cisco Finesse CLI*.

Gadget Source Allowed List

Shindig proxies requests from the Finesse desktop to external servers and this introduces the possibility of server side request forgery (SSRF). To prevent SSRF, you can choose to restrict outgoing connections requested by the gadgets to specific URIs by enabling Shindig allowed listing CLIs and adding the required URIs to the allowed list. For more information on Gadget Source Allowed List CLIs, see *Cisco Finesse CLI*.

Security Enhancements

The security enhancements in Cisco Finesse are as follows:

- By default, Cisco Finesse Notification Service unsecure XMPP port 5222 and BOSH/WebSocket (HTTP) port 7071 are disabled.

  Use the CLI command **utils finesse set_property webservices enableInsecureOpenfirePort true** to enable these ports.

For more information on CLI commands, see *Service Properties*.

Manage Finesse IP Phone Agent

Finesse IP Phone Agent

With Finesse IP Phone Agent (IPPA), agents and supervisors can access Finesse features on their Cisco IP Phones as an alternative to accessing Finesse through the browser. Finesse IPPA supports fewer features than the Finesse desktop in the browser, but it does allow agents and supervisors to receive and manage Finesse calls if they lose or do not have access to a computer.

Supervisor Tasks

Finesse IPPA does not support supervisor tasks such as monitor, barge, and intercept, but supervisors can sign in and perform all agent tasks on their IP Phones.

Administration Tasks

After you configure Finesse IPPA, the administration tasks that you perform for the Finesse desktop also apply for the supported Finesse IPPA features. For example, the Call Variables Layouts that you configure for the desktop also apply for Finesse IPPA, although the column layout is modified to fit the IP Phone screen.

Reason Code Limitations

- On the IP Phone, Finesse can display a maximum of 100 Not Ready, Wrap Up, or Sign Out reason codes. If more than 100 codes are configured, the phone lists the first 100 applicable codes (global or applicable team codes).
- When Finesse IPPA displays reason codes, some IP Phone models truncate the codes due to character length limitations on the phone. To ensure they meet your requirements, verify the display of the reason codes on all phone models in your environment.

Finesse IP Phone Agent Service Access Protocol

Finesse IPPA phone clients communicate with the Finesse server using Secure HTTP (HTTPS) protocol.

Failure Behavior

Unlike the Finesse desktop, the Finesse IP Phone Agent does not automatically failover to the alternate Finesse server. To resume usual operations in a failure scenario, the Finesse IPPA agents must exit from the current Finesse IP Phone service and manually sign in to another configured Finesse service that connects to an alternate Finesse server.

To ensure continued operations in a failure situation, you must configure at least two Finesse IP Phone services in Unified CM, each pointing to different Finesse servers.

One Button Sign In

With One Button Sign In, you can set up the Finesse IPPA phones with prepopulated agent ID, extension, and password. In this case, agents can sign in to Finesse on the IP Phone without credentials just by selecting Cisco Finesse from the Services menu.

Alternatively, you can set up One Button Sign In and prepopulate only a subset of agent credentials. For example:

- You can prepopulate only the agent ID and extension, forcing the agents to manually enter their password at sign-in for increased security.
- You can prepopulate only the extension, forcing agents to manually enter their ID and password at sign-in (useful for agents who share the same phone).

You can use Unified CM Administration to prepopulate the agent credentials, or you can set up the agents with access to the Unified CM Self Care Portal to prepopulate their own credentials.

The following table shows examples of how you can assign the responsibility of defining agent credentials to the administrator or the agent, or share that responsibility between them:

Example Set Up	Prepopulated in Unified CM Administration (by Administrator)	Prepopulated in Self Care Portal (by Agent)	Entered at Sign-In (by Agent)
Administrator populates the extension only	extension	-	id password
Administrator populates the ID and extension	id extension	-	password
Agents enter password only using Self Care Portal	id extension	password	-
Agents enter all credentials using Self Care Portal	-	id extension password	-
Agents enter ID and extension only using Self Care Portal	-	id extension	password

Finesse IP Phone Service Subscription Options

To set up access to Finesse on agent IP phones in Cisco Unified Communications Manager, you must create the Finesse IP Phone service to which the phones can subscribe. To set up the Finesse service, you can choose one of the following options:

- Set up an enterprise subscription to automatically subscribe all IP phones in the cluster to the Finesse service. (Not supported with One Button Sign In.)
- Set up a manual subscription, and manually subscribe each IP phone to the Finesse service.
- Set up a manual subscription, and set up the agents with access to the Unified CM Self Care Portal to subscribe to the Finesse service.

The following table lists the Finesse IPPA configuration procedures and indicates which procedures are required depending on the subscription option you choose:

Finesse IPPA Configuration Procedures	Enterprise Subscription	Manual Subscription	
		Administrator Manually Subscribes the Phones	Agents Manually Subscribe Their Phones Using the Self Care Portal
Set Up Application User, Web Access, and HTTPS Server Parameters	Required	Required	Required
Configure Finesse IP Phone Service in Unified CM	Required	Required	Required
Add Service Parameters for One Button Sign In	Not applicable	Required only with One Button Sign In	Required only with One Button Sign In
Subscribe Agent Phones to Manual Subscription Service	Not applicable	Required	Optional. Allows the administrator to enter agent credentials for One Button Sign In.
Set Up Agent Access to the Self Care Portal	Not applicable	Optional. Allows agents to enter their own credentials for One Button Sign In.	Required

Set Up Application User, Web Access, and HTTPS Server Parameters

To support Finesse IPPA functionality, you must configure an application user in Unified Communications Manager that is associated with all Finesse IPPA phones. For proper Finesse IPPA operation, you must also set the Web Access and HTTPS Server parameters in Unified CM.

The following steps are required for both manual and enterprise subscriptions:

Before you begin

Set up call capabilities for the agent phones in Cisco Unified Communications Manager.

Procedure

Step 1 Set the following parameters in Unified CM:

- Set the **Web Access** parameter to **Enabled**.
- Set the **HTTPS Server** parameter to **HTTPS Only**.

To set these parameters in Cisco Unified CM Administration, use either of the following pages:

- Phone Configuration page (Product Specific Configuration portion of page): choose **Device > Phone**.
- Enterprise Phone Configuration page: choose **System > Enterprise Phone Configuration**.

Step 2 Configure an application user in Unified Communications Manager.

a) In Cisco Unified Communications Manager Administration, select **User Management** > **Application User**.
b) Click **Add New**.
c) Under User Information, enter a user ID and password for the new user.

The password must be 95 characters or less and must contain ASCII characters only.

d) Under Device Information, in the Available Devices pane, select all phones that Finesse IP Phone Agents will use and move them to the Controlled Devices pane using the arrows.
e) Under Permissions Information, click **Add to Access Control Group**.
f) From the list of search results, select **Standard CTI Enabled** and **Standard CTI Allow Control Of All Devices** and then click **Add Selected**.

The application user is added to the Standard CTI Enabled and Standard CTI Allow Control Of All Devices groups.

g) Click **Save** at the bottom of the page.

Note
In UCCX deployments, usage of an existing RMCM User for Finesse IPPA is known to cause problems in functionality, however, the physical phones must be associated with the RMCM User.

Step 3 Enter the application user's credentials in the Finesse IP Phone Agent Settings gadget.

a) Sign in to the Cisco Finesse Administration Console.
b) Choose **Settings** > **IP Phone Agent Settings**.
c) Under Phone URL Authentication Settings, enter the same username and password that you entered in Unified CM for the application user.

The password must be 95 characters or less and must contain ASCII characters only.

d) Click **Save**.
e) Restart Cisco Finesse Tomcat on the primary Unified CCX node.
f) After replication is complete, restart Cisco Finesse Tomcat on the secondary Unified CCX node.

For information to check the replication status, see Step 3 of **Prepare System for IP Address/hostname Change**.

Note
For Finesse IP Phone Agent (IPPA) from 11.0 (1) onwards, the User Device Profile (UDP) must be associated with the Finesse IP Phone Agent Application User along with the physical phones for agents using Extension Mobility. The Finesse Service URL must use the complete FQDN of the Unified CCX server.

Configure Finesse IP Phone Service in Unified CM

The following procedure describes the steps required for manual and enterprise subscription.

Procedure

Step 1 Log in to the Unified CM Administration using administrator credentials.
Step 2 Select **Device** > **Device Settings** > **Phone Services**.
Step 3 Click **Add New** to create a new IP phone service.

Step 4 In the **Service Name** field, enter **`Cisco Finesse`** (or another service name that is appropriate for your environment).

Step 5 In the **Service URL** field, enter: `http://Finesse FQDN:8082/fippa/#DEVICENAME#`

Note
The **Service URL** entry is mandatory for Unified CM.

Step 6 In the **Secure-Service URL** field, enter: `https://Finesse FQDN:8445/fippa/#DEVICENAME#` to configure Finesse IP Phone Agent.

Note
- Support to HTTP is disabled from Cisco Finesse, Release 12.5(1) onwards. Step 5 and Step 6 are mandatory to save the Finesse IP Phone Agent settings.
- Import certificates for Finesse IP Phone Agent to communicate with the Finesse server using Secure HTTP (HTTPS) mode. For more information, see *Finesse IP Phone Agent Certificate Management*.

Step 7 Ensure that the **Service Category** is set to **XML Service**, and the **Service Type** is set to **Standard IP Phone Service**.

Step 8 Check the **Enable** check box.

Step 9 Perform one of the following:

- To automatically subscribe all phones in the cluster to the Finesse service, check the **Enterprise Subscription** check box, and click **Save**. Agents and supervisors can now access Cisco Finesse by selecting it from the **Services** menu on subscribed IP phones.

  Note
  One Button Sign In is not supported with enterprise subscriptions.

- To subscribe only the desired phones to the Finesse service manually, leave the **Enterprise Subscription** check box unchecked and click **Save**.

Step 10 With a two-node Finesse setup (primary and secondary Finesse servers), perform the preceding steps again to create a secondary Finesse service that points to the secondary Finesse server. When you create the secondary service, note the following procedural differences:

- At Step 4, in the **Service Name** field, enter a name that distinguishes the secondary service from the primary service, such as **`Cisco Finesse Secondary`**.
- At Step 5 and Step 6, replace *Finesse FQDN* with the FQDN of the secondary server.

Note
The language used in Finesse IPPA is selected based on the User Locale field in Unified CM. The language selected based on the User Locale must be available in the Unified CCX language pack for Unified CCX deployments. Unified CCX language pack for Unified CCX deployments and Unified CCE pack for Unified CCE deployments.

If the language selected based on the User Locale in Unified CM is not available in the respective deployments Unified CCX deployment, Finesse IPPA displays all content in the default language (U.S. English).

Finesse IP Phone Agent Certificate Management

The administrator must perform the following operations to enable Finesse IP phones to communicate with the Finesse server using HTTPS.

- For a CA-signed certificate, see CA-Signed Certificate, on page 465.
- For a self-signed certificate, see Self-Signed Certificate, on page 465.

CA-Signed Certificate

Procedure

Step 1 Obtain the CA-signed certificate from the signed authority for both Cisco Unified CCX and CUCM server.

Step 2 Import the CA-signed certificate of CUCM to the Cisco Unified CCX server trust store as **tomcat-trust**. For more information, see Import CUCM Certificate , on page 466.

Step 3 Import the CA-signed certificate of Cisco Unified CCX certificate to the CUCM trust store as **Phone-trust**. For more information, see Import Certificate into CUCM Trust Store, on page 467.

Self-Signed Certificate

Procedure

Step 1 Export the self-signed CUCM certificate from the Cisco Unified Operating System Administration. For more information, see Export CUCM Certificate, on page 465.

Step 2 Import the downloaded self-signed CUCM certificate to the Cisco Unified CCX trust store as **tomcat-trust**. For more information, see Import CUCM Certificate , on page 466.

Step 3 Export the self-signed Cisco Unified CCX certificate from the Cisco Unified Operating System Administration. For more information, see Export Cisco Unified CCX Certificate, on page 466.

Step 4 Import the downloaded self-signed Cisco Unified CCX certificate to the CUCM trust store as **Phone-trust**. For more information, see Import Certificate into CUCM Trust Store, on page 467.

Export CUCM Certificate

Procedure

Step 1 Sign in to Cisco Unified OS Administration on the CUCM server using the following URL: `https://FQDN of CUCM server:8443/cmplatform`.

Step 2 Select **Security** > **Certificate Management**.

Step 3 Enter the search criteria as **`tomcat`** and then click **Find** to filter the certificate.

The tomcat certificates list is displayed.

Step 4 Click the tomcat certificate hyperlink in the **Common Name** column.
The tomcat **Certificate Details** dialog box is displayed.

Step 5 Click **Download .PEM File**.

Step 6 Save the .PEM file in your local machine.

What to do next

Follow the same steps for both publisher and subscriber nodes. It is also to be followed for all the CUCM node certificates.

Import CUCM Certificate

Procedure

Step 1 Sign in to Cisco Unified OS Administration on the Cisco Unified CCX server using the following URL: `https://FQDN of Unified CCX server:8443/cmplatform`.

Step 2 Select **Security** > **Certificate Management** > **Upload Certificate/Certificate chain**.

Step 3 From the **Certificate Purpose** drop-down list, select **tomcat-trust**.

Step 4 In the **Upload File** field, click **Choose File** and browse to the tomcat.pem or CA-signed certificate file that you saved on your system.

Step 5 Click **Upload**.

Step 6 Restart Cisco Finesse tomcat and Cisco Unified CCX Notification Service.

Note
Follow the same steps for both publisher and subscriber nodes. It is also to be followed for all the CUCM node certificates.

Export Cisco Unified CCX Certificate

Procedure

Step 1 Sign in to Cisco Unified OS Administration on the Cisco Unified CCX server using the following URL: `https://FQDN of Unified CCX server:8443/cmplatform`.

Step 2 Select **Security** > **Certificate Management**.

Step 3 Enter the search criteria as **`tomcat-trust`** and then click **Find** to filter the certificate.

The tomcat-trust certificates list is displayed. If you do not find the tomcat certificate for your server in the **Certificate List**, then click **Generate Self-signed**. When the certificate generation is complete, reboot your server. Then restart this procedure. For more information on generating the self-signed certificate, see *Cisco Unified Operating System Administration Online Help*.

Step 4 Click the tomcat-trust certificate hyperlink in the **Common Name** column.
The tomcat **Certificate Details** dialog box is displayed.

Step 5 Click **Download .PEM File**.

Step 6 Save the .PEM file in your local machine.

What to do next

Follow the same steps for both publisher and subscriber nodes. It is also to be followed for all the CUCM node certificates.

Import Certificate into CUCM Trust Store

Procedure

Step 1 Sign in to Cisco Unified OS Administration on the CUCM server using the following URL: `https://FQDN of CUCM server:8443/cmplatform`.

Step 2 Select **Security** > **Certificate Management** > **Upload Certificate/Certificate chain**.

Step 3 From the **Certificate Purpose** drop-down list, select **Phone-trust**.

Step 4 In the **Upload File** field, click **Browse** and browse to the tomcat.pem or CA-signed certificate file that you saved on your system.

Step 5 Click **Upload**.

Step 6 Reboot the Cisco Unified Communications Manager (CUCM) server.

Note
Follow the same steps for both publisher and subscriber nodes. It is also to be followed for all the CUCM node certificates.

Add Service Parameters for One Button Sign In

With One Button Sign In, for any agent credentials that you want prepopulated, you must set up corresponding service parameters in Unified CM.

Only perform this procedure if you are setting up One Button Sign In. Otherwise, skip this.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select the Finesse phone service (under **Device** > **Device Settings** > **Phone Services**).

Step 2 Click **New** to the right of the Parameters box.

Step 3 Set up service parameters for the agent id, extension, and password credentials as per the following table. Enter only the parameters that you want prepopulated for the agents. For each parameter, enter the required field values and click **Save**. To add parameters, click **Add New** and enter the required values.

Field	Description
Parameter Name	Enter a parameter name in lower case exactly similar to — id, extension, and password. The values entered are the exact query string parameters used for the subscription URL.
Parameter Display Name	Enter a descriptive parameter name; for example, id, extension, and password.
Default Value	Leave the default value blank for all parameters.

Field	Description
Parameter Description	Enter a description of the parameter. The user can access this text when they subscribe to the service.
Parameter is Required	If the administrator prepopulates the parameter in Unified CM Administration, check the **Parameter is Required** box. However, if the agent prepopulates the parameter in the Self Care Portal, two options are available: • If the agents prepopulates all defined parameters, check the **Parameter is Required** box for each parameter. • If the agent and administrator share the responsibility of prepopulating the parameters, set only the administrator-defined parameters as required. This configuration ensures that the administrator can save the subscription without prepopulating all parameters. In this case, the administrator first prepopulates the required parameters, and then the agents prepopulate the nonrequired parameters.
Parameter is a Password (mask contents)	Check this box for the password only. This check box masks the password entries in the Self Care Portal, to display asterisks rather than the user entry.

When you save the last parameter, click **Save and Close**.

What to do next

You can prepopulate the agent credentials when you subscribe the agent phones, or the agents can prepopulate their own credentials using the Unified CM Self Care Portal.

Subscribe Agent Phones to Manual Subscription Service

If you set up the Finesse service as a manual subscription, you can subscribe the agent phones to the Finesse service in Unified CM and optionally define agent credentials for One Button Sign In.

If you prefer to allow the agents to subscribe to the Finesse service using the Self Care Portal and prefer not to specify One Button Sign In credentials for the agents, you can skip this procedure.

Procedure

Step 1 From the menu bar, select **Device** > **Phone**.

Step 2 Select the phone that you want to subscribe to the Finesse service.

Step 3 From the **Related Links** drop-down list on the upper right side of the window, select **Subscribe/Unsubscribe Services** and click **Go**.

The **Subscribed IP phone services** window displays for this phone.

Step 4 From the **Select a Service** drop-down list, select **Cisco Finesse**.

Step 5 Click **Next**.

Step 6 (*Applicable for One Button Sign In only*) Enter values for any of the defined service parameters (id, password, and extension) that you do not want the agents to enter using the Self Service Portal or at sign-in.

Step 7 Click the **Subscribe** button to subscribe this phone to the Cisco Finesse service.

The Cisco Finesse service displays in the **Subscribed Services** list.

Step 8 Click **Save**.

The subscribed agents or supervisors can now access Cisco Finesse by selecting it from the **Services** menu on their IP phones.

Step 9 With a two-node Finesse setup (primary and secondary Finesse servers), perform this procedure again to also subscribe the phones to the secondary Finesse service that points to the secondary Finesse server.

Set Up Agent Access to the Self Care Portal

You can optionally set up the agents with access to the Unified CM Self Care Portal to prepopulate their own credentials and to subscribe to the Finesse service.

If you are not setting up One Button Sign In, or not enabling the agents with access to the Self Care Portal, skip this procedure.

Procedure

Step 1 From the Unified CM Administration page, select **System** > **Enterprise Parameters**.

Step 2 Under the Self Care Portal Parameters, in the **Self Care Portal Default Server** field, select the IP address of the Unified CM Publisher server from the drop-down list and click **Save**.

Step 3 Select **User Management** > **End User**.

Step 4 Select the user that you want to set up with access to the User Care Portal.

Step 5 Under Permissions Information, click **Add to Access Control Group**.

Step 6 From the list of Access Control groups displayed, check **Standard CCM End Users** and click **Add Selected**.

Step 7 Click **Save**.

With access enabled to the Self Care Portal, agents can sign in to the portal at http://<UCM address>/ucmuser to subscribe to the Finesse service and enter their own credentials under **Phones** > **Phone Settings** > **Services**.

Note In a two-node Finesse setup with two services configured, the agents must enter their credentials on the primary and secondary Finesse services.

Cisco Finesse Failover Mechanisms

CTI Failover

CTI failover is when the Finesse service disconnects from one CTI server and reconnects to the same or another CTI server.

The prerequisites for successful CTI failover are as follows:

- Unified Contact Center Express (Unified CCX) must be configured in High Availability (two-node, publisher and subscriber) setup.
- Unified CCX REST service on the local CCX node must be up and running.

In the two-node setup, if Finesse loses connection to the Unified CCX server, it attempts to connect to the server which is running. Finesse alternates between the configured servers until it makes a successful connection.

While failover is in progress, Finesse transitions to OUT_OF_SERVICE state. During this period, Finesse does not entertain client requests or send out events. Any request made during this time receives a 503 Service Unavailable error message.

After reconnecting to a Unified CCX server and transitioning to IN_SERVICE state, Finesse responds to client requests and publishes events.

Note For Finesse transition to IN_SERVICE,

- Unified CCX REST services on the publisher must be IN_SERVICE.
- Unified CCX server CTI connectivity to the publisher or the subscriber must be successful.

Connection to the Unified CCX server can be lost due to the following reasons:

- Finesse misses three consecutive heartbeats from the connected Unified CCX server (heartbeat interval is five seconds).
- Finesse socket that is opened to the Unified CCX server.
- Unified CCX REST services on the publisher transitions to OUT_OF_SERVICE.

After the failover is complete, the last state of call control, call data, or agent state are published as events to all clients. This allows Finesse clients to reflect an accurate view of the call control, call data, and agent state.

If an agent either makes or answers a call, and then ends that call during failover (that is, the entire call takes place during failover), the corresponding events are not published.

Note An agent or supervisor might experience certain limitations, related to preservation of their states over failover. Examples include, but are not limited to, the following:

- The Finesse desktop does not show the agent state as it was before the failover, instead shows NOT READY state.
- The Finesse desktop does not show the pending state that the agent had set before the failover.
- The Finesse desktop shows NOT READY state even when there is an active call.

Despite these limitations, the agent and supervisor can continue to perform general operations on the phone.

Finesse Desktop Failover

Desktop failover can occur for the following reasons:

- When the Finesse desktop loses network connectivity to the Unified CCX Notification Service.
- When the Finesse Tomcat Service becomes *Unavailable*
- When the Finesse REST API Service becomes *Unavailable*
- When the Unified CCX Notification Service becomes *Unavailable*
- When the Finesse loses connection to the publisher

Note

- After the failover, the pending state of an agent will not be displayed once the agent fails over to the subscriber. The pending state change is lost during the failover, as the agent will be logged out, and logged in again.
- Finesse is IN_SERVICE, coordinates the distribution of desktop reloads, such that failover and consequent desktop reloads are evenly distributed to prevent overwhelming of the Finesse service. Configuration data such as reason codes, workflows and so on are not reloaded during failover to improve the performance.

If the server that an agent is connected transitions to OUT_OF_SERVICE, the agent receives a notification that the connection with the server is lost. The Finesse desktop:

- Checks whether the subscriber is available and IN_SERVICE.
- Continues to check whether the publisher recovers its state.

If the subscriber is available, then the desktop automatically signs the agent into the subscriber. If the publisher recovers its state, the desktop notifies the agent that it has reconnected.

The failover logic has three triggers to detect desktop failure:

- The Finesse desktop receives a SystemInfo event that the publisher is OUT_OF_SERVICE.
- The Unified CCX Notification Service is disconnected.

- The XMPP presence of "Finesse" user changes to *Unavailable*.

No matter which trigger is detected, the desktop reconnection logic is as follows:

1. Poll SystemInfo for publisher every 20 seconds.
2. If SystemInfo API reports Finesse is IN_SERVICE, check the Unified CCX Notification Service.
3. If SystemInfo is IN_SERVICE, check whether the last CTI heartbeat status of the side being connected is a success.

Note The last CTI heartbeat status is checked to ensure that the subscriber is healthy before failover, and thus does not immediately transition to OUT_OF_SERVICE after the client has failed over. Removal of the publisher from the network can cause the Finesse service to disconnect and connect to its local Unified CCX server. Depending on the network topology the subscriber might be slower to sense a network disconnect.

4. If XMPP is disconnected, make the Unified CCX Notification Service request.
5. If the Unified CCX Notification Service is successful and Finesse service is IN_SERVICE, refresh the data.

The failover logic prefers to stay with the publisher. If the failover logic detects that the subscriber is available, it checks the publisher one more time. If the publisher has recovered, the desktop reconnects to the publisher. If the publisher is still down, the desktop connects the agent to the subscriber. In this case, the agent does not automatically reconnect to the failed server after it recovers, but instead remains connected to the subscriber.

If the Unified CCX Notification Service is the source of failure, the desktop makes three attempts to reconnect before changing the state of the desktop to disconnected. These attempts occur before the failover logic begins.

Desktop Behavior

When the agent is forcibly logged out due to the connection failure between the Finesse desktop and the Finesse service, then Finesse sends a reason code 255 to the Unified CCX server. The Unified CCX server places the agent in Logout state.

Note Finesse takes up to 120 seconds to detect when an agent closes the browser. If the browser crashes, Finesse waits 60 seconds before sending a forced logout request to the Unified CCX server. Under these conditions, Finesse can take up to 180 seconds to sign out the agent.

The following table lists the conditions under which Finesse sends this code to the Unified CCX server.

Scenario	Desktop Behavior	Server Action	Results
The agent closes the browser, the browser crashes, or the agent clicks the Back button on the browser.	Finesse desktop makes a best-effort attempt to notify the server.	Finesse receives a presence notification of *Unavailable* from the client. Finesse waits 60 seconds, and then sends a forced logout	**Race Conditions** 1. The agent closes the browser window. Finesse receives a presence notification of

		request to the Unified CCX server.	*Unavailable* for the user. Finesse tries to sign the agent out; however, that agent is already signed out. **2.** If the browser crashes, it can take the Finesse service up to 120 seconds to detect that the client is gone and send a presence notification to Finesse. A situation can occur where the client signs into the subscriber before the publisher receives the presence notification caused by the browser crash. In this case, the agent may be signed out or put into Not Ready state on the subscriber. **3.** If the Finesse desktop is running over a slower network connection, Finesse may not always receive an *Unavailable* presence notification from the client browser. In this situation, the behavior mimics a browser crash, as described in the preceding condition. **4.** The agent is logged out, with reason

			code Connection Failure, which can be seen in the reports.
The client refreshes the browser	—	Finesse receives a presence notification of *Unavailable* from the client. Finesse waits 60 seconds before sending a forced logout request to the Unified CCX server to allow the browser to reconnect after the refresh.	—
The Refresh Token has expired. For more information on tokens, see https://developer.cisco.com/docs/finesse/#single-sign-on-apis.	Finesse desktop sends a forced logout request to the Unified CCX server.	The Finesse service forwards the forced logout request to the Unified CCX server.	The session expiry warning appears 10 minutes and 5 minutes before the Refresh Token expires. In the last minute, a countdown timer appears till the Refresh Token expires. The agent is forcefully logged out when the timer reaches zero and must log in again.

Desktop Chat Failover

The following table lists the desktop chat failover scenarios:

Failover Type	Desktop Chat Behavior
Cisco IM&P server failover	The desktop chat status is retained, and all active chat sessions are lost.
Finesse service failover	The desktop chat status is retained, and all active chat sessions are lost.
Unified CCX server failover	The desktop chat status and all chat sessions are retained.

Finesse IP Phone Agent Failover

Finesse IPPA failover can occur for the following reasons:

- The Finesse REST API Service transitions to OUT_OF_SERVICE.

- The Unified CCX Notification Service transitions to OUT_OF_SERVICE.
- The Finesse connection to the Unified CCX server transitions to OUT_OF_SERVICE.
- If Finesse IPPA detects a server failure before Finesse fails over to the subscriber, then Finesse IPPA declares the Finesse service OUT_OF_SERVICE.

The server that an agent is connected transitions to OUT_OF_SERVICE, the Finesse IP Phone Agent (IPPA) displays a notification that the server is unavailable. Finesse IPPA continues to check whether the current Finesse service recovers its state and notifies the agent if it reconnects.

Finesse IPPA attempts to reconnect to the server every 5 seconds and declares it OUT_OF_SERVICE after three failed attempts. The total time required for the transition to OUT_OF_SERVICE is approximately 15 seconds.

Unlike the Finesse desktop, Finesse IPPA does not check whether the subscriber is available. To connect to subscriber, the agent must exit the publisher, and manually sign into the subscriber.

Finesse IPPA failover logic has the following two triggers to detect failure:

- Finesse IPPA receives a SystemInfo event that the publisher is OUT_OF_SERVICE.

  Finesse IPPA polls SystemInfo every 5 seconds to check whether the Finesse service is IN_SERVICE. After three attempts, if the Finesse service is not IN_SERVICE, Finesse IPPA displays a server unavailable message to the agent.

- Finesse IPPA receives notification that the Unified CCX Notification Service is disconnected.

  Finesse IPPA tries every 5 seconds to reconnect with the XMPP server. After three attempts, if the Unified CCX Notification Service cannot be reestablished, Finesse IPPA displays a server unavailable message to the agent.

While the agent is still signed into the current service, Finesse IPPA continues attempting to reestablish the connections with the Finesse and XMPP servers. If they both resume service, Finesse IPPA displays the **Sign In** screen and the agent can sign in again and continue as usual.

Alternately, the agent must exit the current Finesse service and try to connect using an alternate Finesse service.

Guidelines for Optimal Desktop Failover

The following are the guidelines to optimize failover scenarios, to avoid server overload and unnecessary delays.

- Browser Configuration, on page 476
- Agent Configuration, on page 476
- Finesse Configuration, on page 477
- Common Configuration Safeguards, on page 477

Note The guidelines for optimal failover ensure that desktop initialization time and general system performance is optimized.

Browser Configuration

Finesse browser failover performance depends on the number of requests made to the Finesse service. Fewer the requests, lesser the system load on the Finesse service. The following browser-specific configurations ensure that the browser does not fetch static resources unnecessarily from the server, and it is a key requirement for faster failover.

Note Clear the browser cookies before logging in to the Finesse desktop. This avoids unexpected expiry of the Refresh Token in the Single Sign-On mode for Unified CCX.

- Avoid loading the Finesse desktop with **`bypassServerCache=true&nocache`** as a query parameter in the desktop URL. The **`bypassServerCache`** is to bypass Webproxy cache, and **`nocache`** is to bypass Shindig cache.
- Host systems must have at least 200 MB of free disk space more than the free space required by the operating system (OS).
- Adequate network bandwidth must be available between the Finesse desktop and the Finesse service. Lower latency results in faster failover.

  For more information on bandwidth measurements, see *Cisco Unified Contact Center Express Bandwidth Calculator* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-technical-reference-list.html.
- Host systems must have adequate memory and CPU without being overloaded at any point in time. A slow host slows the browser enough to cause it to fail and reload resources randomly during failover.
- External gadget hosting servers must prefer CA-signed certificates for easy integration with the browser. If they are self-signed, then import those certificates into the agent browser.

  For more information, see *Accept Security Certificates* section in *Cisco Finesse Agent and Supervisor Desktop User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html.

Firefox Configurations

Disable the Race Cache With Network (RCWN) in all the agent desktops to avoid any unwanted requests to the Finesse service. If RCWN is enabled, the Firefox browser by-passes the cached data and fetches the static requests again from the server. Set the **network.http.rcwn.enabled** configuration as **`false`**.

For more information, see https://support.mozilla.org/en-US/questions/1267945.

Google Chrome, and Edge Chromium (Microsoft Edge) Configurations

Import the Finesse self-signed certificates on Google Chrome, and Microsoft Edge browsers trust store.

For more information, see the *Accept Security Certificates* section in *Cisco Finesse Agent and Supervisor Desktop User Guide for Cisco Unified Contact Center Express* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-user-guide-list.html.

Agent Configuration

Agents configured must be evenly distributed between the publisher and subscriber. This prevents all agents from failing over when there is an outage that affects only one of the deployed Finesse service.

The number of agents failing over impacts system load and has a linear relationship with the maximum time taken for the operation to complete.

Finesse Configuration

The number of signed-in users, the gadget types, and the average number of gadgets configured per user, significantly impacts failover load.

The following are the best practices for ensuring a trouble-free failover.

- Number of Gadgets per Agent—Gadget-initiated requests constitute the bulk of the requests made during Finesse desktop failover or startup. Configuring fewer gadgets in the desktop layout results in faster desktop failover and startup. The administrator must configure the team or desktop layouts such that only the required gadgets for each team are available in the desktop layout.
- Type of Gadget—XML-based gadgets load much faster. The gadget content is also cached at the WebProxy Service, which allows the Finesse service to scale further.
- Gadget Configuration—Gadgets developers must follow certain best practices to ensure that gadgets load faster.

  For more information, see *Best Practices for Gadget Development* section of *Cisco Finesse Web Services Developer Guide* at https://developer.cisco.com/docs/finesse/#best-practices-for-gadget-development.
- Secondary Resources—The preloading of server resources reduces latency and improves performance during desktop failover. By default, the **preLoadSecondaryResources** property is enabled. Disabling this property impacts failover time. For more information, see *Desktop Properties*.

Common Configuration Safeguards

- Import the self-signed certificates into the browser.
- Do not disable browser caching for Finesse desktop.
- Do not clear the cache every time the browser is launched.
- Distribute the agents between the publisher and subscriber.

Failover Planning

CTI Failover

CTI failover happens when Finesse service disconnects from the Unified CCX server due to network failure or server error. If the desktop is connected, it displays that the server is unavailable, and tries to reconnect to the available Unified CCX server.

The duration required for Finesse CTI failover depends on the following factors.

- Available bandwidth from the remote Unified CCX to the Finesse service.
- Round Trip Time (RTT) between the Unified CCX server and the Finesse service in case of WAN deployments.
- The number of signed-in users.
- The number of gadgets configured.

Note The time indicated does not include the Unified CCX server recovering from the failure it encountered. It indicates only the time taken for Finesse to reconnect and be IN_SERVICE.

Desktop Failover

The Finesse desktop failover happens in all failure scenarios. The Finesse desktop tries to find an active server and fails over to it, once it has located a reachable server which is IN_SERVICE.

The duration required for Finesse desktop failover depends on the following factors.

- Bandwidth available to the client to reach the Finesse service.
- Time taken for Unified CCX server to become IN-SERVICE.
- RTT between the client and the network gateway.
- The number of signed-in users.
- The number of gadgets configured in the desktop per user.
- Type of gadgets (XML) and the resources it loads. For more information on Finesse gadgets, see https://developer.cisco.com/docs/finesse/#finesse-gadgets.

The average time taken for desktop failover, with 400 logged in users, and system defined gadgets per agent, is 35-75 seconds, after an IN-SERVICE Finesse service is identified. If Unified CCX server failover is involved, then the time taken is longer as it includes the time taken for Finesse service failover.

The numbers indicated varies depending on the customer configuration and the above-stated factors. It must be used as a guideline to determine the approximate range for failover time.

Note

- The time indicated does not include the Unified CCX server recovering from the failure it encountered. It only indicates the time taken for Finesse to reconnect and be IN_SERVICE. Unified CCX server sometimes takes up to 2 minutes to acquire mastership, and become IN_SERVICE, consequently. This causes delay in Finesse service becoming IN-SERVICE.

  For more information on mastership, see https://www.cisco.com/c/en/us/support/docs/contact-center/unified-contact-center-express/214639-understand-the-algorithm-to-determine-ma.html.

- During failover, agents are redirected to the subscriber and are signed in automatically, and desktop is reloaded.

Backup and Restore

The Unified CCX backup and restore component also backs up and restores Finesse configurations and data.

For more information about backup and restore, see *Cisco Unified Contact Center Express Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html

.

Additional Language Support

For the list of languages that are supported by Finesse, see the Unified CCX Compatibility related information, located at:

https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

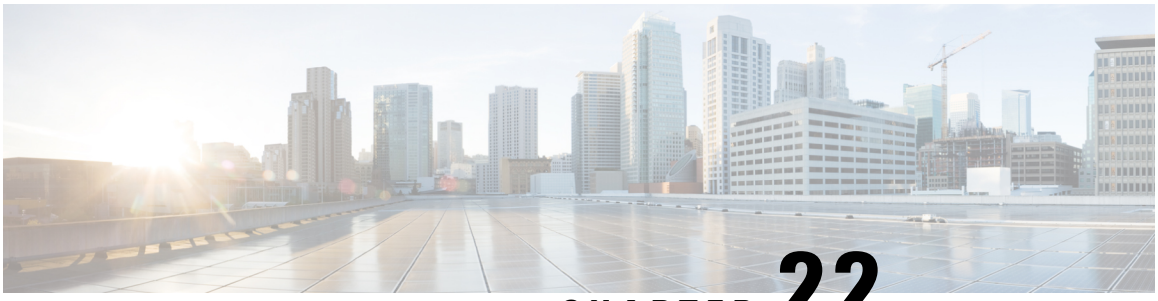
If you want to use the Finesse desktop interface in a language other than English, download and install the language COP file. For more information, see the "COP File" section of the *Cisco Unified Contact Center Express Install and Upgrade Guide*, located at:

https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-installation-guides-list.html.

Cisco Finesse Agent and Supervisor Desktop

Cisco Finesse Desktop provides easy access to the applications and information sources from a single customizable cockpit. Providing this unique access to information helps the agents deliver fast and accurate service.

For more information about Cisco Finesse Agent and Supervisor Desktop , see *Cisco Finesse Agent and Supervisor Desktop User Guide for Cisco Unified Contact Center Express* at https://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_user_guide_list.html.



CHAPTER 22

CUIC Cluster Configuration

- Cluster Configuration for JVM Using Hazelcast, on page 481
- Troubleshooting Cluster Configuration, on page 483

Cluster Configuration for JVM Using Hazelcast

Cisco Unified Intelligence Center uses Hazelcast for application clustering. Hazelcast provides a second-level cache for the Unified Intelligence Center application layer. When any entity (for example: report, report definition, and so on) cached by Hazelcast is updated in one of the Unified Intelligence Center nodes, it must be invalidated and reloaded in all the other Unified Intelligence Center nodes in the cluster. The Hazelcast cluster automatically takes care of it by publishing clusterwide notifications containing the identifiers of such entities which must be invalidated.

In Unified Intelligence Center, the default mechanism for Hazelcast cluster discovery or formation is UDP multicast. Unified Intelligence Center uses the Multicast group IP address 224.2.2.3 and port 54327. You cannot change these settings in Unified Intelligence Center.

The UDP multicast based discovery mechanism will not work for the customer in the following scenarios:

- When the network has multicasting disabled.
- If the nodes in the Unified Intelligence Center cluster are in different subnets.

In such scenarios, you can change the discovery mechanism to TCP/IP. You can form the CUIC application cluster using TCP/IP instead of the default UDP Multicast based discovery mechanism.

Use the following CLI commands to manage the cluster mode (UDP Multicast vs TCP/IP). That is, use the following CLI commands to switch to TCP/IP only if the customer's network does not support Multicasting:

- **utils cuic cluster show**—This command shows the current cluster mode that is enabled on this node and the other member details.

Note The member details are available only in the TCP/IP mode. The member details displayed are of the configured members and does not represent the cluster in real time.

- **utils cuic cluster mode**—This command is used to switch the Hazelcast cluster join configuration from Multicast to TCP/IP and the opposite way.

Note After changing the cluster mode in all the nodes, restart "Intelligence Center Reporting Service" in all the nodes starting from the publisher sequentially.

- **utils cuic cluster refresh**—This command refreshes the cluster member information only when run in the TCP/IP mode. Run this command when there is an addition or deletion of nodes to the CUIC cluster, which is already in TCP/IP.

Note To update IP addresses in application cluster after changing IP addresses of systems in CUIC cluster, run the **utils cuic cluster refresh** command on each node.

Usage

You can use these commands using to switch to TCP/IP only when the customer's network does not support the Multicasting requirements that are specified in *Port Utilization Guide for Cisco Unified Contact Center Solutions* > *Intracluster Ports Between Cisco Unified Intelligence Center* section available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Note

- Stop the "Cisco Unified Intelligence Center Reporting Service" on all the Unified Intelligence Center nodes before performing cluster configuration changes using these CLI commands.
- When you have completed the cluster configuration changes on all nodes, use the "utils cuic cluster show" command to ensure that all nodes have identical configuration before starting "Cisco Unified Intelligence Center Reporting Service" on any one of them.
- Unified Intelligence Center cluster / application will work only if all the nodes use the same mode–that is, either Multicast or TCP/IP. Mixed mode is not allowed.
- If the network is disconnected and after the cluster nodes retain the network, ensure to perform "synchronize cluster" from all the nodes after logging into the Unified Intelligence Center reporting application.

Steps

Run the following CLIs on all nodes in the given sequence starting from the Publisher node:

Note Run every step on all nodes before performing the subsequent step.

Procedure

Step 1 utils service stop Cisco Unified Intelligence Center Reporting Service

Step 2 utils cuic cluster mode

Step 3 utils cuic cluster show

Note
Ensure that all nodes have identical configuration.

Step 4 utils service start Cisco Unified Intelligence Center Reporting Service

Note
If there is a network disconnect and reconnect, check if the database replication is successfully set up across all nodes in the cluster and then perform "Synchronize Cluster" from the legacy Cisco Unified Intelligence Center. This ensures that cache is in sync across the cluster.

Troubleshooting Cluster Configuration

Verify the Hazlecast Cluster Formation using Hazelcast REST client. To verify, replace <CUIC-IP> with the IP address of any CUIC member in the following URL.

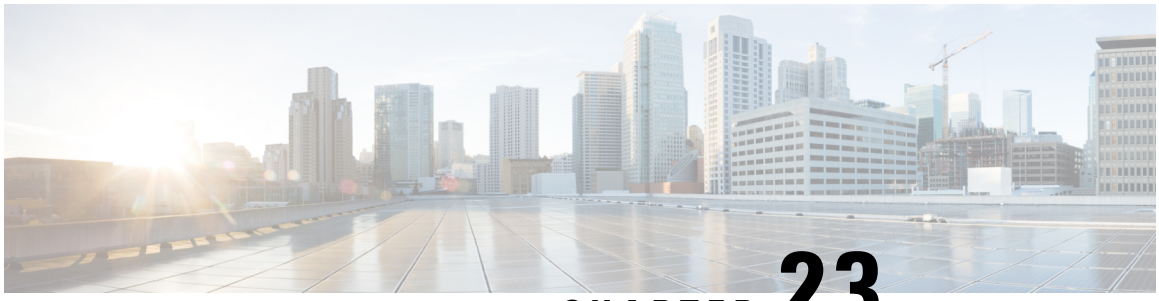
http://<CUIC-IP>:57011/hazelcast/rest/cluster

The Unified Intelligence Center application cluster can be down in the following cases:

- Common Cases:
  - Node is not reachable
  - Unified Intelligence Center Reporting Service is down
  - Hazelcast default Port 57011 is not enabled in Unified Intelligence Center nodes in the customer environment, which is used to communicate between cluster members.
- When multicasting is being used for the member discovery (Default method):
  - Network has UDP multicast disabled
  - UDP port 54327 used for Hazelcast member discovery is disabled
  - Multicast default group IP 224.2.2.3 is not allowed in the network
  - UCCX nodes are distributed across different subnets

Note If any of the above mentioned cases cause issue because of the restrictions on multicasting in the customer environment, you can use TCP/IP for Hazelcast discovery.

For more information, contact Cisco support to troubleshoot and reset the cluster.



CHAPTER 23

Extend and Connect

- Overview of Extend and Connect, on page 485
- Server Configuration, on page 488
- Persistant Connection, on page 490

Overview of Extend and Connect

With the Extend and Connect feature, Unified Contact Center Express agents and supervisors can work from a remote location using any device.

This feature gives the user (agent or supervisor) the flexibility to answer or make calls using devices that are connected to the PSTN or to mobile or other PBX networks. Extend and Connect functions by leveraging CTI remote device and persistent connection features of Cisco Unified Communications Manager (CUCM).

You can enable the Extend and Connect feature through the Cisco Jabber client by selecting only the Extend mode. This feature provide the following connections:

- CTI remote device—CTI remote devices are Unified CCX off-cluster devices for users that can be connected to any of the third-party networks, such as PSTN, mobile, or PBX.
- Persistent connection—Unified CCX users use this feature to set up a persistent call connection to remote destination. The advantage of this connection is that call establishment to the remote destination is much faster.

For information about Extend and Connect feature, see *Features and Services Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/10_0_1/ccmfeat/CUCM_BK_F3AC1C0F_00_cucm-features-services-guide-100/CUCM_BK_F3AC1C0F_00_cucm-features-services-guide-100_chapter_010111.html.

For more information about remote destination, see *Cisco Unified Communications Manager Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Server Configuration

To use the Extend and Connect, follow these server configuration steps:

Procedure

Step 1 Perform the preinstallation tasks for IM and Presence nodes.

See "Perform pre-installation tasks for IM and Presence nodes" section in *Installing Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html

Step 2 Configure the Cisco IM and Presence node details on Call Manager before you install Cisco IM and Presence. From Cisco Unified CM Administration on the publisher node, choose **System** > **Server** > **Server Type** and then choose **CUCM IM and Presence**.

For information about server setup, see the *Cisco Unified Communications Manager Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Step 3 Install Cisco IM and Presence as a Call Manager subscriber.

For information about Cisco IM and Presence installation, see *Installing Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html

Step 4 Activate and start all the Cisco IM and Presence services in **Cisco Unified Serviceability**.

For information about activating services, see the "Activate services" section in *Installing Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html

Step 5 Create Presence Redundancy groups in Call Manager.

a) Choose **System** > **Presence Redundancy Groups** > **Add New**.
b) Select Cisco IM and Presence, which you installed from the **Presence Server** drop-down list.

For information about the Presence redundancy group setup, see the "Presence redundancy group setup" section in *Cisco Unified Communications Manager Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Step 6 Create UC services for CTI and IM Presence services in Call Manager.

Note
You must select CTI and IM Presence services.

For information about creating UC services, see the "Add CTI service" section in *Cisco Unified Communications Manager Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Step 7 Set up the service profile in Call Manager.

Note
You must specify CTI and IM Presence service that you created in step 6.

For information about Service profile setup, see the "Service profile setup" section in *Cisco Unified Communications Manager Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Step 8 Set up the end user in Call Manager.

Perform the following steps:

a) Navigate to **User Management** > **End User**.
b) Click the User ID that you want to set up.
c) In the **Service Settings** section, select **Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)** and then in **UC Service Profile**, select the profile that you created.
d) In the **Mobile Information** section, select **Enable Mobility**.
e) In **Permission Information**, add **Standard CCM End user** and **Standard CTI enabled**.
f) Navigate to **User Management** > **Assign Presence End Users.**
g) Click the User ID that you want to set up and then choose **Assign Selected Users**.

Step 9 Set up the trunk in Call Manager.

For information about the Trunk setup, see the "Trunk setup" section in *Cisco Unified Communications Manager Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Step 10 Add the route pattern in Call Manager to route the calls to the remote device.

For information about route pattern setup, see the "Route pattern setup" section in *Cisco Unified Communications Manager Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Step 11 Configure the Presence Gateway configuration on IM and Presence.

For information about configuring Presence Gateway on IM and Presence, see the "Configure Presence Gateway configuration on IM and Presence" section in *Cisco Unified Communications Manager Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Persistent Connection

Unified CCX makes a persistent connection call to the agent's remote phone when an agent logs in to the agent desktop.

Note The agent must first answer the persistent connection call and then change the status to Ready in the agent desktop to answer the incoming call.

After establishing the persistent connection, the call remains connected until the Maximum Call Duration timer expires or until the agent logs out, provided that no other problems occur in the remote destination network. You must specify to match the time on the Maximum Call Duration timer with your company shift time or specify more than your company shift time. If the persistent connection gets disconnected, it retries until the connection is established.

Add Customized Announcement for Persistent Connection Call

When an agent answers persistent connection call, make an announcement to the agent indicating that the persistent connection must be retained so that further calls from or to customers are established over persistent connection.

If the agent's remote device supports Caller ID display, it displays `EC Mode` as the caller name, which indicates a persistent connection call.

By default, the Cisco Unified Communications Manager has announcements created. Unified CCX, through JTAPI communication to Cisco Unified Communications Manager, calls the announcement ID **UCCX Persistent Connection Prompt**. You must create the **UCCX Persistent Connection Prompt** customized announcement ID.

To add the customized announcement ID, see the"Upload customized announcement" procedure in the *Cisco Unified Communications Manager Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html. Enter **`UCCX Persistent Connection Prompt`** in the **Announcement Identifier** field.

Note

- Add a customized prompt to the created UCCX Persistent Connection Prompt, click **Upload Files** and select the desired prompt (.wav file).
- When the announcement is played, the Caller ID information on agent's remote phone changes to `Voice Connect`.
- If no announcement ID is created, Cisco Unified Communications Manager does not play any announcement to the agent when the persistent call is answered.

Incoming Call Notification

An agent can configure a sound alert to notify an incoming call when the customer calls are routed through Persistent Connection Calls of the agents.

To receive the sound alert, in Cisco Unified Communications Manager, configure the Announcement ID as **UCCX Customer Call Prompt**. When the Announcement ID is configured, Unified CCX plays the announcement before the call is routed to a desktop. If you do not configure an Announcement ID, Unified CCX does not play an announcement, and then the agent relies on desktop signal for an incoming call.

Note Configure **UCCX Customer Call Prompt** in the English language in Cisco Unified Communications Manager.

Server Configuration

To use the Extend and Connect, follow these server configuration steps:

Procedure

Step 1 Perform the preinstallation tasks for IM and Presence nodes.

See "Preinstall Tasks for the IM and Presence Service" section in *Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html

Step 2 Configure the Cisco IM and Presence node details on Call Manager before you install Cisco IM and Presence. From Cisco Unified CM Administration on the publisher node, choose **System** > **Server** > **Server Type** and then choose **CUCM IM and Presence**.

For information about the server setup, see "Manage the Server" in *Cisco Unified Communications Manager Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Step 3 Install Cisco IM and Presence as a Call Manager subscriber.

For information about Cisco IM and Presence installation, see "Installation Tasks" in *Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html

Step 4 Activate and start all the Cisco IM and Presence services in **Cisco Unified Serviceability**.

For information about activating services, see the "Configure the IM and Presence Publisher" section in *Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html

Step 5 Create Presence Redundancy groups in Call Manager.

a) Choose **System** > **Presence Redundancy Groups** > **Add New**.
b) Select Cisco IM and Presence, which you installed from the **Presence Server** drop-down list.

For information about the Presence redundancy group setup, see the "Configure Presence Redundancy Groups" section in *System Configuration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Step 6 Create UC services for CTI and IM Presence services in Call Manager.

Note
You must select CTI and IM Presence services.

For information about creating UC services, see the "Add CTI service" section in *System Configuration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Step 7 Set up the service profile in Call Manager.

Note
You must specify CTI and IM Presence service that you created in step 6.

For information about the Service profile setup, see the "Configure Service Profile" section in *System Configuration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Step 8 Set up the end user in Call Manager.

Perform the following steps:

a) Navigate to **User Management** > **End User**.
b) Click the User ID that you want to set up.
c) In the **Service Settings** section, select **Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)** and then in **UC Service Profile**, select the profile that you created.
d) In the **Mobile Information** section, select **Enable Mobility**.
e) In **Permission Information**, add **Standard CCM End user** and **Standard CTI enabled**.
f) Navigate to **User Management** > **Assign Presence End Users.**
g) Click the User ID that you want to set up and then choose **Assign Selected Users**.
h) Create a CTI Remote Device.
i) Associate Jabber and CTI Remote device to end user.
j) Associate the CTI Remote device to UCCX RmCm application user.

Step 9 Set up the trunk in Call Manager.

For information about the Trunk setup, see the "Configure Cisco Unified Communications Manager for IM and Presence Service" section in *Configuration and Administration of the IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Step 10 Add the route pattern in Call Manager to route the calls to the remote device.

For information about the route pattern setup, see the "Configure Advanced Routing" section in *Configuration and Administration of the IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Step 11 Configure the Presence Gateway configuration on IM and Presence.

For information about configuring Presence Gateway on IM and Presence, see the "Configure the Presence Gateway" section in *Configuration and Administration of the IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Example

For an example about how to configure Extend and Connect for Unified CCX, see https://www.cisco.com/c/en/us/support/docs/contact-center/unified-contact-center-express/215536-configure-extend-and-connect-feature-for.html.

Persistant Connection

Unified CCX makes a persistent connection call to the agent's remote phone when an agent logs in to the agent desktop.

Note The agent must first answer the persistent connection call and then change the status to Ready in the agent desktop to answer the incoming call.

After establishing the persistent connection, the call remains connected until the Maximum Call Duration timer expires or until the agent logs out, provided that no other problems occur in the remote destination network. You must specify to match the time on the Maximum Call Duration timer with your company shift time or specify more than your company shift time. If the persistent connection gets disconnected, it retries until the connection is established.

Add Customized Announcement for Persistent Connection Call

When an agent answers persistent connection call, make an announcement to the agent indicating that the persistent connection must be retained so that further calls from or to customers are established over persistent connection.

If the agent's remote device supports Caller ID display, it displays `EC Mode` as the caller name, which indicates a persistent connection call.

By default, the Cisco Unified Communications Manager has announcements created. Unified CCX, through JTAPI communication to Cisco Unified Communications Manager, calls the announcement ID **UCCX Persistent Connection Prompt**. You must create the **UCCX Persistent Connection Prompt** customized announcement ID.

To add the customized announcement ID, see "Media Resources" in the *Cisco Unified Communications Manager Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Enter **`UCCX Persistent Connection Prompt`** in the **Announcement Identifier** field.

Note

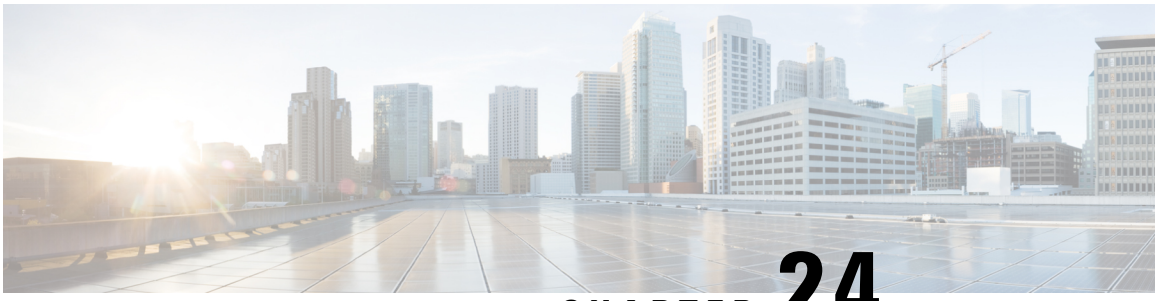
- Add a customized prompt to the created UCCX Persistent Connection Prompt, click **Upload Files** and select the desired prompt (.wav file).
- When the announcement is played, the Caller ID information on agent's remote phone changes to `Voice Connect`.
- If no announcement ID is created, Cisco Unified Communications Manager does not play any announcement to the agent when the persistent call is answered.

Incoming Call Notification

An agent can configure a sound alert to notify an incoming call when the customer calls are routed through Persistent Connection Calls of the agents.

To receive the sound alert, in Cisco Unified Communications Manager, configure the Announcement ID as **UCCX Customer Call Prompt**. When the Announcement ID is configured, Unified CCX plays the announcement before the call is routed to a desktop. If you do not configure an Announcement ID, Unified CCX does not play an announcement, and then the agent relies on desktop signal for an incoming call.

Note Configure **UCCX Customer Call Prompt** in the English language in Cisco Unified Communications Manager.



CHAPTER 24

VPN-less Access to Finesse Desktop

This feature provides the flexibility for agents and supervisors to access the Finesse desktop from anywhere through the Internet without requiring VPN connectivity to the data center. To enable this feature, a reverse-proxy pair must be deployed in the DMZ.

Cisco Unified CCX supports Historical and Real Time report gadgets in agent and supervisor desktops in VPN-less deployments. The reverse-proxy configuration enables authentication of all requests at the proxy, along with other security enhancements as detailed in the Reverse-Proxy selection and configurations, on page 502 section.

Media access remains unchanged in reverse-proxy deployments. To connect to the media, agents and supervisors can use Cisco Jabber or Webex over Mobile and Remote Access solution (MRA). They can also enable the Extend and Connect feature in this deployment.

When deployed with VPN-less reverse-proxy, Customer Collaboration Platform can be deployed within the DMZ or can be moved within the enterprise.

If you have already deployed a reverse-proxy and want to access the Finesse desktop without connecting to VPN, refer to the *VPN-Less Finesse Configurations* section. Otherwise, refer to the *Reverse-Proxy Selection and Configurations* section.

Note For deployments at multiple sites, configure the reverse-proxy close to the Unified CCX cluster to reduce latencies and WAN bandwidth consumption.

For OpenResty Nginx-based reverse-proxy rules, installation, configuration, and security hardening instructions, refer to Reverse-Proxy Configuration, on page 695. Any reverse-proxy supporting the required criteria (as mentioned in Reverse proxy selection criteria, on page 502) can be used in place of OpenResty Nginx for supporting this feature.

For the list of caveats, see the Caveats, on page 509section.

- Prerequisites, on page 494
- VPN-less Finesse configurations, on page 494
- Serviceability, on page 501
- Reverse-Proxy selection and configurations, on page 502
- Historical and Real Time Gadgets, on page 508
- Security Guidelines, on page 509
- Caveats, on page 509

Prerequisites

To configure a VPN-less access to the Finesse desktop:

- Unified CCX must be 12.5(1) SU2 and above.
- Customer Collaboration Platform must be 12.5(1) SU2 and above.
- DMZ with internet connectivity must be available to host the reverse-proxy

VPN-less Finesse configurations

To configure VPN-less access to Finesse desktop, the Contact Center administrators and the network administrators must work in tandem.

Note Don't allow access to the reverse-proxy in your external firewall until all security configurations are in place. To test your changes, use a host that isn't publicly accessible.

The configuration steps are as follows:

1. Populate Network Translation Data
2. Host the Mapping File
3. Add Proxy IP by Using CLI
4. Configure Reverse-Proxy Host Verification
5. Configure Proxy Mapping by Using CLI
6. Configure CORS and Frame-Ancestors
7. Configure SSO

Populate Network Translation Data

The proxy-config map file is similar to a plain property file in which the values are separated by the equal sign. Left Hand Side (LHS) contains the host and port of Unified CCX and Customer Collaboration Platform. Right Hand Side (RHS) contains the values of the host and port that are exposed via reverse-proxy to access the Finesse desktop.

The network administrator and Unified CCX administrator should create a proxy-config map file that has the mapping for all the default ports of the Cisco components, to which external traffic from the Internet clients have to be redirected. For example, 443 port of Customer Collaboration Platform.

The proxy-config map file must be hosted on a web server that is accessible by the Unified CCX and Customer Collaboration Platform servers. The following list is an example of systems and hosts that are required for a two-node Unified CCX cluster with one Customer Collaboration Platform node using SSO mode:

- Proxy Node1 = ccxproxy1.xyz.com

- Proxy Node2 = ccxproxy2.xyz.com
- Publisher = ccxnode1.internal.com
- Subscriber = ccxnode2.internal.com
- CCP = ccp.internal.com

The following is an example of a mapping file that contains the entries required for a two-node Unified CCX cluster with one Customer Collaboration Platform node using non-SSO mode.

```
ccxnode1.internal.com:443 = ccxproxy1.xyz.com:443
ccxnode2.internal.com:443 = ccxproxy2.xyz.com:443
ccp.internal.com:443 =  ccxproxy1.xyz.com:8442
ccp.internal.com:7443 = ccxproxy1.xyz.com:7442
```

Figure 3: Hostname Mapping Example

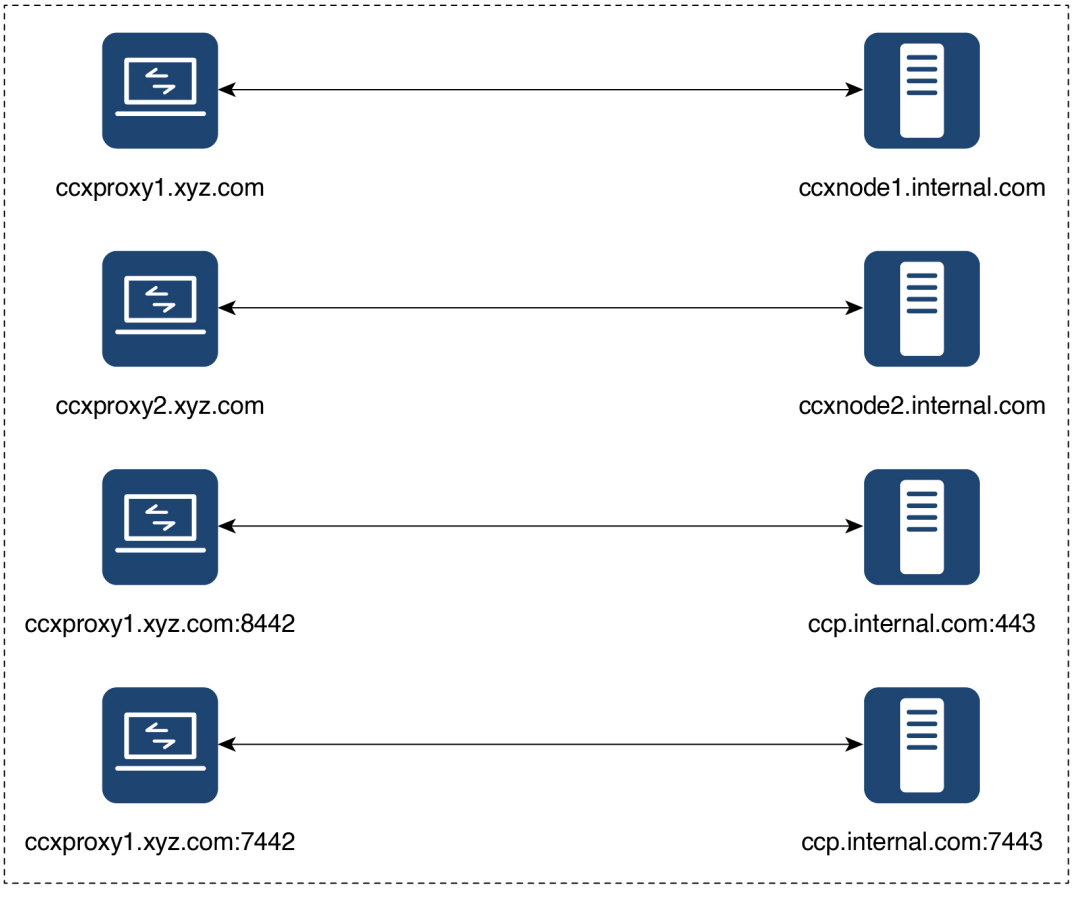
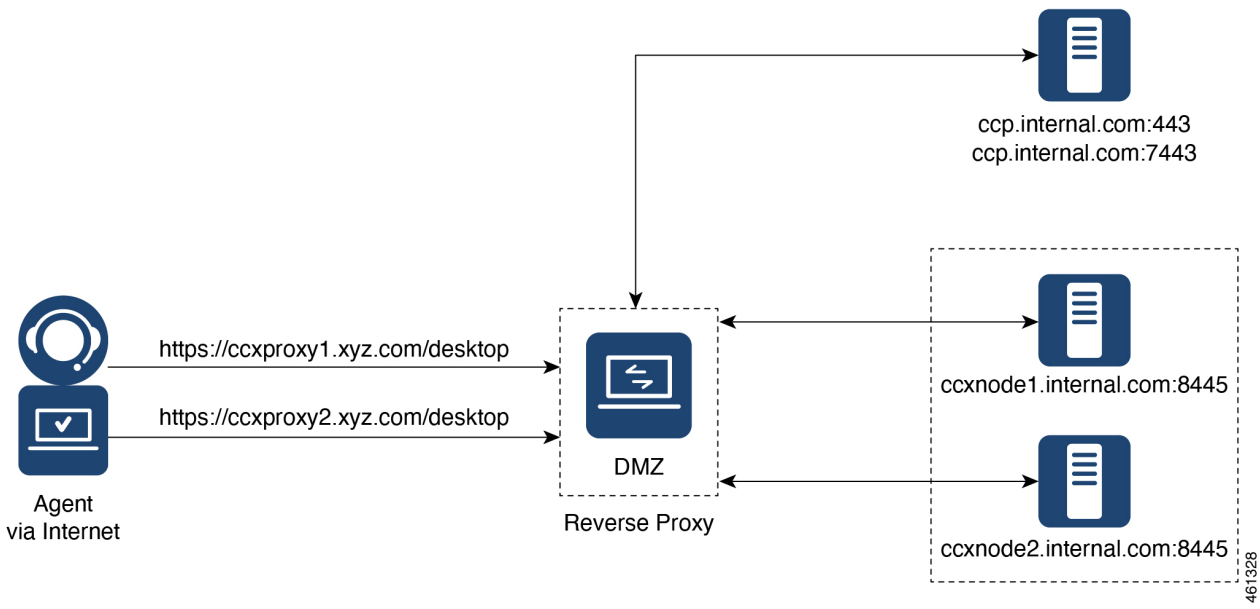


Figure 4: Network Architecture Example



Host the Mapping File

The mapping file that is created in the *Populate Network Translation Data* section, is used by the solution components (Unified CCX and Customer Collaboration Platform) servers to modify their responses, to enable clients to access the solution via the reverse-proxy. This requires the file to be hosted on any web server accessible by the component servers. The reverse-proxy server, Unified CCX server, or any web server configured by the administrator can be used for this purpose.

To access the mapping file, the host server's SSL certificate must be uploaded (using Cisco Unified OS Administration in Unified CCX server) to the individual nodes of the services. After uploading the file, verify if the URL is accessible from Unified CCX and Customer Collaboration Platform servers. For example, *https://proxyserver.xyz.com:10000/proxymap.txt*. HTTP-based URLs are allowed for hosting the mapping file through HTTPS, which is the recommended access scheme.

Add Proxy IP by Using CLI

The administrator must use CLI to add the list of trusted reverse-proxy IP addresses and their corresponding hostnames. This must be done on all the nodes of Unified CCX and Customer Collaboration Platform. These components consider only requests from the configured hosts or IP addresses as valid.

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

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

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

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

```
admin:utils system reverse-proxy allowed-hosts add group.facebook

Either IPv4 address or hostname is invalid or is not resolvable. Now validating IPv6 address
 for source group.facebook

Operation failed, please enter valid source(s). Source group.facebook is invalid
```

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

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

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

Source proxy.xyz.com successfully added list

The following source(s) are configured:

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

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

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

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

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

Delete operation successful
```

Configure Reverse-Proxy Host Verification

You can configure SSL certificate verification for communication between reverse-proxy host and the Cisco Web Proxy Service by running the following CLI command on both publisher and subscriber nodes of Finesse:

utils system reverse-proxy client-auth

This command has the following parameters:

- enable
- disable
- status

By default, the host authentication is enabled.

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

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

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

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

```
admin:utils system reverse-proxy client-auth enable
SSL certificate verification enabled for connections established from reverse proxy hosts

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

Note After enabling the reverse-proxy host authentication, browser-based clients that connect to Finesse Desktop via LAN hostname must select a client certificate. A pop-up is displayed on systems where client certificates are installed. Clients can choose any of the certificates listed in the pop-up, and continue to connect to Finesse.

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

```
admin:utils system reverse-proxy client-auth disable
SSL certificate verification disabled for connections established from reverse proxy hosts

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

Configure Proxy Mapping by Using CLI

The proxy-config map file can be configured in the Unified CCX and Customer Collaboration Platform servers using the `utils system reverse-proxy config-uri` command. If the URL is configured to use HTTPS protocol, Unified CCX and Customer Collaboration Platform must have the certificate (certificate of the web server hosting the URL) uploaded in */cmplatform*. The administrator can configure a maximum of two URLs. The URL that is added first takes precedence and that URL is polled to detect changes in the mapping file. When the URL is not accessible, the alternate URL is used. The following is an example of the CLI to list the configured proxy-config map URLs:

```
admin:utils system reverse-proxy config-uri list

Currently no source is configured
```

The following is an example of the CLI to configure the proxy-config map URL on the Unified CCX and Customer Collaboration Platform servers:

```
admin:utils system reverse-proxy config-uri add https://saproxy.xyz.com:10000/proxymap.txt

Source https://saproxy.xyz.com:10000/proxymap.txt successfully added

admin:utils system reverse-proxy config-uri list

The following source(s) are configured:

1. https://saproxy.cisco.com:10000/proxymap.txt
```

The following is an example of the CLI to delete existing proxy-config map URLs. This command lists all the configured proxy-config URLs and gets user input to delete specific or all proxy-config URLs:

```
admin:utils system reverse-proxy config-uri delete
Select the reverse-proxy source URI to delete:

 1) https://saproxy.xyz.com:10000/proxymap.txt
 2) all
 q) quit

Please select an option (1 - 2 or "q" ): 1

Delete operation successful
```

The following is an example of the CLI to set the proxy-config update frequency (in minutes). Based on the set frequency, the local file system of Unified CCX and Customer Collaboration Platform are updated with the content from the proxy-config map file. Before configuring the URL, this command does not return any value. After configuring the proxy-config map URL, by default it returns one minute as the value.

```
admin:utils system reverse-proxy show-config-update-frequency
No config-uri configured

admin:utils system reverse-proxy config-uri add https://saproxy.xyz.com:10000/proxymap.txt

Source https://saproxy.xyz.com:10000/proxymap.txt successfully added

admin:utils system reverse-proxy show-config-update-frequency
1 minute

admin:utils system reverse-proxy set-config-update-frequency 5

admin:utils system reverse-proxy show-config-update-frequency
5 minutes
```

Configure CORS and Frame-Ancestors

Add both the primary and secondary reverse-proxy origins on publisher and subscriber nodes of Unified CCX. If you change Cross-Origin Resource Sharing (CORS) allowed list and frame-ancestors, you must restart Finesse Notification and Tomcat services. For information about restarting Finesse notification service, see the *Cisco Finesse Services* section in *Cisco Finesse Administration Guide*.

- Administrators must add the list of proxy server origins on the allowed list of CORS origins, if the CORS setting is enabled on Unified CCX and Customer Collaboration Platform.

  Set the reverse proxy URL in the `utils cuic cors allowed_orgins add <URL>` command as the allowed list of CORS origins. For example:

  ```
  utils cuic cors allowed_orgins add https://saproxy.xyz.com:8445
  ```

Note Run this command on both the Publisher and Subscriber Unified CCX nodes.

- Frame-ancestors are added automatically while adding the reverse-proxy trusted hosts in Unified CCX servers.

- Administrators must delete the corresponding allowed list of CORS and frame-ancestors entries while deleting the trusted hosts of a reverse-proxy.

Caution If you do not delete the corresponding CORS and frame-ancestors entries, it becomes a security vulnerability.

Note CORS and frame-ancestors are not applicable to IdS.

For information about deleting CORS see the *Cross-Origin Resource Sharing (CORS)* section in the *Cisco Finesse Administration Guide*.

For more information about configuring CORS, see the Live Data CORS Configuration section in Cisco Unified Contact Center Enterprise Installation and Upgrade Guide.

For information about deleting frame-ancestors see the *Supported Content Security Policy Directives* section in the *Cisco Finesse Administration Guide*.

Import of Reverse-Proxy Certificates

Ensure the certificates from both the OpenResty Nginx reverse-proxies are imported from the Publisher nodes.

To import the certificates, do the following:

1. In the **Cisco Unified OS Administration** interface, select **Security > Certificate Management > Upload Certificate/Certificate chain**.
2. Upload the certificate.
   a. From the **Certificate Purpose** drop-down list, select **tomcat-trust**.
   b. In the **Upload File** field, click **Browse** and select the certificate file.
   c. Click **Upload File**.
3. Run the `utils system restart` command to restart both the Unified CCX nodes in the cluster.

Configure SSO

If SSO is enabled , SSO must be configured for VPN-less access. Otherwise, agents and supervisors can't login to the Cisco Finesse desktop.

The steps to configure SSO are as follows:

1. Administrator must download proxy specific SAML SP metadata from IdS administration interface.
2. Add proxy relying party trust with IdP.
3. Add proxy redirect URIs to Finesse clients manually via IdS admin interface.
4. Validate SSO configuration for reverse-proxy from IdS admin

For more information, see the *Single-Sign On* chapter in *Cisco Unified Contact Center Express Features Guide*.

Note

- Proxy configuration does not reflect in IdS in any one of the following scenarios:
  - IdP metadata is not uploaded
  - IdS is in maintenance mode
  - Maintenance mode is completed.
- If proxy configuration is changed for IdS hosts, administrator must reestablish trust on IdP for new IdS proxy hosts after downloading new metadata file from IdS admin. Administrator must reestablish **Relying Party Trusts** with IdP. For more information, refer to the Integrate Cisco IdS with AD FS *Configure the Cisco Identity Service* section in the *Cisco Unified Contact Center Express Features Guide*
- If proxy configuration is changed for Cisco Finesse hosts, administrator must manually update the allowed Finesse client redirect URIs list on IdS admin interface. For more information, refer to theConfigure the Cisco Identity Service*Configure the Cisco Identity Service* section in the *Cisco Unified Contact Center Express Features Guide*.. Client name is "Finesse" and the URLs that are to be added are as follows:
  - `https://<finesseReverseProxySideAHost:finesseReverseProxySideAPort>/desktop/sso/authcode`
  - `https://<finesseReverseProxySideBHost:finesseReverseProxySideBPort>/desktop/sso/authcode`
- If SAML certificate is regenerated, the SAML certificate must be updated for corresponding **Relying Party Trusts** in IdP. Configure the same port used to access IdP via LAN to access IdP via proxy. For more information, refer to the *Hostname or IP Address Change* section in the *Cisco Unified Contact Center Express Features Guide*.

Serviceability

Monitor Connected Agents and Supervisors

The reverse-proxy has to be monitored by using the proxy-specific features. For more information, refer to the specific reverse-proxy documentation.

Cisco Finesse allows administrators to view the list of currently connected agents and supervisors. The administrator can filter and see the agents and supervisors who are connected to the Finesse desktop based on the connection type. For example, agents and supervisors connected through the Contact Center network and those connected through reverse-proxy can be seen. For more information, see the *Connected Agents* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html. Administrators can also view the summary of connected users by using the following CLI command:

```
admin:utils finesse show_connected_users summary

Total Connected Users: 6

Desktop Users: 1
```

```
FIPPA Users: 2
Third-party Users: 3

Users connected to Finesse via LAN/WAN: 5
Users connected to Finesse via Proxy: 1

To view the complete list of signed-in users, log in to the Cisco Finesse
Administration Console, and navigate to the Connected Agents tab.
```

To view the real-time list of connected users by using an API, see the *ConnectedUsersInfo* section in *Cisco Finesse Web Services Developer Guide* at https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide.

API Modifications to Support Reverse-Proxy Deployments

Finesse SystemInfo API

SystemInfo API is now secured when it is accessed through a reverse-proxy. The API is accessible with agent and supervisor credentials. The following field has been added to support this feature:

- **httpsPort:** HTTPS port has to be used for all Finesse API and desktop notifications.

For more information, see the *SystemInfo* and *ConnectedUsersInfo* sections in *Cisco Finesse Web Services Developer Guide* at https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide.

Reverse-Proxy selection and configurations

Reverse proxy selection criteria

Contact Center administrators must select an appropriate reverse-proxy. Any reverse-proxy that meets the following minimum requirements can be used:

- Supports HTTP2/TLS 1.2 and secure Websockets.
- Has proper logging mechanism for easy debugging of issues
- Supports multiple Unified CCX and Customer Collaboration Platform servers from a single reverse-proxy.
- Supports periodic revalidation of cached content. This is required because any updates or installations on the internal hosts don't require a manual intervention to clear the cached content of the proxy.
- Supports custom authentications or provides alternative mechanisms such as an enterprise login to prevent unauthenticated access of solution components.

Note When you use Cisco-provided reverse-proxy configuration, the requests are authenticated at the proxy before they are forwarded to the upstream servers. When you are configuring a custom reverse-proxy, you must create this authentication layer if they have to be as secure as the Cisco provided configuration. You should consider this configuration step while planning to implement VPN-less access to Finesse using a custom reverse-proxy.

- Enables caching of static resources with support for cache-control header to reduce DoS/DDoS attack vectors and to scale the proxy. Any proxy that needs to support more than a few hundred users and does not provide response caching features should be deployed with a Content Delivery Network (CDN) with support for cache-control headers so that load and security guidelines are met.

Note CDN deployment is also recommended with caching proxies such as OpenResty® Nginx to eliminate the impact of DDoS attacks.

- Supports X-Forwarded headers. These headers are used by the solution to decide how to handle a request.

Additional Requirements

Some desirable requirements in a reverse-proxy are as follows:

- Consider deploying proxies that are built on non-blocking IO-based technology instead of the traditional thread-per-request architecture, to scale better.
- Consider proxies that provide response substitution capabilities which allow workarounds for custom gadgets as custom gadgets may not work with reverse-proxy directly.

Note Finesse Desktop Chat over reverse-proxy requires response substitution capability.

- Support for port-based forwarding can be used to reduce the cost of deployment by avoiding the need for multiple externally resolvable hostnames, public DNS records, and corresponding certificates for each internal server that has to be accessed.
- Support for custom plugin/modules, which can be used to enhance the authentication model and provide a more robust security posture.

Performance and hardware recommendation

For details, see Performance and Hardware Recommendations.

Configure Reverse-Proxy

Install the host OS and reverse-proxy of your choice. Consider the following points while configuring the reverse-proxy:

- Configure SSL certificates as required.
- Refer to the specific proxy documentation and configure the proxy rules for each service with the same host and port that is configured in the mapping file.
- IdS and IdP trust should be configured before proxy mapping configuration is done. Otherwise, proxy configuration changes will not be processed by IdS.
- For IdS hosts, if proxy configuration is changed, the administrator must re-establish trust on IdP for new IdS proxy hosts after downloading new metadata file from IdS admin.

- For Finesse hosts, if proxy configuration is changed, the administrator must manually add or update the allowed Finesse client redirect URIs from IdS administration interface.
- Whenever SAML certificate is regenerated or IdP metadata is uploaded, proxy configurations are generated afresh.

To secure the reverse-proxy, refer to the *Security Guidelines* section in the *Solution Design Guide for Cisco Unified Contact Center Express* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-implementation-design-guides-list.html.

Determine Scale and Hardware for Proxy

Contact Center administrators should analyze the hardware required for the reverse-proxy, based on the number of agents and supervisors who may access the Finesse desktop without connecting to VPN. You can use the reference request rates provided for Unified CCX and Customer Collaboration Platform in Reverse-Proxy Configuration, on page 695.

The type of proxy selected guides the hardware to be used, depending on whether the proxy is shipped as an installable software or is a hardware-based application.

Sizing configurations are pre-tested for OpenResty® Nginx proxy. Custom proxy deployments should consult their product documentation or run basic scaling tests to determine the rates that can be supported by the respective proxy and scale their hardware accordingly.

Hardware Recommendations

A standard Unified CCX can be supported by OpenResty Nginx 1.19 running on a CentOS 7.4.1708 distribution, with the configurations and settings (mentioned in the Installing Nginx site) on a dual core 2 CPU (4 logical CPU) Intel Xeon CPU E5-2690 v2 (3.00GHz, 25MB cache) at an average of 10% CPU usage and peak of 15% CPU usage during logins.

A minimum of 8 GB memory is recommended for the proxy server when all other nonessential services and graphical subsystems are disabled.

Note Additional memory has to be configured based on the in-memory cache configuration added to OpenResty Nginx as described in the Cache Configuration section of Reverse-Proxy Configuration, on page 695.

It is recommended that deployments gradually onboard new solution components to the proxy until the proxy is always left with 50-55% free CPU so that it can cope with unexpected spikes in traffic from the internet.

Determine Gadget Compatibility

Determining the gadget compatibility is an important activity for planning a VPN-less Finesse deployment.

After deploying the reverse-proxy, all Cisco-provided gadgets (Unified CCX and Customer Collaboration Platform) work seamlessly with their respective servers of Release 12.5(1) SU2 or later. The Webex Experience Management and CCAI gadgets also work seamlessly with VPN-less Finesse deployments.

In some scenarios, depending on the gadget design, custom third-party gadgets require workarounds to enable them to work with the reverse-proxy deployment. Refer to the following sections to determine if any of your gadgets require workarounds.

Note

- Gadgets that are loaded from servers other than Finesse server should use **exclude-url** feature in the gadget XML specification to load the Finesse resources such as Finesse.js. For more information, refer to the **Use Gadget URI Exclude Feature to Refer to Finesse Resources** section.
- If you use two different URLs, one internal and one external, in Enterprise Chat and Email (ECE), you must update the Finesse desktop layout to use only the external URL. If you use an internal-only ECE (for integrations that support only ECE email routing), you must change the ECE web server to ensure that the ECE services are accessible externally.

Gadget Types and VPN-less Compatibility

Finesse gadgets are classified into the following types based on how they are designed operationally:

- Gadgets that are self-contained within the desktop. These gadgets do not have to make any additional network requests, or are restricted to invoking Finesse APIs and APIs on the internet.
- Gadgets that provide their functionality by communicating with an accompanying server that is deployed in the DMZ and is reachable directly from the internet and LAN.

Note To enable the same desktop layout to be used by both LAN-based and internet-based clients, the server installed in a DMZ should also be reachable from servers such as Finesse in LAN, and from clients that are running within the LAN.

- Gadgets that need to communicate with an accompanying server deployed in LAN, but uses desktop-provided **makeRequest** API to communicate to the server. The **makeRequest** API routes all the requests through the Finesse server and does not directly reach the server that is deployed in the LAN.

Note These requests succeed in a reverse-proxy deployment only if the requests are made using the hostname and port. The hostname and the port must be reachable from LAN because the requests are run by Finesse server which runs on LAN.

- Gadgets that have to communicate directly with any one of the following types of accompanying server:
  - Server deployed within the LAN and is not reachable directly from the internet.
  - Server that communicates with an additional port apart from the HTTP port used to load the gadget.

The last two types of gadgets have to be modified to be used in a reverse-proxy deployment. The steps required to enable these gadgets to be accessed from internet clients are as follows:

- Enable VPN-less access for custom gadgets

- Send hostname and port information to gadgets
- Use gadget's **URI Exclude** feature to refer to Finesse resources

Enable VPN-less Access for Custom Gadgets

Gadgets that communicate directly with accompanying servers that are deployed in LAN must handle the following aspects to work correctly in a reverse-proxy deployment:

- Use the right hostname and port for communicating with its accompanying server.

  A gadget can find the correct hostname and port corresponding to the server from which the gadget was loaded, by using the **gadgets.util.getUrlParameters().up_urlPrefs** API provided by the Finesse Javascript API.

  To find additional ports or hostnames that are required, data can be passed in as gadget preference such that the additional host and port information can be sent to the gadget. For more information, refer to the **Send Hostname and Port Information to Gadgets** section.

- Ensure that the communications are forwarded correctly by the reverse-proxy.

  After the gadget starts communicating with the correct host and port information, the hostname and port number have to be forwarded to the server deployed in the LAN. This can be done by opening the appropriate ports in the DMZ firewall. Also, ensure that the appropriate ports and rules are added to the reverse-proxy rules to forward the traffic to the correct server in the LAN.

- **Best Practice:** If requests to external servers are made using Finesse authentication headers, a common validation is enabled to authenticate the requests at the proxy. Gadgets that do not use Finesse authentication should plan to implement their own custom authentication schemes to ensure that the requests are validated at the proxy before sending to the Finesse server.

Send Hostname and Port Information to Gadgets

Gadgets that send host and port information corresponding to a server deployed within the LAN can use the **UserPreferences** feature supported by Finessse gadgets. This feature allows a configurable, named information to be passed to the gadget. The information can be referenced within the gadget XML or programmatically by using a Javascript.

For more information on how to use **UserPreferences** method, refer to https://developer.cisco.com/docs/finesse/#!gadget-preferences.

The **UserPreferences** that are created for this purpose should start with the keyword *externalServerHostAndPort* in its name. This enables Finesse to substitute the host and port that are provided with the corresponding entry from the **proxyMap** file. For example:

```
<UserPref name="externalServerHostAndPort_chat” display_name="Chat_externalServerHostAndPort"
default_value="SMHostName:7443" datatype ="hidden"/>
```

Note The `default_value` parameter is not case sensitive.

When accessed from the LAN, the **UserPreferences** continues to have the default value that is configured in the XML. However, when accessed through the reverse-proxy, the **UserPreferences** receives the value from the **proxyMap** file. For example:

```
SMHostName:7443=external-proxy-host:4043
```

When accessed through the reverse-proxy, the gadget receives the port **4043** and host name as **external-proxy-host**.

Use Gadget URI Exclude Feature to Refer to Finesse Resources

Add the following content within the `ModulePrefs` tag of the gadget XML to ensure that the resources that are loaded from Finesse server are excluded from concatenation. This step is mandatory for gadgets that load their XML from custom servers.

```
<Optional feature="content-rewrite">
<!-- these files will be directly served by Finesse, not through shindig -->
<Param name="exclude-url">finesse.min.js</Param></Optional>
```

Host Header Configuration

The following are the mandatory HTTP headers that reverse-proxy has to set along with the actual headers set by the client before forwarding the headers to the Finesse server.

Table 18:

Header	Description
X-Client-IP	The reverse-proxy should populate this custom header as the client's IP address before forwarding it to the Finesse server. This is used to log the client's IP in the Finesse server.
Host	The Host request header specifies the host and port number of the server to which the request is being sent. If no port is included, the default port for the service requested (for example, 443 for an HTTPS URL and 80 for an HTTP URL) is used. An HTTP/1.1 proxy ensures that any request message it forwards contains an appropriate Host header field to identify the service being requested by the proxy. This value is used by Finesse to find if the request is sent via the allowed list of proxies configured in Finesse. The hostname and port value of the reverse-proxy should be set. Otherwise, the Finesse validation fails and returns HTTP 400 Error.

Header	Description
X-Forwarded-For	The `X-Forwarded-For` (XFF) header is used for identifying the originating IP address of a client connecting to a web server through an HTTP proxy or a load balancer. The IP of the reverse-proxy has to be appended or set. Finesse uses this header to find if the request is from the allowed list of reverse-proxies. When the request is forwarded through multiple reverse-proxies, the values of all reverse-proxies are appended to the rightmost value of this header.
X-Forwarded-Port	The reverse-proxy should set the listening port on this header. Finesse server receives all the requests internally via 8445 port. This header value helps Finesse to set the valid configuration.

The following are the standard headers manipulated by the proxy:

Table 19:

Header	Description
Connection	Any Connection value in the HTTP header that is set by the client should be cleared and forwarded to the Finesse server. This has to be done so that the Finesse server decides the connection management and not the Finesse client. This prevents security outages.
Accept-Encoding	The reverse-proxy clears the Accept-Encoding header to have better control over compression aspects of the response.

Finesse URL

Agents and supervisors should bookmark two different pairs of URLs (publisher and subscriber) for accessing the Finesse desktop through both the Contact Center network and the reverse-proxy.

Historical and Real Time Gadgets

Cisco Unified CCX supports Historical and Real Time report gadgets in agent and supervisor desktops in VPN-less deployments. To configure the Historical and Real Time report gadgets, refer to the *Configure Historical Report Gadgets in Cisco Finesse* section in *Cisco Unified Intelligence Center User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-user-guide-list.html.

Note

- Stock reports and custom reports can be viewed in VPN-less supervisor desktop. However, before viewing the custom reports as gadgets in VPN-less supervisor desktop, run the command, **set cuic properties allow-proxy-custom-report on**.
- To configure the data set size for Historical report, run the command, **set cuic properties vpnless-response-size-ht**. By default, the data set size for HT is set to 8MB.
- To configure the data set size for Real Time report, run the command, **set cuic properties vpnless-response-size-rt**. By default, the data set size for RT is set to 300KB.

  If the data set size is more than the configured value, the gadget will display the following error message:

  ```
  Failed to load the gadget. Response size is more than allowed limit. Please contact your Administrator.
  ```

  This limitation is applicable on VPN-less deployments only. For more information about configuring the data set size, see *set Cisco Unified Intelligence Center properties* section in *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

Security Guidelines

For information about security guidelines, see the *Security Guidelines for Reverse-Proxy* in *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at

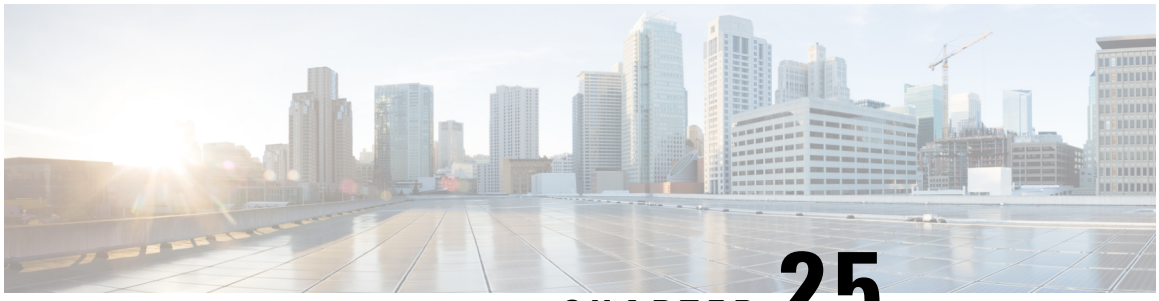
https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Caveats

Reverse-proxy deployment allows agents and supervisors to concurrently access the Cisco Finesse desktop from both LAN and through reverse-proxy. After configuring the reverse-proxy, when the agents and supervisors access the Finesse desktop through LAN, all the features work seamlessly. However, when the Finesse desktop is accessed through the reverse-proxy, the caveats are as follows:

- Finesse IP Phone Agent (FIPPA) isn't supported.
- Administrative applications and the corresponding APIs of Finesse, IdS, and Cisco Unified Intelligence Center aren't supported.
- Multiple devices accessing the Finesse desktop through Network Address Translation (NAT) isn't supported.
- Multiple users accessing the VPN-less desktop from behind a common proxy isn't supported when multiple sites are involved.
- If threshold images are used in Live Data, Real Time, and Historical gadgets, add the reverse-proxy rules to allow images to be accessed through reverse-proxy. For more information on threshold images rules, refer to the section.

- **Finesse API Compatibility:**
  - Finesse Desktop supports only the WebSocket notification mechanism over reverse-proxy. For third-party servers, BOSH or XMPP over TCP communication through reverse-proxy isn't supported.
  - When the SystemInfo API is accessed through a reverse-proxy, the authorization headers are required.



CHAPTER 25

Cisco Unified CCX Serviceability

- Cisco Unified CCX Serviceability , on page 511
- Alarms, on page 512
- Traces, on page 514
- Serviceability Tools, on page 528

Cisco Unified CCX Serviceability

Access Cisco Unified CCX Serviceability

When you complete the AppAdmin inital setup, the end user with administrator capability as configured in AppAdmin web interface can login to Cisco Unified CCX Serviceability. You can also log in as an Application user with default administrator capability configured during the installation of Unified CCX. See the *Cisco Unified Contact Center Express Install and Upgrade Guide* and *Cisco Unified Contact Center Express Administration Guide* for detailed instructions on initial AppAdmin setup and how to assign administrator capability to end users.

To access Cisco Unified CCX Serviceability:

Procedure

Step 1 By using a supported web browser, open a browser session.

Step 2 Go to `https://<server name or IP address>/uccxservice/.`

Step 3 Enter an applicable username and password, and click **Login**.

Note
If you log in as an end user, you can access Cisco Unified CCX Administration from the Navigation drop-down list box without logging in again. If you log in as an Application user, you can access Cisco Unified Serviceability in addition to these web applications.

Alarms

Cisco Unified CCX Serviceability alarms provide information on runtime status and the state of the system so that you can monitor the status and troubleshoot problems that are associated with the system. Alarm information includes the catalog, name, severity, explanation, recommended action, routing list, and parameters.

You can view alarm information by using the SysLog Viewer in Cisco Unified Real-Time Monitoring Tool (RTMT). See *Cisco Unified Real-Time Monitoring Tool Administration Guide for Cisco Unified Contact Center Express and Cisco Unified IP IVR* for detailed information on how to view alarm information.

Note Use the Alarm Definitions web page in Cisco Unified Serviceability to find information about an alarm message.

For information on alarm definitions, see the *Cisco Unified Serviceability Administration Guide* available at: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Alarm Configuration

Use the Alarm Configuration web page in Unified CCX Serviceability to view and configure alarm server settings for different Unified CCX components.

Note Alarm Server Configuration is applicable for the following Unified CCX components: Unified CCX Administration, Unified CCX Engine, and Unified CCX Cluster View Daemon .

The alarm configuration submenu allows you to:

- Enable or disable sending of alarms to local or remote syslog server.
- Configure alarm event level for local or remote syslog server

Select **Alarm** > **Configuration** from the Cisco Unified CCX Serviceability menu bar to access the Alarm Configuration web page.

Related Topics

Configure alarm settings , on page 512
Alarm configuration settings , on page 513

Configure Alarm Settings

The Alarm Configuration page is used to view and update Cisco Unified CCX Alarm Configuration for local and remote syslogs.

Procedure

Step 1 From the Unified CCXServiceability menu bar, choose **Alarm** and click **Configuration**.

The Alarm Configuration web page opens and the following fields are displayed on the Alarm Configuration web page, if configured on your Unified CCX server:

Field	Description
Local Syslogs	
Enable Alarm	Use the check box next to Enable Alarm field to enable or disable the alarms for local syslog.
Alarm Event Level	Lists the alarm severity level.
Remote Syslogs	
Enable Alarm	Use the check box next to Enable Alarm field to enable or disable the alarms for remote syslog.
Alarm Event Level	Lists the alarm severity level.
Server Name	IP address or hostname of the Syslog server to which system should send the alarm messages. If you are using CiscoWorks, enter the IP address or the hostname of the CiscoWorks server.

Step 2 To update the Alarm Event Level for local or remote syslogs, check the check box before Enable Alarm field.

Step 3 Modify Alarm Event Level for the local or remote syslogs by selecting from the Alarm Event Level drop-down list. Modify the syslog server name in case of remote syslog.

Step 4 Click **Update** icon that displays in the tool bar in the upper, left corner of the window or the **Update** button that displays at the bottom of the window to save your configuration. Click **Clear** to reset data to the previous values.

In case of a High Availability deployment, the alarm configuration changes are automatically propagated to the second node. If the second node cannot be contacted, an alert message indicating that the update has failed on the remote node is displayed.

Caution
You should activate logging **only** for the purpose of debugging and remember to **deactivate** logging once the debugging session is complete.

Alarm Configuration Settings

Use the **Alarm Configuration** page to modify alarm settings.

In the case of a High Availability deployment, the alarm configuration changes are automatically propagated to the second node. If the second node cannot be contacted, an alert message indicating that the update has failed on the remote node is displayed.

Following table defines the options available on this page:

Setting	Description
Enable Alarm for Local Syslogs	The SysLog viewer serves as the alarm destination. The program logs errors in the Application Logs within SysLog Viewer and provides a description of the alarm and a recommended action. You can access the SysLog Viewer from the Cisco Unified Real-Time Monitoring Tool. For information on viewing logs with the SysLog Viewer, see *Cisco Unified Real-Time Monitoring Tool Administration Guide for Cisco Unified Contact Center Express and Cisco Unified IP IVR*.
Enable Alarm for Remote Syslogs	The Syslog file serves as the alarm destination. Check this check box to enable the Syslog messages to be stored on a Syslog server and to specify the Syslog server name.
Alarm Event Level	Alarm event level messages range from severity 0 (most severe) to severity 7 (least severe) description of which is mentioned below. When you choose a severity level, all messages of that severity level and higher are sent. For example, if you choose ERROR_ALARM (Severity 3), all messages of severity 3, severity 2, severity 1, and severity 0 are sent. The default is "INFORMATIONAL_ALARM (Severity 6)", which will send messages of all severity levels starting from 6 to severity level 0. You can choose one of the following alarm event level options from the drop-down list box: **Emergency** This level designates system as unusable. **Alert** This level indicates that immediate action is needed. **Critical** The system detects a critical condition. **Error** This level signifies an error condition exists. **Warning** This level indicates that a warning condition is detected. **Notice** This level designates a normal but significant condition. **Informational** This level designates information messages only. **Debug** This level designates detailed event information that Cisco TAC engineers use for debugging.

Traces

A trace file is a log file that records activity from the Cisco Unified CCX components. Trace files let you obtain specific, detailed information about the system that can help you troubleshoot problems.

The Cisco Unified CCX system can generate trace information for different services. This information is stored in a trace file. To help you control the size of a trace file, you can specify the services for which you want to collect information and the level of information that you want to collect.

The Cisco Unified CCX system also generates information about all threads that are running on the system. This information is stored in the thread dump file and is useful for troubleshooting.

Component Trace Files

The component trace file contains information about each component. You can create a trace file for any of the following Unified CCX components:

- Cisco Unified CCX Administration
- Cisco Unified CCX Cluster View Daemon
- Cisco Unified CCX Editor
- Cisco Unified CCX Engine
- Cisco Unified CM Telephony Client
- Cisco Unified CCX Recording and Monitoring Services
- Cisco Unified CCX Socket.IO Service

Note You must use Cisco Unified Intelligence Center CLIs for Log Trace Settings. For more information see *Cisco Unified Intelligence Center Commands*.

The component trace file contains information about each component. To set up the trace file, follow the procedure mentioned in **Configure Trace Parameters** section.

After configuring the information that you want to include in the trace files for the various services, you can collect and view trace files by using the trace and log central option in the Cisco Unified Real-Time Monitoring Tool. See *Cisco Unified Real-Time Monitoring Tool Administration Guide for Cisco Unified Contact Center Express and Cisco Unified IP IVR* for detailed information.

Configure Trace Parameters

To update trace file information and to activate and deactivate logging, follow the procedure mentioned below:

Procedure

Step 1 From the Cisco Unified CCX Serviceability menu bar, choose **Trace** > **Configuration**.

The Trace Configuration web page opens displaying the default trace configuration for Unified CCX Engine.

Step 2 From the **Select Service** drop-down list box, choose a service or component for which you want to configure trace then, click **Go**.

You should be able to view the existing Trace configurations and debug levels for the selected Unified CCX service with check boxes for the various Debugging and XDebugging levels for each sub facility.

The debug levels for different Unified CCX subfacilities or services might vary depending on the selected service and are listed in the following table:

Table 20: Debug Levels for Different Unified CCX Subfacilities

Cisco Unified CCX Components	Subfacilities or Services
Cisco Unified CCX Administration	
	Libraries
	Managers
	Miscellaneous
Cisco Unified CCX Cluster View Daemon	
	Libraries
	Managers
	Miscellaneous
Cisco Unified CCX Editor	
	Libraries
	Managers
	Miscellaneous
	Steps
Cisco Identity Service	
	Error
	Warning
	Information
	Debugging
Cisco Unified CCX Engine	
	Libraries
	Managers
	Miscellaneous
	Steps
	Subsystems

Cisco Unified CCX Components	Subfacilities or Services
Cisco Unified CM Telephony Client or JTAPI Debug Levels	
	Warning
	Information
	Debugging
Cisco Unified CCX Socket.IO Service	
	Service
	DataProcessing
	Communication

Table 21: Debug Levels for Different Cisco VVB Subfacilities

Cisco VVB Components	Subfacilities or Services
Cisco VVB Administration	
	Libraries
	Managers
	Miscellaneous
Cisco VVB Engine	Libraries
	Managers
	Miscellaneous
	Steps
	Subsystems

Step 3 Update the debug level for one or more of the libraries or sub facilities for the selected service by doing the following:

a) To activate traces for a specific component or logging for a server, check the check box for the service that you chose.

b) To deactivate logging for a server, uncheck the specific check box.

Caution

If you modify the trace level settings for Cisco Unified CM Telephony Client, you have to restart the Unified CCX Engine for the changes to take effect.

Step 4 To limit the number and size of the trace files, you can specify the trace output setting using the following two fields. See the following table for description and default values for these two fields.

Field	Description
Maximum No. of Files	The maximum number of trace files to be retained by the system. This field specifies the total number of trace files for a given service. Cisco Unified CCX Serviceability automatically appends a sequence number to the file name to indicate which file it is; for example, Cisco001MADM14.log. When the last file in the sequence is full, the trace data begins writing over the first file. The default value varies by service.
Maximum File Size	This field specifies the maximum size of the trace file in kilobytes or megabytes depending on the selected service. The default value varies by service.

Step 5 Click **Save** icon that displays in the tool bar in the upper, left corner of the window or the **Save** button that displays at the bottom of the window to save your trace parameter configuration. The settings are updated in the system and the trace files will be generated as per the saved settings. Click **Restore Defaults** icon or button to revert to the default settings for the selected service.

In a High Availability deployment, the changes are propagated to the second node. If the second node cannot be contacted, an alert message indicating that the update has failed on the remote node is displayed.

Caution
You should activate logging **only** for the purpose of debugging and remember to **deactivate** logging once the debugging session is complete.

Note
You will not be able to save the trace configuration if the Socket.IO service is down. When the node containing the socket.IO service is down then the log levels will not be saved on that particular node.

Related Topics

Trace file location , on page 523

Trace Level Options

A trace file is a log file that records activity from the Cisco Unified CCX component subsystems and steps. Trace files let you obtain specific, detailed information about the system that can help you troubleshoot problems.

The Cisco Unified CCX system can generate trace information for every component. This information is stored in an trace file. To help you control the size of an trace file, you specify the components for which you want to collect information and the level of information that you want to collect.

A trace file that records all information for a component, such as the Cisco Unified CCX Engine, can become large and difficult to read. To help you manage the trace file, the Cisco Unified CCX system lets you specify the subfacilities for which you want to record information.

For each component, you can select one or more Debugging trace levels. These selections specify the level of details in the debugging messages that the system sends to a trace file. For instance, if you select Debugging, the system sends only the basic error messages while if you select XDebugging5, the system will send errors, warnings, informational, debugging, verbose messages and so on in detail to the trace file.

The table below describes the Trace file subfacilities.

Table 22: Trace File Subfacilities

Component Code	Description
AC_CLUSTER	Archive Cluster Component
AC_CONFIG	Archive Configuration Component
AC_DATABASE	Archive Database Component
AC_JTAPI	JTAPI Archive Component
AC_OS	Archive Operating System Component
ADM	Administration Client
ADM_CFG	Administration Configuration
APP_MGR	Applications Manager
ARCHIVE_MGR	Archive Manager
AW_CFG	Restore Administration Configuration
BARBI_CLI	Backup and Restore Client Interface
BOOTSTRAP_MGR	Cisco Unified CCX Bootstrap Manager
CFG_MGR	Configuration Manager
CHANNEL_MGR	Channel Manager
CLUSTER_MGR	Cluster Manager
CONTACT_MGR	Contact Manager
CONTACT_STEPS	Contact Steps
CRA_CMM	Cisco Unified CCX ClusterMsgMgr Component
CRA_HRDM	Cisco Unified CCX Historical Reporting Data Manager
CVD	Cluster View Daemon
DB	Database
DBPURGE_MGR	Database Purge Manager
DESKTOP	Cisco Unified CCX Editor Desktop
DOC_MGR	Document Manager
EDT	Cisco Unified CCX Editor general
ENG	Cisco Unified CCX Engine
EXECUTOR_MGR	Executor Manager

Component Code	Description
EXPR_MGR	Expression Manager
FILE_MGR	File Manager
GENERIC	Generic catalog for a facility
GRAMMAR_MGR	Grammar Manager
GRP_CFG	Group Configuration
HOLIDAY_MGR	Holiday Manager
HR_MGR	Historical Reports Manager
ICD_CTI	Cisco Unified CCX CTI Server
ICD_HDM	IPCC Express Historical Data Manager
ICD_RTDM	Cisco Unified CCX ICD Real-Time Data Manager
IVR_RTDM	Cisco Unified CCX IP IVR Real-Time Data Manager
IO_ICM	Cisco Unified ICME Input/Output
JASMIN	Java Signaling and Monitoring Interface
LIB_APPADMININTERCEPTOR	Cisco Unified CCX Administration Interceptor Library
LIB_AXL	AXL Library
LIB_CFG	Configuration Library
LIB_CLUSTER_CFG	Configuration Library for the cluster
LIB_CRTP	CRTP Library
LIB_DATABASE	Database Library
LIB_DIRECTORY	Directory Access Library
LIB_EVENT	Event Message Library
LIB_ICM	Cisco Unified ICME Library
LIB_JASPER	Jasper Tomcat Library
LIB_JCUP	JavaCup Library to parse expressions
LIB_JDBC	JDBC Library
LIB_JINI	JINI Services
LIB_JMAIL	Java Mail Library
LIB_JLEX	JLEX Library used to parse expressions

Component Code	Description
LIB_LICENSE	License Library
LIB_MEDIA	Media Library
LIB_RMI	Java Remote Method Invocation Library
LIB_SERVLET	Servlet Library
LIB_TC	Tomcat Library
LOG_MGR	Log Manager
MRCP_CFG	MRCP Configuration
MGR_MGR	Manager Manager
NODE_MGR	Node Manager
PALETTE	Editor Palette
PROMPT_MGR	Prompt Manager
PURGING	Purging
RPT	Reporting
RTPPORT_MGR	RTP Manager
SCRIPT_MGR	Script Manager
SESSION_MGR	Session Manager
SIP_STACK	SIP Stack logging
SOCKET_MGR	Socket Manager
SS_APP	Application Subsystem
SS_CHAT	Chat Subsystem
SS_CM	Contact Manager Subsystem
SS_CMT	Cisco Media Termination Subsystem
SS_DB	Database Subsystem
SS_EMAIL	Email Subsystem
SS_HTTP	HTTP Subsystem
SS_ICM	Cisco Unified ICME Subsystem
SS_MRCP_ASR	MRCP ASR Subsystem
SS_MRCP_TTS	MRCP TTS Subsystem

Component Code	Description
SS_OUTBOUND	Outbound Dialer Express Subsystem (uses MIVR log file)
SS_RM	Resource Manager Subsystem
SS_RMCM	Resource Manager Contact Manager Subsystem
SS_ROUTEANDQUEUE	Route and Queue Subsystem
SS_RTR	Real-Time Reporting Subsystem
SS_SIP	SIP Subsystem
SS_TEL	JTAPI Subsystem (Telephony)
STEP_CALL_CONTROL	Call Control Steps
STEP_MEDIA_CONTROL	Media Control Steps
STEP_SESSION	Sessions Steps
STEP_SESSION_MGMT	Session Management Steps
STEP_USER	User Steps
STEP_CALL_CONTACT	Call Contact Steps
STEPS_CONTACT	Contact Steps
STEPS_DB	Database Steps
STEPS_DOCUMENT	Document Steps
STEPS_EMAIL	E-mail Steps
STEPS_GENERAL	General Steps
STEPS_GRAMMAR	Grammar Steps
STEPS_HTTP	HTTP Steps
STEPS_ICM	Cisco Unified ICME Steps
STEPS_IPCC_EXP	Cisco Unified CCX Steps
STEPS_JAVA	Java Steps
STEPS_PROMPT	Prompt Steps
STEPS_SESSION	Session Steps
UCCX_WEBSERVICES	Chat Subsystem
USR_MGR	User Manager
WEB_STEPS	HTTP Contact Steps

When the Cisco Unified CCX product is running on a 7845 machine and tracing is ON (the default), limit the Busy Hour Call Completions (BHCC) to 4500 calls per hour. If you want to run a higher BHCC, turn the debug traces OFF. The trace subfacilities to be turned OFF are ICD_CTI, SS_TEL, SS_RM, SS_CM, and SS_RMCM.

Trace file location

The Unified CCX server stores the trace files in the Log directory under the directory in which you installed the Unified CCX component. You can collect and view trace information using the Real-Time Monitoring Tool (RTMT).

Trace File Information

The trace files contain information in standard Syslog format. The file includes some or all of the following information for each event that it records:

- Line number
- Date and time the event occurred
- Facility and subfacility (component) name
- Severity level
- Message name
- Explanation
- Parameters and values

Log Profiles Management

Log Profile is an aggregated entity that preserves trace settings of the following Unified CCX services:

- Cisco Unified CCX Engine (Traces termed as MIVR)
- Cisco Unified CCX Administration (Traces termed as MADM)
- Cisco Unified CCX Cluster View Daemon (Traces termed as MCVD)

Choose **Trace** > **Profile** from the Unified CCXServiceability menu bar to access the Log Profiles Management web page. The Log Profiles Management web page opens displaying the available log profiles each with a radio button. You can perform different operations on the listed log profiles, which are explained in detail in the following sub-sections.

Note Log Profiles Management does not support Socket.IO service.

Log profiles in Unified CCX can be one of the following two types:

1. System Log Profiles: These log profiles are pre-installed with Unified CCX and you cannot modify these profiles.

   The following table provides information on the log profiles that are factory shipped with Unified CCX:

Table 23: System Log Profiles

Name	Scenario in which this profile must be activated
Default	Activate this profile once an issue is resolved.
Outbound	For issues with Unified CCX Outbound Dialer AppAdmin.
AppAdmin	For issues with web administration through AppAdmin, Unified CCX Serviceability, and other web pages.
Media	For issues with media setup or media transmission.
HRDM (Historical Reporting Data Manager)	For issues with historical data that is written to the database.
StuckSession	For issues with application sessions, sessions that are not being deleted when appropriate and appearing stuck in AppAdmin Real Time Reports.
Database	For issues with Unified CCX Informix database.
EDBS (Enterprise Database Subsystem)	For issues with external database connectivity and integration.
CallsStuckInQueue	For issues with calls in queue that are not being allocated to available agents or appearing stuck in queue in reports.
Serviceability	For issues with the functionality in Unified CCX Serviceability Administration Interface.
RealTimeDataProblems	For issues with Real Time Reports in AppAdmin.

2. Custom Log Profiles: If the trace settings generated by system profiles are not sufficient in a particular scenario, you can create custom log profiles for better troubleshooting. You can upload and activate these custom log profiles, on a need basis.

Note

- In a HA deployment of Unified CCX, all the log profile operations will be reflected on both the nodes in the cluster.
- You cannot delete the profile if the selected log profile is the last-enabled profile in the system.

Related Topics

Create profile , on page 525
Save as another profile , on page 525
Enable profile , on page 526
Save current trace settings , on page 527
Upload profile , on page 527
Update profile , on page 528

Create Profile

To create a log profile for a specific trace, perform the following steps:

Procedure

Step 1 From the Unified CCXServiceability menu bar, choose **Trace** > **Profile**. The Log Profiles Management web page displays.

Step 2 Click **Add New** icon that displays in the tool bar in the upper, left corner of the window or the **Add New** button that displays at the bottom of the window.

The Log Profile Configuration web page displays. You can view lists of subfacilities such as libraries, managers, steps, subsystems, and so on with check boxes for the various Debugging and XDebugging levels for each subfacility for the MIVR tab by default.

Step 3 Select desired trace setting for different subfacilities in a service by clicking the corresponding check box.

Step 4 Click MCVD and MADM tabs to navigate to view and enable trace setting for these profiles.

Step 5 On successful configuration of these log profiles, click **Save** to save the profile or **Save and Enable** to save and enable the profile. The new profile will be displayed in the main profile page.

Related Topics

Update Profile, on page 528
Enable Profile, on page 526
Save Current Trace Settings, on page 527

Save as Another Profile

To save an existing profile as another profile, perform the following steps:

Procedure

Step 1 From the Unified CCXServiceability menu bar, choose **Trace** > **Profile**. The Log Profiles Management web page displays.

Step 2 Click the radio button to select a log profile.

Step 3 Click **Save As**.

The Log Profile Configuration web page for the selected profile is displayed where you can view and update the existing profile settings. Click MIVR, MCVD, and MADM tabs to view and modify the trace settings.

Step 4 You can save these updated trace settings with a new name. You will see a message confirming successful saving of the new profile.

Related Topics

Update Profile, on page 528
Enable Profile, on page 526
Save Current Trace Settings, on page 527

Enable Profile

To enable or activate a log profile, perform the following steps:

Procedure

Step 1 From the Unified CCXServiceability menu bar, choose **Trace** > **Profile**. The Log Profiles Management web page displays.

You can enable a log profile using any one of the following methods from the Log Profiles Management web page:

a) Select the radio button for the profile and click **Enable** icon or button
b) Click the hyperlink for the desired profile. Log Profile Configuration web page for the selected profile is displayed. Click **Enable** icon or button in the Profile Configuration web page
c) Click **Add New**. Enter the desired trace settings in the Profile Configuration web page and click **Save and Enable** icon or button in the Profile Configuration web page.

Step 2 The trace setting for the selected profile is transferred to system's trace settings and on successful activation, a message will be displayed in the status bar.

Related Topics

Create Profile, on page 525
Update Profile, on page 528

Delete Profile

To delete an existing log profile, perform the following steps:

Procedure

Step 1 From the Unified CCXServiceability menu bar, choose **Trace** > **Profile**.
The Log Profiles Management web page displays.

Step 2 Select the radio button for an existing profile and click **Delete** icon or button to delete a log profile.

Alternatively, you can click the hyperlink of the profile that you want to delete from the Log Profiles Management web page. Log Profile Configuration web page for the selected profile is displayed where you can view the existing profile settings. Click **Delete** to delete the selected log profile.

Step 3 The selected log profile is deleted and you will see a confirmation message in the status bar.

Note
You cannot delete the default and system log profiles. If the selected log profile happens to be the last-enabled profile in the system, then you cannot delete the profile. If you try to delete the last-enabled profile, the following alert message—"This is the last enabled profile in system and hence not allowed to be deleted." will be displayed.

Related Topics

Update Profile, on page 528
Enable Profile, on page 526

Save Current Trace Settings

The trace settings that are currently enabled in Unified CCX can be saved by clicking **Save Current Trace Settings** so that it can be enabled at a later date. For example, you might be asked to enable certain trace levels or a log profile during troubleshooting. In such a scenario, before doing the troubleshooting, you can save the current trace settings of your system as a profile so that you can enable the same trace settings after resolving the issue.

Use the procedure mentioned below to save the current trace settings in the system as a profile:

Procedure

Step 1 From the Unified CCXServiceability menu bar, choose **Trace** > **Profile**. The Log Profiles Management web page displays.

Step 2 Click **Save Current Trace Settings** icon in the tool bar or the **Save Current Trace Settings** button at the bottom of the window.

Step 3 The Explorer User Prompt dialog box opens. Enter a name for your log profile.

Step 4 Click **OK** to save this profile. All the existing trace settings in your system is saved as a profile. Click **Cancel** to cancel this operation.

You should be able to view this new log profile along with the existing profiles in the Log Profiles Management web page. You can select and click **Enable** to enable the same profile at a later date.

Related Topics

Update Profile, on page 528
Enable Profile, on page 526
Save as Another Profile, on page 525

Upload Profile

To upload a log profile, perform the following steps:

Procedure

Step 1 From thUnified CCXServiceability menu bar, choose **Trace** > **Profile**. The Log Profiles Management web page displays.

Step 2 To locate the log profile, click the **Browse** button next to **Enter a Profile File to Upload** field, navigate to the directory in which the profile (.xml file) is located, and click **Open**. The path for the profile appears in this field.

Step 3 Click **Upload** to upload the profile.

Step 4 You should be able to view the uploaded profile along with the existing profiles in the Log Profiles Management web page.

Related Topics

Update Profile, on page 528
Enable Profile, on page 526
Save Current Trace Settings, on page 527

Update Profile

You can update only custom log profiles. To view and update an existing log profile, perform the following steps:

Procedure

Step 1 From the Unified CCXServiceability menu bar, choose **Trace** > **Profile**. The Log Profiles Management web page displays.

Step 2 Click the hyperlink of the profile you wish to view or update.

The Log Profile Configuration web page for the selected profile is displayed where you can view the existing profile settings.

Step 3 Click MIVR, MCVD, and MADM tabs to view and modify the trace settings.

Step 4 Click **Save** to save the updated profile settings or **Save and Enable** to enable the updated profile. You will see a message confirming successful saving or enabling of the updated profile. Click **Cancel** to go back to Log Profiles Management web page.

Related Topics

Create Profile, on page 525
Upload Profile, on page 527
Enable Profile, on page 526
Save Current Trace Settings, on page 527

Serviceability Tools

Access Control Center — Network Services Menu

Control Center in Cisco Unified CCX Serviceability lets you do the following tasks:

- Start, stop, and restart Unified CCX services
- View the status the status of Unified CCX services
- Refresh the status of Unified CCX services

Unified CCX Serviceability provides Control Center - Network Services menu option, which is essential for your system to function.

Procedure

Choose **Tools** > **Control Center - Network Services** from the Unified CCXServiceability menu bar to perform the above-mentioned actions.

Tip

You may need to manage services in both Unified CCX Serviceability and Cisco Unified Serviceability to troubleshoot a problem. For information on Unified Serviceability services, see the *Cisco Unified Serviceability Administration Guide* available at: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Network Services

Installed automatically, network services include services that the system requires to function; for example, database and system services. Because these services are required for basic functionality, you cannot activate them in the Service Activation window.

After the installation of your application, network services start automatically. The list of services displayed in the Control Center—Network Services web page depends on the license package of your Unified CCX. If you have a Unified CCX Premium license, Unified CCX Serviceability categorizes the network services into the following categories, which are explained in the subsequent sections:

- System Services
- Admin Services, on page 530
- DB Services, on page 530

The Control Center—Network Services web page displays the following information for the network services:

- Name of the network services, their dependant subsystems, managers, or components
- Status of the service (IN SERVICE, PARTIAL SERVICE, or SHUT DOWN; for individual subsystems, the status could be OUT OF SERVICE or NOT CONFIGURED).
- Start Time of the service
- Up Time of the service

Note

- Unified CCX Engine Services information will be removed from UCCX Serviceability page, when an invalid license is uploaded.
- Only System and Admin Services Information will be visible in Unified CCX Node Services Information.

System Services

The Unified CCX Serviceability service supports starting and stopping of the following System Services:

- Cisco Unified CCX Perfmon Counter Service
- Cisco Unified CCX Cluster View Daemon—List of Managers
- Cisco Unified CCX Engine—List of Subsystems and Managers
- Cisco Unified CCX Voice Subagent
- Cisco Unified CCX Notification Service

- Cisco Unified CCX SNMP Java Adapter
- Cisco Unified Intelligence Center Reporting Service
- Cisco Unified Intelligence Center Serviceability Service
- Cisco Unified CCX DB Perfmon Counter Service
- Cisco Unified CCX Socket IO Service
- Cisco Identity Service
- Cisco Unified Web Proxy Service

Admin Services

The Unified CCX Serviceability service supports starting and stopping of the following Admin Services:

- Cisco Unified CCX Administration
- Cisco Unified CCX Serviceability - List of Managers

Note You cannot start or stop this service from the Unified CCX Serviceability web interface and you need to use CLI.

- Cisco Unified CCX WebServices

DB Services

You can start and stop Cisco Unified CCX Database service.

Finesse Services

The Unified CCX Serviceability service supports starting and stopping of the following Cisco Finesse Services:

- Cisco Finesse Tomcat

Manage Network Services

Control Center in Cisco Unified CCX Serviceability allows you to view status, refresh the status, and to start, stop, and restart network services.

Perform the following procedure to start, stop, restart, or view the status of services for a server (or for a server in a cluster in a Unified CCXCisco VVB cluster configuration). You can start, stop, or refresh only one service at a time. Be aware that when a service is stopping, you cannot start it until the service is stopped. Likewise, when a service is starting, you cannot stop it until the service starts.

Procedure

Step 1 Choose **Tools** > **Control Center—Network Services** from the Unified CCXServiceability menu bar.

Step 2 From the **Server** drop-down list box, choose the sever and then click **Go**.

The window displays the following items:

a) The service names for the server that you chose.
b) The service status; for example, In Service, Shutdown, Partial Service and so on. (Status column)
c) The exact time that the service started running. (Start Time column)
d) The amount of time that the service has been running. (Up Time column)

Step 3 Perform one of the following tasks:

a) Click the radio button before the service that you want to start and click the **Start** button.

The Status changes to reflect the updated status.

b) Click the radio button before the service that you want to stop and click the **Stop** button.

The Status changes to reflect the updated status.

c) Click the radio button before the service that you want to restart and click the **Restart** button.

A message indicates that restarting may take a while. Click **OK**.

d) To get the latest status of the services, click the **Refresh** button. The status information is updated to reflect the current status.

Command Line Interface

You can start and stop some services though the Command Line Interface (CLI). For a list of services that you can start and stop though the CLI and for information on how to perform these tasks, refer to the *Cisco Unified Contact Center Express Command Line Interface Reference Guide*.

Unified CCX Datastore

Datastores are components that allow you to manage and monitor historical, repository, and configuration data across all servers in the Unified CCX cluster.

Note Support for High Availability and remote servers is available only in multiple-server deployments.

The Unified CCX Cluster uses the publisher/subscriber database model for data replication across the system. Under normal circumstances, the database master acts as the source of data and the other node acts as the target for the data. In other words, the database master is the *publisher* and the other node is the *subscriber*.

Note In the **Tools** > **Datastore Control Center** > **Datastores** web page, the first node installed in the cluster is marked as publisher (with an icon marked P). This should not be confused with the publisher/ subscriber model being discussed here. The term publisher is used to denote only the first node in the cluster and does not indicate that node to be the source of the data. The publisher/subscriber mentioned in these pages refer to the source and destination of the data respectively. Typically, the database master node acts as the source and the other node acts as the destination.

The publisher/subscriber database model enables Unified CCX to provide high-availability and failover support. To support this on the database level, the data must be available on multiple nodes of the cluster. To have such data availability, replication is used for the Historical, and Repository datastore. The Configuration datastore does not use replication; instead, it uses atomic transactions to commit data changes to all active Configuration datastores in the cluster.

The database master is the main database. All data is written to this database, with the other database synchronizing with it. If the database master fails, then data can be written to the database on the second node. When the database master is back online, it returns to accepting writes. It also synchronizes with the other database to ensure data consistency is maintained in the cluster.

Network Outage

By default, replication between two nodes is removed if they are not able to synchronize with each other due to network outage for a substantial period of time. If the replication is dropped due to network outage, an alert is sent to the administrator so that the administrator can take corrective action.

Note Even though the replication between the nodes is removed, data could still be written to the database, which is accessible to the Unified CCX engine.

If the replication is removed, the administrator can go to **Tools** > **Datastore Control Center** > **Replication Servers** submenu from the Cisco Unified CCX Serviceability menu bar and click **Reset Replication**. This ensures that the replication is established between the nodes and the data synchronization (repair) process is initiated. Click **Check Details** icon in this web page to monitor the status of the repair.

If the network outage did not result in the replication setup being removed, once the network is up, the synchronization of data between the databases will happen automatically. For outages that last a few seconds, typically the administrator need not take any action and the system will be able to synchronize automatically.

Datastore Replication Status

Unified CCX Cluster configuration is not complete until Historical, and Repository publishers are configured. The Datastore Control Center in Unified CCX displays the status of datastore replication, allows you to synchronize data, and reset replication functions.

Note Support for High Availability is available only in multiple-server deployments.

Use the Datastore Control Center to perform the following functions:

- Obtain an overview of the datastores in the cluster and their relationships.
- Manage the datastore read/write access.
- Monitor and control the replication state (available only for Historical, and Repository datastores.)

Tip The Datastore Control Center page is available even in single-node deployments but you can only monitor the read and write access. You cannot synchronize data, reset replication, or control the replication state.

The Datastore Control Center will have the following two submenus:

- Reset Replication Between Nodes, on page 533
- Datastores, on page 534

The following table describes the datastores available and what they contain.

Datastore Name	Description
Historical	This datastore contains Historical Report data.
Repository	This datastore contains user prompts tables, grammar tables, and document tables.
Configuration	This datastore contains Unified CCX system configuration information.

Reset Replication Between Nodes

The Replication Servers menu option in Datastore Control Center allows you to view replication status and reset the replication between two nodes for the above-mentioned three datastores across all servers in the cluster. This menu will be available only in a High Availability deployment.

Follow the procedure below to access the Replication Servers web page:

Procedure

Step 1 Choose **Tools** > **Datastore Control Center** > **Replication Servers** from the Unified CCXServiceability menu bar.

The Replication Servers web page opens displaying the list of servers and the following fields in a High Availability deployment.

Datastore Name	Description
Server	Host name of the server.
Node ID	Node ID of the server in the Unified CCX cluster.
State	The current connectivity status of the node in the replication network, which can be one of the following values: **DROPPED/ TIMED OUT** The server cannot be reached and is not available in the replicated network. **ACTIVE/ CONNECTED** The server is connected in the replication network and sends or receives updates.
Job Status	The current state of this database.
Last Changed	The time the connection state was last changed.

Step 2 Click **Reset Replication** to reset the replication if the replication is not functional between the two nodes.

The **Reset Replication** button will be enabled only when the database on both the nodes are enabled.

When the subscriber goes down and it is required to make configuration updates from the publisher, you can disable Config Datastore (CDS) and Historical Datastore (HDS) on the subscriber using **Disable CDS and HDS** icon or button. The database information for the cluster is displayed at the bottom of the window. Once the subscriber is up, you can enable CDS and HDS on the subscriber using the same toggle button.

Caution
Any configuration in Application Administration and Historical data on the Subscriber node would get over written, when CDS is enabled again.

Related Topics

Datastores , on page 534
Datastore replication status , on page 532

Datastores

Procedure

Step 1 Choose **Tools** > **Datastore Control Center**.

Step 2 Click **Datastores** from the Unified CCXServiceability menu bar to view replication status of all the Unified CCX datastores and to synchronize data.

Step 3 Click **Synchronize Data** to synchronize data for each datastore except for the Configuration datastore between the two nodes in case of mismatch.

Related Topics

Reset replication between nodes, on page 533
Datastore replication status , on page 532
Datastore Control Center contents , on page 534

Datastore Control Center contents

The following table describes the Datastore Control Center contents common to all the Unified CCX datastores.

Field	Description
Server	Server machine name.
Replication Type	One of the following Enterprise Replication (ER) values in a High Availability deployment: • ER—Publication • ER—Subscription
Node ID	Node ID of server/node in Unified CCX cluster.
Read Access	Indicates whether data can be read from the datastore. Options: Yes, No.
Write Access	Indicates whether data can be written to the datastore. Options: Yes, No.

Replicate Status	Can be one of the following values: **RUNNING** All the necessary database services are up and the datastore is functioning as expected. **RETRYING** The datastore is in partial service and might be in the state of restart. **SHUTDOWN** The datastore is shutdown. **UNKNOWN** Unable to determine the current status of the datastore. This value is shown in a single-node deployment only.
Last Update Time	Indicates the last action the replication agent was performing.
Info	Use these icons to view further information in a new window: **Check Details** Click this icon to view information about data synchronization or repair jobs that might have been initiated. **History** Click this icon to view information about the replication latency (the time it takes to replicate transactions).

Related Topics

Reset replication between nodes , on page 533
Datastore replication status , on page 532

Update Parameters

Use the Service Parameters page to view and update different services in Unified CCX servers. Ensure the following prerequisites are met before configuring the parameters:

- The servers are configured.
- The service is available on the servers.

Caution Some changes to service parameters may cause system failure, thus do not make any changes to service parameters unless you fully understand the feature that you are changing or unless the Cisco Technical Assistance Center (TAC) specifies the changes.

Use the following procedure to configure the service parameters for a particular service on a particular Unified CCX server.

Procedure

Step 1 From the Unified CCXServiceability menu bar, choose **Tools** and click **Service Parameters**.

Step 2 Choose a server from the Server drop-down list box. If parameters are available for that server, the service drop down list box appears displaying the following services:

- Cisco AMC Service.
- Cisco Log Partition Monitoring Tool.
- Cisco Trace Collection Service.
- Cisco RIS Data Collector.
- Cisco Serviceability Reporter.
- Cisco DRF local.
- Cisco DRF Master.

Note
Only the common platform services mentioned above are supported currently for Unified CCX.

Step 3 Choose the service that contains the parameter that you want to update from the Service drop-down list box.

Note
The Service Parameter Configuration window displays all services (active or not active).

Step 4 The parameters for the selected service are displayed and the suggested values (if available) are listed against each one of them. Update the appropriate parameter value.

Step 5 Click **Save**.

The modified values are saved and the new values are reflected on subsequent access to the service's parameters.

Click **Set to Default** to set all service parameters for this instance of the service to the default value. A warning is displayed that this action cannot be undone and only on confirmation, the parameter values for the selected service is set to the default values.

Note
Currently, you cannot configure any parameters for the following platform services: Cisco Trace Collection Service and Cisco Log Partition Monitoring Tool.

Configure Performance Monitoring of Unified CCX Servers

Use the Performance Configuration and Logging page to configure JVM parameters and dump Thread and Memory traces for performance monitoring of Unified CCX servers. You can configure settings only for the following services of Unified CCX:

- Cisco Unified CCX Cluster View Daemon
- Cisco Unified CCX Engine
- Cisco Unified CCX Serviceability

Use the following procedure to configure JVM parameters for a particular service on a particular server.

Procedure

Step 1 From the Cisco Unified CCXServiceability menu bar, choose **Tools** > **Performance Configuration and Logging**.

Step 2 Choose a server from the Server drop-down list box and click **Go**.

The first node is selected by default and JVM options for the Unified CCX Engine service in the first node is displayed.

Step 3 Choose a service for which you want to see the JVM options from the Service drop-down list box. You should be able to select any one of the following services from this list box:

- Cisco Unified CCX Cluster View Daemon
- Cisco Unified CCX Engine
- Cisco Unified CCX Serviceability

The following JVM options are displayed for each service:

- PrintClassHistogram
- PrintGCDetails
- PrintGC
- PrintGCTimeStamps

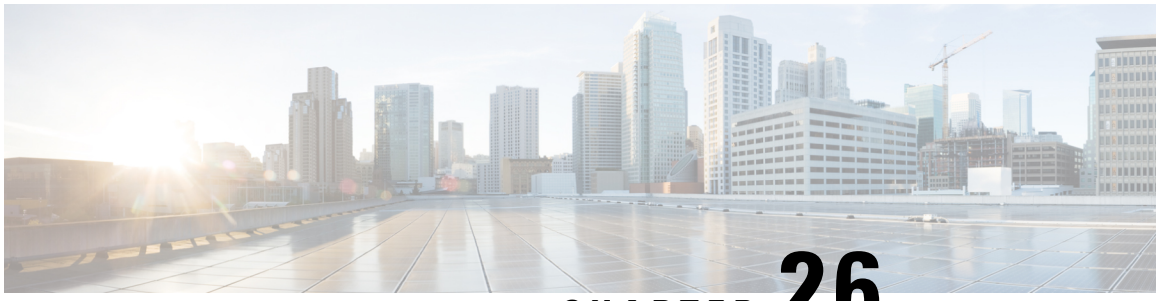
Step 4 Click the **Dump Thread Trace** icon or button to dump the thread traces for the selected service in the selected server. You can collect the corresponding jvm.log from the log folder for that facility using Real-Time Monitoring Tool (RTMT).

Step 5 Click the **Dump Memory Trace** icon or button to dump the memory traces. This creates the following two logs in the log folder for that facility.

a) Memory-<facility name>-<time stamp>.hprof (for heap dump)
b) histo-<facility name> <time stamp>.log (for histogram)

Step 6 You can change the JVM options by clicking **Enable** or **Disable** radio buttons in this page.

Click the **Update JVM Options** icon or button to update the new settings for selected service on selected node.



CHAPTER 26

Real-Time Monitoring

- Installation and Configuration, on page 539
- Performance Monitoring , on page 539
- Tools, on page 541

Installation and Configuration

The Unified RTMT installer can be downloaded using **Tools** > **Plug-ins** menu on the **Cisco Unified Contact Center Express Administration** web interface. See "Cisco Unified Real-Time Monitoring Tool" section in *Cisco Unified Real-Time Monitoring Tool Administration Guide for Cisco Unified Contact Center Express and Cisco Unified IP IVR* for installation and configuration procedures, available here:

https://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Performance Monitoring

Unified CCX provides performance counters (called perfmon counters) for application performance monitoring. The perfmon counters help expose various performance values and enables to track application performance in real time.

The perfmon counters contain counter-based information, such as the name and index of the counter, the scale, the type, subcounters to set when setting a counter, the current values, and a map containing counter instance data. Each performance counter instance object contains instance-based data, like the instance ID and current values.

You can log perfmon counters locally on the computer and use the performance log viewer in Unified RTMT to display the perfmon CSV log files that you collected or the Real-time Information Server Data Collection (RISDC) perfmon logs. Choose **System** > **Performance** on the Unified RTMT tool to view perfmon counters.

Performance Objects

Unified RTMT provides a set of default monitoring objects that assist you in monitoring the health of the system. Default objects include performance counters or critical event status for the system and other supported services.

The system logs information every 10 seconds for predefined system counters.

Performance Counters

To troubleshoot system performance problems, you add a counter (query) that is associated with the perfmon object to the performance monitor, which displays a chart for the counter. Choose **System** > **Performance** > **Open Performance Monitoring** to add a new counter.

For more information about monitoring objects and counters, see "Performance Monitoring" section in the *Cisco Unified Real-Time Monitoring Tool Administration Guide for Cisco Unified Contact Center Express and Cisco Unified IP IVR*, available here:

https://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Performance Objects and Counters for Unified CCX

Following are the Unified CCX application specific objects:

- Unified CCX database monitors
- Unified CCX engine JVM heap
- Intelligence center database performance Info
- Intelligence center JVM statistics
- Intelligence center system condition table
- Intelligence center thread pool section
- Intelligence center tomcat connector
- Reporting engine info
- Ramfs
- SchedulerInfo

Note Expand the objects in RTMT to display the counters. Right click on each counter and select **Counter Description** for the description.

Critical Services

The Critical Services monitoring function provides the name of the critical service, the status (whether the service is up, down, activated, stopped by the administrator, starting, stopping, or in an unknown state), and the elapsed time during which the services are functional on the system.

Note Unified RTMT does not display a partial running status of a service in Unified CCX. For example, it does not display a service as "running" under "Critical Services" if some of its subsystems are down. The partial status of the Unified CCX services will only be viewable from the **Unified CCX Serviceability Administration** web interface.

Note You can view and manage Cloud Connect services using Cloud Connect CLIs. For more information, see *Cloud Connect* section in the *Command Line Interface* chapter.

Tools

Unified RTMT provides various tools to monitor and troubleshoot system issues. The following section briefly describes these tools.

Alerts

Unified CCX generates alert messages to notify the administrator when a predefined condition is met, such as when an activated service fails to start. The system sends alerts as email or displays alerts as a popup message on RTMT.

RTMT contains preconfigured and user-defined alerts that support alert modifications. Although you can perform configuration tasks for both types, you cannot delete preconfigured alerts (whereas you can add and delete user-defined alerts). Predefined alerts are configured for perfmon counter value thresholds as wells as event (alarms) notifications.

Unified CCX Alerts

The following list contains preconfigured Unified CCX alerts:

Table 24:

Alert Name	Syslog Alarm Name	Description
DB CRA % Space Used	DB CRA % Space Used	The percentage of used space in the Unified CCX database, db_cra. The database, db_cra, contains the Unified CCX historical and configuration data.
DBReplicationStopped	DB_REPLICATION_STOPPED	Unified CCX Database Replication has been removed. This typically happens when the replication queues become full due to the inability to contact the other node.

HistoricalDataWrittenToFiles	UCCX_HISTORICAL_DATA_WRITTEN_TO_FILES	Historical data is not written to the Unified CCX database and has been written to the file system. Please verify the state of the Unified CCX database.
Intelligence Center CUIC_DATABASE_UNAVAILABLE	CUIC_DATABASE_UNAVAILABLE	This alert occurs when the Intelligence Center CUIC_DATABASE_UNAVAILABLE event gets generated. This indicates the system detected critical error with database.
Intelligence Center CUIC_DB_REPLICATION_FAILED	CUIC_DB_REPLICATION_FAILED	This alert occurs when the Intelligence Center CUIC_DB_REPLICATION_FAILED event gets generated. This indicates the Database replication failed.
Intelligence Center CUIC_REPORT_EXECUTION_FAILED	CUIC_REPORT_EXECUTION_FAILED	This alert occurs when the Intelligence Center CUIC_DB_REPLICATION_FAILED event gets generated. This indicates that the reporting server could not run a report. This could be because the associated datasource is offline.

Intelligence Center CUIC_UNRECOVERABLE_ERROR	CUIC_UNRECOVERABLE_ERROR	This alert occurs when the Intelligence Center CUIC_UNRECOVERABLE_ERROR event gets generated. This indicates that the system has detected an internal error within Reporting Server which may prevent it from functioning correctly. Restart may be required.
CCXToCUICAdminSyncFailed	UCCX_TO_CUIC_SYNC_FAILED	This alert occurs when the Unified CCX has failed to notify CUIC on any resource change.
CCXToCUICCVDSyncFailed	UCCX_TO_CUIC_SYNC_FAILED	This alert occurs when the Unified CCX has failed to notify CUIC on any resource change.
CCXToCUICEngineSyncFailed	UCCX_TO_CUIC_SYNC_FAILED	This alert occurs when the Unified CCX has failed to notify CUIC on any resource change.
PurgeInvoked	AUTO_PURGE_COMPLETE	This alert occurs when the Unified CCX Auto Purging has completed.
UnifiedCCXEngineMemoryUsageHigh	UnifiedCCXEngineMemoryUsageHigh	This alert occurs when the percentage of JVM heap memory used by Cisco Unified CCX Engine process is greater than the configured threshold value.

EMAIL_SERVER_DOWN	EMAIL_SERVER_DOWN	This alert occurs when the email server is not reachable.
EmailOAuthConnectionFailed	EMAIL_OAUTH_CONNECTION_FAILED	This alert occurs when CCP is unable to connect to the email OAuth server or get the access token.
EmailAuthenticationFailed	EMAIL_AUTHENTICATION_FAILED	This alert occurs when the email credentials are wrong.
CCPTomcatServiceDown	SS_PARTIAL_SERVICE_CCP_TOMCAT_DOWN	This alert occurs when CCP Tomcat is not reachable.
CCPXMPPServiceDown	CCP_XMPP_SERVICE_DOWN	This alert occurs when the Unified CCX has failed to contact CCP runtime server (XMPP).
OutboundScheduledContactImportFailed	OB_SCHEDULED_CONTACT_IMPORT_FAILED	Scheduled import of outbound contacts failed.
OutboundContactImportSchedulingFailed	OB_CONTACT_IMPORT_SCHEDULING_FAILED	Scheduling of outbound import contact failed.
UserPasswordMismatchAcrossNodes	UserPasswordMismatchAcrossNodes	One or more user passwords are not same across both the nodes.
ReasonCodesSyncRetryFailure	REASONCODE_SYNC_RETRY_ERROR	Reason Codes Sync from Finesse failed and reached to Maximum number of retries. Ensure that Finesse service and Unified CCX database are active.

CCPCacheStatusFull	CCP_CACHE_STATUS_FULL	Unable to cache emails as disk space is low. No new emails will be fetched.
CCPCacheStatusReachedLowThreshold	CCP_CACHE_STATUS_REACHED_LOW_THRESHOLD	Existing emails have consumed a considerable amount of disk space.
CacheStatusOnline	CCP_CACHE_STATUS_ONLINE	Considerable amount of disk space is now available. New emails would now be fetched.
CCPSSLError	SS_PARTIAL_SERVICE_CCP_SSL_ERROR	This alert occurs when SSL Connectivity with Customer Collaboration Platform fails.

Note To view or edit values for any alert, right click on the alert and select **Set Alert/Properties...**.

Cisco Identity Service Alerts

You can view the Cisco Identity Service alerts from the **Unified CCX** pane.

The following list contains preconfigured Cisco Identity Service alerts:

Table 25:

Alert Name	Syslog Alarm Name	Description
IdSInitializationFailure	IDS_INIT_ERROR	This alert occurs when an error is encountered during IdS initialization.
IDPMetaDataLoadError	IDP_META_DATA_LOAD_ERROR	This alert occurs when the trust could not be established between IdS and IdP during initialization.
SPMetaDataLoadError	SP_META_DATA_LOAD_ERROR	This alert occurs when SAML SP metadata Initialization fails.

IDPMetaDataUpdateError	IDP_META_DATA_UPDATE_ERROR	This alert occurs when there is an error updating IdP metadata and propagating across the cluster.
SPMetaDataUpdateError	SP_META_DATA_UPDATE_ERROR	This alert occurs when SAML SP certificate regeneration fails.
TokenMetaDataUpdateError	TOKEN_META_DATA_UPDATE_ERROR	This alert occurs when TOKEN Keystore regeneration or update fails.
IdSSecurityConfigNotPresent	IDS_SECURITY_CONFIG_NOT_PRESENT	This alert occurs when some IdS security configuration files are not present on the secondary node.
IdSSecurityConfigPullFailure	IDS_SECURITY_CONFIG_PULL_FAILURE	This alert occurs when the security config could not be pulled from the primary IdS node.
SAMLCertificateLoadFailed	SAML_CERTIFICATE_LOAD_FAILED	This alert occurs when the system is unable to read the SAML SP certificate.
IdSStateNotConfigured	STATE_NOT_CONFIGURED	This alert occurs when the trust between IdS node and IdP is yet to be established or when the IdS configuration could not be synchronized from the master node.
IdSStateOutOfService	STATE_OUT_OF_SERVICE	This alert occurs whenever a system error results in the IdS Application failing to start.

Note To view or edit values for any alert, right-click the alert and select **Set Alert/Properties**.

Syslog and Alert

Below are the set of syslog messages and alert which can be viewed from RTMT.

Syslog Alarm Name	Description
CONTM_INIT_FAILURE	Container Manager initialisation failed
CONTM_INIT_HTTP_FAILURE	Container Manager HTTP Server initialisation failed
CONTM_INIT_PROVISIONING_FAILURE	Container Manager fails to initialise the provisioning
CONTAINER_AUTO_UPDATE_FAILURE	Container Manager fails to update containers based on the provisioning
CONTAINER_AUTO_UPDATE _RECOVERY_FAILURE	Container Manager failed to update containers based on new provisioning, and failed to revert back containers based on existing provisioning

Syslog Alarm Name	Description
CONTAINER_AUTO_UPDATE_PERSIST _PROVISIONING_FAILURE	Container Manager failed to persist the new provisioning after container auto update

Syslog Support for Critical Cisco Finesse Log Messages

Cisco Finesse generates syslogs for critical log messages. Use the following procedure to view the logs using Unified RTMT.

Before you begin

Download and install RTMT on a client computer from the following URL: `https://FQDN:8443/plugins/CcmServRtmtPlugin.exe`, where FQDN is the Fully Qualified Domain Name of the Finesse server.

Procedure

Step 1 Log in to Unified RTMT using Finesse administrator credentials.

Step 2 In the tree hierarchy, select **SysLog Viewer** or choose **System** > **Tools** > **SysLog Viewer** > **Open SysLog Viewer**.

Step 3 From the **Select a Node** drop-down list, choose the server where the logs that you want to view are stored.

Step 4 Under the **Logs** tab, select **Application Logs** > **CiscoSyslog** to view and save the syslog file.

Tip
When you double-click the CiscoSyslog message, the **Show Detail** dialog displays the syslog definition and recommended actions in an adjacent pane.

For more information, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Note
System log messages generated by Cisco Finesse are also available under **SysLog Viewer** > **System Logs** > **messages**.

The following are the different types of messages and corresponding descriptions that are captured in the **SysLog Viewer** > **System Logs** > **messages**.

- CTI_SOCKET_ERROR

  System has encountered an error connecting to the CTI server.

- CTI_CONNECTION_LOST

  System has lost contact with the CTI server.

- CTI_OPEN_FAILURE

  CTI Server rejected open request.

- CTI_CONNECTION_RETRIES_EXCEEDED

  System has failed to connect to the CTI server in the allowed number of retries.

- CTI_CONNECTION_ESTABLISHED

System has successfully connected to the CTI server.

- SUBSYS_INIT_ERROR

  Error initializing subsystem.

- UNABLE_TO_CONNECT_TO_XMPP_SERVER

  Unable to connect xmpp server.

- DB_SS_CONNECTION_CHECK

  There was an error connecting to the database.

- cfservice_CORE_ERROR_DB_CONNECTION

  Unable to connect to the Database.

- AWDB_NOT_ACCESSIBLE

  Unable to connect to AWDB server.

- VOS_DB_ADAPTER_ERROR

  There was an error on the VOS DB Adapter operation.

- FINESSE_APP_STARTUP_ERROR

  Error during Finesse Application Startup.

- OF_STATE_CHANGED

  OF subsystem state successfully changed.

- CONNECTED_TO_XMPP_SERVER

  Successfully connected to xmpp server.

- SSO_API_ERROR

  Error processing REST API Request for SSO.

- API_ERROR_DETAIL

  Error processing REST API request.

- AWDB_CONNECTION_ERROR

  Error while connecting the AWDB server.

- AWDB_CONNECTION_SWITCH_SUCCESS

  AWDB server connection successfully switched.

- DRAPI_HOST_ALERT

  Failover of Digital Routing API host-pair.

  Failover isn’t supported when the Digital Routing API host backup isn’t configured.

- DRAPIAsyncRestClient

  Failed to create SSL connection to Digital Routing API.

Traces and Logs

The trace and log central feature in RTMT allows you to configure on-demand trace collection for a specific date range or an absolute time. You can collect trace files that contain search criteria that you specify and save the trace collection criteria for later use, schedule one recurring trace collection and download the trace files to a SFTP or FTP server on your network, or collect a crash dump file.

After you collect the files, you can view them in the appropriate viewer within the RTMT. You can also view traces on the server without downloading the trace files by using the remote browse feature. You can open the trace files by either selecting the internal viewer that is provided with RTMT or choosing an appropriate program as an external viewer.

For more information about traces and logs, see "Tools for traces, logs, and plug-ins" in *Cisco Unified Real-Time Monitoring Tool Administration Guide for Cisco Unified Contact Center Express and Cisco Unified IP IVR*, available here:

https://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Cloud Connect Serviceability

Use the Cisco Unified Real-Time Monitoring Tool (RTMT) to collect Cloud Connect logs.

You can use the Cloud Connect CLIs to:

- List all the containers in your deployment.
- View details of the specified container in JSON format.
- Start the specified container.
- Stop the specified container.
- Generate the heap dump for the specified container that is running JVM.
- Generate the thread dump for the specified container that is running JVM.
- Set log level for the specified service.
- Update the Cloud Connect Cherry point connector configuration details.
- Download and install RTMT on a client computer.

For more information on Cloud Connect CLIs, see *Cloud Connect*.

CUCM Telephony Data Monitoring

Following entities can be monitored using **CUCM Telephony Data** RTMT:

- Triggers
- Call Control Groups
- CTI ports

To access **CUCM Telephony Data**, click **Cisco Unified CCX** tab in RTMT.

Triggers Page

The Triggers page displays the following information for the triggers that are configured for Unified CCX:

Table 26: Triggers Page Options

Counters	Description
TriggerDN	This field displays the directory number that is associated with the trigger.
Trigger State	This field displays the state of the trigger, which can be In Service, Out of Service, or Unknown.
Application Name	This field displays the name of Unified CCX application that is associated with the trigger.
Ready for Call	This field indicates whether the trigger is ready to accept the call.
CallControlGroup ID	This field displays the ID of the call control group that is associated with the trigger.
Media Group ID	This field displays the ID of the media group that is associated with the trigger.
Last State Change Time	This field displays the time of last state change for the trigger.
Recommended Action	This field provides the reason the trigger state is Out of Service or Unknown and provides the recommended action to return the trigger state to In Service. **Note** This field is populated only if the trigger is in Out of Service state or Unknown state.

Call Control Groups page

The Call Control Groups page provides the following information about the current Call Control Group that is configured for Unified CCX:

Table 27: Call Control Groups Page Options

Counters	Description
CallControlGroup ID	This field displays the ID that is associated with the call control group.
Group State	This field displays the state of the call control group, which can be In Service, Partial Service, or Out of Service.
Total Ports	This field displays the total number of CTI ports that are configured for the call control group.
InService Ports	This field displays the number of in-service CTI ports.
OOS Ports	This field displays the number of out-of-service CTI ports.

CTI Ports Page

The CTI Ports page provides the following information about the current CTI ports that are configured for Unified CCX:

Table 28: CTI Ports Page Options

Counters	Description
CTI Port DN	This field displays the directory number of the CTI port.
CallControlGroup ID	This field displays the ID of call control group to which the CTI port belongs.
Port State	This field displays the state of CTI port, which can be In Service or Out of Service.
CallID	This field displays the call ID of the last call that is available on the CTI port before the port state changed to Out of Service. **Note** This field is populated only if the port state is Out of Service.
Last State Change Time	This field displays the last time when the CTI port state changed.

Summary Page

The Summary page provides the following information:

Table 29: Summary Page Options

Counters	Description
Overall Telephony Subsystem State	This field displays the state of the Unified CCX telephony subsystem, which can be In Service, Partial Service, or Out of Service.
Call Control Groups In Service	This field displays the number of call control groups that are in service.
Call Control Groups Out Of Service	This field displays the number of call control groups that are out of service.
Call Control Groups In Partial Service	This field displays the number of call control groups that are in partial service.
Enabled Triggers	This field displays the number of triggers that are associated with valid call control group IDs.
Disabled Triggers	This field displays the number of triggers that are associated with invalid call control group IDs.
Triggers With Config Errors	This field displays the number of triggers with configuration errors.

Note In UCCX system, if we do not configure any Trigger and CTI Ports then CM Telephony displays Out of Service status. Similarly in IPIVR, if we do not configure ICM Subsystem then ICM Subsystem displays Out of Service status.

Cisco Unified Analysis Manager

Use Cisco Unified Analysis Manager, a tool included with the Unified RTMT to perform troubleshooting operations. Unified Analysis Manager also allows you to monitor various aspects of the devices added to the tool. Unified Analysis Manager is used to collect troubleshooting information from your system and analyze the information. It can identify the supported Unified Communications (UC) products and applications that you have in your system and troubleshoot call failures across these UC applications, collecting trace and log files and other platform and configuration information. You can use this information to troubleshoot on your own or send the information to Cisco Technical Assistance for analysis.

Unified Analysis Manager for Unified CCX

To monitor and troubleshoot a Unified CCX-based solution with the help of Unified Analysis Manager, you must connect to a Unified Communications Manager server and then add the Unified CCX nodes accordingly. You can add following nodes/servers for monitoring:

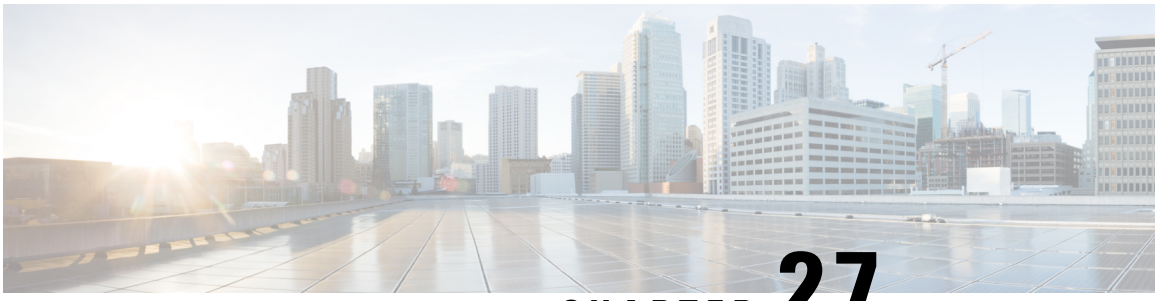
- Unified CCX node
- Call record server

Consider the following points while adding nodes/servers for monitoring:

- To add nodes/servers, ensure that you select **Node Type** as **Unified CCX**.
- To add a call record server, enter **uccxsct** in the **JDBC User Name** field.

  For detailed procedures to perform these actions, see “Cisco Unified Analysis Manager preferences” section in the *Cisco Unified Real-Time Monitoring Tool Administration Guide for Cisco Unified Contact Center Express and Cisco Unified IP IVR*, available here:

  https://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html



CHAPTER 27

Backup and Restore

- Important Considerations, on page 553
- SFTP Requirements, on page 554
- Master and Local Agents, on page 554
- Backup Tasks, on page 555
- Restore Scenarios, on page 557
- Trace Files, on page 563
- Command Line Interface, on page 563
- Alarms, on page 564

Important Considerations

Following are the important considerations when you perform backup and restore procedures:

- Before you run a backup or a restore, make sure that both nodes in a cluster are running the same version of Unified CCX. If different nodes are running different versions of Unified CCX, you will have a certificate mismatch and your backup or restore will fail.
- Before you restore Unified CCX, make sure that the hostname, IP address, DNS configuration, version, and deployment type matches the hostname, IP address, DNS configuration, version, and deployment type of the backup file that you want to restore.
- Before you restore Unified CCX, ensure that the Unified CCX version that is installed on the server matches the version of the backup file that you want to restore. Cisco DRS supports restore only for matching versions of Unified CCX. For example, Cisco DRS does not allow you to restore from Version 12.0(1) to Version 12.5(1).
- Schedule backups during off-peak hours to avoid call-processing interruptions and impact to service.
- After you use the recovery disk to bring a server with a corrupted file system into a bootable and semi-functional state, rebuild the server.
- The deployment and configuration values must be identical, and restoration must be carried out using the same network configuration and OVA deployment size in order to prevent UCCX database failure.

Note If you do not rebuild the server, you may notice missing directories, lost permissions, or corrupted soft links.

SFTP Requirements

To back up data to a remote device on the network, you must have an SFTP server that is configured and accessible from the Unified CCX node to run the backup. Cisco allows you to use any SFTP server products that have been certified with Cisco through the Interoperability Verification Testing (IVT) process. Cisco Developer Network (CDN) partners, such as GlobalSCAPE, certify their products with a specified version of Unified CCX. For information about which vendors have certified their products with your version of Unified CCX, see the following URL:

https://marketplace.cisco.com/catalog

For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to the following URL:

https://www.globalscape.com/managed-file-transfer/cisco

Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH (see http://sshwindows.sourceforge.net/)
- Cygwin (see http://www.cygwin.com/)
- Titan (see http://www.titanftp.com/)

Cisco does not support use of the SFTP product freeFTPD, because it has a 1-GB file-size limit.

Note

- For issues with third-party products that have not been certified through the IVT process, contact the third-party vendor for support.
- While a backup or restore is running, you cannot perform any Operating System (OS) Administration tasks because Cisco DRS blocks all OS Administration requests. However, you can use CLI commands to back up or restore the system.

Master and Local Agents

The system automatically starts the Master Agent service on each node of the cluster, but it is functional only on the first node. Both servers in a Unified CCX cluster must have Local Agent running to perform the backup and restore functions.

Note By default, a Local Agent automatically gets activated on each node of the cluster.

Primary Agent Duties

The Primary Agent performs the following duties:

- Stores system-wide component registration information.
- Maintains a complete set of scheduled tasks in an XML file. The Primary Agent updates this file when it receives updates of schedules from the user interface. The Primary Agent sends executable tasks to the applicable Local Agents, as scheduled. Local Agents runs immediate-backup tasks without delay.
- Lets you perform activities such as configuring backup devices, scheduling backups by adding new backup schedules, viewing or updating an existing schedule, displaying status of schedules that are run, and performing system restoration.
- Stores backup data on a remote network location.

Local Agent Duties

In a Unified CCX cluster, the Local Agent runs backup and restore scripts on each node in the cluster.

Note Cisco DRS uses an SSL-based communication between the Master Agent and the Local Agent for authentication and encryption of data between the Unified CCX publisher and subscriber nodes. Cisco DRS uses IPSec certificates for its Public/Private Key encryption. This certificate exchange is handled internally; you do not need to make any configuration changes to accommodate this exchange.

Backup Tasks

You can perform the following backup tasks using Cisco DRS:

- Manage backup devices
- Create backup schedules
- Manage backup schedules
- Estimate size of backup tar file
- Perform manual backup
- Check backup status
- View history of last 20 backups

Manage Backup Devices

Before using Cisco DRS, you must configure the locations where the backup files will be stored. You can configure up to ten backup devices. Perform the following steps to configure backup devices.

Procedure

Step 1 On **Disaster Recovery System** page, choose **Backup** > **Backup Device**.

Step 2 Click appropriate button to add a new device or to edit settings of an existing backup device.

Step 3 Enter the backup device name and choose the backup device type.

Note
You cannot delete a backup device that is configured as the backup device in a backup schedule.

Manage Backup Schedules

You can create up to ten backup schedules. Each backup schedule has its own set of properties, including a schedule for automatic backups, and a storage location.

Caution Schedule backups during off-peak hours to avoid call-processing interruptions and impact to service.

Procedure

Step 1 On the **Disaster Recovery System** page, choose **Backup** > **Scheduler**.

Step 2 Click the appropriate button to add a new schedule or to edit settings of an existing backup schedule.

Step 3 Fill out the form and enable the backup schedule.

Note
- If you plan to schedule a backup on a two-node deployment, ensure that both the servers in the cluster are running the same version of Unified CCX and are communicating in the network. Servers that are not communicating at the time of the scheduled backup will not be backed up.
- Do not schedule a backup to run while the **Update Database Statistics** task is running. By default, this task is set to run every Saturday at 3:00 am and Shrink-repack on Sunday at 3:00 am.

Perform Manual Backup

Procedure

Step 1 On the **Disaster Recovery System** page, choose **Backup** > **Manual Backup**.

Step 2 Select a backup device and start the backup.

Step 3 Click **Estimate Size** to get the approximate size of the disk space that the backup file will consume on the SFTP server.

To perform backup tasks on virtual machines, see *Unified Communications VMware Requirements*, available here:

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-software-requirements.html

Check Backup Status

On the **Disaster Recovery System** page, choose **Backup** > **Current Status** to check the backup status.

Caution Be aware that if the backup to the remote server is not completed within 20 hours, the backup session will time out. You will then need to begin a fresh backup.

Restore Scenarios

You can choose to restore any node in the cluster.

Note

- Do not attempt a restore when there is a version mismatch between the Unified CCX nodes.
- If no backup is available, you may not be able to run the restore activity on any of the nodes through Cisco DRS.
- If restore is performed without rebuild, both the nodes have to be restored.
- **One-Step Restore** option is not supported in Unified CCX.
- When SRTP is disabled on your system and you are restoring from a backup that was taken when SRTP was enabled, you must disable SRTP in the **System Parameters** page after the restore.
- When SRTP is enabled on your system and you are restoring from a backup that was taken when SRTP was disabled, you must disable and enable SRTP again in the **System Parameters** page after the restore.

Caution

- Be aware that your backup `.tar` files are encrypted by a randomly generated password. Unified CCX uses the cluster security password to encrypt this password and save it along with the backup `.tar` files. If you change this security password between the backup and restore, Cisco DRS prompts you for the old security password. Therefore, to use old backups, remember the old security password or perform a fresh backup immediately after you reset or change the password.
- Cisco DRS supports only matching versions of Unified CCX for restore. For example, Cisco DRS does not allow a restore from version 8.5(1).1000-1 to Version 9.0(1).1000-1, or from Version 8.5(1).1000-2 to Version 9.0(1).1000-1. (The last parts of the version number change when you install a service release or an engineering special.) The product versions must match, end-to-end, for Cisco DRS to run a successful Unified CCX database restore.
- After you restore a node, reboot the node, and then perform the Data Resync manually by logging in to the web interface of **Cisco Unified CCX Administration**.
- The backup process does not back up the passwords that you set for Wallboard and Recording SFTP external database users. After data is restored, passwords revert to the original default value. If you set passwords for external database users, you must manually reset them from the **Password Management** window.

Restore SA or HA Setup (Without Rebuild)

Perform this procedure if you are restoring an SA or HA setup of Unified CCX to the last known good configuration, without reinstalling Unified CCX on any of the nodes. Do not perform this procedure after a hard drive failure or other hardware failure.

Note Before you restore a cluster, make sure that the second node in the cluster is functional and is communicating with the first node. Run the CLI command **utils network connectivity** to know if second node is communicating with the first node.

You must carry out a fresh installation for the second node if it is not functional or if it is not communicating with the first node at the time of the restore.

Caution You should not perform the restore activity of a SA backup in a HA setup; otherwise the cluster will break and the second node will be an orphan.

Procedure

Step 1 In the **Disaster Recovery System** page, choose **Restore** > **Restore Wizard**.

Follow the on-screen instructions in the wizard to complete the restore process. You can select a single node or both nodes while performing restore.

Note

Restoring the node restores the entireUnified CCX database. This may take up to several hours based on the size of database that is being restored.

Step 2 Restart the SA server or the HA cluster when the restore is successful and the status shows 100 per cent.

For more information on restarting, see *Cisco Unified Operating System Administration Guide* available here: https://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_maintenance_guides_list.html.

Step 3 After you restart the SA server or HA cluster, perform the data resync by choosing **Subsystems** > **Cisco Unified CM Telephony** > **Data Resync** from **Cisco Unified CCX Administration** web interface.

Restore SA Setup (with Rebuild)

You can restore a SA setup (with rebuild) in the following cases:

- The hard drive fails, and you have a valid backup that was taken before the hard drive failure.
- The server hardware is to be replaced. Take a backup of Unified CCX when it is running in the old server hardware that is to be replaced. Note the backup device details before you shut down the Unified CCX setup.
- To correct a virtual machine with unaligned partitions, you will need to perform a manual backup first and follow the procedure by performing a fresh installation using the latest OVF Template from Unified Contact Center Express Virtual Machine Templates

Tip If you are performing any other type of hardware upgrades, such as replacing a network card or adding memory, you do not need to perform the following procedure.

Procedure

Step 1 Perform a fresh installation of the same version of Unified CCX (using the same administrator credentials, network configuration, and security password that you used earlier) on the node before you restore it.

Step 2 In the **Disaster Recovery System** page, choose **Restore** > **Restore Wizard**.

Follow the on-screen instructions in the wizard to complete the restore process.

Note

- There is no need to perform initial configuration in the **Unified CCX Administration** page for any restore with rebuild scenarios.
- To view the current license package, go to **System > Licensing > Display License**.

Step 3 Restart the server when the restore is successful and perform data resync manually using **Unified CCX Administration** page.

Note

- Apply the same license type on node the backup was taken to restore.

- If the License MAC has changed during the rebuild, the UCCX license will need to be rehosted. When applying the new license after the restore process has completed, apply a rehosted license with the same package (Enhanced, Premium, IP IVR) as the license contained within the backup that was restored.

For more information on the license rehosting mechanism, see the *Cisco Unified Contact Center Express Install and Upgrade Guide*, available here: https://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html.

Restore Only First Node in HA Setup (with Rebuild)

In a High Availability (HA) setup, if there is a hard-drive failure or any other critical hardware or software failure which needs rebuild of the first node, then perform the following procedure to recover the publisher node to the last backed up state of the publisher.

To rebuild the first node, a new CA-signed certificate must be regenerated. Before regenerating the certificate, first take a backup of the first node and restore it. Regenerate the CA-signed certificate and upload it. For information on uploading CA-signed certificate, see the Obtain and Upload CA Certificate section.

Procedure

Step 1 Perform a fresh installation of the same version of Unified CCX (using the same administrator credentials, network configuration, and security password that you used earlier) on the node before you restore it.

Step 2 Navigate to Cisco Unified Contact Center Express Administration, select **Disaster Recovery System** from the Navigation drop-down list box in the upper-right corner of the Cisco Unified CCX Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

Note
To view the current license package, go to **System** > **License Management**.

Step 3 After the restore process is successful, run the following CLI command from the second node.

```
utils uccx setuppubrestore
```

Step 4 Run the following CLI command on the target node; that is, if you want to retrieve the publisher node's data, then run this command on the subscriber node, but if you want to retrieve the subscriber node's data (which is more up-to-date), then run this command on the publisher node.

```
utils uccx database forcedatasync
```

Step 5 Restart both the nodes and run the following CLI command on the Publisher node to set up replication:

```
utils uccx dbreplication reset
```

Step 6 To set up replication for the Cisco Finesse database:

a) Run the following CLI command on the Subscriber node:

```
utils dbreplication stop
```

b) Run the following CLI command on the Publisher node:

```
utils dbreplication reset all
```

Caution

- Apply the same license type on node the backup was taken to restore.
- If the License MAC has changed during the rebuild, the UCCX license will need to be rehosted. When applying the new license after the restore process has completed, apply a rehosted license with the same package (Enhanced, Premium, IP IVR) as the license contained within the backup that was restored.

For more information on the licensing rehosting mechanism, see *Cisco Unified Contact Center Express Install and Upgrade Guide* available here: https://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html.

Restore Second Node in HA Setup (with Rebuild)

In a high availability (HA) setup, if there is a hard-drive failure or any other critical hardware or software failure which needs rebuild of the second node, then perform the following procedure to recover the second node to the last backed up state of the second node.

Caution In case the second node crashes during upgrade and there is no backup available, you may not be able to restore anything. To restore the second node, enter **utils system enableAdministration** command in the first node, delete the second node from the first node, add the second node details again and then rebuild the second node.

The recording and monitoring data which was present in the server cannot be recovered since there is no backup.

To rebuild the second node, a new CA-signed certificate must be regenerated. Before regenerating the certificate, first take a backup of the second node and restore it. Regenerate the CA-signed certificate and upload it. For information on uploading CA-signed certificate, see the Obtain and Upload CA Certificate section.

Procedure

Step 1 Perform a fresh installation of the same version of Unified CCX (using the same administrator credentials, network configuration, and security password that you used earlier) on the node before you restore it.

Step 2 In the **Disaster Recovery System** web interface, choose **Restore** > **Restore Wizard**.

Follow the on-screen instructions in the wizard to complete the restore process.

Note
When you are prompted to choose the nodes to restore, choose only the second node.

Step 3 Restart the server when the restore status is 100 per cent.

For more information on restarting, see *Cisco Unified Operating System Administration Guide* available here: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.

Restore Both Nodes in HA Setup (with Rebuild)

In a High Availability (HA) setup, if a major hard drive failure occurs on both the nodes in the cluster, or in the event of a hard drive migration or replacement, you may need to rebuild both the nodes.

- In case of a hard drive failure if you have taken a valid backup before the failure, follow this procedure to restore both the nodes, starting with the first node.
- In case of server hardware replacement, take a backup of Unified CCX when running in the old server hardware that is to be replaced. Note the backup device details before you bring down the Unified CCX setup. Follow this procedure to bring up a new server.
- To correct a virtual machine with unaligned partitions, you need to perform a manual backup first and follow the procedure by performing a fresh installation using the latest OVF Template from Unified Contact Center Express Virtual Machine Templates to restore both the nodes, starting with the first node.

Caution Set up a new cluster if you do not have a valid backup for the first node.

Procedure

Step 1 Rebuild the first node by performing a fresh installation of the same version of Cisco Unified Contact Center Express (using the same administrator credentials, network configuration and security password being used before the failure).

For more information on installing Cisco Unified Contact Center Express, see *Cisco Unified Contact Center Express Install and Upgrade Guide* available here: https://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html.

Step 2 Restore only the first node by following the procedure in Restore Only First Node in HA Setup (with Rebuild), on page 560.

Note
To view the current license package, go to **System > Licensing > Display License**.

Step 3 Restart the first node.

For more information on restarting, see the *Cisco Unified Operating System Administration Guide* available here: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.

Caution
- Apply the same license type on node the backup was taken to restore and should be applied for first node only.
- If the License MAC has changed during the rebuild, the UCCX license will need to be rehosted. When applying the new license after the restore process has completed, apply a rehosted license with the same package (Enhanced,

Premium, IP IVR) as the license contained within the backup that was restored. For more information on the licensing rehosting mechanism, see the Installing Cisco Unified Contact Center Express available here: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-installation-guides-list.html.

Step 4 Rebuild the second node by performing a fresh installation of the same version of Cisco Unified Contact Center Express (using the same administrator credentials, network configuration and security password being used before the failure).

Step 5 Restore only the second node by following the procedure in Restore Second Node in HA Setup (with Rebuild), on page 561.

Step 6 Restart the second node. Your data is restored on both the nodes of the cluster.

Trace Files

The trace files for the Master Agent, the user interface, each Local Agent, and the JSch (Java Secure Channel) library are found in the following locations:

- For the Master Agent, find the trace file at platform/drf/trace/drMA0*
- For each Local Agent, find the trace file at platform/drf/trace/drfLA0*
- For the user interface, find the trace file at platform/drf/trace/drfConfLib0*
- For the JSch, find the trace file at platforms/drf/trace/drfJSch*

You can view trace files by using the command line interface. For more information, see Command Line Interface, on page 563.

Command Line Interface

Cisco DRS also provides command-line access to few backup and restore tasks, as listed in the following table:

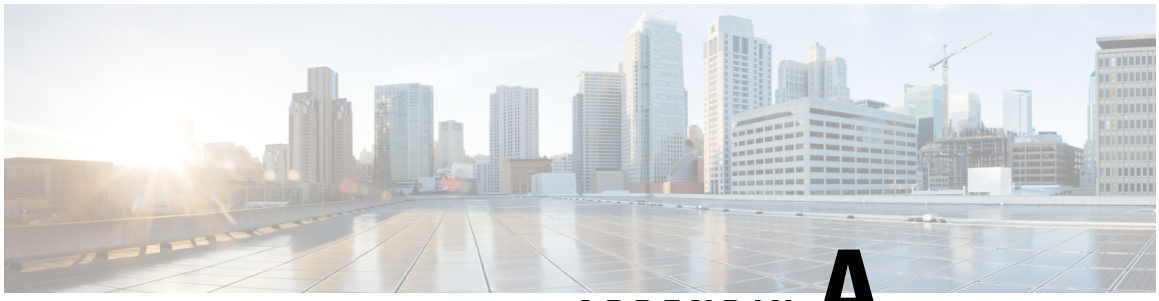
Table 30: Disaster Recovery System Command Line Interface Commands

Command	Description
utils disaster_recovery backup	Starts a manual backup by using the feature that is configured in the Cisco DRS interface
utils disaster_recovery restore	Starts a restore and requires parameters for backup location, filename, feature, and nodes to restore
utils disaster_recovery status	Displays the status of ongoing backup or restore job
utils disaster_recovery history	Displays the history of previous backup and restore operations
utils disaster_recovery show_backupfiles	Displays existing backup files

Command	Description
utils disaster_recovery cancel_backup	Cancels an ongoing backup job
utils disaster_recovery show_registration	Displays the currently configured registration
utils disaster_recovery show_tapeid	Displays the tape identification information
utils disaster_recovery device add	Adds the network or tape device
utils disaster_recovery device delete	Deletes the device
utils disaster_recovery device list	Lists all the devices
utils disaster_recovery schedule add	Adds a schedule
utils disaster_recovery schedule delete	Deletes a schedule
utils disaster_recovery schedule disable	Disables a schedule
utils disaster_recovery schedule enable	Enables a schedule
utils disaster_recovery schedule list	Lists all the schedules

Alarms

Cisco DRS (DRF) displays alarms for errors that can occur during a backup or restore procedure. The Cisco DRS alarms can be found detailed in the *Disaster Recovery System Administration Guide for Cisco Unified Communications Manager and IM & Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.



APPENDIX A

Command Line Interface

- Command Line Interface Basics, on page 565
- Show Commands, on page 568
- Set Commands, on page 590
- run Commands, on page 602
- Utils Commands, on page 605
- File Commands, on page 630
- High Availability Commands, on page 635
- Cisco Finesse Commands, on page 644
- Cisco Unified Intelligence Center Commands, on page 669
- Specific License Reservation Commands, on page 681

Command Line Interface Basics

Start CLI Session

Access the Cisco Unified Contact Center Express (Unified CCX) Command Line Interface (CLI) either remotely or locally using one of these two methods:

- From an SSH-enabled client workstation, use SSH to connect securely to the Unified CCX.
- Access the Unified CCX CLI directly or by using a terminal server that is connected to the serial port. Use this method if a problem exists with the IP address.

To start a CLI session:

Procedure

Step 1 Perform one of the following tasks:

- From a remote system, use SSH to connect securely to the Cisco CCX Platform. In your SSH client, enter

  ssh adminname@hostname

  where *adminname* specifies the platform administrator ID and *hostname* specifies the hostname that was entered during installation.

For example, **ssh admin@ccx-1**.

- From a direct connection, you receive this prompt automatically:

```
ccx-1 login:
```

where **ccx-1** represents the hostname of the system.

Enter your administrator ID.

In either case, the system prompts you for a password.

Step 2 Enter password.

The CLI prompt displays. The prompt represents the administrator ID, for example:

```
admin:
```

Get Help with Commands

You can get two kinds of help for any command:

- Detailed help that includes a definition of the command and an example of its use.
- Short query help that includes only command syntax.

To get detailed help, at the CLI prompt, enter

help *command*

where *command* specifies the command name or the command and parameter.

Detailed Help Example:

```
admin:help file list activelog help: This will list active logging files options
 are: page - pause output detail - show detailed listing reverse - reverse sort
order date - sort by date size - sort by size file-spec can contain '*' as
wildcards
```

```
admin:file list activelog platform detail 02 Dec,2004 12:00:59 <dir> drf 02
Dec,2004 12:00:59 <dir> log 16 Nov,2004 21:45:43 8,557 enGui.log 27 Oct,2004
11:54:33 47,916 startup.log dir count = 2, file count = 2
```

Note If you enter the **help** *command* without specifying the name of a particular command as the optional parameter, the system provides information about the CLI system.

To query only command syntax, at the CLI prompt, enter

command **?**

where *command* represents the command name or the command and parameter.

Query Example

```
admin:file list activelog?Syntax: file list activelog file-spec [options] file-spec
 mandatory file to view options optional page|detail|reverse|[date|size]
```

Note If you enter a **?** after a menu command, such as **set**, it acts like the **Tab** key and lists the commands that are available.

Exit Command with Ctrl-C Key Sequence

You can stop most interactive commands by entering the **Ctrl-C** key sequence.

```
admin:utils system upgrade initiate Warning: Do not close this window without
first exiting the upgrade command. Source: 1) Remote Filesystem 2) DVD/CD q) quit
 Please select an option (1 - 2 or "q"): Exiting upgrade command. Please wait...
 Control-C pressed admin:
```

Note If you run the command **utils system switch-version** and enter **Yes** to start the process, entering **Ctrl-C** exits the command but does not stop the switch-version process.

End CLI Session

To end the CLI session, enter **quit** at the CLI prompt.

If you are logged in remotely, you get logged off, and the SSH session is terminated. If you are logged in locally, you get logged off, and the login prompt appears.

Additional CLI Commands

Besides the commands available on Unified CCX , more commands are available that can be run as a part of Unified Operating System. For detailed information about all the CLI commands available for the Cisco Unified Operating System, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* available here:

https://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

The following Unified Operating System commands are **not applicable** to Unified CCX :

- delete dscp
- file delete license
- file get license
- file list license
- file view license

- set cert bulk
- set dscp
- set network cluster publisher
- set network dhcp
- set network ipv6 dhcp
- set network ipv6 service
- set network ipv6 static_address
- show ctl
- show dscp
- show itl
- show network ipv6 settings
- show tech ccm_service
- run loadxml
- utils sso unavailable
- utils system upgrade dataexport initiate

Important When **file get** CLI command is used with the **abstime** as an option to collect log files, this filters the files based on the last modified timestamp. If the last modified time is updated, this CLI may not give desired results. Use the log collection feature in RTMT instead to collect the log files.

Show Commands

Custom values are set on the VVB servers by the `VoiceBrowser.properties` and `SIPSubsystem.properties` properties files. The following commands may reset the custom values to their default values:

```
show vvb cache *
show vvb call *
show vvb mrcp *
show vvb http client response timeout
```

show uccx version

This command displays the Unified CCX versions on the active partition and the inactive partition. The inactive version is displayed only if the inactive partition is available.

Command syntax

show uccx version

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx version
Active UCCX Version: 10.5.0.95000-152
Inactive UCCX Version: NA
Command successful.
```

show uccx jtapi_client version

This command displays the JTAPI client version that the Unified CCX is using on the active and the inactive partitions. The inactive version is displayed only if the inactive partition is available.

Command syntax

show uccx jtapi_client version

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx jtapi_client version
Active:Cisco JTAPI version 9.0(0.96000)-4 Release
Inactive: NA
Command successful.
```

show uccx components

This command displays the various components in Unified CCX for which tracing can be turned on or off from CLI commands. This command is useful when you need the list of components to modify the trace settings of Unified CCX.

Command syntax

show uccx components

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx components
Various UCCX components are as follows -

 UCCXEngine
 UCCXCVD
 UCCXEditor
 JTAPI_CLIENT
 UCCXAppAdmin
```

show uccx subcomponents

This command displays the various subcomponents in specific Unified CCX component. This command is useful when you need the list of subcomponents to modify the trace settings of Unified CCX.

Command syntax

show uccx subcomponents *component* [options]

Options

- **component**—(Mandatory) Component such as UCCXEngine or UCCXEditor. For example, some of the UCCX subcomponents for 'UCCX_ENGINE' component are:
  - APP_MGR
  - ARCHIVE_MGR
  - BOOTSTRAP_MGR
  - CFG_MGR
  - CHANNEL_MGR and so on
- **page**—Displays the output one page at a time

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx subcomponents uccxengine
```

show uccx license

This command displays various licenses that are configured for Unified CCX and the features which have been activated. This command works only if the Unified CCX Cluster View Daemon (CVD) is running.

Note This command does not display license-expiry information. For more information about viewing licenses, see the *Cisco Unified Contact Center Express Administration Guide*.

This command is not applicable when you are using Smart Licensing.

Command syntax

show uccx license

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx license
Configured Licenses:

Package: Cisco Unified CCX Premium
IVR Port(s): 300
Cisco Unified CCX Premium Seat(s): 300
High Availability : Enabled
Cisco Unified CCX Preview Outbound Dialer: Enabled
Cisco Unified CCX Quality Manager Seat(s): 300
Cisco Unified CCX Advanced Quality Manager Seat(s): 300
Cisco Unified CCX Workforce Manager Seat(s): 300
Cisco Unified CCX Compliance Recording Seat(s): 300
Cisco Unified CCX Maximum Agents: 400
Cisco Unified CCX Licensed Outbound IVR Port(s): 150
Cisco Unified CCX Licensed Outbound Agent Seat(s): 150
For dynamic content like the Inbound ports In Use and Outbound IVR Ports/Agent
Seats In Use please check using the Cisco Unified CCX Administration.

Command successful.
```

show uccx trace levels

This command displays the names and trace levels of the various Unified CCX components and subcomponents. If the optional component is specified, then the trace settings of all the subcomponents of the specified component are displayed. If both the optional component and subcomponent are specified, then the trace settings of the specified subcomponent of the specified component are displayed.

Command syntax

show uccx trace levels [options]

Options

- **Component**—Displays the trace levels of all the subcomponents of this component
- **Sub-component**—Displays the trace levels of this subcomponent for the specified component. The trace levels can be displayed only if the component was specified
- **page**—Displays the output one page at a time

- **file**—Stores the output to a file instead of showing it on the console. The name of the file is displayed after the completion of the command

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx trace levels UCCXEngine
 Trace settings for component 'UCCX_ENGINE' and module  are
  ALARM = true
  DEBUGGING = false
  XDEBUGGING1 = false
  XDEBUGGING2 = false
  XDEBUGGING3 = false
  XDEBUGGING4 = false
  XDEBUGGING5 = false

 Command successful.
```

```
admin:show uccx trace levels UCCXEngine
 Trace settings for component 'UCCX_ENGINE' and module  are
  ALARM = true
  DEBUGGING = false
  XDEBUGGING1 = false
  XDEBUGGING2 = false
  XDEBUGGING3 = false
  XDEBUGGING4 = false
  XDEBUGGING5 = false

 Command successful.
```

show uccx provider ip axl

This command shows the Unified CCX AXL provider IP address.

Command syntax

show uccx provider ip axl

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin: show uccx provider ip axl
Cisco Unified Communications Manager IP is 10.78.14.140

Command Successful.
```

show uccx provider ip jtapi

This command shows the Unified CCX JTAPI provider IP address.

Command syntax

show uccx provider ip jtapi

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin: show uccx provider ip jtapi
UCCX JTAPI Provider is 10.78.14.140

Command Successful.
```

show uccx provider ip rmcm

This command shows the Unified CCX Resource Manager-Contact Manager provider IP address.

Command syntax

show uccx provider ip rmcm

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin: show uccx provider ip rmcm
UCCX RMCM Provider is 10.78.14.140

Command Successful.
```

show uccx trace file size

This command shows the trace file size for the specified component.

Command syntax

show uccx trace file size ***[component]***

Options

component—(Mandatory) Component such as UCCXEngine or UCCXEditor

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: Yes

Example

```
admin: show uccx trace file size UCCXEngine
Trace file size for UCCXEngine is 3000000 bytes.

Command Successful.
```

show uccx trace file count

This commands shows the trace file count for the specified component, which is the maximum number of trace files. The new file overwrites the older files.

Command syntax

show uccx trace file count [component]

Options

component—(Mandatory) Component such as UCCXEngine or UCCXEditor

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: Yes

Example

```
admin: show uccx trace file count UCCXEngine
Trace file count for UCCXEngine is 300.

Command Successful.
```

show uccx livedata connections

This command displays the status of the Socket.IO service and the following details of the LiveData connection:

- Total Active Client Connections to Socket.IO server.
- Total Long Polling clients connected to Socket.IO server.

Command syntax

show uccx livedata connections

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx socketio connection
Server Status: Active
Client Count: 2 (polling: 1)

Command successful.
```

show tls server cert_type

This command displays the configured certificate type used by the server for TLS connections.

Command syntax

show tls server cert_type

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

```
admin:show tls server cert_type
The server certificate type is set to ECDSA

Command successful
```

You can also use this command in Customer Collaboration Platform to display the certificate types.

ECDSA does not work with Webex Experience Management (WxM) because WxM does not support Elliptic Curve (EC) certificates.

show tls server min-version

This command allows you to show the minimum TLS version in the server that is currently configured.

Command syntax

show tls server min-version [tls server minVersion]

Options

tls server minVersion—Refers to 1.2 (TLS Version 1.2)

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:show tls server min-version
The server tls min-version is set to 1.2
Command successful
```

show tls client min-version

This command allows you to show the minimum TLS version in the client that is currently configured.

Command syntax

show tls client min-version [tls client minVersion]

Options

tls client minVersion—Refers to 1.2 (TLS Version 1.2)

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:show tls client min-version
The client tls min-version is set to 1.2
Command successful
```

show uccx tech dbserver all

This command runs the commands **show uccx tech dbserver log diagnostic** and **show uccx tech dbserver status** in succession and stores the output of the commands in a file.

Command syntax

show uccx tech dbserver all

Note The name of the file containing the output from each **show uccx tech** command run is automatically generated by the command script. The file path and filename are displayed after the completion of the operation.

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx tech dbserver all
This operation may take a few minutes to complete. Please wait...

Output is in file: uccx/cli/DbServerAll_1250664874580.txt

Command successful.
```

show uccx tech dbserver log diagnostic

This command checks for the existence of Informix assertion failure and shared memory dump logs. If logs exist, the name and path of the log files are displayed.

Command syntax

show uccx tech dbserver log diagnostic [options]

Options

page—Displays the output one page at a time

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx tech dbserver log diagnostic
This operation may take a few minutes to complete. Please wait...

The following diagnostic logs are available for the UC database server.
 core/log.txt
 core/gskit.log

 Command successful.
```

show uccx tech dbserver status

This command outputs a detailed status report of the Unified CCX database server (IDS engine) instance, that is **onstat -a** to a txt file.

Command syntax

show uccx tech dbserver status

Note The name of the file is automatically generated by the command script. The file path and filename are displayed after the completion of the operation.

Requirements

Level privilege—0

Command privilege level—0

Allowed during upgrade—Yes

Example

```
admin:show  uccx tech dbserver status
This operation may take a few minutes to complete. Please wait...
```

```
Output is in file: uccx/cli/DbServerStatus_1250666138379.txt

Command successful.
```

show uccx dbcontents

This command dumps the contents of the specified database. This command can be used to recreate a customer database on a test system for troubleshooting. For each Unified CCX database table, a dump csv file is created. Because there are huge numbers of files, these files are created in a subdirectory which will have the name as DbContents_<TIMESTAMP>. After the completion of the command, the subdirectory name and subdirectory path are displayed.

Command syntax

show uccx dbcontents database_name

Arguments

database_name—(Mandatory) Database whose contents will be output to CSV file

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:show uccx dbcontents db_cra
 This operation may take a few minutes to complete. Please wait...
 Database contents dump is in directory: uccx/cli/DbContents_1250666234370

 Command successful.
```

show uccx dbtable schema

This command displays the column names of the specified table.

Command syntax

show uccx dbtable schema database_name table_name [options]

Arguments

database_name—(Mandatory) Name of the database (db_cra, db_cra_repository etc.,) in which the table resides

table_name—(Mandatory) Name of the table

Options

page—Displays the output one page at a time

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx dbtable schema db_cra_repository documentsfiletbl
List of columns in table 'documentsfiletbl' in database 'db_cra_repository' is -
filename (nvarchar)
parentfolderid (nvarchar)
payload (blob)
lastmodifystamp (datetime year to fraction(3))
lastmodifyuser (nvarchar)
length (int)
checksum (int)

Command successful.
```

show uccx dbschema

This command outputs the schema for all the tables, views, and stored procedures in the specified database to a text file. The output consists of SQL statements that are necessary to replicate a specified database. The IDS “dbschema” utility is used to create the file. This command only displays the DB schema; it does not provide any data in the tables.

Command syntax

show uccx dbschema database_name

Arguments

database_name—(Mandatory) Name of the database whose schema will be output

Note The name of the file containing the schema is automatically generated by the command script. The file path and filename are displayed after the completion of the operation.

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx dbschema db_cra
Output is in file: uccx/cli/schema_db_cra_080212-110543.txt
```

show uccx dbtable list

This command displays the names of all the tables contained in the specified Unified CCX IDS database. The database names can be db_cra, db_cra_repository, FCRasSvr, sysmaster.

Command syntax

show uccx dbtable list database_name [options]

Arguments

database_name—(Mandatory) Database name where tables reside

Options

page—Displays the output one page at a time

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx dbtable list
db_craList of tables in database 'db_cra' is -
 agentconnectiondetail
 agentroutingsetting
 agentstatedetail
 application
 areacode
 campaign
 campaigncsqmap
 configlog
 configschema
 configschemacolumn
 configseed
…
…
teamcsqmapping
 workflowtask
 Command successful.
```

show uccx dbserver disk

This command displays information for each storage space (chunks and dbspaces).

Command syntax

show uccx dbserver disk [options]

Options

page—Displays the output one page at a time

file—Outputs the information to a .txt file. The filename is generated dynamically at runtime and the filename and path are displayed to user after the completion of the operation.

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx dbserver disk
SNO. DATABASE NAME      TOTAL SIZE (MB) USED SIZE (MB) FREE SIZE (MB) PERCENT
FREE
---- ------------------ --------------- -------------- -------------- ------------

 1    rootdbs                      358.4           66.3          292.1
81%
 2    log_dbs                      317.4          307.3           10.1
3%
 3    db_cra                       512.0            8.8          503.2
98%
 4    db_hist                    13000.0         3651.4         9348.6
71%
 5    db_cra_repository             10.2            2.9            7.3
71%
 6    db_frascal                   512.0            2.8          509.2
99%
 7    temp_uccx                   1572.9            0.1         1572.7
99%
 8    uccx_sbspace                3145.7         2988.1          157.6
5%
 9    uccx_er                      204.8            0.1          204.7
99%
 10   uccx_ersb                   1572.9         1494.1           78.8
5%


CHUNK NO. OFFSET TOTAL SIZE (MB) FREE SIZE (MB) FILENAME
--------- ------ --------------- --------------
-----------------------------------------------
 1         0               358.4          292.1
/var/opt/cisco/uccx/db/root_uccx_dbs
 2         0               317.4           10.1  /var/opt/cisco/uccx/db/log_dbs
 3         0              512.0          503.2  /var/opt/cisco/uccx/db/db_cra_dbs

 4         0             13000.0         9348.6  /common/var-uccx/dbc/db_hist_dbs

 5         0                10.2            7.3
/var/opt/cisco/uccx/db/db_cra_repository_dbs
 6         0               512.0          509.2
/var/opt/cisco/uccx/db/db_frascal_dbs
 7         0             1572.9        1572.8  /common/var-uccx/dbc/temp_uccx_dbs

 8         0              3145.7          157.6
/var/opt/cisco/uccx/db/uccx_sbspace_dbs
 9         0               204.8          204.7  /common/var-uccx/dbc/uccx_er_dbs

 10        0             1572.9           78.8  /common/var-uccx/dbc/uccx_ersb_dbs
```

show uccx dbserver sessions all

This command displays detailed session and SQL-related information for each database user session. The content of the information displayed is equivalent to running the IDS command **onstat -g ses** for each active session.

Command syntax

show uccx dbserver sessions all [options]

Options

- page—Displays the output one page at a time
- file—Outputs the information to a txt file. The filename is generated dynamically at runtime and the filename and path are displayed to user after the completion of the operation.

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx dbserver sessions all
IBM Informix Dynamic Server Version 10.00.UC5XD  -- On-Line -- Up 58 days 02:26:37
 -- 444676 Kbytes

session                                    #RSAM    total      used       dynamic
id       user     tty      pid      hostname threads  memory     memory     explain
27       cudbeven -        6750     crslnx   1        151552     75400      off

tid      name     rstcb    flags    curstk   status
75       sqlexec  52477164 Y--P---  4208     cond wait(netnorm)

Memory pools    count 2
name         class addr     totalsize freesize #allocfrag #freefrag
27           V     5309a020 147456    73704    148        50
27*O0        V     5442f020 4096      2448     1          1

name           free       used           name           free       used
overhead       0          3296           scb            0          96
opentable      0          6456           filetable      0          1088

sqscb info
scb      sqscb    optofc   pdqpriority sqlstats optcompind  directives
52fda4d0 53234018 0        0           0        0           1

Sess  SQL            Current            Iso Lock       SQL  ISAM F.E.
Id    Stmt type      Database           Lvl Mode       ERR  ERR  Vers Explain
27    -              uccxdirdb         CR  Wait 30    0    0    9.03 Off

Last parsed SQL statement :
  SELECT FIRST 100 *, CAST(Timestamp AS varchar(32)) AS strTimestamp,
    CAST(Object_Id AS varchar(64)) AS strObject_Id FROM
    UccxDb: DbChangeEventQ WHERE EventId > ? ORDER BY EventId ASC
```

show uccx dbserver session

This command displays detailed session and SQL-related information for a specific session, which represents a user connected to the database server. The content of the information displayed is equivalent to running the IDS command **onstat -g ses** for an active session specified by the session-id.

Command syntax

show uccx dbserver session session_id [options]

Arguments

session_id—(Mandatory) The Informix session ID number

Options

page—Displays the output one page at a time

file—Outputs the information to a .txt file. The filename is generated dynamically at runtime and the filename and path are displayed to user after the completion of the operation.

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx dbserver session 58
IBM Informix Dynamic Server Version 11.50.UC4     -- On-Line -- Up 14 days 04:43:40
 -- 254160 Kbytes

session           effective                              #RSAM    total      used
      dynamic
id       user     user      tty      pid      hostname threads  memory     memory
     explain
58       uccxuser -         -        -1       sakkumar 1        126976     107496
     off

tid      name     rstcb    flags    curstk   status
93       sqlexec  4b2deca0 Y--P---  5680     cond wait  netnorm   -

Memory pools    count 2
name         class addr     totalsize freesize #allocfrag #freefrag
58           V     4caa9028 122880    17064    332        18
58*O0        V     4c9d0028 4096      2416     1          1

name            free       used           name            free       used
overhead        0          3360           scb             0          96
opentable       0          8344           filetable       0          1104
ru              0          464            log             0          16512
temprec         0          21600          keys            0          1392
ralloc          0          5120           gentcb          0          1240
ostcb           0          2600           sqscb           0          29384
sql             0          40             rdahead         0          848
hashfiletab     0          280            osenv           0          1552
sqtcb           0          7464           fragman         0          368
GenPg           0          592            udr             0          5136

sqscb info
scb      sqscb    optofc   pdqpriority sqlstats optcompind  directives
4c907018 4cc92018 1        0           0        2           1

Sess       SQL             Current            Iso Lock       SQL  ISAM F.E.
Id        Stmt type      Database          Lvl Mode       ERR  ERR  Vers  Explain
58         -              db_cra              LC  Not Wait   0    0    9.28  Off

Last parsed SQL statement :
  select campaignen0_.campaignID as campaignID3_, campaignen0_.profileID as
    profileID3_, campaignen0_.recordID as recordID3_, campaignen0_.active as
    active3_, campaignen0_.ansMachineRetry as ansMachi5_3_,
    campaignen0_.cacheSize as cacheSize3_, campaignen0_.callbackTimeLimit as
    callback7_3_, campaignen0_.campaignName as campaign8_3_,
    campaignen0_.createDateTime as createDa9_3_, campaignen0_.dateInactive as
    dateIna10_3_, campaignen0_.description as descrip11_3_,
```

```
    campaignen0_.enabled as enabled3_, campaignen0_.endTime as endTime3_,
    campaignen0_.maxAttempts as maxAtte14_3_,
    campaignen0_.missedCallbackAction as missedC15_3_,
    campaignen0_.privateData as private16_3_, campaignen0_.startTime as
    startTime3_ from Campaign campaignen0_ where campaignen0_.active=?
Command successful.
```

show uccx dbserver sessions list

This command displays a one-line summary of each active Unified CCX database session. The summary includes the database name, username, session ID, and process ID. The session ID information can be used to display more detailed information about a specified session using the **show uccx dbserver session** command.

Command syntax

show uccx dbserver sessions list [options]

Options

page—Displays the output one page at a time

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx dbserver sessions list
DATABASE           USERNAME     SESSION PROCESS ID
------------------ ------------ ------- ----------
 db_cra             uccxuser         49         -1
 db_cra             uccxuser         44         -1
 db_cra             uccxuser         46         -1
 db_cra             uccxuser         61         -1
 db_cra             uccxuser         24         -1
 db_cra             uccxuser         18         -1
 db_cra             uccxhruser    31224         -1
 db_cra             uccxuser         62         -1
 db_cra             uccxuser         60         -1
 db_cra             uccxuser         47         -1
 db_cra             uccxuser         59         -1
 db_cra             uccxuser         58         -1
 db_cra             uccxuser         48         -1
 db_cra             uccxuser         50         -1
 db_cra             uccxcliuser   31616         -1

 Command successful.
```

show uccx dbserver user list

This command displays a one-line summary of each active uccx database user. The summary includes the database name, session ID and process ID. The session ID information can be used to display more detailed information about a specified user session using the **show Unified CCX dbserver session** command.

Command syntax

show uccx dbserver user list [option]

Option

page—Displays the output one page at a time

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx dbserver user list
DATABASE           USERNAME     SESSION PROCESS ID
------------------ ------------ ------- ----------
 sysadmin           informix         15          0
 sysadmin           informix         16          0
 sysadmin           informix         17          0
 sysmaster          uccxuser         18         -1
 db_cra             uccxuser         18         -1
 sysmaster          uccxuser         24         -1
 db_cra             uccxuser         24         -1
 db_cra_repository  uccxuser         25         -1
 sysmaster          uccxuser         25         -1
 fcrassvr           uccxuser         26         -1
 sysmaster          uccxuser         26         -1
 sysmaster          uccxuser         44         -1
 db_cra             uccxuser         44         -1
 db_cra_repository  uccxuser         45         -1
 sysmaster          uccxuser         46         -1
 db_cra             uccxuser         46         -1
 sysmaster          uccxuser         47         -1
 db_cra             uccxuser         47         -1
 db_cra             uccxuser         48         -1
 sysmaster          uccxuser         48         -1
 sysmaster          uccxuser         49         -1

 Command successful.
```

show uccx dbserver user waiting

This command displays a one-line summary of each Unified CCX database user and also displays whether a user session is waiting for a resource.

Command syntax

show uccx dbserver user waiting [option]

Option

page—Displays the output one page at a time

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx dbserver user waiting
USERNAME     SESSION ID LATCH LOCK BUFFER CHECKPOINT TRANSACTION INCRITICAL
------------ ---------- ----- ---- ------ ---------- ----------- ----------
 informix            16     N    N      N          N           N          N
 informix            17     N    N      N          N           N          N
 informix            15     N    N      N          N           N          N
 uccxcliuser      33927     N    N      N          N           N          N
 uccxcliuser      32784     N    N      N          N           N          N
 uccxcliuser      32737     N    N      N          N           N          N
 uccxcliuser      32631     N    N      N          N           N          N
 uccxcliuser      34424     N    N      N          N           N          N
 uccxcliuser      32522     N    N      N          N           N          N
 uccxcliuser      34364     N    N      N          N           N          N
 uccxcliuser      32508     N    N      N          N           N          N
 uccxcliuser      32480     N    N      N          N           N          N
 uccxcliuser      31616     N    N      N          N           N          N
 uccxcliuser      31601     N    N      N          N           N          N
 uccxcliuser      34327     N    N      N          N           N          N
 uccxcliuser      34071     N    N      N          N           N          N
 uccxcliuser      33981     N    N      N          N           N          N
 uccxcliuser      33939     N    N      N          N           N          N
 uccxhruser       31224     N    N      N          N           N          N
 uccxuser         30278     N    N      N          N           N          N
 uccxuser            60     N    N      N          N           N          N

 Command successful.
```

show uccx tech dbserver log message

This command displays the most recent messages in the Informix message log. The number of messages displayed is determined by the lines parameter.

Command syntax

show uccx tech dbserver log message [lines] [option]

Arguments

lines—(Optional) Number of lines from message log that will be displayed. Defaults to 20.

Option

page—Displays the output one page at a time

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx tech dbserver log message 10
Message Log File: online.uccx.log

The last 10 lines of the log file are -
```

```
16:05:19  Maximum server connections 33
16:05:19  Checkpoint Statistics - Avg. Txn Block Time 0.000, # Txns blocked 0,
Plog used 21, Llog used 12

16:10:19  Checkpoint Completed:  duration was 0 seconds.
16:10:19  Wed Aug 19 - loguniq 8, logpos 0x93c018, timestamp: 0xb0244c Interval:
 4106

16:10:19  Maximum server connections 33
16:10:19  Checkpoint Statistics - Avg. Txn Block Time 0.000, # Txns blocked 0,
Plog used 2, Llog used 2


 Command successful.
```

show uccx dbtable contents

This command displays the contents of the specified table.

Command syntax

show uccx dbtable contents database_name table_name [option]

Arguments

database_name—(Mandatory) Name of the database for example, db_cra, db_cra_repository in which the table resides

table_name—(Mandatory) Name of the table

Option

page—Displays the output one page at a time

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx dbtable contents db_cra resource
Output is in file: uccx/cli/resource_Contents_1250666550481.csv

 Command successful.
```

show vmtools version

This command displays the current version of the vmtools that are installed on the system.

Command syntax

```
show vmtools version
```

Requirements

Level privilege: 0

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:show vmtools version
Current VMWare Tools running version: 10.0.9.55972 (build-3917699)
```

show uccx asr sessions

This command shows the number of concurrent active ASR sessions.

Command syntax

show uccx asr sessions

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:show uccx asr sessions
10.11.12.13 : Concurrent = 0 , Aggregate [Success = 0 , Failure = 0 ]
11.12.13.14 : Concurrent = 0 , Aggregate [Success = 0 , Failure = 0 ]
Total : Concurrent = 0 , Aggregate [Success = 0 Failure = 0 ]

Command successful.
```

show uccx tts sessions

This command shows the number of concurrent active TTS sessions.

Command syntax

show uccx tts sessions

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:show uccx tts sessions
10.11.12.13 : Concurrent = 0 , Aggregate [Success = 0 , Failure = 0 ]
11.12.13.14 : Concurrent = 0 , Aggregate [Success = 0 , Failure = 0 ]
Total : Concurrent = 0 , Aggregate [Success = 0 Failure = 0 ]
```

```
Command successful.
```

show webapp session timeout

This command displays the webapp session timeout value in minutes, that has been set to invalidate any inactive Unified CCX web application sessions. After the set time elapses, the users are logged off from any of the inactive Unified CCX web sessions. The default value is 30 minutes. This command is node specific and displays the value that is configured for the node on which this command is run.

Command syntax

show webapp session timeout

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin: show webapp session timeout
The current session-timeout used for web sessions and applications is 10 minutes.
```

Applies to: Cisco Identity Service Management, Disaster Recovery System, Cisco Unified CCX Administration, Cisco Finesse Administration, Cisco Unified Serviceability, Cisco Unified CCX Serviceability, Cisco Unified OS Administration, and Cisco Unified Intelligence Center.

show cli session timeout

This command displays the CLI session timeout value in minutes, that has been set to invalidate any inactive Unified CCX CLI sessions. After the set time elapses, the users are logged off from any of the inactive Unified CCX CLI sessions. The default value is 30 minutes. This command is node specific and displays the value that is configured for the node on which this command is run.

Command syntax

show cli session timeout

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin: show cli session timeout
CLI session-timeout is set to 20 minutes for new CLI sessions.
```

Set Commands

set uccx trace defaults

This command sets the default trace levels for all components and subcomponents in Unified CCX. If the optional component is specified, it sets the default trace levels only for all the subcomponents of the specified component. If both the optional component and subcomponent are specified, it sets the default trace levels only for the specified subcomponent under the component.

Command syntax

set uccx trace defaults [component] [subcomponent]

Options

- **Component**—(Mandatory) Sets the default trace levels for all the subcomponents of this component. The various components are UCCXEngine, UCCXCvd, UCCXAppAdmin and JTAPI_CLIENT.
- **Sub-component**—(Optional) Sets the default trace levels for this subcomponent for the specified component. This trace level can be specified only if the component was specified preceding it.

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:set uccx trace defaults uccxengine
SS_HTTP
Default traces restored successfully for the module.
```

set uccx trace file size component size

This command sets the trace file size for the specified component.

Command syntax

set uccx trace file size [component] [size]

Parameters

component—(Mandatory) The component such as UCCXEngine or UCCXEditor

size—(Mandatory) Specifies the file size in bytes

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:set uccx trace file size uccxengine 3145728
Trace file size for uccxengine is set to 3145728 bytes.
```

set uccx trace file count component no-of-files

This command sets the trace file count for the specified component, that is the maximum number of trace files after which older files will start getting overwritten.

Command syntax

set uccx trace file count [component] [no-of-files]

Arguments

- **component**—(Mandatory) The component such as UCCXEngine or UCCXEditor.
- **no-of-files**—(Mandatory) Specifies the number of files after which older files will get overwritten.

Requirements

Level privilege—1

Command privilege level—1

Allowed during upgrade—No

Example

```
admin:set uccx trace file count uccxengine 300
Trace file count for uccxengine is set to 300
```

set uccx trace enable

Enables the specified logging level for the sub-component in the component mentioned in the command. The user can enter multiple levels of logging by separating them by commas.

After the completion of the command, a message is displayed showing the current log trace settings enabled.

Restart the Unified CCX services for the trace changes to take effect.

Command syntax

set uccx trace enable *[component] [sub-component]* [level]

Options

component—(Mandatory) The component such as UCCXEngine or UCCXEditor or JTAPI_CLIENT

sub-component—(Mandatory) The subcomponent within the component such as JTAPI Subsystem within the UCCXEngine component. For the JTAPI_CLIENT component, there are no sub-components.

sub-component—(Mandatory) The subcomponent within the component such as SS_SIP within the UCCXEngine component. For the SS_SIP component, there are no sub-components.

Level—(Mandatory) The logging level which will be enabled. Tracing levels are Debugging, XDebugging1, XDebugging2, XDebugging2, XDebugging3, XDebugging4 and XDebugging5. For the JTAPI_CLIENT, the

tracing levels are Warning, Informational, Debug, Jtapi_Debug, JtapiImpl_Debug, Cti_Debug, CtiImpl_Debug, Protocol_Debug and Misc_Debug.

Level—(Mandatory) The logging level which will be enabled. Tracing levels are Debugging, XDebugging1, XDebugging2, XDebugging2, XDebugging3, XDebugging4 and XDebugging5.

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example 1

```
admin:set uccx trace enable uccxengine SS_VB debugging
 Trace for uccxengine:SS_VB:debugging is enabled.
 Command successful.
```

Example 2

```
admin:set uccx trace enable UCCXengine SS_SIP XDEBUGGING1,XDEBUGGING2
Trace for uccxengine:SS_SIP:XDEBUGGING1 is enabled
Trace for uccxengine:SS_SIP:XDEBUGGING2 is enabled
Command successful.
```

set uccx trace disable

Disables the specified logging level for the subcomponent in the component mentioned in the command. The user can enter multiple levels of logging by separating them by commas. You cannot use this command to turn off Alarm tracing.

After the completion of the command, a message is displayed showing the current log trace settings enabled.

Restart the Unified CCX services for the trace changes to take effect.

Command syntax

set uccx trace disable ***[component] [sub-component]*** **[level]**

Options

Component—The component such as UCCXEngine or UCCXEditor or JTAPI_CLIENT.

Sub-component—The subcomponent within the component such as JTAPI Subsystem within the UCCXEngine component. For the JTAPI_CLIENT component, there are no subcomponents.

Sub-component—The subcomponent within the component such as SS_SIP within the UCCXEngine component.

Level—(Mandatory) The logging level which will be disabled. Tracing levels are Debugging, XDebugging1, XDebugging2, XDebugging2, XDebugging3, XDebugging4 and XDebugging5. The tracing levels will also be available as part of the help of the command.

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example 1

```
admin:set uccx trace disable uccxengine SS_VB debugging
 Trace for uccxengine:SS_VB:debugging is disabled.
 Command successful.
```

Example 2

```
set uccx trace disable UCCXEngine SS_SIP XDEBUGGING1,XDEBUGGING2
Trace for uccxengine:SS_SIP:XDEBUGGING1 is disabled
Trace for uccxengine:SS_SIP:XDEBUGGING2 is disabled
Command successful.
```

set password user security

This command changes the security/SFTP password on Unified CCX. In addition to changing the security password, it also changes the passwords of the internal Unified CCX users.

Command syntax

set password user security

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:set password user security
Please enter the old password: ******
Please enter the new password: ******
Reenter new password to confirm: ******
WARNING:
Please make sure that the security password on the publisher is changed first.
The security password needs to be the same on all cluster nodes,
including the application server, therefore the security password on all nodes
need to be changed.

After changing the security password on a cluster node, please restart that node.

Continue (y/n)?y

Please wait...

Command successful.
```

set tls server cert_type

Use this command to set the server certificate type to either RSA or ECDSA ciphers for TLS connections. The certificate set to the specified type is then presented for the cipher negotiations on all incoming TLS communications.

Command syntax

set tls server cert_type [option]

Option

ecdsa—Sets the certificate type to ECDSA.

rsa—Sets the certificate type to RSA.

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:set tls server cert_type rsa

Configuring the server to use RSA certificates for all inbound connections.

Do you want to continue (y/n) ? y
Yes entered
Configuring the server to use RSA ciphers for inbound connections.

Successfully configured the server to use RSA certificate for all inbound
connections.

******************************************************
A system reboot will occur for the changes to take effect.
It is highly recommended that you perform a system backup
after the system reboot.
Ensure all the nodes in the cluster are running on the same
certificate type by running the 'set' command
******************************************************

Broadcast message from root@uccxfirstnode (Mon Jul 5 10:31:04 2021):

The system is going down for reboot in 1 Minute

Broadcast message from root@uccxfirstnode (Mon 2021-07-05 10:31:05 IST):

The system is going down for reboot at Mon 2021-07-05 10:32:04 IST!
```

Note After the system reboots, the self-signed and CA certificates of the servers, whose certificate type has changed, must be regenerated and re-uploaded into the client servers.

You can also use this command to set the certificates in Customer Collaboration Platform.

ECDSA does not work with Webex Experience Management (WxM) because WxM does not support Elliptic Curve (EC) certificates.

set tls server min-version

This command allows you to configure the minimum TLS version in the server that can be used for inbound SSL connections. You must restart the system for the changes to take effect.

Note In a high availability (HA) deployment, run this CLI command on both the nodes of the cluster. Restart both the nodes after executing the CLI command.

Command syntax

set tls server min-version [tls server minVersion]

Options

tls server minVersion—Refers to 1.2 (TLS Version 1.2)

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:set tls server min-version 1.2
**WARNING** If you are lowering the TLS version it can lead to security issues
**WARNING**
Do you really want to continue (yes/no) ? yes
Execute this command in the other nodes of the cluster.
Restart the system using the command 'utils system restart' for the changes to
take effect
Command successful
```

set tls client min-version

This command allows you to configure the minimum TLS version in the client that can be used for outbound SSL connections. You must restart the system for the changes to take effect.

Note In a high availability (HA) deployment, run this CLI command on both the nodes of the cluster. Restart both the nodes after executing the CLI command.

Command syntax

set tls client min-version [tls client minVersion]

Options

tls client minVersion—Refers to 1.2 (TLS Version 1.2)

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:set tls client min-version 1.2
**WARNING** If you are lowering the TLS version it can lead to security issues
**WARNING**
Do you really want to continue (yes/no) ? yes
Execute this command in the other nodes of the cluster.
Restart the system using the command 'utils system restart' for the changes to
take effect
Command successful
```

set uccx provider ip axl

This command sets the Unified CCX AXL provider IP address. Use this command only when the IP address of Unified Communications Manager has been changed and Unified CCX is being pointed to the new IP address.

Note After you run this command, restart the Unified CCX Engine service. After Unified CCX Engine service starts successfully, restart Cisco Tomcat using the CLI command **utils service restart Cisco Tomcat**.

Command syntax

set uccx provider ip axl [ip-address]

Arguments

[ip-address]—The IP address of the AXL provider.

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: No

Example

```
admin: set uccx provider ip axl 10.78.14.140
Cisco Unified Communications Manager IP is set to 10.78.14.140

Command Successful.
```

set uccx provider ip jtapi

This command sets the Unified CCX JTAPI provider IP address. Use this command only when the IP address of Unified Communication Manager has been changed and Unified CCX is being pointed to the new IP address.

Note After you run this command, restart the Unified CCX Engine service. After Unified CCX Engine service starts successfully, restart Cisco Tomcat using the CLI command **utils service restart Cisco Tomcat**.

Command syntax

set uccx provider ip jtapi ***[ip-address]***

Arguments

[ip-address]—The IP address of the JTAPI provider.

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: No

Example

```
admin: set uccx provider ip jtapi 10.78.14.140
UCCX JTAPI Provider is set to 10.78.14.140

Command Successful.
```

set uccx provider ip rmcm

This command sets the Unified CCX Resource Manager-Contact Manager provider IP address. Use this command only when the IP address of Unified Communications Manager has been changed and Unified CCX is being pointed to the new IP address.

Note After you run this command, restart the Unified CCX Engine service. After Unified CCX Engine service starts successfully, restart Cisco Tomcat using the CLI command **utils service restart Cisco Tomcat**.

Command syntax

set uccx provider ip rmcm ***[ip-address]***

Arguments

[ip-address]—The IP address of the RMCM provider.

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: No

Example

```
admin: set uccx provider ip rmcm 10.78.14.140
UCCX RMCM Provider is set to 10.78.14.140

Command Successful.
```

set uccx appadmin administrator

Administrator capability can be added to a user in Unified Communications Manager using this command.

Note Run this command to set the administrator for a configured Unified CCX system only. For a newly installed system, you must login with the platform login password that you specified during installation.

Command syntax

set uccx appadmin administrator *[username]*

Options

[username]—Username is set as the Cisco Unified CCX application administration.

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:set uccx appadmin administrator username
UCCX appadmin adminstrator is set to username
```

Note You cannot assign Administrator capability to a user ID that is the same as the application administrator user ID that you created during the Unified CCX installation. If you assign Administrator capability to such a user ID, a “Command failed” error message is displayed on the console.

set authmode

This command is used to set the authentication mode.

Command syntax

set authmode <non_sso>

Options

non_sso - to set authentication to Non-SSO mode.

Requirements

Level privilege: 4

Command privilege level: 4

Allowed during upgrade: No

Example

```
admin:set authmode non_sso
```

set uccx asr count clear

This command clears all the counts that were recorded from the ASR hosts.

Command syntax

set uccx asr count clear

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:set uccx asr count clear
ASR reset successfully

Command successful.
```

set uccx tts count clear

This command clears all the counts that were recorded from the TTS hosts.

Command syntax

set uccx tts count clear

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:set uccx tts count clear
ASR reset successfully

Command successful.
```

set webapp session maxlimit

This command sets the maximum limit for the number of concurrent Unified CCX web application sessions per user.

For the new setting to become effective, you must restart the node. Until you restart the node, the system continues to use the old values. In a HA setup, you must run this command on both the nodes. This command prompts you to restart the node.

Note Restart the nodes during off-peak traffic hours to avoid impact on the system performance.

This setting is preserved during software upgrades on both the nodes.

If the number of sessions is limited to 1 on both nodes, a user is allowed to have one session each on both the nodes.

Command syntax

set webapp session maxlimit *number*

Syntax Description

Parameters	Description
number	Specifies the number to limit the concurrent web application sessions. The value ranges from 1 to 10. Default value is 10. **Note** When you exceed the defined limit for maximum number of signed in sessions, the interface sign-in page displays the Logon Status message as: `The Session limit has already been reached for <username>. Please logout from those sessions or wait <Value> minutes for inactive sessions to be automatically closed.`

Command Modes

Administrator

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Identity Service Management, Disaster Recovery System, Cisco Unified CCX Administration, Cisco Finesse Administration, Cisco Unified Serviceability, Cisco Unified CCX Serviceability, Cisco Unified OS Administration, and Cisco Unified Intelligence Center.

Example

```
admin:set webapp session maxlimit 4

**********************************W A R N I N
G**********************************
The node needs to be restarted for the changes to take effect.This will
disconnect active web sessions and all web applications on this node will be
unavailable
until the node restarts.This node restart will take several minutes to complete.
Do you want to continue (yes/no) ? yes

*************Restarting node***************

The system is going down for reboot in 1 Minute
The webapp session limit has been successfully set to 4.
```

set webapp session timeout

This command sets the time in minutes to invalidate any inactive Unified CCX web application sessions. After the set time elapses, the users are logged off from any of the inactive Unified CCX web sessions. The default session timeout value is 30 minutes.

For the new setting to become effective, you must restart the node. Until you restart the node, the system continues to use the old values. In a HA setup, you must run this command on both the nodes. This command prompts you to restart the node.

Note Restart the nodes during off-peak traffic hours to avoid impact on the system performance.

This setting is preserved during software upgrades on both the nodes.

Command syntax

set webapp session timeout *minutes*

Syntax Description

Parameters	Description
minutes	Specifies the time, in minutes, that must elapse before a web application times out and logs off the user. • Value range: 5-35000 minutes • Default value: 30 minutes

Command Modes

Administrator

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Identity Service Management, Disaster Recovery System, Cisco Unified CCX Administration, Cisco Finesse Administration, Cisco Unified Serviceability, Cisco Unified CCX Serviceability, and Cisco Unified OS Administration.

Example

```
admin:set webapp session timeout 20
Continuing with this operation will set the session-timeout for web sessions to
20 minutes
after the node has been rebooted.
Continue (y/n)?y
web session-timeout updated to 20 minutes.

The node has to be rebooted for the changes to take effect immediately.
This will disconnect active web sessions.
Continue (y/n)?n
The updated web session time-out would take effect on next reboot

The current session-timeout used for web sessions and applications is 30 minutes.
The updated session-timeout value of 20 minutes will take effect on restart of
the node.
```

run Commands

run uccx hrdataexport

This command dumps the historical reporting data and related configuration information to `csv` files, and a `tar` file is created that contains all the exported csv files. The `tar` file is saved in the local file system, under `<activelog>/uccx/log/db/hrdataexport`.

The command output indicates the filename and specific commands that you must run to transfer the generated `tar` file to a remote server and to delete the file from the local disk.

If the Start Date and End Date are specified, then the data between those dates, including the start and end dates, is exported. If only one date parameter is passed, it is considered as start date and all the data from that date onwards is exported.

Note When the command is run, any previous `tar` file that was created is deleted. At any point only one Historical Reporting data export file is saved in the local file system. So after the Historical Reporting data is exported, transfer the `tar` file to remote server before running the command again.

Command Syntax

run uccx hrdataexport all [Start Date] [End Date]

Dumps all the historical reporting data.

run uccx hrdataexport reports *report names* [Start Date] [End Date]

Dumps all the historical reporting data for given reports.

run uccx hrdataexport tables *table names* [Start Date] [End Date]

Dumps all the historical reporting data for given table names.

Parameters

report names—(Mandatory) Comma separated names of the specific reports for which the corresponding data has to be exported. Enclose the list of report names in " " (double quotes).

table names—(Mandatory) Comma separated names of the specific tables from which the data is exported. Enclose the list of table names in " " (double quotes).

[Start Date]—(Optional) Must be in the format "yyyy-MM-dd HH:mm:ss", including the double quotes.

[End Date]—(Optional) Must be in the format "yyyy-MM-dd HH:mm:ss", including the double quotes.

Examples

```
admin:run uccx hrdataexport all "2012-01-01 00:00:00" "2012-02-01 00:00:00"
```

```
admin:run uccx hrdataexport reports "abandoned call detail activity report,aborted
 rejected call detail report"
"2012-01-01 00:00:00" "2012-02-01 00:00:00"
```

```
admin:run uccx hrdataexport tables
"agentconnectiondetail,agentstatedetail,contactcalldetail"
"2012-01-01 00:00:00" "2012-02-01 00:00:00"
```

run uccx sql database_name sql_query

Runs an SQL "select" statement from the CLI. Read-only operations are permitted. Insert, Update, Delete and any DML statements are disallowed. This command allows queries to be run against the Unified CCX databases (data stores) and sysmaster database for the Unified CCX Informix instance (IDS engine).

Command syntax

run uccx sql database_name sql_query [options]

Arguments

database_name—(Mandatory) Database on which the SQL statement is run

sql_query—(Mandatory) The sql statement to run

Options

page—Displays the output one page at a time

file—Stores the output to a file instead of showing it on the console. The name of the file is displayed after the completion of the command.

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: No

Example

```
admin:run uccx sql db_cra select resourceid,resourcename from resource
RESOURCEID      RESOURCENAME
```

```
----------------------
1        b
2        agent22
3        sacagent3
4        sacagent1
7        user
8        sacagent2
9       user agent2
10      user rtlite1
11       agent130
14       sk1
15       sk2
24      User RT Pro
```

run uccx sp database_name sp_name

Runs a stored procedure that is specified as a parameter on the database, which is also mentioned as a parameter. This command runs only a stored procedure.

Command Syntax

run uccx sp database_name sp_name [options]

Arguments

database_name—(Mandatory) Database on which the stored procedure is run

sp_name—(Mandatory) The stored procedure to be run

Options

page—Displays the output one page at a time

file—Stores the output to a file instead of showing it on the console. The name of the file is displayed after the completion of the command.

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: No

Example

```
admin:run uccx sp db_cra sp_email_contact_detail('2016-12-06 18:30:00','2016-12-07
 18:29:59','testemailcsq1','FinesseAgent1','')
CONTACT_ID      SEQUENCE_NUMBER CSQ_NAME        AGENT_NAME      RECEIVED
RETRIEVED       REPLIED DISCARDED       FROM_ADDRESS    REPLY_TO_ADDRESS
TO_ADDRESS      SUBJECT CONTACT_TYPE CONTACT_DISPOSITION     EMAIL_REPLY_TO
EMAIL_REPLY_CC  EMAIL_REPLY_BCC
------------------------------------------------------------------------------------------------------------


 D82AC14C1000015800000EFF0A4E5D8A        0       testemailcsq1   FinesseAgent1
 2016-12-07 07:22:49.0   2016-12-07 07:59:45.051 2016-12-07 08:00:47.06  null
 reboottest2@sky13.sm   "RebootTestUser2 Reboot." <reboottest2@sky13.sm>
reboottest1@sky13.sm   test    1       2
reboottest2@sky13.sm,reboottest1@sky13.sm

 Command successful.
```

Utils Commands

utils remote_account

This command allows you to enable, disable, create, and check the status of a remote account.

Command Syntax

- utils remote_account status
- utils remote_account enable
- utils remote_account disable
- utils remote_account create username life

Arguments

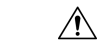
- **username**—Specifies the name of the remote account. The username can contain only lowercase characters and must be more than six characters long.
- **life**—Specifies the life of the account in days. After the specified number of days, the account expires.

Usage Guidelines

A remote account generates a pass phrase that allows Cisco support personnel to access the system for the specified life of the account. You can have only one remote account that is enabled at a time.

Example

```
admin:utils remote_account status
Remote Support
Status         : disabled
Decode Version : 2
```



Caution Avoid creating remote account usernames starting with "uccx" or "UCCX" because such usernames may conflict with system account names that are used internally within the Cisco Unified Contact Center Express server.

utils reset_application_ui_administrator_name

This command resets the application user interface administrator name for Serviceability, CUIC Admin property, and CUIC Administrator.

Command syntax

utils reset_application_ui_administrator_name

Command Modes

Administrator (admin)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Note Restart the service (Cisco Unified Intelligence Center Reporting Service) on all nodes in the cluster to enable the new administrator to log in to Unified Intelligence Center.

```
admin:utils reset_application_ui_administrator_name

-------------------- utils reset_ui_administrator_name --------------------


Reset user interface administrator user name

New administrator user name:

User_1
Serviceability Administrator user name has been successfully updated to User_1

CUIC Admin property has been successfully updated to User_1

CUIC Administrator user name has been successfully updated to User_1
```

utils reset_application_ui_administrator_password

This command resets the application user interface administrator password.

Command syntax

utils reset_application_ui_administrator_password

Command Modes

Administrator (admin)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:utils reset_application_ui_administrator_password
New password:********
Confirm new Password:********
```

utils service

This command allows start, stop, activate, deactivate, list, auto-restart and restart of the following services:

- System SSH
- Service Manager

- Entropy Monitoring Daemon
- Cisco SCSI Watchdog
- A Cisco DB
- A Cisco DB Replicator
- Cisco AMC Service
- Cisco Audit Event Service
- Cisco CDP
- Cisco CDP Agent
- Cisco CallManager Serviceability
- Cisco Certificate Change Notification
- Cisco Certificate Expiry Monitor
- Cisco Cloud Connect Container Manager
- Cisco Database Layer Monitor
- Cisco DRF Local
- Cisco DRF Master
- Cisco Finesse Tomcat
- Cisco Identity Service
- Cisco Log Partition Monitoring Tool
- Cisco RIS Data Collector
- Cisco RTMT Reporter Servlet
- Cisco Syslog Agent
- Cisco Tomcat
- Cisco Tomcat Stats Servlet
- Cisco Trace Collection Service
- Cisco Trace Collection Servlet
- Cisco Unified Serviceability RTMT
- Cisco Finesse Tomcat
- Cisco Unified CCX Administration
- Cisco Unified CCX CVD Dependent Webapp
- Cisco Unified CCX Cluster View Daemon
- Cisco Unified CCX Configuration API
- Cisco Unified CCX DB Perfmon Counter Service

- Cisco Unified CCX Database
- Cisco Unified CCX Engine
- Cisco Unified CCX Notification Service
- Cisco Unified CCX Perfmon Counter Service
- Cisco Unified CCX SNMP Java Adapter
- Cisco Unified CCX Serviceability
- Cisco Unified CCX Socket.IO Service
- Cisco Unified CCX Voice Subagent
- Cisco Unified CCX WebServices
- Cisco Unified Intelligence Center Reporting Service
- Cisco Unified Intelligence Center Serviceability Service
- Cisco Unified Serviceability RTMT
- Cisco Web Proxy Service
- Docker Engine
- Host Resources Agent
- MIB2 Agent
- Platform Administrative Web Service
- Platform Communication Web Service
- SNMP Master Agent
- SOAP -Log Collection APIs
- SOAP -Performance Monitoring APIs
- SOAP -Real-Time Service APIs
- System Application Agent
- Cisco DirSync
- Cisco Serviceability Reporter

Command syntax

utils service [option] [service-name]

Arguments

option—The option to {start | stop | activate | deactivate | list | auto-restart | restart} a service.

service-name—The name of the service.

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:utils service start Cisco Unified CCX Administration
Service Manager is running
Cisco Unified CCX Administration[STARTING]
Cisco Unified CCX Administration[STARTING]
Cisco Unified CCX Administration[STARTED]
Cisco Unified CCX Administration[STARTED]
```

utils system upgrade

This command allows you to install upgrades and Cisco Option Package (COP) files from both local and remote directories.

Command syntax

utils system upgrade [Options]

Options

initiate—Starts a new upgrade wizard or assumes control of an existing upgrade wizard. The wizard prompts you for the location of the upgrade file for Unified CCX.

status—Displays status of the upgrade

cancel—Stops the upgrade process

Example

```
admin:utils system upgrade initiate

Warning: Do not close this window without first canceling the upgrade.

Source:

 1) Remote Filesystem via SFTP
 2) Remote Filesystem via FTP
 3) Local DVD/CD
 q) quit

Please select an option (1 - 3 or "q" ):
```

utils system switch-version

This command restarts and switches the system to the Unified CCX product release that is installed on the inactive partition.

Command syntax

utils system switch-version

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

When the user initiates a switch version, system restart, or system shutdown from the CLI, a warning message is displayed and user confirmation is requested before Unified CCX runs the command. This command is applicable for the following scenarios:

- The system detects that a switch version is in progress.
- The system detects that a previous switch version was abruptly terminated.

Note A switch version operation is abruptly terminated if a power reset or hard reboot is performed on the Unified CCX system when the operation is in progress.

Example

```
admin:utils system switch-version

   ** There is no inactive side available **
```

utils uccx database dbserver integrity

This command checks the integrity of the database server disk structures and displays results. It also checks the DB configuration integrity and performs a fix if integrity is broken. Detailed information is output to a text file. The Informix oncheck utility is used for the command.

Command Syntax

utils uccx database dbserver integrity

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:utils uccx database dbserver integrity
 This operation may take a few minutes to complete. Please wait...

 Output is in file: uccx/cli/DbServerIntegrity_1372844998930.txt

 Command successful.
Starting DB config integrity check
 This operation may take a few minutes to complete. Please wait...

 Output is in file: uccx/cli/DbConfigIntegrity_1372845048816.txt
 Use "file view activelog  uccx/cli/DbConfigIntegrity_1372845048816.txt" command
 to see output
 Command successful.
```

Note The name of the file containing the output from all the checks performed is automatically generated by the command script. For the filename to be unique, the naming format is DbServerIntegrity_<TIMESTAMP>.txt. This format ensures the uniqueness across processes and over time. The file path and filename are displayed after the completion of the operation.

utils uccx list license

This command lists the licenses that are uploaded into the uccx system.

Note This command is not applicable when you are using Smart Licensing.

Command syntax

utils uccx list license

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:utils uccx list license
The following licenses are uploaded in the system:
ccx90_pre_demo.lic
UCCXLicense.lic
ccx100_premium_300seat_allfeatures_dummy.lic
ccx90_enh_demo.lic
ccx_10.5-300_Seat_DummyLicense.lic
 Command successful.
```

utils uccx delete license licenseName

This command deletes a license, permanent or temporary, that is already uploaded into the Unified CCX system.

Caution Use this command with extreme care, because it will delete any license that has been uploaded to the Unified CCX system, without checking whether the license is a temporary or a permanent one. Use this command only to delete wrong or invalid permanent licenses. You can delete temporary licenses by using Unified CCX Administration.

Note For the single-node system, run the delete command first, and then restart the Unified CCX node. For the HA system, run the delete command separately on each of the two nodes, and then restart both the Unified CCX nodes in the cluster.

Command syntax

utils uccx delete license licenseName

Arguments

licenseName is deleted from the Unified CCX system

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:utils uccx delete license ccx10_premium_300seat.lic
Warning:
Deleting the license may have adverse effect on the working of the uccx system.
After deleting the license from all UCCX nodes, restart the UCCX nodes in the
cluster.
Are you sure you want to run this command?
Continue (y/n)?n
Exiting the command.
Command successful.
```

utils uccx jtapi_client update

This command updates the JTAPI Client version on the active partition on the Unified CCX box to match JTAPI version on the Unified Communications Manager. This command downloads the JTAPI Client from the Unified Communications Manager and checks whether the downloaded version needs to be installed. If the downloaded version needs to be installed, it installs the downloaded JTAPI Client and displays a message that the JTAPI Client was updated with the previous and the current versions. If the downloaded version does not need to be installed, it displays a message saying the same and displays the current JTAPI Client version.

The JTAPI client update occurs only on the local node and not the second node in case of an HA deployment.

Note After you run this command, you must reboot the Unified CCX server and restart all the Unified CCX services.

Command syntax

utils uccx jtapi_client update

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:utils uccx jtapi_client update
Node ID: 1 -- Cisco JTAPI Client versions are consistent
 Command successful.
```

utils uccx prepend custom_classpath

This command adds the CustomJarName to the classpath ahead of the system classpath.

Note You must use this command when there are common classes being used in the custom code as well as by Unified CCX and there is a version mismatch between the common classes that are being used.

Caution You must add the custom classpath only if the Custom class files have a newer version than the class files used by Unified CCX. Adding class files that are of older version at the start of the classpath could lead to system instability.

Command syntax

utils uccx prepend custom_classpath ***[CustomJarName]***

Arguments

CustomeJarName—Custom jar filename to be prepended to classpath

Example

```
admin:utils uccx add custom_classpath jsafe.jar
Command successful.
```

utils uccx switch-version db-check

This command allows you to check whether the database was corrupted after an unsuccessful switch version due to a restart in the middle of a switch version attempt. The command displays the status of last switch version. If there is a database backup available that can be restored, it prints the time stamp of the backup and display the CLI command **utils uccx switch-version db-recover** to recover from this backup.

Command Syntax

utils uccx switch-version db-check

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:utils uccx switch-version db-check
ccx DB was found to be corrupted.

Last switch version was aborted at 05/29/2012 16:18:07
05/29/2012 16:18:07|root:Switch Version 9.0.1.10000-41 to 9.0.10000-42 Aborted

There is a CCX backup with timestamp 2012-05-29 16:16:19.000000000 +0530 that was
 taken during a prior switch version.

!!!WARNING!!! IF YOU CHOOSE TO RECOVER FROM THIS BACKUP, ANY CHANGES DONE TO THE
 DATABASE AFTER THE TIMESTAMP OF THIS BACKUP WILL BE LOST.

You can run the CLI command "utils uccx switch-version db-recover" to restore the
 DB from this backup.
```

utils uccx switch-version db-recover

This command first checks whether the database was corrupted after an unsuccessful switch version due to the restart in the middle of a switch version attempt. The command displays the status of the last switch version. If there is a database backup available that can be restored, it prints the time stamp of the backup and offer an option to restore the database from this backup. If the restore option is chosen, the command completes after restoring the database from this backup and bringing up all the services.

Command Syntax

utils uccx switch-version db-recover

Requirements

Level privilege: 1

Command privilege:1

Allowed during upgrade: No

Example

```
admin:utils uccx switch-version db-recover
CCX DB was found to be corrupted.

Last switch verison was aborted at 05/29/2012 16:18:07
05/29/2012 16:18:07|root:Switch Version 9.0.1.10000-42 Aborted

There is a CCX DB backup with timestamp 2012-05-29 16:16:19:000000000 +530 that
was taken during a prior switch version.

!!!WARNING!!! IF YOU CHOOSE TO RECOVER FROM THIS BACKUP, ANY CHANGES DONE TO THE
 DATABASE AFTER THE TIMESTAMP OF THIS BACKUP WILL BE LOST.

Are you sure you want to continue?
Continue (y/n)?y
This operation may take a few minutes to complete. Please wait
```

utils uccx syncusers

This command allows you to synchronize the Unified CCX user passwords with the security password.

Command syntax

utils uccx syncusers

Example

```
admin:utils uccx syncusers
Command successful.
```

utils uccx synctocuic

Synchronizes the users, teams and grants permissions to the reports and stock folders from Unified CCX to Unified Intelligence Center. The following are the configurations that are pushed from Unified CCX to Unified Intelligence Center:

- Users
- Teams
- Stock folders
- Reports
- Value lists

If you make any changes to the above mentioned configurations in Unified Intelligence Center, then such changes are overwritten during the sync.

Note If the sync fails, then running this command or the auto sync that is part of the purge schedule will not revoke the permissions for the previously-synced users or user groups.

Command Syntax

utils uccx synctocuic

Example

```
admin:utils uccx synctocuic
Warning:
Synchronizing all the data to cuic will take some time.
Are you sure you want to run this command?
Continue (y/n)?y
Synchronization of the data from UCCX to CUIC is in progress...
Command successful.
```

utils uccx icd clid status

This command allows you to view the current configuration parameter values for the Caller ID (CLID) feature.

Command syntax

utils uccx icd clid status

Example

```
admin:utils uccx icd clid status
CLID Feature: Disabled
CLID Text Header: Caller Details
CLID Text Prefix: Calling Party Number :
```

utils uccx icd clid enable

This command allows you to enable the CLID feature.

Restart the Unified CCX Engine service for the changes to take effect.

In HA deployments, run this command separately on both the Unified CCX nodes.

After upgrade, run this command again to enable the CLID feature.

Command syntax

utils uccx icd clid enable

Example

```
admin:utils uccx icd clid enable
Successfully enabled the CLID feature
Please restart the "Cisco Unified CCX Engine" service for changes
to take effect
In case of Cisco Unified CCX HA cluster, enable the CLID feature in
remote node as well by running the CLI command
"utils uccx icd clid enable" on the remote node
```

utils uccx icd clid disable

This command allows you to disable the CLID feature.

Restart the Unified CCX Engine service for the changes to take effect.

In HA deployments, run this command separately on both the Unified CCX nodes.

After upgrade, run this command again to disable the CLID feature.

Command syntax

utils uccx icd clid disable

Example

```
admin:utils uccx icd clid disable
Successfully disabled the CLID feature
Please restart the "Cisco Unified CCX Engine" service for changes
to take effect
In case of Cisco Unified CCX HA cluster, disable the CLID feature in
remote node as well by running the CLI command
"utils uccx icd clid disable" on the remote node
```

utils uccx icd clid header

This command allows you to set the display header on the phone screen.

Restart the Unified CCX Engine service for the changes to take effect.

In HA deployments, run this command separately on both the Unified CCX nodes.

After upgrade, run this command again to set the values for the display header.

If the header string has space, enclose the entire string in double quotes.

You can set the header string to "" if you do not want to provide any values.

Command syntax

utils uccx icd clid header <header string>

Example

```
admin:utils uccx icd clid header "Caller Details"
Successfully set the CLID text header to "Caller Details"
Please restart the "Cisco Unified CCX Engine" service for changes
to take effect
In case of Cisco Unified CCX HA cluster, set the CLID text header in
remote node as well by running the CLI command
"utils uccx icd clid header <header string>" on the remote node
```

utils uccx icd clid prefix

This command allows you to set the prefix string for the calling party number displayed on the phone screen.

Restart the Unified CCX Engine service for the changes to take effect.

In HA deployments, run this command separately on both the Unified CCX nodes.

After upgrade, run this command again to set the values for the prefix string.

If the prefix string has space, enclose the entire string in double quotes.

You can set the prefix string to "" if you do not want to provide any values.

Command syntax

utils uccx icd clid prefix <prefix string>

Example

```
admin:utils uccx icd clid prefix "Calling Party Number : "
Successfully set the CLID text prefix to "Caller Party Number: "
Please restart the "Cisco Unified CCX Engine" service for changes
to take effect
In case of Cisco Unified CCX HA cluster, set the CLID text prefix in
remote node as well by running the CLI command
"utils uccx icd clid prefix <prefix string>" on the remote node
```

utils uccx security_filter enable

Run this command to enable Unified CCX administration security filter settings.

In HA deployments, run this command separately on both the Unified CCX nodes.

Command syntax

utils uccx security_filter enable

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:utils uccx security_filter enable
The status of security filter is: enabled
Please restart Unified CCX service using
'utils service restart Cisco Tomcat' for changes to take effect.
In case of Cisco Unified CCX HA cluster, set the security filter in
remote node as well.
```

utils uccx security_filter disable

Run this command to disable Unified CCX administration security filter settings.

In HA deployments, run this command separately on both the Unified CCX nodes.

Command syntax

utils uccx security_filter disable

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:utils uccx security_filter disable
The status of security filter is: disabled
Please restart Unified CCX service using
'utils service restart Cisco Tomcat' for changes to take effect.
In case of Cisco Unified CCX HA cluster, set the security filter in
remote node as well.
```

utils uccx security_filter status

Run this command to check the status of Unified CCX administration security filter flag.

Command syntax

utils uccx security_filter status

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:utils uccx security_filter status
uccx security filter is :enabled
```

utils uccx dbreplication dump configfiles

Run this command to append the data of dbreplication configuration files to a text file. This command is only available in the High Availability deployment of Unified CCX.

Command syntax

utils uccx dbreplication dump configfiles

Requirements

Level privilege: 1

Command privilege level: 0

Allowed during upgrade: No

Example

```
admin:utils uccx dbreplication dump configfiles
Command Started
Output is in file: DbConfigFiles_120813161827.txt
Use "file view activelog uccx/cli/DbConfigFiles_120813161827.txt" command to view
 the file
Use "file get activelog uccx/cli/DbConfigFiles_120813161827.txt" command to get
the file
Command Successful
```

utils uccx database healthcheck

This command runs the database health check script, which checks the health of the Unified CCX database.

After running this command, a health check report is generated. If any issues are found by this script then they are recorded in the health check report. A solution file is also generated that consists of suggested solutions for the problems reported in the health check report file.

Command syntax

utils uccx database healthcheck

Requirements

Level privilege: 1

Command privilege level: 0

Allowed during upgrade: No

Example

```
admin:utils uccx database healthcheck
Command Started
This command may take few minutes to complete
UCCX database health report is available at:
/var/log/active/uccx/cli/healthcheck.rpt
UCCX database health report suggested solutions is available at:
/var/log/active/uccx/cli/healthcheck.soln
Use "file view activelog uccx/cli/healthcheck.rpt" command to view the file
Use "file get activelog uccx/cli/healthcheck.rpt" command to get the file
Use "file view activelog uccx/cli/healthcheck.soln" command to view the file
Use "file get activelog uccx/cli/healthcheck.soln" command to get the file
Command Successful
```

utils uccx database dbperf start

Run this command to monitor the CPU and database utilization on the Unified CCX server.

After successfully running this command, a successful message appears on the screen. This command runs in the background for the total duration specified in the command at periodic intervals and generates a file, which consists of the details related to CPU and database utilization.

Command syntax

utils uccx database dbperf start totalHours interval

Arguments

- **Interval**— Period of time between the running the command / operation.
- **TotalHours**—Total duration to run this command.

Requirements

Level privilege: 1

Command privilege level: 0

Allowed during upgrade: No

Example

```
admin: utils uccx database dbperf start 10 20
The script runs every 20 minutes over a total duration of 10 hours.
Please collect files after 10 hours
Use "file get activelog uccx/cli/dbperf_250913131546.log" to get the file
Use "file view activelog uccx/cli/dbperf_250913131546.log" to view the file
Command Successful
```

utils uccx database dbperf stop

Run this command to stop the current active instance of **utils uccx database dbperf start** before it runs to completion.

Command syntax

utils uccx database dbperf stop

Requirements

Level privilege: 1

Command privilege level: 0

Allowed during upgrade: No

Example

```
admin:utils uccx database dbperf stop
Execution of dbperf has been stopped
Command Successful
```

utils ids sync-security-config

This command is used to synchronize the security configuration files from the primary node to secondary node.

Note This CLI is available only on the secondary node(s) in a cluster.

Command Syntax

utils ids sync-security-config

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: True

Example

```
admin:utils ids sync-security-config
```

utils uccx healthcheck

Run this command to perform checks on the Unified CCX system to ensure that the potential issues are detected at an early stage. When you run this command, you are prompted to enter the category on which health check must be performed. For example, you can select to check the Unified CCX system hardware usage to detect if it is within the threshold limit and return the health check status. A report can be generated with all the plug-in details.

Note If you run **utils uccx healthcheck all**, you are not prompted to select the category. This command will run health check on all the categories.

Command Syntax

utils uccx healthcheck

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: Yes

Available Categories:

- Hardware Usage
- System Parameters
- Database
- Unified CM Configurations

Hardware Usage

This section provides information on the Unified CCX system hardware usage. Plug-ins of this category checks and provides the Unified CCX system CPU usage, memory usage, disk space usage, and disk I/O latency status. If the hardware usage exceeds the threshold limit, then the system will display the appropriate status message.

For example, if the CPU usage in the last ten minutes is within the threshold limit, an OK state is displayed. If the CPU usage in the last ten minutes exceeded the threshold limit, a Not OK state is displayed with the appropriate message.

The following table lists the available plug-ins, their threshold limits and the message displayed when the threshold limit is exceeded.

Plug-in	Threshold Limit	Message Displayed
CPU Usage	System CPU usage exceeds 70 percent.	`The CPU usage has exceeded the threshold limit.`
Memory Usage	System memory usage exceeds 70 percent.	`The memory usage has exceeded the threshold limit.`
Disk Space Usage	System disk space usage exceeds 70 percent.	`The disk usage has exceeded the threshold limit.`
Disk I/O Latency	Time taken to read 1 MB and write 1 MB of data exceeds 500 milliseconds.	`Disk I/O exceeded the permissible limit.`

Example

```
admin:utils uccx healthcheck
Healthcheck is available for the following categories:
1) Hardware Usage
```

```
2) System Parameters
3) Database
4) Unified CM Configurations
q) Quit
Select an option (1 - 4 or "q"):1
       Checking CPU Usage.....................................................OK
       Checking Memory Usage..................................................OK
       Checking Disk Usage....................................................OK
       Checking Disk I/O Latency..............................................Not OK
              Disk I/O exceeded the premissible limit.
Use 'file get activelog healthcheck/report_2019-11-11-09-40-04.json' command to
download the health report.
Command Successful.
```

CCX Configuration

This section provides information on the Unified CCX system parameters usage. If the configured values for the following system parameters exceeds the threshold limit, then the Unified CCX system will display the appropriate status message. For example, if the configured number of agents is within the capacity limits, an OK state is displayed. If the configured number of agents exceeds the capacity limits, a Not OK state is displayed with the appropriate message.

The following plug-ins check the various configuration limits in the Unified CCX system:

- Configured Agents
- Configured Agents per Team
- Configured CSQs
- Configured Skills per Agent
- Configured Outbound Campaigns
- Configured Supervisors per Team
- Configured Teams per Supervisor
- Configured Contacts per Outbound Campaign
- Configured Contact Service Queues
- Configured Skills
- Configured Skills per CSQ

For more information on team configuration limits, see ***Server Capacities and Limits*** section in the Solution Design Guide for Cisco Unified Contact Center Express.

Database

This section provides a list of plug-ins that runs to check the health of database components. The available plug-ins include the following:

- CCX DB Status: This plug-in checks if the Unified CCX database service is running. If the Unified CCX database service is down, an appropriate status message is displayed.

- CCX DB Replication Status: This plug-in checks if all the Unified CCX database replications are running. If the Unified CCX database replications are not in synchronization, an appropriate status message is displayed.
- CCX DB Space Usage: This plug-in checks if all the three Unified CCX database (db_cra, db_cra_repository, and db_hist) usage is within the threshold limit. If any of the database usage exceeds the threshold limit, the system displays the name of that particular database along with the percentage used.
- CCX Config DB tables consistency in HA: This plug-in checks if the Unified CCX configuration tables are in synchronization across the Unified CCX cluster. If any of the configuration tables are not in synchronization, an appropriate status message is displayed.
- Number of Wallboard/External clients: This plug-in checks the number of wallboards and external clients that are connected to the database. If the configured number of wallboards and external clients is within the threshold limit, an OK state is displayed. If the configured number of wallboards and external clients exceeds the threshold limit, a Not OK state is displayed with the appropriate message.

Example

```
admin:utils uccx healthcheck
Healthcheck is available for the following categories:
1) Hardware Usage
2) System Parameters
3) Database
4) Unified CM Configurations
q) Quit
Select an option (1 - 4 or "q"):3
       Checking CCX DB Status.....................................OK
       Checking CCX DB Replication Status.............................OK
       Checking CCX DB Space Usage................................Not OK
       Reason:DB space usage has exceeded the threshold limit of 75% for the
       following:db_hist and db_cra_repository
       Checking CCX Config DB tables consistency in HA..............Not OK
       Reason:DB table(s) out of sync:Skill
              ID in configseed table out of sync:Crsuser
       Checking the number of Wallboard/External Clients.............Not OK
       Reason:Found 3(allowed:1)wallboard/external clients.
Use 'file get activelog healthcheck/report_2019-11-11-09-40-04.json' command to
download the health report.
Command Successful.
```

Unified CM Configurations

This section provides a list of plug-ins that can be run to check the configurations of Unified CM configured in Unified CCX.

The available plug-ins include the following:

- AXL Configuration:

  This plug-in validates the following:

  - If the AXL configurations are available in Unified CCX.
  - If the configured Unified CM is reachable.
  - If the configured Unified CM certificates stored in Unified CCX are correct.

- If the AXL service is running in the configured Unified CM.
- If the configured user in Unified CM has AXL API Access role.
- If the configured AXL user is available in Unified CM, if the credentials are valid, or if the user is locked in Unified CM.

- Telephony Provider (JTAPI) Configuration:

  This plug-in validates the following:

  - If the Telephony Provider configuration is available in Unified CCX.
  - If the configured Unified CM is reachable or if the CTIManager service is running in the configured Unified CM.
  - If the configured Telephony Provider in Unified CCX has Standard CTI Enabled role in Unified CM.
  - If the configured Telephony Provider is available in Unified CM or if the configured Telephony Provider credentials are valid.
  - If the configured Telephony Provider is locked in Unified CM.

- RmCm Provider Configuration:

  This plug-in validates the following:

  - If the RmCm Provider configuration is available in Unified CCX.
  - If the configured Unified CM is reachable or the CTIManager service is running in the configured Unified CM.
  - If the configured RmCm Provider has the following different Access Control roles in the Unified CM:
    - Standard CTI Allow Call Monitoring.
    - Standard CTI Allow Call Recording.
    - Standard CTI Allow Control of Phones supporting Connected Xfer and conf.
    - Standard CTI Enabled.
  - If the configured RmCm Provider is available in Unified CM or if the credentials are valid.
  - If the configured RmCm Provider is locked in Unified CM.

Example

```
admin:utils uccx healthcheck
Healthcheck is available for the following categories:
1) Hardware Usage
2) System Parameters
3) Database
4) Unified CM Configurations
q) Quit
Select an option (1 - 4 or "q"):4
```

```
       Checking AXL Configuration  ......................................OK
       Checking Telephony Provider (JTAPI) Configuration.................OK
       Checking RmCm Provider Configuration..........................Not OK
       Reason:The configured RmCm Provider is not assigned with the following
       roles in Unified CM: Standard CTI Allow Call Recording
       Checking CCX Config DB tables consistency in HA................Not OK
Use 'file get activelog healthcheck/report_2019-11-11-09-40-04.json' command
to download the health report.
Command Successful.
```

utils cloudconnect start

Run this command to start the specified container.

Command Syntax

utils cloudconnect start *container_name*

Arguments

container_name - Name of the container that has to be started.

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: Yes

Example

```
admin:utils cloudconnect start dataconn
Starting the container dataconn ...
Container dataconn is started successfully.
```

utils cloudconnect stop

Run this command to stop the specified container.

Command Syntax

utils cloudconnect stop *container_name*

Arguments

container_name - Name of the container that has to be stopped.

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: Yes

Example

```
admin:utils cloudconnect stop dataconn
Stopping the container dataconn ...
Container dataconn is stopped successfully.
```

utils fips

This command enables, disables, or displays the status of FIPS 140-2 mode. By default, FIPS 140-2 mode is disabled.

utils fips {**enable | disable| status**}

For using FIPS 140-2 mode, consider the following points:

Note FIPS 140-2 mode is supported only on releases that have been through FIPS compliance.

- In a HA setup, FIPS 140-2 mode must be first enabled or disabled on the publisher and then on the subscriber. Before enabling or disabling FIPS 140-2 mode on the subscriber, ensure that all the services are running on the publisher.
- Ensure that SRTP is disabled before enabling or disabling FIPS 140-2 mode in Unified CCX. You can enable SRTP after enabling or disabling FIPS 140-2 mode in Unified CCX.
- When FIPS 140-2 mode is enabled or disabled, the keys and certificates are regenerated, and the Unified CCX server reboots. While rebooting, the system performs the cryptographic modules integrity check, and runs certification self-tests.
- After the FIPS 140-2 mode setting is enabled or disabled, the system reboots automatically. To bring the Live Data datasource online, perform the following:
  - Open the tomcat-trust certificate in Cisco Unified Operating System Administration
  - Restart the Cisco Unified Intelligence Center Reporting Service

Caution Back up the system before and after enabling FIPS 140-2 mode.

If any of the startup self-tests fail, the Unified CCX server halts. Restart the Unified CCX server. If the startup self-test error persists, it indicates that there is a critical problem in the FIPS module and the only option is to use a recovery CD.

utils fips enable

Use this command to enable FIPS 140-2 mode on the system.

Note Before enabling security modes such as FIPS, Common Criteria, and Enhanced Security, the cluster security password must be at least 14 characters. Update the cluster security password by using the `set password user security` command on all nodes and then run this command.

Caution After you enable FIPS 140-2 mode on a server, please wait until the server reboots and the phones re-register successfully before enabling FIPS 140-2 mode on the next server.

Command syntax

utils fips enable

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:utils fips enable

Security Warning: The operation will regenerate certificates for
1)Tomcat
2)IPsec

Any third party CA signed certificates that have been uploaded for the above
components will need to be re-uploaded.
If there are other servers in the cluster, please wait and do not change the
FIPS settings on any other node until the FIPS operation on this node is complete
and the system is back up and running.
******************************************************************************
This will change the system to FIPS mode and will reboot.
******************************************************************************


WARNING: Once you continue, do not press Ctrl+C. Canceling this operation after
it
starts will leave the system in an inconsistent state; rebooting the system and
running "utils fips status" will be required to recover.
******************************************************************************

Do you want to continue (yes/no) ? yes

Generating certificates...

Setting FIPS mode in operating system.
FIPS mode enabled.

FIPS mode enabled successfully.
**************************************************
It is highly recommended that after your system restarts,
a system backup is performed.
**************************************************
The system will reboot in a few minutes.
```

utils fips status

Use this command to know if FIPS 140-2 mode has been enabled on the system. When you run the **utils fips status** command, the system runs the certification self-tests and displays the result.

Command syntax

utils fips status

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
The system is operating in FIPS mode. Self test status:

- S T A R T --------------------
Executing FIPS selftests
runlevel is N3
Start time: Thu Apr 9 08:50:59 IST 2020
NSS self tests passed.
Kernel Crypto tests passed.
Operating System OpenSSL self tests passed.
Libreswan self tests passed.
OpenSSL self tests passed.
CryptoJ self tests passed.
```

utils fips disable

Use this command to disable FIPS 140-2 mode on the system.

Command syntax

utils fips disable

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
Security Warning : The operation will regenerate certificates for
1)Tomcat
2)IPsec

Any third party CA signed certificates that have been uploaded for the above
components will need to be re-uploaded.
If there are other servers in the cluster, please wait and do not change the
FIPS settings on any other node until the FIPS operation on this node is complete
and the system is back up and running.
******************************************************************************
This will change the system to NON FIPS mode and will reboot.
******************************************************************************


WARNING: Once you continue do not press Ctrl+C. Canceling this operation after
it
starts will leave the system in an inconsistent state; rebooting the system and
running "utils fips status" will be required to recover.
******************************************************************************
```

```
Do you want to continue (yes/no) ? yes

Warning: All IPSEC Policies created in FIPS mode will be retained

Generating certificates...

Setting Non FIPS mode in operating system.

FIPS mode disabled successfully.
*******************************************************
It is highly recommended that after your system restarts,
a system backup is performed.
*******************************************************
The system will reboot in a few minutes.
============================
```

Enhanced Security Mode

Enhanced Security Mode runs on a FIPS-enabled system. Unified CCX can be enabled to operate in Enhanced Security Mode, which enables the system with the following security and risk management controls:

- Stricter credential policy is implemented for user passwords and password changes.
- If the protocol for remote audit logging is set to TCP or UDP, the default protocol is changed to TCP. If the protocol for remote audit logging is set to TLS, the default protocol remains TLS. In Common Criteria Mode, strict hostname verification is implemented. So, it is required to configure the server with a fully qualified domain name (FQDN) which matches the certificate.

Credential Policy Updates

When the Enhanced Security Mode is enabled, a stricter credential policy takes effect for new user passwords and password changes. After Enhanced Security Mode is enabled, administrators can use the set password ******* series of CLI commands to modify any of the following requirements:

- The length of the password must be between 14 and 127 characters.
- A password must have at least one lowercase, one uppercase, one numeral, and one special character.
- Any of the previous 24 passwords cannot be reused.
- Minimum age of the password is one day and maximum age of the password is 60 days.
- Character sequence in the newly-generated password must differ by at least four characters from the character sequence in the old password.

File Commands

File commands help in creating custom files that are stored in a specific directory in UCCX Filesystem.

file uccx view

Use this command to view custom files created by Unified CCX scripts.

Command syntax

file uccx view custom_file file-spec

Arguments

file-spec—(Mandatory) The file to view. The file-spec must resolve to a single file. File-spec can contain asterisks (*) as wildcards, providing it resolves to a single file.

Options

None

Requirements

Level privilege: 0

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:file uccx view custom_file test.txt
```

file uccx list custom_file

This command lists custom files that were created by Unified CCX scripts.

Command syntax

file uccx list custom_file file-spec ***[options]***

Arguments

file-spec—(Mandatory) The file to view. File-spec can contain asterisks (*) as wildcards.

Options

page—Pauses output

detail—Shows detailed listing

reverse—Reverses sort order

date—Sorts by date

size—Sorts by size

Requirements

Level privilege: 0

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:file uccx list custom_file * detail
08 Dec,2009 16:56:11 0 text.txt

dir count = 0, file count = 1
```

file uccx list prompt_file

This command lists prompt files created for various locales.

Command syntax

file uccx list prompt_file file_spec ***[options]***

Arguments

file-spec—(Mandatory) The file to view. File-spec can contain asterisks (*) as wildcard.

Options

page—Pauses output

detail—Shows detailed listing

reverse—Reverses sort order

date—Sorts by date

size—Sorts by size

Requirements

Level privilege: 0

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:file uccx list prompt_file system/G711_ULAW/en_US detail
16 May,2012 17:50:19      <dir>    AA
16 May,2012 17:50:19      <dir>    ICD
16 May,2012 17:50:19      <dir>    ICM
16 May,2012 17:50:19      <dir>    SNU
16 May,2012 17:50:19      <dir>    SSA
16 May,2012 17:50:19      <dir>    UserDialog
16 May,2012 17:50:19      <dir>    gen
05 Dec,2002 06:19:03       13,822  continue_enter_number.wav
05 Dec,2002 06:19:03        7,280  credit_of.wav
05 Dec,2002 06:19:04       18,310  did_not_hear_name.wav
05 Dec,2002 06:19:04       11,430  enter_phone_number.wav
05 Dec,2002 06:19:05       12,926  finished.wav
05 Dec,2002 06:19:05        4,448  goodbye.wav
05 Dec,2002 06:19:06        8,546  name_cancelled.wav
05 Dec,2002 06:19:06       47,572  name_confirm.wav
05 Dec,2002 06:19:07       22,990  name_not_found.wav
05 Dec,2002 06:19:08       36,142  no_phone_number.wav
05 Dec,2002 06:19:08        3,902  of.wav
05 Dec,2002 06:19:09        5,492  past.wav
05 Dec,2002 06:19:09        5,110  pound.wav
05 Dec,2002 06:19:10        8,070  spell.wav
05 Dec,2002 06:19:10       11,524  spell_again.wav
05 Dec,2002 06:19:11       12,724  spell_another.wav
05 Dec,2002 06:19:11        5,596  star.wav
05 Dec,2002 06:19:12       45,074  system_problem.wav
05 Dec,2002 06:19:12        5,038  thankyou.wav
05 Dec,2002 06:19:13        8,910  try_again.wav
05 Dec,2002 06:19:14       51,810  unrecov_error_rec.wav
```

```
05 Dec,2002 06:19:14        5,216  welcome.wav
dir count = 7, file count = 22
admin:
```

```
admin:file vvb list prompt_file system/default/vb detail
no such file or directory can be found
admin:file vvb list prompt_file system/G711_ULAW/default/vb detail
09 May,2017 22:07:43       32,110  ringback.wav
dir count = 0, file count = 1
```

file uccx get

This command transfers the custom files created by Unified CCX scripts outside the box.

Command syntax

file uccx get custom_file file-spec ***[options]***

Arguments

file-spec—(Mandatory) File to transfer. File-spec can contain asterisks (*) as wildcards.

Options

reltime—(Mandatory) File to transfer. File-spec can contain asteriks (*) as wildcards.

abstime—(Mandatory) Absolute time to filter.

match—Search pattern to filter.

recurs—Obtains all the files located in file-spec and subdirectories

compress—Transfers files as compressed file

Requirements

Level privilege: 0

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:file uccx get custom_file text.txt abstime 00:00:12/01/08 01:00:12/30/08
```

file uccx tail

This command will tail a custom file that was created by a Unified CCX script.

Command syntax

file uccx tail custom_file file-spec ***[options]***

Arguments

file-spec—(Mandatory) File to tail.

Options

hex,[num lines],regexp "expression"

recent—To tail the most recently changed file in the directory.

Requirements

Level privilege: 0

Command privilege level: 1

Allowed during upgrade: No

Example

Tail file starting with the last ten lines with pagination enabled:

```
admin:file uccx tail custom_file text.txt page 102005-08-03 15:01:41,248 DEBUG
[main] - cmdMVL size = 0
2005-08-03 15:01:41,248 INFO [main] - adding command in level3 (password/security)
2005-08-03 15:01:41,249 DEBUG [main] - begin for level4, topVL size = 0
2005-08-03 15:01:41,250 DEBUG [main] - begin for level4, topVL size = 0
2005-08-03 15:01:41,256 DEBUG [main] - begin for level3, topVL size = 0
2005-08-03 15:01:41,257 DEBUG [main] - begin for level2, topVL size = 0
2005-08-03 15:01:41,884 INFO [main] - merging complete
2005-08-03 15:06:27,619 INFO [main] - got to save history
2005-08-03 15:06:27,620 INFO [main] - Exiting CLI
```

file uccx dump

This command dumps the contents of a file on the Unified CCX custom files area.

Command syntax

file uccx dump custom_file file-spec ***[options]***

Arguments

file-spec—(Mandatory) File to dump.

Options

hex, regexp "expression"

recent—To dump the most recently changed file in the directory

Requirements

Level privilege: 0

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:file uccx dump custom_file text.txt
23640935: Dec 06 22:59:43.407 IST Unable to process call,
Exception=java.lang.NullPointerException
23640936: Dec 06 22:59:43.407 IST java.lang.NullPointerException
```

file uccx delete

This command deletes a custom file that was created by a Unified CCX script. The command deletes one or more files on the Unified CCX custom files area.

Note Files that are in use cannot be deleted.

Command Syntax

file uccx delete custom_file file-spec [options]

Arguments

file-spec—(Mandatory) File to delete. File-spec can contain asterisk (*) as a wildcard.

Options

detail, noconfirm

Requirements

Level privilege: 0

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:file uccx delete custom_file log/*.log det noconfirmdeleting file :
log/cli00001.log
deleting file : log/cli00002.log
deleting file : log/cli00003.log
deleting file : log/cli00004.log
files:       found = 4, deleted = 4
```

High Availability Commands

Note If the Unified CCX database in either of the node is down or is Out of Service, High Availability commands do not work.

show uccx dbreplication tables

This command is only available in the High Availability deployment of Unified CCX. This commands list all the database tables which are involved in replication in the high availability deployment.

Command syntax

show uccx dbreplication tables *[options]*

Options

Page—Displays the output one page at a time

File—Stores the output to a file and displays the filename

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx dbreplication tables
This operation may take a few minutes to complete. Please wait...

CURRENTLY DEFINED REPLICATES
--------------------------------
REPLICATE:        template_db_cra_pshree_dactyl_sub_uccx_1_2_agentstatedetail
STATE:            Active ON:g_pshree_dactyl_pub_uccx
CONFLICT:         Timestamp
FREQUENCY:        immediate
QUEUE SIZE:       0
PARTICIPANT:      db_cra:informix.agentstatedetail
OPTIONS:          transaction,ris,ats,fullrow
REPLID:           131075 / 0x20003
REPLMODE:         PRIMARY  ON:g_pshree_dactyl_pub_uccx
APPLY-AS:         INFORMIX ON:g_pshree_dactyl_pub_uccx
REPLTYPE:         Master

.............
.............
.............

REPLICATE:        template_fcrassvr_pshree_dactyl_sub_uccx_3_3_fcrascalllogweek
STATE:            Active ON:g_pshree_dactyl_pub_uccx
CONFLICT:         Timestamp
FREQUENCY:        immediate
QUEUE SIZE:       0
PARTICIPANT:      fcrassvr:informix.fcrascalllogweek
OPTIONS:          transaction,ris,ats,fullrow
REPLID:           131104 / 0x20020
REPLMODE:         PRIMARY  ON:g_pshree_dactyl_pub_uccx
APPLY-AS:         INFORMIX ON:g_pshree_dactyl_pub_uccx
REPLTYPE:         Master

 Command successful.
admin:
```

show uccx dbreplication servers

This command is only available in the High Availability deployment of Unified CCX. This commands list all the database servers which are involved in replication in the high availability deployment and whether replication is still connected or if replication is broken.

Command syntax

show uccx dbreplication servers ***[options]***

Options

- **Page**—Displays the output one page at a time
- **File**—Stores the output to a file and displays the filename

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show uccx dbreplication servers
SERVER                ID STATE    STATUS     QUEUE  CONNECTION CHANGED
-------------------------------------------------------------------------
10.76.253.106        110 Active   Connected       0 Apr  7 22:01:19
10.76.253.107        100 Active   Local           0
```

utils uccx modify remote_IPAddress

This command is available only in the High Availability deployment of Unified CCX. This command updates IP address of remote node in the server. Use this command during IP address change of remote node.

Note Use this command only when the IP address of the other node is going to be changed.

After you run this command, reboot the Unified CCX server and restart all the Unified CCX services.

Command syntax

utils uccx modify remote_IPAddress <remote_server_old_ip_address> <remote_server_new_ip_address>

Arguments

remote_server_old_ip_address—Old IP address of the remote server

remote_server_new_ip_address—New IP address of the remote server

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:utils uccx modify remote_IPAddress 10.76.253.82 10.76.253.83
 Old Remote IP Address: 10.76.253.82
 New Remote IP Address: 10.76.253.83

This command should be executed only in case you are changing IP Address of remote
 server.
Are you sure you want to run this command?
Continue (y/n)?y
 Command successful.
```

utils uccx modify remote_hostname

This command is available only in the High Availability deployment of Unified CCX. This command updates hostname of remote node in the server. Use this command during hostname change of remote node.

Note Use this command only when the hostname of the other node is changed.

After you run this command, reboot the Unified CCX server and restart all the Unified CCX services.

Command syntax

utils uccx modify remote_hostname < remote_server_old_hostname> <remote_server_new_hostname>

Arguments

remote_server_new_hostname—New hostname of the remote server

remote_server_old_hostname—Old hostname of the remote server

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:utils uccx modify remote_hostname uccx-node-1 uccx-node-2
 Old Remote Hostname: uccx-node-1
 New Remote Hostname: uccx-node-2

This command should be executed only in case you are changing Host name of remote
 server.
 Are you sure you want to run this command?
Continue (y/n)?y
Command Successful.
```

utils uccx database forcedatasync

This command gets the data from the other node in the cluster, effectively overwriting the data on this node.

Command syntax

utils uccx database forcedatasync

Arguments

None

Options

None

Requirements

Level privilege: 1

Command privilege level: 0

Allowed during upgrade: No

Example

```
admin: utils uccx database forcedatasync
Are you sure you want to overwrite the local database? (y/n).
 Command successful.
```

utils uccx setuppubrestore

This command sets up a passwordless communication between Unified CCX cluster nodes. Passwordless communication is required to perform the restore operation. Run this command only on the subscriber node. Use this command while running restore using the "Publisher Only" option.

Note This command is available only in high availability mode.

Command syntax

utils uccx setuppubrestore

Example

```
admin:utils uccx setuppubrestore
```

utils uccx dbreplication setup

This command is available only in the High Availability deployment of Unified CCX. This command is used to set up database replication. The command can be run on any node and it sets up database replication in the cluster.

Command syntax

utils uccx dbreplication setup

Options

Page—Displays the output one page at a time

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:utils uccx dbreplication setup
The DB replication for the UCCX cluster has been setup.
```

utils uccx dbreplication status

This command is available only in the High Availability deployment of Unified CCX. This command is used to check the Unified CCX database replication status.

Command syntax

utils uccx dbreplication status

Options

None

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
utils uccx dbreplication status
SERVER                 ID STATE    STATUS     QUEUE  CONNECTION CHANGED
------------------------------------------------------------------------
g_alpha_ha_n1_uccx      1 Active   Connected       0 Aug  8 18:45:26
g_alpha_ha_n2_uccx      2 Active   Local           0


------------------------------------------------------------------
REPLICATE                                                 STATE
------------------------------------------------------------------
db_cra:informix.agentconnectiondetail                     Active
db_cra:informix.contactcalldetail                         Active
db_cra:informix.contactroutingdetail                      Active
db_cra:informix.eememailstatusdescription                 Active
db_cra:informix.eemreasoncodedescription                  Active
db_cra:informix.eemcontactemaildetail                     Active
db_cra:informix.eememailagentstatedetail                  Active
db_cra_repository:informix.promptsfoldertbl               Active
db_cra_repository:informix.promptsfiletbl                 Active
db_cra_repository:informix.grammarsfiletbl                Active
db_cra_repository:informix.documentsfiletbl               Active
db_cra_repository:informix.sysgrammarsfiletbl             Active
db_cra_repository:informix.latestsynchedtime              Active
fcrassvr:informix.fcrascalllogweek                        Inactive
fcrassvr:informix.fcrasrecordlog                          Inactive
fcrassvr:informix.latestsynchedtime                       Inactive
db_cra:informix.agentstatedetail                          Active
db_cra_repository:informix.scriptsfiletbl                 Active
fcrassvr:informix.fcrascalllogtoday                       Inactive
db_cra:informix.monitoredresourcedetail                   Active
db_cra:informix.latestsynchedtime                         Active
db_cra:informix.eemactiveemail                            Active
db_cra_repository:informix.grammarsfoldertbl              Active
db_cra_repository:informix.documentsfoldertbl             Active
db_cra_repository:informix.scriptsfoldertbl               Active
fcrassvr:informix.fcrasstatelogtoday                      Inactive
db_cra:informix.contactqueuedetail                        Active
db_cra:informix.remotemonitoringdetail                    Active
db_cra:informix.eemstatedescription                       Active
db_cra:informix.eemqueueagentdetail                       Active
```

```
db_cra_repository:informix.sysgrammarsfoldertbl         Active
------------------------------------------------------------------------
```

utils uccx dbreplication templatestatus

This command is available only in the High Availability deployment of Unified CCX. This command is used to see the template status of the database replication.

Command syntax

utils uccx dbreplication templatestatus

Options

Page—Displays the output one page at a time

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:utils uccx dbreplication templatestatus
The DB replication templatestatus is as follows.
```

utils uccx dbreplication repair

This command is available only in the High Availability deployment of Unified CCX. You can run this command on any node. This command repairs mismatched data between cluster nodes; it does not repair replication setup. The command initiates the repair, which runs in the background. To monitor the status of the repair process, the user must go to the data store control center in Serviceability Administration. For more information, see the *Cisco Unified Serviceability Administration Guide* available at: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Command syntax:

utils uccx dbreplication repair [database_name]|all

Arguments

[database_name]|all—(Mandatory) Database_name, which database to repair replication on. (Argument) all—Fix replication on all nodes.

Options

Page—Displays the output one page at a time

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:utils uccx dbreplication repair all
Repair has been initiated in the background...
Please go to Data Control Center in Serviceability Admin to monitor the status
of the repair.
```

utils uccx dbreplication start

This command is available only in the High Availability deployment of Unified CCX. This command is used to start the database replication. Run this command on any node to start database replication in the entire cluster.

Command syntax

utils uccx dbreplication start

Options

Page—Displays the output one page at a time

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:utils uccx dbreplication start
The DB replication for the UCCX cluster has been started.
```

utils uccx dbreplication stop

This command is available only in the High Availability deployment of Unified CCX. This command is used to stop database replication. Run this command on any node to stop database replication in the entire cluster.

Command syntax

utils uccx dbreplication stop

Options

Page—Displays the output one page at a time

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:utils uccx dbreplication stop
The DB replication for the UCCX cluster has been stopped.
```

utils uccx dbreplication reset

This command is available only in the High Availability deployment of Unified CCX. This command is used to reset the database replication. Resetting replication involves the following activites, in the same order, and is equivalent to the commands presented in parentheses.

- Remove database replication (utils uccx dbreplication teardown)
- Setup database replication (utils uccx dbreplication setup)
- Initiate a data repair process for all the databases (utils uccx dbreplication repair all)

Command syntax

utils uccx dbreplication reset

Options

Page—Displays the output one page at a time

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:utils uccx dbreplication reset
The DB replication for the UCCX cluster has been reset.
```

utils uccx dbreplication teardown

This command is available only in the High Availability deployment of Unified CCX. This command is used to remove the database replication. Running this command on any node with the cluster removes database replication between all nodes.

Command syntax

utils uccx dbreplication teardown

Options

page—Displays the output one page at a time

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:utils uccx dbreplication teardown
The DB replication for the UCCX cluster has been teardown.
```

Cisco Finesse Commands

utils reset_3rdpartygadget_password

Run this command to set or reset the password of the 3rdpartygadget account (where password is the new password for the account).

Use the 3rdpartygadget account to upload third-party gadgets to the Cisco Unified CCX Server so that you can use the gadgets from Cisco Finesse. Before you use this account, you must set the password.

Note The password length must be between 5 and 32 characters long and must not contain spaces or double quotes.

Command syntax

utils reset_3rdpartygadget_password

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

```
admin: utils reset_3rdpartygadget_password
New Password:
Confirm New Password:

Updating password for 3rdpartygadget...

Password updated successfully.
admin
```

Note Password values entered by the user is not echoed on the console.

Finesse Log Configuration

Use the following CLI commands to add, delete, update, or view the logger configuration in the system for Finesse.

utils finesse log configuration add

Creates a custom log configuration in the Finesse system. The logs record information about the encountered issues of different severity levels for a specific Finesse module.

Command Syntax

utils finesse log configuration add *[module] [name] [level]*

Options

Note

- Adding multiple module names, log configuration names, and log configuration level values are not supported.
- Log configuration with name ROOT is not allowed.

- *module*—Unique name of Finesse module for which log configuration has to be added. The module name is case sensitive. The following are the valid Finesse modules.
  - *admin*—Finesse administration module.
  - *audit*—Finesse audit module for all administration (including Finesse admin UI and REST client) and supervisor operations.
  - *desktop*—Finesse desktop module.
  - *diagnostics*—Finesse diagnostics module.
  - *FIPPA*—Finesse IP Phone Agent (IPPA) application module.
  - *realm*—Finesse realm module.
  - *shindig*—Shindig web application module.
  - *valve*—Finesse valve module.
  - *webservices*—Finesse webservices module.
- *name*—Package name or fully qualified class name of the Finesse application. The name is case sensitive.
- *level*—Defines the different severity level associated with the log configuration. The following are the valid log configuration levels.
  - *OFF*—Turns off the severity level.
  - *ERROR*—Sets the severity level to error.
  - *WARN*—Sets the severity level to warning.
  - *INFO*—Sets the severity level to information.
  - *DEBUG*—Sets the severity level to debug.
  - *TRACE*—Sets the severity level to trace.
  - *ALL*—Sets the severity level to all.

Note Setting the log configuration level to DEBUG or TRACE impacts system performance. This must be done in consultation with Cisco support to ensure that the modules with high log output are not be enabled with TRACE levels in production severs.

Example

The following is the sample output for creating the log configuration named *com.cisco.cc.common.subsystem* under the Finesse *webservices* module with log configuration level as *DEBUG*.

```
admin:utils finesse log configuration add webservices com.cisco.cc.common.subsystem DEBUG

Warning: Creating the custom log configurations may affect the performance of the Finesse
system.

Press ENTER to continue. Press any other key to exit :

Creating the log configuration, please wait...

Successfully added the log configuration. Changes might take approximately 30 seconds to
take effect..
```

utils finesse log configuration update

Updates an existing custom log configuration in the Finesse system.

Note
- Updating multiple module names, log configuration names, and log configuration level values are not supported.
- Audit log configuration cannot be updated.

Command Syntax

utils finesse log configuration update *[module] [name] [level]*

Options

- *module*—Unique name of Finesse module for which log configuration has to be updated. The module name is case sensitive. For more information on the Finesse modules, see utils finesse log configuration add.
- *name*—Package name or fully qualified class name of the Finesse application. The name is case sensitive.
- *level*—Defines the different severity level associated with the log configuration. For more information on the severity levels, see utils finesse log configuration add.

Note Setting the log configuration level to DEBUG or TRACE impacts system performance.

Example

The following is the sample output for updating the log configuration named *com.cisco.cc.common.subsystem* under the Finesse *webservices* module with log configuration level as *TRACE*.

```
admin:utils finesse log configuration update webservices com.cisco.cc.common.subsystem TRACE

Warning: Updating the log configuration level to DEBUG or TRACE may affect the performance
 of the Finesse system.

Press ENTER to continue. Press any other key to exit :

Updating the log configuration, please wait...

Successfully updated the log configuration. Changes might take approximately 30 seconds to
 take effect.
```

utils finesse log configuration delete

Deletes an existing custom log configuration in the Finesse system.

Note

- ROOT log configurations cannot be deleted.
- Deleting multiple log configuration names are not supported.

Command Syntax

utils finesse log configuration delete *[module] [name]*

Options

- *module*—Unique name of the Finesse module. The module name is case sensitive.
- *name*—Package name or fully qualified class name of the Finesse application. The name is case sensitive.

Example

The following is the sample output for deleting the log configuration named *com.cisco.cc.common.subsystem* under the Finesse *webservices* module.

```
admin:utils finesse log configuration delete webservices com.cisco.cc.common.subsystem
Deleting log configuration, please wait...

Successfully deleted the log configuration. Changes might take approximately 30 seconds to
 take effect.
```

utils finesse log configuration list

Lists all log configurations in the Finesse system.

Command Syntax

utils finesse log configuration list

Example

The following is the sample output for all the log configuration in the Finesse system.

```
admin:utils finesse log configuration list
Requesting log configurations, please wait...
Below is the list of log configurations in Finesse.
+----+-------------+-------------------------------------------------------------------------------+-------+
| No. |     Module     |                                                                    Name
                                    |  Level  |
+----+-------------+-------------------------------------------------------------------------------+-------+
| 1.  | admin          | ROOT
                                    | INFO    |
| 2.  | audit          | ROOT
                                    | INFO    |
| 3.  | desktop        | ROOT
                                    | INFO    |
| 4.  | diagnostics    | ROOT
                                    | INFO    |
| 5.  | FIPPA          | ROOT
                                    | INFO    |
| 6.  | realm          | ROOT
                                    | INFO    |
| 7.  | shindig        | ROOT
                                    | INFO    |
| 8.  | valve          | ROOT
                                    | INFO    |
| 9.  | webservices    | ROOT
                                    | INFO    |
| 10. | FIPPA          | org.jivesoftware
                                    | WARN    |
| 11. | webservices    | org.hibernate
                                    | INFO    |
| 12. | webservices    | com.cisco.cc.common.subsystem
                                    | TRACE   |
+----+-------------+-------------------------------------------------------------------------------+-------+
```

Toaster Notifications

Toaster notifications are enabled by default after a fresh installation of Cisco Finesse. Use the following CLI commands to disable, enable, and check the status of the toaster notifications:

- **utils finesse toaster enable [closeTimeout]**: This command enables the Cisco Finesse toaster notification.

  While enabling toaster notification, use the **closeTimeout** parameter (timeout in seconds) to set the time interval after which toaster automatically closes. If no parameter is specified, timeout is set to 8 seconds by default. The valid range for timeout activity is between 5-15 seconds. The browser must be refreshed for timeout changes to take effect.

Note The configured timeout for browser notifications depends on the operating system and browser settings. The timeout value is honored in Chrome browser in Windows OS. However, the other supported browsers do not honor the configured notification timeout value consistently.

- **utils finesse toaster disable**: This command disables the Cisco Finesse toaster notification.
- **utils finesse toaster status**: This command displays the status (enable or disable) of the Cisco Finesse toaster notification.

Finesse IPPA Inactivity Timeout

Use the following CLI commands to enable or disable the Inactivity Timeout feature in Finesse IPPA. You must either disable the Finesse Inactivity Timeout feature or increase the timeout in the range of 120 seconds to one day (in seconds), so that the Finesse IPPA agent is not logged out if on any other screen:

- **utils finesse ippa_inactivity_timeout enable**: This command enables Finesse IPPA Inactivity Timeout.

Note The default time set for inactivity timeout is 120 seconds.

- **utils finesse ippa_inactivity_timeout disable**: This command disables Finesse IPPA Inactivity Timeout.

Note When inactivity timeout is disabled, you will not be logged out of Finesse IPPA, if the agent is on any other screen.

- **utils finesse ippa_inactivity_timeout enable inactivity_timeout**: This command enables the Finesse IPPA Inactivity Timeout with timeout set to n seconds.

Note Minimum value of n must be 120 seconds and maximum value can be up to one day (86400 seconds).

- **utils finesse ippa_inactivity_timeout status**: This command checks the status of Finesse IPPA Inactivity Timeout.

Note The Finesse IPPA Inactivity Timeout CLIs should be run on primary and secondary Finesse servers. Enabling or disabling this feature requires a restart of Cisco Finesse Tomcat, and restart must be done in the maintenance window. During upgrade, the inactivity timeout configuration is not retained and should be re-configured post upgrade.

To know how this feature works on specific IP phone models, see https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html

Supported Content Security Policy Directives

Note To enable this feature in Cisco Finesse, install Finesse 12.5(1) ES3 COP or higher.

Content Security Policy (CSP) is a standardized set of security directives that can inform the browser of the policies to be used to help mitigate various forms of attacks. CSP frame-ancestor policy defines the allowable locations from where the Finesse desktop can be accessed as an embedded HTML content, which can help prevent click-jacking attacks.

Note From Cisco Finesse Release 12.5(1) ES4 COP onward, all references to **whitelist** in the CLIs are changed to **allowed_list**.

Use the following CLI commands to view, add, or delete the frame-access sources in the response header of Cisco Finesse. This ensures that only the configured sources can embed the Cisco Finesse in an iFrame within their HTML pages.

- **utils finesse frame_access_allowed_list add** *[source1,source2]*—This command adds one or more frame sources, thereby allowing the configured sources to embed the Cisco Finesse in their iFrames. Multiple sources can be provided as a comma-separated list. The source should be of the following format:
  - https://<fqdn>:[port]
  - https://IP:[port]
  - https://<fqdn1>:port, https://<fqdn2>:port

Note
- Wildcard character * is also supported for the FQDN and port entries, which indicates that all the legal FQDN or ports are valid.
- The maximum number of characters (cumulative) that are permissible in allowed list is 2000.

```
admin:utils finesse frame_access_allowed_list add
https://www.abc.com:8445,https://*.abc.com,https://*.abc.com:*,https://10.21.255.25

Source(s) successfully added.
Ensure Source(s) is added to the frame access list in all Finesse nodes in the cluster.

Restart Cisco Finesse Tomcat and Cisco Unified CCX Notification Service for the changes
 to take effect:
utils service restart Cisco Finesse Tomcat
utils service restart Cisco Unified CCX Notification Service
```

- **utils finesse frame_access_allowed_list delete**—This command displays an indexed list of all the configured frame sources that have been allowed to access Cisco Finesse. Enter the corresponding index number to delete a single source or all the configured sources.

```
admin:utils finesse frame_access_allowed_list delete

1: https://www.abc.com:8445
2: https://*.abc.com
3: https://*.abc.com:*
4: https://10.21.255.25
a: all
q: quit

Select the index of source to be deleted [1-4 or a,q]: 1
Sources deleted successfully.

Restart Cisco Finesse Tomcat and Cisco Unified CCX Notification Service for the changes
 to take effect:
 utils service restart Cisco Finesse Tomcat
```

```
utils service restart Cisco Unified CCX Notification Service
```

- **utils finesse frame_access_allowed_list list**—This command lists all the frame sources that are allowed to access Cisco Finesse.

```
admin:utils finesse frame_access_allowed_list list

The following source(s) are configured in the frame access list:
1: https://www.abc.com:8445
2: https://*.abc.com
3: https://*.abc.com:*
4: https://10.21.255.25
```

Finesse System Commands

Configure the following Cisco Finesse system CLIs:

Node Statistics

Use the following CLI command to view the run-time statistics for the current node.

- To view: **utils finesse node_statistics list**

```
admin:utils finesse node_statistics list

Warning: Running this command frequently will affect system performance.
Press ENTER to continue. Press any other key to exit :

Wait while the statistics (updated every 5 secs) are being fetched...

The following are the runtime statistics for the current node.

Active Dialogs Count: 0

Active Tasks Count: 0

Average Configured Media per Agent Count: 0

Average Logged in Media per Agent Count: 0

Average Skill Groups per Agent Count: 0

Max Skill Groups per Agent Count: 0

Total Time for Finesse to Start (in seconds): 32

Logged in Agents on current node: 0

Unique Configured Skill Groups per Agent Count: 0
```

For more information, see *RuntimeConfigInfo API Parameters* section in the *Cisco Finesse Web Services Developer Guide* at https://developer.cisco.com/docs/finesse/.

Desktop Properties

Configure the desktop properties using the following CLIs for the features.

Note Refresh the browser for the changes to take effect.

Active Call Details in the Team Performance Gadget

Use the following CLI commands to enable or disable the active call details:

- To enable: **utils finesse set_property desktop showActiveCallDetails true**
- To disable: **utils finesse set_property desktop showActiveCallDetails false**

View History in the Team Performance Gadget

Use the following CLI commands to enable or disable the agent history:

- To enable: **utils finesse set_property desktop showAgentHistoryGadgets true**
- To disable: **utils finesse set_property desktop showAgentHistoryGadgets false**

Force Wrap-Up Reason

Use the following CLI commands to enable or disable the force wrap-up reason:

Note This is applicable to both voice and non-voice channels.

- To enable: **utils finesse set_property desktop forceWrapUp true**
- To disable: **utils finesse set_property desktop forceWrapUp false**

Show Wrap-Up Timer

Use the following CLI commands to show or hide the timer in wrap-up state:

Note This is applicable to both voice and non-voice channels.

- To hide the timer in wrap-up state: **utils finesse set_property desktop showWrapUpTimer false**
- To display the timer in wrap-up state: **utils finesse set_property desktop showWrapUpTimer true**

By default, the value of this property is set to true.

Wrap-Up Timer Count Down

Use the following CLI commands to set the wrap-up timer to count down or count up the time:

Note This is applicable to both voice and non-voice channels.

- To count up the time: **utils finesse set_property desktop wrapUpCountDown false**
- To count down the time: **utils finesse set_property desktop wrapUpCountDown true**

By default, the value of this property is set to true.

Notification Connection Type

Use the following CLI commands to update the desktop notification connection type as WebSockets or BOSH:

- For WebSockets: **utils finesse set_property desktop notificationConnectionType websocket**
- For BOSH: **utils finesse set_property desktop notificationConnectionType bosh**

By default, the connection type is WebSockets.

Desktop Chat Attachment

Use the following CLI commands to enable or disable the attachment support in Desktop Chat:

- To enable: **utils finesse set_property desktop desktopChatAttachmentEnabled true**
- To disable: **utils finesse set_property desktop desktopChatAttachmentEnabled false**

By default, attachments are enabled in the Desktop Chat.

Desktop Chat Maximum Attachment Size

Use the following CLI commands to configure the attachment size in Desktop Chat:

- **utils finesse set_property desktop desktopChatMaxAttachmentSize** *Attachment Size*

  For example, to set the maximum attachment size to 2 MB, use:

  utils finesse set_property desktop desktopChatMaxAttachmentSize 2097152

Note The maximum attachment size configurable is up to 10 MB.

If you don't configure the maximum attachment size, by default, the maximum attachment size is set to 5 MB.

Desktop Chat Unsupported File Types

The .exe, .msi, .sh, and .bat file types are not supported by default. Use the following CLI commands to override the default list and customize the file types that won't be supported in the Desktop Chat:

- **utils finesse set_property desktop desktopChatUnsupportedFileTypes** *File Types*

  For example, to set the .jar and .bin as unsupported file types, use:

  utils finesse set_property desktop desktopChatUnsupportedFileTypes jar,bin

Multiple file types can be added using a comma-separated string.

Automatic Desktop Login Retries

Cisco Finesse supports automatic desktop login retries when the desktop login fails due to device-related errors. The following properties allow the administrator to control how this feature behaves:

- To enable: **utils finesse set_property desktop enableRetryLoginFeature true**

Attention The **utils finesse set_property desktop enableRetryLoginFeature true** command is not enabling automatic desktop login retries. So, to enable automatic desktop login retries, use the following command:

utils finesse set_property desktop retryLoginAfterLogoutPhoneFailure true

To view the status of automatic desktop login retries, use the following command:

utils finesse show_property desktop retryLoginAfterLogoutPhoneFailure

To disable the automatic desktop login retries, use the following command:

utils finesse set_property desktop enableRetryLoginFeature false

- If this feature is enabled, you can define the retry attempts and intervals.
  - To set the number of retry attempts: **utils finesse set_property desktop loginFailureRetryAttempts <value>**

    The maximum retry attempts are 10. Default value is 3.
  - To set intervals: **utils finesse set_property desktop loginFailureRetryInterval <value>**

    The login retry has a configurable amount of delay between each retry to allow the device to recover. The minimum and maximum interval between retries is 15-180 seconds. Default value is 60 seconds.

Note Reducing the retry interval increases the load on the system when there is a system-wide outage of devices.

By default, the value of this property is set to true.

Enable or Disable Keyboard Shortcuts

Use the following CLI commands to enable or disable the keyboard shortcuts for the Cisco Finesse agent and supervisor desktop:

- To enable: **utils finesse set_property desktop enableShortCutKeys true**
- To disable: **utils finesse set_property desktop enableShortCutKeys false**

By default, the value of this property is set to true.

Enable or Disable Drag-and-Drop and Resize for a Gadget or Component

Use the following CLI commands to enable or disable the drag-and-drop and resize features for a gadget or component in the Cisco Finesse desktop:

- To enable: **utils finesse set_property desktop enableDragDropAndResizeGadget true**
- To disable: **utils finesse set_property desktop enableDragDropAndResizeGadget false**

By default, the value of this property is set to false. For more information on using the drag-and-drop and resize features, see the *Cisco Finesse Agent and Supervisor Desktop User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html.

Configure Desktop Chat Organization Unit (OU) Search

Use the following CLI commands to configure the OU-based user search for the base LDAP context for desktop chat in HCS for CC:

To set field key: **utils finesse set_property desktop desktopChatOUSearchFieldKey** *<value>*

To set field value: **utils finesse set_property desktop desktopChatOUSearchFieldValue** *<value>*

By default, the whole LDAP base context is configured in Cisco Unified Communications Manager IM and Presence Service LDAP search settings. For more details on desktop search see, *Desktop Chat Server Settings*.

The following example displays the search criteria set for chat users who belong to specific OU.

```
admin:utils finesse set_property desktop desktopChatOUSearchFieldKey "OU"

Property successfully updated.
Ensure property is updated in all Finesse nodes in the cluster.

No service restart required. Ensure browser is refreshed for the changes to take effect.

admin:utils finesse set_property desktop desktopChatOUSearchFieldValue "chat"

Property successfully updated.
Ensure property is updated in all Finesse nodes in the cluster.

No service restart required. Ensure browser is refreshed for the changes to take effect.
```

Enable or Disable Preloading of the Secondary Resources

Use the following CLI commands to enable or disable the preloading of the secondary server resources from the alternate side during desktop sign in:

- To enable: **utils finesse set_property desktop preLoadSecondaryResources true**
- To disable: **utils finesse set_property desktop preLoadSecondaryResources false**

The preloaded resources are **images**, **CSS**, **JS**, and **HTML**. The preloading reduces latency and improves performance during desktop failover. By default, the value of this property is set to true.

Security Banner Message for Desktop Users

Cisco Finesse supports custom banner messages in the desktop Sign In page. The administrator defines the banner message for Cisco Finesse desktop users so that they are aware of the security policy while using Cisco Finesse. The banner message can have a maximum of 220 characters. It supports both alphanumeric and special characters. By default, the banner message is not displayed.

- To add the security banner message to the desktop Sign In page: **utils finesse set_property desktop desktopSecurityBannerMessage** *<value>*

  The following example displays the sample security banner that is defined for desktop Sign In page.

  ```
  admin:utils finesse set_property desktop desktopSecurityBannerMessage "IMPORTANT: Finesse
   may only be accessed by authorized users!"

  Property successfully updated.
  Ensure property is updated in all Finesse nodes in the cluster.

  No service restart required. Ensure browser is refreshed for the changes to take effect.
  ```

- To remove the security banner message in the desktop Sign In page: **utils finesse set_property desktop desktopSecurityBannerMessage ""**

Note Cisco Finesse Administration Console and Cisco Finesse desktop now support messages configured in Cisco Unified OS Administration by using the custom logon message feature. From Unified CCX Release 12.5(1)SU1, it's recommended that you use the custom logon message feature as an alternative to the security banner message feature to convey important information to Cisco Finesse desktop users and administrators. For more information about setting up custom logon message, see the *Set Up Customized Logon Message* section in the *Cisco Unified Operating System Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.

Dual-Tone Multi-Frequency (DTMF) Desktop Behavior

The **Wrap-Up** button and the call control buttons, **Hold**, **Transfer**, **Consult**, and **End** are disabled across all calls when DTMF **Keypad** is opened, and until the responses to all DTMF requests are completed or have timed out.

DTMF Pending Requests Threshold Count

When the network or the server is slow to respond, then the response to DTMF requests are delayed. DTMF keypad prevents new operations when more than a configured number of outstanding responses are pending. The default value is 20.

- To configure the DTMF threshold count for pending requests: **utils finesse set_property desktop pendingDTMFThresholdCount** <*value*>

  The following example displays the sample DTMF threshold count.

```
admin:utils finesse set_property desktop pendingDTMFThresholdCount 15

Property successfully updated.
Ensure property is updated in all Finesse nodes in the cluster.

No service restart required. Ensure the desktop browser is refreshed for the changes
to take effect.
```

DTMF Request Timeout

Cisco Finesse waits for a configured time for each DTMF request. The default timeout is 5 seconds.

- To configure the DTMF timeout for pending requests: **utils finesse set_property desktop dtmfRequestTimeoutInMs** <*value*>

Note The timeout value must be entered in milliseconds.

The following example displays the sample DTMF timeout count.

```
admin:utils finesse set_property desktop dtmfRequestTimeoutInMs 4000

Property successfully updated.
Ensure property is updated in all Finesse nodes in the cluster.

No service restart required. Ensure the desktop browser is refreshed for the changes
to take effect.
```

Maintenance Mode

When Cisco Finesse maintenance mode is initiated in Unified CCE deployments using Agent PG 12.5 or lower, the agents' part of the failover experiences a state change of **Ready** or **NotReady** as configured in the property **agentStateAfterMigration**. Use the following CLI commands to control the agent state when migrating to the secondary Cisco Finesse node during maintenance mode. By default, the **agentStateAfterMiigration** value is **Ready**, which can be changed using the following command:

utils finesse set_property desktop agentStateAfterMigration NotReady

If the default state of agents after migration is set as **NotReady**, administrator has to define the **NotReady** reason code. The following command is an example to set **5448** as the **NotReady** reason code, which will be applied while migrating to the alternate side:

utils finesse set_property desktop migrationNotReadyReasonCode 5448

Note These commands are not applicable when Cisco Finesse is connected to CTI versions that are greater than or equal to 12.6.

WebProxy Service

WebProxy Service acts as a transparent reverse proxy between external clients and the Finesse service. It provides SSL termination and caching services to the Finesse server to reduce latency and improve performance.

Configuration changes done on the Finesse server may not be immediately available to the clients due to the intermediary webproxy cache. The administrator can clear the intermediary webproxy cache using **utils webproxy cache clear**.

WebProxy cache is automatically cleared when you restart the Finesse Tomcat service. Static resources (images and scripts), Shindig gadget XML, and resources are cached until the Finesse Tomcat service is restarted or explicitly cleared by the administrator.

For more information on REST API Response Caching, see *REST API Developer Guide* at https://developer.cisco.com/docs/finesse/.

The logging level of the WebProxy Service is managed using the web proxy log-levels CLI.

Note WebProxy Service CLIs are node-specific and must be run on all nodes in the cluster.

Proxy cache bypassing reduces performance and must be used for debugging purposes during the gadget development or troubleshooting.

Server cache for the Finesse API can be bypassed by including `bypassServerCache=true` as a query parameter in the request or clear server cache using **utils webproxy cache clear**.

Server cache for the Finesse desktop can be bypassed by including `bypassServerCache=true&nocache` as a query parameter in the desktop URL.

utils webproxy cache clear

This command clears the cache from the WebProxy Service.

Command Syntax

utils webproxy cache clear {*all* | *webproxy* | *desktop* | *rest* | *shindig* | *notification_service*}

Options

- *all*—Clears all the configured caches.
- *webproxy*—Clears the default webproxy cache.
- *desktop*—Clears the desktop cache. The desktop cache contains static HTML, CSS, scripts, and icons used in the Finesse desktop.
- *rest*—Clears the REST APIs cache. The REST API responses cached are:
  - MediaDomain
  - TeamResource APIs include ReasonCodes, WrapUpReasons, MediaPropertiesLayouts, PhoneBooks, and WorkFlows. The responses of the TeamResource API are cached at the team-level.
- *shindig*—Clears the Shindig cache. The Shindig cache contains XML gadget definition (ifr request-response) and gadget resources (concat request-response).
- *notification_service*—Clears the Notification Service cache. The Notification Service cache contains scripts and HTML used by the Finesse desktop to connect to notification service.
- *authmode*—Clears the UserAuthMode API cache.

Command Modes

Administrator (admin)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CCE, Unified CCX, and Packaged CCE

Example

```
admin:utils webproxy cache clear desktop
Successfully cleared desktop cache
```

set webproxy access-log-level

This command sets the log-level for the access logs generated by the WebProxy Service. The access logs record information about all external requests that reach the proxy. The requests are logged in the access log after the request is processed.

Command Syntax

set webproxy access-log-level {*off* | *info* | *debug*}

Options

- *off*—Turns off the logging into the access logs of the WebProxy Service.
- *info*—Sets the log-level for access logs of the WebProxy Service to information. This captures the data of each request such as time, client, host, user, and so on.

- *debug*—Sets the log-level for access logs of the WebProxy Service to debug. This captures the detailed data of each request for debugging.

Note Setting the access logs to debug impacts performance. Hence, avoid using in the production deployment.

Command Default

The default value is *off*.

Command Modes

Administrator (admin)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CCE, Unified CCX, and Packaged CCE

Example

```
admin:set webproxy access-log-level off
Webproxy access log-level is turned off

admin:set webproxy access-log-level info
Successfully set webproxy access log-level to info
Service restarted
```

set webproxy log-severity

This command sets the severity of the error logs that are generated by the WebProxy Service. The error logs record information about encountered issues of different severity levels.

Command Syntax

set webproxy log-severity {*debug* | *warn* | *error* | *crit* | *alert* | *emerg*}

Options

- *debug*—Sets the severity level to debug.

Note Setting the error logs to debug impacts performance. Hence, avoid using in the production deployment.

- *warn*—Sets the severity level to warning.
- *error*—Sets the severity level to error.
- *crit*—Sets the severity level to critical.
- *alert*—Sets the severity level to alert.
- *emerg*—Sets the severity level to emergency.

Command Default

The default value is *warn*.

Command Modes

Administrator (admin)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CCE, Unified CCX, and Packaged CCE

Example

```
admin:set webproxy log-severity warn
Successfully set webproxy log severity to warn
Service restarted
```

show webproxy access-log-level

This command displays the configured log-level for the access logs of the WebProxy Service.

Command Syntax

show webproxy access-log-level

Command Modes

Administrator (admin)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CCE, Unified CCX, and Packaged CCE

Example

```
admin:show webproxy access-log-level
Current webproxy access log-level is: info
```

show webproxy log-severity

This command displays the configured severity level for the error logs of the WebProxy Service.

show webproxy log-severity

Command Modes

Administrator (admin)

Requirements:

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CCE, Unified CCX, and Packaged CCE

Example

```
admin:show webproxy log-severity
Current webproxy log-severity is: warn
```

Service Properties

Configure the service properties using the following CLIs for the features.

Note The CLIs require Cisco Finesse Tomcat restart except for desktop related properties.

Security Banner Message for Administrators

Cisco Finesse supports custom banner messages in the administration Sign In page. The administrator defines the banner message for the users so that they are aware of the security policy while using Cisco Finesse. The banner message can have a maximum of 220 characters. It supports both alphanumeric and special characters. By default, the banner message is not displayed.

- To add the security banner message to the administrator Sign In page: **utils finesse set_property admin adminSecurityBannerMessage <value>**

The following example displays the sample security banner that is defined for the administrator Sign In page.

```
admin:utils finesse set_property admin adminSecurityBannerMessage "IMPORTANT: Finesse may
only be accessed by authorized users!"

Property successfully updated.
Ensure property is updated in all Finesse nodes in the cluster.

Restart Cisco Finesse Tomcat Service for the changes to take effect:
utils service restart Cisco Finesse Tomcat
```

- To remove the security banner message in the administrator Sign In page: **utils finesse set_property admin adminSecurityBannerMessage ""**

Note Cisco Finesse Administration Console and Finesse desktop now support messages configured in Cisco Unified OS Administration by using the custom logon message feature. From Unified CCX Release 12.5(1)SU1, it is recommended that you use the custom logon message feature as an alternative to the security banner message feature to convey important information to Finesse desktop users and administrators. For more information about setting up a custom logon message, see the *Set Up Customized Logon Message* section in the *Cisco Unified Operating System Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.

Enable or Disable Plain XMPP Socket—Port 5222

Use the following CLI commands to enable or disable the Cisco Unified CCX Notification Service plain XMPP port (5222). This port can be enabled only if you have third-party solutions that connect directly to the Cisco Unified CCX Notification Service over plain Transmission Control Protocol (TCP) connection.

This port is not required for the Finesse desktop or BOSH/WebSocket based integrations. By default, the port is disabled.

- To enable: **utils finesse set_property webservices enableInsecureOpenfirePort true**
- To disable: **utils finesse set_property webservices enableInsecureOpenfirePort false**

Enable or Disable Secure XMPP Socket—Port 5223

Use the following CLI commands to enable or disable the external access to the Cisco Unified CCX Notification Service TCP-based XMPP port (5223). The port must be enabled for external client connectivity only if you have third-party solutions that connect directly to the Cisco Unified CCX Notification Service over this port. By default, the port is enabled (value is set to *true*).

- To enable: **utils finesse set_property webservices enableExternalNotificationPortAccess true**
- To disable: **utils finesse set_property webservices enableExternalNotificationPortAccess false**

Note Restart Cisco Finesse Tomcat and Cisco Finesse Notification Services for the changes to take effect.

Enable or Disable Enforcement of X.509 Certificate Trust Validation

Use the following CLI commands to enable or disable the validation of the X.509 CA or the selfsigned certificate. From Release 12.5(1) onwards, Cisco Finesse validates SSL certificates of all the servers (CUCM and Customer Collaboration Platform) it communicates. This requires the custom CA providers or the selfsigned certificates of the server it communicates to be present in the Cisco Finesse Tomcat trust store. If the certificates are not added into the Cisco Finesse trust store, then certain interactions can fail. It is advised to add the certificates into the Cisco Finesse trust store. If any user chooses to ignore the validation, enforcement can be turned off. This CLI allows users to disable or enable validation. By default, the validation is turned on.

- To enable: **utils finesse set_property webservices trustAllCertificates true**
- To disable: **utils finesse set_property webservices trustAllCertificates false**

Enable or Disable Call Variables Logging

Use the following CLI commands to enable or disable the call variables logging. The callVariables contain sensitive user information and this property allows the administrator to decide whether the information must be captured in the logs. By default the property is disabled.

- To enable:

  utils finesse set_property webservices logCallVariables true

  utils finesse set_property fippa logCallVariables true

- To disable:

  utils finesse set_property webservices logCallVariables false

  utils finesse set_property fippa logCallVariables false

Cross-Origin Resource Sharing (CORS)

In a fresh install of Cisco Finesse, CORS mode is in a permissive state (**enable_all**) by default, which permits CORS preflight requests from browser-based applications from any domain. You can configure the CORS mode to be more restrictive by charging the mode to **enable** and by adding the required browser origins to be allowed using the following CORS CLIs.

Important After you make changes to the CORS status or to the allowed origin list, restart Cisco Finesse Tomcat and Notification Services for the changes to take effect.

- **utils finesse cors enable**: This command allows CORS for Cisco Finesse APIs and OpenFire requests for allowed origin list. It responds to browser CORS preflight requests and allows valid domains to make Finesse API/OpenFire requests.

Note
- Use the **utils finesse cors allowed_origin** CLI to customize the allowed origin list.
- Any custom headers used in the CORS requests must be added using **utils finesse cors allowed_headers** CLI.

- **utils finesse cors enable_all**: This command allows all origins to make cross domain requests. It responds and allows CORS preflight requests from any domain to make Finesse API/OpenFire requests.

Note This isn't a secure configuration and is included only to support backward compatibility.

- **utils finesse cors disable**: This command restricts CORS for Cisco Finesse APIs and OpenFire requests. It disallows or prevents CORS preflight requests from any external domain to make Finesse API and OpenFire requests.

Note If the allowed origin list is already present, the list is preserved and used when CORS is enabled. The CLI changes are reflected only after you clear your cache and close and reopen the browser.

- **utils finesse cors status**: This command displays the CORS status (enable_all, enabled, or disabled) on the console.

For allowing any other header, the following set of CLI commands are added to enable CORS for both Cisco Finesse and OpenFire and to configure the allowed origin list:

- **utils finesse cors allowed_origin list**: This command lists all the origins in the allowed origin list.
- **utils finesse cors allowed_origin add**: This command adds origins to the allowed origin list. Origins can be added by using a comma-separated string. For example:

utils finesse cors allowed_origin add https://origin1.com:[port]

utils finesse cors allowed_origin add https://origin1.com: [port], https://origin2.com:[port]

Note
- The wildcard character star (*) isn't a valid origin in the allowed origin list.
- The maximum number of characters (cumulative) that are permissible in allowed origin is 4000.

- **utils finesse cors allowed_origin delete**: This command deletes origins from the allowed origin list.

Note Delete lists all the origins in the allowed origin list. The origins can be deleted by selecting the appropriate ones from the list. For example:

utils finesse cors allowed_origin delete

1: http://google.com

2: https://www.cisco.com

3: https://def.com

4: https://abc.com:7777

a: all

q: quit

Select the index of origin(s) to be deleted [1-4 or a,q]

By default the following headers are allowed and exposed:

- **allowed_headers**: Content-Type, X-Requested-With, accept, Origin, Authorization, Access-Control-Request-Method, Access-Control-Request-Headers, requestId, Range.
- **exposed_headers**: Access-Control-Allow-Origin, Access-Control-Allow-Credentials, Access-Control-Allow-Methods, Access-Control-Allow-Headers, Access-Control-Max-Age.

Note These headers can't be modified. Custom headers can be added or removed using the following CLIs:

- **utils finesse cors allowed_headers list**: This command lists all the allowed headers for CORS. The list is used to validate incoming requests to Finesse.
- **utils finesse cors allowed_headers add**: This command adds one or more allowed headers for CORS. Multiple headers can be added as a comma-separated string. For example:
  - utils finesse cors allowed_headers add header1
  - utils finesse cors allowed_headers add header1,header2,header3

Note The wildcard character star (*) isn't supported.

- **utils finesse cors allowed_headers delete**: This command lists the choices for deleting the allowed headers. The choice should be an index as displayed in the list of allowed headers. The list provides the option to delete a single header or all configured custom headers. For example:

  utils finesse cors allowed_headers delete

  1: header1

  2: header2

  a: all

  q: quit

  Select the index of the allowed header to be deleted [1-2 or a,q]: 1

- **utils finesse cors exposed_headers list**: This command lists all the exposed headers for CORS. The list will be used by the browser to validate the accessible headers in the response.

- **utils finesse cors exposed_headers add**: This command adds one or more exposed headers for CORS. Multiple headers can be added by a comma-separated string. For example:

  utils finesse cors exposed_headers add header1

  utils finesse cors exposed_headers add header1,header2,header3

Note The wildcard character star (*) isn't supported

- **utils finesse cors exposed_headers delete**: This command lists the choices for deleting the exposed headers. The choice should be an index as displayed in the list of allowed headers. The list provides option to delete a single header or all configured custom headers. For example:

  utils finesse cors exposed_headers delete

  1: header1

  2: header2

  a: all

  q: quit

  Select the index of the exposed header to be deleted [1-2 or a,q]: 1

All CLIs are node specific and must be run on all nodes in the cluster.

Gadget Source Allowed List

Shindig proxies requests from the Finesse desktop to external servers and this introduces the possibility of server side request forgery (SSRF). To prevent SSRF, you can choose to allow outgoing connections for specified sources to be used in the gadgets by adding URLs to the allowed list. Note that this functionality is disabled by default for Cisco Finesse.

Use the following CLIs to enable or disable Gadget Source allowed list functionality and to configure source(s) in the allowed list:

Note From Cisco Finesse Release 12.5(1) ES4 COP onward, all references to **whitelist** in the CLIs are changed to **allowed_list**.

- **utils finesse gadget_source_check enable**: This command enables allowed list for Cisco Finesse.
- **utils finesse gadget_source_check disable**: This command disables allowed list for Cisco Finesse.
- **utils finesse gadget_source_check status**: This command prints the allowed list status (enabled or disabled) on Cisco Finesse console.
- **utils finesse gadget_source_check allowed_list list**: This command lists all the source(s) in the allowed list.
- **utils finesse gadget_source_check allowed_list add**: This command adds source(s) to the allowed list. For example,
  - **utils finesse gadget_source_check allowed_list add** https://www.abc.com:8445.
  - **utils finesse gadget_source_check allowed_list add** https://www.abc.com:8445, http://www.abc.com.

Note Wildcard character * is not supported.

The allowed list feature does not perform hostname resolutions. The format of the allowed list entry should match the format in which the gadget requests for a resource.

If **utils finesse gadget_source_check** is enabled, you must add the CUIC URLs to **utils finesse gadget_source_check allowed_list** for the stock gadgets to load. For example,

- utils finesse gadget_source_check enable
- utils finesse gadget_source_check allowed_list add https://<CUIC_Pub_FQDN>
- utils finesse gadget_source_check allowed_list add https://<CUIC_Pub_FQDN>:8444
- utils finesse gadget_source_check allowed_list add https://<CUIC_Sub_FQDN>
- utils finesse gadget_source_check allowed_list add https://<CUIC_Sub_FQDN>:8444

If you do not add the CUIC URLs, Finesse Desktop fails to load and an appropriate error message is displayed.

- **utils finesse gadget_source_check allowed_list delete**: This command deletes source(s) from the allowed list. For example:
  - **utils finesse gadget_source_check allowed_list delete**
    - 1: http://origin1:8080
    - 2: https://origin2:7777
    - a: all

• q: quit

Select the index of origin to be deleted [1-2 or a,q]: 1

Note All CLIs are node-specific and must be run on all nodes in the cluster.

After any changes are done to gadget source status or to the allowed list, restart Cisco Finesse Tomcat for changes to take effect.

Log Collection Schedule

Use the following CLIs to create, list, and delete automatic desktop log collection schedules for agents and supervisors. This can also be used for debugging purposes.

utils finesse desktop_auto_log_collection create: This command creates a schedule that collects the agent's browser logs. You can create up to five log collection schedules for up to 15 agents.

While creating the log schedule, specify the agent IDs, log collection interval, and duration up to when the logs are to be collected.

The log collection interval and the duration have to be between 30 to 900 seconds. The logs that are collected during the schedule are received in a .zip file format. The logs are collected at: `/opt/cisco/desktop/logs/clientlogs`.

Example:

```
admin:utils finesse desktop_auto_log_collection create

Initializing command line interface...
Checking Cisco Finesse Tomcat status...

Enter agent IDs to continue. (Maximum 15 agents) [Example : 1001001,1001002] : 1001002
Agent IDs entered: 1001002
Enter duration in seconds.(value between 30 and 900) : 240
Duration entered: 240
Enter interval in seconds.(value between 30 and 240) : 60
Interval entered: 60

Successfully scheduled client log collection for the specified agent(s).

Ensure the same is enabled in all the Finesse nodes in the cluster..
```

utils finesse desktop_auto_log_collection list: This command lists all active log collection schedules.

Example:

```
admin:utils finesse desktop_auto_log_collection list

Initializing command line interface...
Checking Cisco Finesse Tomcat status...
These are the live log collection schedules:

Schedule ID:1 Created At: Thu Jun 6 23:23:53 PDT 2019
Duration: 240 seconds
Frequency: 60 seconds
Agent Ids: 1001002
```

utils finesse desktop_auto_log_collection delete: This command deletes the active log collection schedules. When this command is run, all the active log collection schedules are displayed and you are prompted to enter the Schedule ID that you want to delete.

Example:

```
admin:utils finesse desktop_auto_log_collection delete

Initializing command line interface...
Checking Cisco Finesse Tomcat status...
These are the live log collection schedules:

Schedule ID:1 Created At: Thu Jun 6 23:23:53 PDT 2019
Duration: 240 seconds
Frequency: 60 seconds
Agent Ids: 1001002
Enter schedule ID to delete (enter 'all' to delete all): 1
Schedule ID entered: 1

Successfully deleted the log collection with schedule id : 1
```

View Property

Use the following CLIs to view the property values across all property files.

- **utils finesse show_property fippa property_name**: To view the specified Finesse IPPA property's value.
- **utils finesse show_property desktop property_name**: To view the specified desktop property's value.
- **utils finesse show_property webservices property_name**: To view the specified web service property's value.
- **utils finesse show_property admin securityBannerMessage**: To view the specified banner message for the administrator Sign In page.

Note The View property CLIs do not support multiple values.

Update Property

Use the following CLIs to update the property values across all property files.

- **utils finesse set_property desktop property_name property_value**: To update an existing property value used by the Finesse desktop service.
- **utils finesse set_property fippa property_name property_value**: To update an existing property value used by the Finesse IPPA service.
- **utils finesse set_property webservices property_name property_value**: To update an existing property value used by the Finesse web service.
- **utils finesse set_property admin adminSecurityBannerMessage**: To update an existing property value used by the Finesse administrator for the security banner message.

ConnectedUsersInfo

Use the following CLI command to view the list of users connected to the Cisco Finesse server where the CLI is run.

utils finesse show_connected_users summary

Provides the summary information about the connected users in the Cisco Finesse server where the CLI is run.

If the above command is run, it lists the total number of users connected to the Cisco Finesse server where the CLI is run along with the number of users connected through Cisco Finesse Desktop, Finesse IP Phone, and third-party desktops.

Example is as follows:

```
admin: utils finesse show_connected_users summary
Total Connected Users: 2
Desktop Users: 2
FIPPA Users: 0
Third-party Users: 0
Users connected to Finesse via LAN/WAN: 1
Users connected to Finesse via Proxy: 1
To view the complete list of signed-in users, log in to the Cisco Finesse
Administration Console, and navigate to the Connected Agents tab.
```

utils finesse show_connected_users detail

Provides the detailed information about the connected users in the Cisco Finesse server where the CLI is run.

If the above command is executed, it lists the total number of users connected to the current Cisco Finesse server along with the number of users connected through Cisco Finesse Desktop, Finesse IP Phone, and third-party desktops with the agent details.

Example is as follows:

```
admin: utils finesse show_connected_users detail
Total Connected Users: 3
Desktop Users: 2
FIPPA Users: 1
Third-party Users: 0

Desktop Users List [1001002, 1001003]
FIPPA Users List [1001004]
```

Cisco Unified Intelligence Center Commands

show cuic component-status

This command shows the status of the Unified Intelligence Center components. The *Component name* parameter is mandatory.

Command syntax

show cuic component-status *Component name*

Component name

- **CuicStatus**—Shows status of Unified Intelligence Center web engine and the DB replication

- **DBRepStatus**—Shows status of database replication on this node
- **DBStatus**—Shows the database status

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: No

Example

```
admin:show cuic component-status CuicStatus
```

show cuic properties

This command shows information about Cisco Unified Intelligence Center properties.

Command syntax

show cuic properties [options]

Options

- **host-to-ip**—Current host-to-IP translation for the Cisco Unified Intelligence Center databases in the cluster
- **purge-retention**—Number of days data is retained in the Cisco Unified Intelligence Center database before it is purged
- **purge-time**—Time of day and the regular interval in minutes when the Cisco Unified Intelligence Center database is purged
- **session-timeout**—Session timeout for the Cisco Unified Intelligence Center web applications
- **show cuic properties dashboard-customwidget-enabled**—Displays the value *on* or *off* depending on the current value set for the **dashboard-customwidget-enabled property**. This value can be set using the CLI **set cuic properties dashboard-customwidget-enabled**.

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show cuic properties purge-retention
purge_retention
===============
1
```

show cuic tech

Command syntax

This command provides technical details on the Cisco Unified Intelligence Center setup, such as database tables, triggers, procedures and so on.

show cuic tech procedures

This command displays the stored procedures in use for the database.

show cuic tech systables

This command displays the names of all the tables in the Unified Intelligence Center database.

show cuic tech dbschema

This command displays the database schema in a CSV file. This displays output to a `.csv` file.

show cuic tech table table_name

The command shows the contents of a table on the Unified Intelligence Center database. This displays output to a `.out` file.

show cuic tech triggers

This command displays Unified Intelligence Center table names and the triggers associated with those tables.

show cuic tech table cuicreport

This command redirects the contents of the specified database table into a file.

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:show cuic tech dbschema
------------show cuic tech dbschema--------------
Database schema
Output is in /cm/trace/dbi/dbSchema1331705967878.csv
Use "file view activelog/cm/trace/dbi/dbSchema1331705867878.csv" command to see
output
```

```
admin:show cuic tech systables
--------Show cuic tech system tables-----------
SYSTEM TABLES
tabname
===================
GL_COLLATE
GL_CTYPE
VERSION
cdr_deltab_000657
cdr_deltab_000658
cdr_deltab_000659
cdr_deltab_000660
cdr_deltab_000661
cdr_deltab_000662
```

```
cdr_deltab_000663
cdr_deltab_000664
cdr_deltab_000665
cdr_deltab_000666
cdr_deltab_000667
cdr_deltab_000668
cdr_deltab_000669
cdr_deltab_000670
cdr_deltab_000671
cdr_deltab_000672
cdr_deltab_000673
cdr_deltab_000674
```

```
admin:show cuic tech table ?
Syntax:
   show cuic tech table table_name
   table_name mandatory table name
```

```
admin:show cuic tech triggers
-------------show cuic tech triggers---------

Triggers
tablename  trigger
=========================================

cuiccategory          tr_del_category
cuiccategory          tr_ins_category
cuiccategory          tr_upd_category
cuiccollection        tr_del_collection
cuiccollection        tr_ins_collection
cuiccollection        tr_upd_collection
cuicdashboard         tr_del_dashboard
cuicdashboard         tr_ins_dashboard
cuicdashboard         tr_upd_dashboard
cuicdatasource        tr_del_datasource
cuicdatasource        tr_ins_datasource
cuicdatasource        tr_upd_datasource
cuicreport            tr_del_report
cuicreport            tr_ins_report
cuicreport            tr_upd_report
cuicreportdefinition  tr_del_reportdefinition
cuicreportdefinition  tr_ins_reportdefinition
cuicreportdefinition  tr_upd_reportdefinition
cuicuser              tr_upd_userdefaultgroup
cuicvaluelist         tr_del_valuelist
cuicvaluelist         tr_ins_valuelist
```

set cuic properties

Use these commands to set values for the Cisco Unified Intelligence Center database and session timeout.

Command syntax

set cuic properties host-to-ip

Parameter

host—Enter the value for the host DNS name for the server, as displayed on the Data Sources interface

ip_adddress—Enter the IP address of the server for the historical or real-time database

Command Syntax

set cuic properties session-timeout

Parameter

#numberofSeconds—This command sets the session timeout for the Cisco Unified Intelligence Center Reporting web application. The default is 14,400 seconds (4 hours).

Example

```
admin:set cuic properties session-timeout 1900
Value has been successfully set
```

Command Syntax

set cuic properties dashboard-customwidget-enabled

Parameter

on|off—This command sets the dashboard-customwidget-enabled property to *on* or *off*. By setting the value to *on* or *off*, you can enable or disable the Custom Widget feature in Dashboards respectively. By default, the value is set to *off*.

Note Enabling the custom widget configuration can lead to injection vulnerabilities.

Command Syntax

set cuic properties report-query-timeout

Parameter

number of seconds—This command sets the report query running timeout value.

Range: 180-3600 seconds

Example

```
set cuic properties report-query-timeout 250
WARNING : Do not change it to a higher value, as it may cause performance issue.

cuic.query.timeout has been updated
This command requires a restart of Intelligence Center service.
Ensure that this command is run on all nodes in the cluster.
```

Note By default, the report query running timeout value is three minutes (180 seconds).

unset cuic properties

Use this command to unset the translation of host-to-IP hostname.

Command syntax

unset cuic properties host-to-ip [hostname]

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:unset cuic properties host-to-ip ccxbox1
```

set cuic syslog

Command syntax

set cuic syslog [disable|enable]

Options

- **disable**—To disable Cisco Unified Intelligence Center application remote syslogs
- **enable**—To enable Cisco Unified Intelligence Center application remote syslogs

Requirements

Level privilege: 0

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:set cuic syslog enable
```

utils cuic purge

Command Syntax

utils cuic purge

This command runs a manual purge of the cuic database tables. You might do this if you receive an alert that the database is nearing capacity and you do not want to wait for the daily automatic purge.

The tables purged are:

- CuicDataSetInfo
- CuicDataSet
- CuicReportDefinitionFilter
- CuicReportDefinitionFilterField
- CuicReportDefinitionFilterParameter

- CuicCollection
- CuicCollectionValue

This command prompts for the password of the administration user. When the password is confirmed, the purge runs immediately.

Options

None

Requirements

Level privilege—1

Command privilege level—1

Allowed during upgrade—Yes

Example

```
admin:utils cuic purge
Executed Purge Sucessfully
```

utils cuic user make-admin [user-name]

In Single Sign-On (SSO) mode the **Application User** created during installation will not be able to access the Cisco Unified Intelligence Center application with administrator privileges. To enable the Cisco Unified CCX Administrator to have administrator privileges in Cisco Unified Intelligence Center as well, assign reporting capability first and then run this command to make this user the administrator.

After the Unified Intelligence Center user is made an Administrator using this CLI, this user looses Unified Intelligence Center Administrator capabilities after the upgrade.

Thus, this user would not be able to view all the reports that were available to view before the upgrade. The user would have access to reports based on the assigned role (Agent or Supervisor) and not as an Administrator. You must run this CLI after the upgrade such that the user is made the Unified Intelligence Center Administrator.

Note The domain must always be, **UCCX**.

In an HA deployment, the Cisco Unified Intelligence Center Reporting Service must be restarted on both the nodes.

Command Syntax

utils cuic user make-admin [user-name]

Tip: User name should be the complete user name, including the prefix, as listed in Cisco Unified Intelligence Center User List page.

Options

None

Example

```
admin:utils cuic user make-admin UCCX\ABCD

Command executed successfully.
```

utils cuic cluster show

This command shows the current cluster mode enabled on this node and the other member details.

Note The member details are available only in the TCP/IP mode. The member details displayed are of the configured members and does not represent the cluster in real-time.

Command Syntax
utils cuic cluster show

utils cuic cluster mode

This command is used to switch the CUIC cluster join configuration from Multicast to TCP/IP and vice versa.

Note After changing the cluster mode in all the nodes, restart “Cisco Unified Intelligence Center Reporting Service ” in all the nodes starting from the publisher sequentially.

Command Syntax
utils cuic cluster mode

utils cuic cluster refresh

This command refreshes the cluster node information only when run in the TCP/IP mode and must be run when there is an addition or deletion of nodes to the CUIC cluster.

Command Syntax
utils cuic cluster refresh

utils cuic cors

Important After you make changes to the CORS status, allowed origins list, exposed header, or allowed header, restart Cisco Intelligence Center Reporting Service for changes to take effect. All CLIs are node-specific and must be run on all nodes in the cluster.

Command Syntax
utils cuic cors enable

This command enables Cross Origin Resource Sharing (CORS) support in Unified Intelligence Center.

Command Syntax
utils cuic cors disable

This command disables CORS support in Unified Intelligence Center.

Command Syntax
utils cuic cors status

This command displays the current CORS status in Unified Intelligence Center.

Command Syntax
utils cuic cors allowed_origin list

This command displays the list of allowed URLs that can make CORS requests to Unified Intelligence Center.

Command Syntax
utils cuic cors allowed_origin add <URL1,URL2,URL3>

Parameter: Comma-separated list of URLs (without spaces) that has to be added to the allowed origins list.

The URL format: *http[s]://<hostname>[:port]*

This command adds the given set of comma-separated URLs to the allowed origins list.

Command Syntax
utils cuic cors allowed_origin delete

This command prompts for a choice to delete a particular allowed origin URL or all the allowed origin URLs.

utils cuic cors allowed_origin delete

1. http://google.com

2. http://www.cisco.com

a: all

q: quit

Select the index of origin to be deleted [1-2 or a,q]

Command Syntax
utils cuic cors allowed_headers list

This command lists all the configured allowed headers for CORS. This list is used to validate incoming requests to CUIC.

Command Syntax
utils cuic cors allowed_headers add <header1,header2,header3>

Parameter: Comma-separated list of headers (without spaces) that have to be added to the allowed headers list.

This command adds one or multiple allowed headers for CORS. You can add multiple headers using a comma-separated string.

Command Syntax
utils cuic cors allowed_headers delete

This command prompts for a choice to delete a particular custom allowed header or all the custom allowed headers.

utils cuic cors allowed_headers delete

1: header1

2: header2

a: all

q: quit

Select the index of allowed header to be deleted [1-2 or a, q]: 1

Command Syntax
utils cuic cors exposed_headers list

This command lists the response headers available for a client.

Command Syntax
utils cuic cors exposed_headers add <header1,header2,header3>

Parameter: Comma-separated list of headers (without spaces) that have to be added to the exposed headers list.

This command adds one or multiple exposed headers for CORS. You can add multiple headers using a comma-separated string.

Command Syntax
utils cuic cors exposed_headers delete

This command prompts for a choice to delete a particular custom exposed header or all the custom exposed headers.

utils cuic cors exposed_headers delete

1: header1

2: header2

a: all

q: quit

Select the index of exposed header to be deleted [1-2 or a, q]: 1

utils cuic logging

The **utils cuic logging** commands update or display the configuration only on the nodes on which the commands are run. To change the logging configuration on each node in the cluster, you must run the command separately on each node.

utils cuic logging config set

This command sets the value for log file configuration.

Command Syntax
utils cuic logging config set [config-name] [config-value]

Options

- [config-name] - mandatory log file configuration name

  Valid configuration names are `max-file-size`, `max-file-count`, `syslog-primary-host` and `syslog-secondary-host`. The maximum limit of `max-file-size` and `max-file-count` is 50 MB and 50 respectively.

  Only one [config-name] option can be set at a time.

- [config-value] - mandatory log file configuration value. For `syslog-primary-host` and `syslog-secondary-host` configuration names, the configuration values are the primary syslog server hostname and the secondary syslog server hostname, respectively.

utils cuic logging config show

This command prints the current log configuration for the given configuration name.

Command Syntax
utils cuic logging config show [config-name]

Options

[config-name] - mandatory log file configuration name

Valid configuration names are `max-file-size`, `max-file-count`, `syslog-primary-host` and `syslog-secondary-host`.

Only one [config-name] option can be printed at a time.

utils cuic logging config clear

This command clears the log file configuration for the primary and secondary syslog servers.

Command Syntax
utils cuic logging config clear [config-name]

Options

[config-name] - mandatory log file configuration name

Valid configuration names are `syslog-primary-host` and `syslog-secondary-host`.

Only one [config-name] option can be cleared at a time.

utils cuic logging list

This command lists the module and the logging level for the specified module. If a module name is specified, the logging level is displayed only for that module.

Command Syntax
utils cuic logging list [module-name]

Options

[module-name] - optional

Possible module names for which, the log levels can be printed are as follows:

```
REPORT, REPORTENGINE, REPORTDEFINITION, SCHEDULER, DASHBOARD, AUTHORIZATION, AUTHENTICATION,
VALUELISTCOLLECTION, SECURITY, CUICUI, DATASOURCE, CUICCONFIG
```

utils cuic logging reset

This command resets any modifications done to the logging configuration to the default value. For all the modules, the default value is `Info`.

Command Syntax
utils cuic logging reset

Options

No parameters

utils cuic logging update

This command updates the log level for the given module name.

Command Syntax
utils cuic logging update [module-name] [log-level]

Options

- [module-name] - mandatory

  Possible module names are as follows:

  ```
  REPORT, REPORTENGINE, REPORTDEFINITION, SCHEDULER, DASHBOARD, AUTHORIZATION,
  AUTHENTICATION, VALUELISTCOLLECTION, SECURITY, CUICUI, DATASOURCE, CUICCONFIG
  ```

- [log-level] - mandatory

  New log level for the module. Valid log-level values are as follows:

  ```
  ERROR, WARN, INFO, DEBUG
  ```

utils cuic session list

This command lists the current Cisco Unified Intelligence Center sessions.

Command Syntax
utils cuic session list

Options

No parameters

Example

```
admin:utils cuic session list
Command run successfully
Session ID details saved to file.
To view file, type "file view activelog cuic-session.out"
To SFTP file, type "file get activelog cuic-session.out"
```

utils cuic session delete

This command deletes the Cisco Unified Intelligence Center sessions based on the session IDs that you pass to this command.

Command Syntax
utils cuic session delete <sessions ID1,sessions ID2> utils cuic session delete <username 1,username 2>

Parameter

Sessions IDs are IDs of the current Cisco Unified Intelligence Center sessions.

To get the current session IDs, you must first run the `utils cuic session list` command and then run `file view activelog cuic-session.out` command.

Example

```
admin:utils cuic session delete a5fB22f89658e97D089Ab51Ee859b2c1
Session Deleted successfully
```

Specific License Reservation Commands

license smart reservation enable

Use this command to enable the license reservation feature in Smart Licensing. Before running this command, ensure the following:

- Smart Licensing must be enabled.
- Smart Account must be enabled for reservation.
- Smart Licensing must be in unregistered state.

Command syntax

license smart reservation enable

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:license smart reservation enable
License reservation is enabled successfully.
Command successful.
```

Result: Smart Licensing is enabled and you can continue with the license reservation process.

Note With license reservation enabled, **Smart License Management** page, option to **Register**, update **Transport Settings** and other allied operations in Unified CCX Administration are not available for this product instance.

license smart reservation request

Use this command to initiate the license reservation request process. Before running this command, ensure the following:

- Enable command has been run.

Command syntax

license smart reservation request specific

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:license smart reservation request specific
License reservation requested successfully.
Reservation Request Code is: CB-ZUCCX:059d8a992467-AAwxxawE5-73
Use this code in Cisco SSM to obtain the Authorization Code.

Reserve the following License Names in Cisco SSM to use the associated features.

SL NO. LICENSE NAME                          MANDATORY
------ --------------------------------
-----------------------------------------------------
1      CCX Flex Standard Seat 12.5        Yes, if standard agent seats are
required.
2     CCX Flex Premium Seat 12.5        Yes, if premium agent seats are required.
3     CCX Inbound Port 12.5-Flex 12.5    Yes, if Advanced IVR ports are required.
4     CCX Outbound Port 12.5-Flex       Yes, if Outbound IVR ports are required.

Command successful.
```

Result: Reservation Request Code is generated. Use the code in Cisco SSM to generate the Authorization Code.

license smart reservation install

Use this command to install or update the license reservation. Before running this command, ensure the following:

- Request command has been run.
- Authorization Code is obtained from Cisco SSM.

Note If you have already installed an Authorization Code and want to modify the reserved licenses, you must generate a new Authorization Code and run this command again.

Command syntax

license smart reservation install "<*authorization code*>"

The <*authorization code*> has to be obtained from Cisco SSM. Ensure to put the Authorization Code in double quotes.

Note Authorization Code is also available in a file. You cannot provide file name as the parameter. You must copy the entire content of the file and use it as Authorization Code.

After successfully installing the license reservation, restart the system.

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example 1: Install License Reservation for the First Time

```
admin:license smart reservation install
"<specificPLR><authorizationCode><flag>A</flag><version>C</version>
<piid>4e0f17d0-4d83-4a74-8009-6e1a909f505a</piid><timestamp>1583227289333</timestamp>
<entitlements><entitlement><tag>regid.2019-06.com.cisco.CCX_FLEX_PREMIUM,
12.5_0ecc396f-9a80-4b7b-a4c1-35011a2bc68f</tag><count>1</count><startDate>2020-Feb-26
 UTC</startDate>
<endDate>2021-Feb-20 UTC</endDate><licenseType>TERM</licenseType><displayName>
CCX Flex Premium Seat 12.5</displayName><tagDescription>CCX Flex Premium
License</tagDescription>
<subscriptionID></subscriptionID></entitlement></entitlements></authorizationCode>
<signature>MEYCIQDNodtb0VfzvyJfLenhGMCeprSELdAMXaCpsqW8e/mBBAIhAIYXW+80inS9e+
9J1i0MSFzWbuJ93YnQM/yoSTcDwzst</signature><udi>P:UCCX,S:1f2b5461b8ed</udi></specificPLR>"


This operation has to be performed in maintenance window.
Continue (y/n)?y

License reservation is being installed. Please wait ...
License reservation is installed successfully. Reboot the system for the changes
 to take effect.
Command successful.
```

Example 2: Update License Reservation

```
admin:license smart reservation install
"<specificPLR><authorizationCode><flag>A</flag><version>C</version>
```

```
<piid>4e0f17d0-4d83-4a74-8009-6e1a909f505a</piid><timestamp>1583227289333</timestamp>
<entitlements><entitlement><tag>regid.2019-06.com.cisco.CCX_FLEX_PREMIUM,
12.5_0ecc396f-9a80-4b7b-a4c1-35011a2bc68f</tag><count>1</count><startDate>2020-Feb-26
 UTC</startDate>
<endDate>2021-Feb-20 UTC</endDate><licenseType>TERM</licenseType><displayName>
CCX Flex Premium Seat 12.5</displayName><tagDescription>CCX Flex Premium
License</tagDescription>
<subscriptionID></subscriptionID></entitlement></entitlements></authorizationCode>
<signature>MEYCIQDNodtb0VfzvyJfLenhGMCeprSELdAMXaCpsqW8e/mBBAIhAIYXW+80inS9e+
9J1i0MSFzWbuJ93YnQM/yoSTcDwzst</signature><udi>P:UCCX,S:1f2b5461b8ed</udi></specificPLR>"


This operation has to be performed in maintenance window.
Continue (y/n)?y

License reservation is being installed. Please wait ...
License reservation is installed successfully. Reboot the system for the changes
 to take effect.
Confirmation Code is: 125ffe1b
Use this code in Cisco SSM to the complete license reservation update process.
Command successful.
```

Result: Unified CCX gets automatically refreshed with the reserved licenses.

Caution If the installed licenses are incorrect, all the critical services of the contact center will go down. Be cautious while reserving licenses and ensure that the appropriate licenses are reserved.

license smart reservation return

Use this command to return the license reservation if you have already installed the Authorization Code.

Command syntax

license smart reservation return

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:license smart reservation return

This command will return the license reservation and this product instance will
transition back to the unregistered state.
Continue (y/n)?y

License reservation is being returned. Please wait ...
License reservation is returned successfully.
Reservation Return Code is:
Cb3AEN-61XgQW-YGBXWm-FgS16L-LFRQ7n-aHU9Y1-cJDQGL-DtZGhJ-2D3
Use this code in Cisco SSM to complete the reservation return process.
Command successful.
```

Result: Reservation Return Code is generated and the product instance will transition back to the unregistered state. Enter the code in Cisco SSM to return the reserved licenses to the virtual pool. The product instance will enter evaluation or evaluation expired mode.

Note The best practice is to restart the system after returning the reservation.

If the evaluation period has expired, this product instance will enter into enforcement mode. For more information on enforcement mode, see *Cisco Unified Contact Center Express Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-feature-guides-list.html.

license smart reservation return-authorization

Use this command to return the license reservation if you have not yet installed the Authorization Code.

Note This command is primarily for executing before installing the Authorization Code. However, you can also run this command after installing the Authorization Code.

Command syntax

license smart reservation return-authorization "<authorization code>"

The *<authorization code>* that has to be obtained from Cisco SSM. Ensure to put the Authorization Code in double quotes.

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:license smart reservation return-authorization
"<specificPLR><authorizationCode><flag>A</flag><version>C</version>
<piid>4e0f17d0-4d83-4a74-8009-6e1a909f505a</piid><timestamp>1583227289333</timestamp>
<entitlements><entitlement><tag>regid.2019-06.com.cisco.CCX_FLEX_PREMIUM,
12.5_0ecc396f-9a80-4b7b-a4c1-35011a2bc68f</tag><count>1</count><startDate>2020-Feb-26
 UTC</startDate>
<endDate>2021-Feb-20 UTC</endDate><licenseType>TERM</licenseType><displayName>
CCX Flex Premium Seat 12.5</displayName><tagDescription>CCX Flex Premium
License</tagDescription>
<subscriptionID></subscriptionID></entitlement></entitlements></authorizationCode>
<signature>MEYCIQDNodtb0VfzvyJfLenhGMCeprSELdAMXaCpsqW8e/mBBAIhAIYXW+80inS9e+
9J1i0MSFzWbuJ93YnQM/yoSTcDwzst</signature><udi>P:UCCX,S:1f2b5461b8ed</udi></specificPLR>"

License reservation is being returned. Please wait ...
License reservation is returned successfully.
Reservation Return Code is: gfgh677hn
Use this code in Cisco SSM to complete the reservation return process.
Command successful.
```

Result: Reservation Return Code is generated and the product instance will transition back to the unregistered state. Enter the code in Cisco SSM to return the reserved licenses to the virtual pool. The product instance will enter evaluation or evaluation expired mode.

Note The best practice is to restart the system after returning the reservation.

If the evaluation period has expired, this product instance will enter into enforcement mode. For more information on enforcement mode, see *Cisco Unified Contact Center Express Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-feature-guides-list.html.

license smart hostname enable

Use this command to enable the privacy of UCCX during smart license registration with CSSM/On-Prem SSM.

Command syntax

license smart hostname enable

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:license smart hostname enable
Command successful.
```

Result: UCCX privacy is enabled, hostname and IP address of UCCX will not be shared with CSSM/On-Prem SSM. The license serial number of UCCX will be displayed in CSSM/On-Prem SSM portal, instead of UCCX hostname.

license smart hostname disable

Use this command to disable the privacy of UCCX during smart license registration with CSSM/On-Prem SSM.

Command syntax

license smart hostname disable

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
license smart hostname disable
Command successful.
```

Result: UCCX privacy is disabled, hostname and IP address of UCCX will be shared with CSSM/On-Prem SSM. The hostname of the UCCX will be displayed in CSSM/On-Prem SSM portal, instead of UCCX license serial number.

Caution Be aware that when you enable the privacy, you are exposing your internal address or domain details.

After enabling or disabling license smart hostname, utils system restart must be performed.

license smart reservation cancel

Use this command to cancel the license reservation process for Smart Licensing.

Prerequisites:

- Request command has been run.
- Authorization Code has not been installed.

Command syntax

license smart reservation cancel

Requirements

Level privilege: 1

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:license smart reservation cancel
License reservation request is canceled successfully.
Command successful.
```

Result: Reservation Request Code that was generated will be made invalid on the product instance.

Caution After you run the cancel command, do not use the earlier generated Reservation Request Code to generate Authorization Code.

license smart reservation disable

Use this command to disable the license reservation feature in Smart Licensing. Before disabling the license reservation, you must return the reserved licenses to the virtual pool, so that you can use the licenses without reservation.

Note Before running this command, if you have requested or installed license reservation, cancel or return the license reservation respectively.

Command syntax

license smart reservation disable

Requirements

Level privilege: 1

Command privilege level: 1

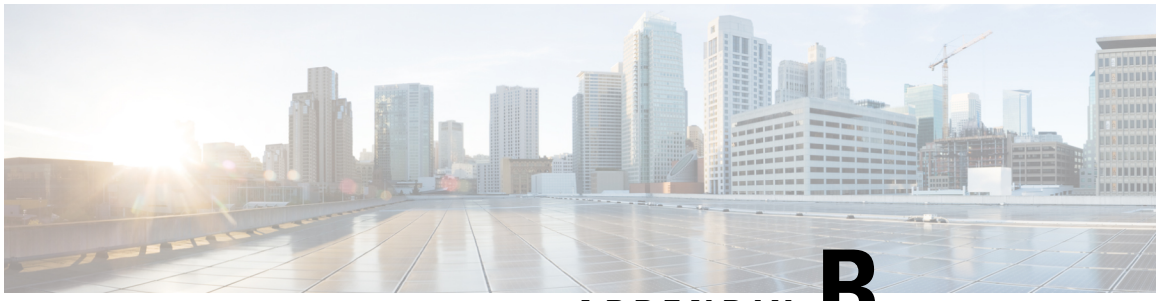
Allowed during upgrade: No

Example

```
admin:license smart reservation disable
License reservation is disabled successfully.
Command successful.
```

Result: License Reservation is disabled.

Note After disabling the license reservation, you have the option to register the product instance by using **Smart Licensing** in Unified CCX Administration.



APPENDIX B

Unified CCX License Packages

- Application Availability by License Package, on page 689
- Trigger Availability by License Package, on page 689
- Subsystem Availability by License Package, on page 689
- Unified CCX Services Availability by License Package, on page 690
- Unified CCX Component Availability by License Package, on page 690

Application Availability by License Package

The following table lists the applications available with each license package:

Application	Unified IP IVR	Unified CCX Enhanced	Unified CCX Premium
Cisco Script Application	X	X	X
Busy	X	X	X
Ring No Answer	X	X	X

Trigger Availability by License Package

The following table lists the triggers available with each license package:

Trigger	Unified IP IVR	Unified CCX Enhanced	Unified CCX Premium
Unified CM Telephony	X	X	X
HTTP	X		X

Subsystem Availability by License Package

The following table lists the subsystems available with each license package:

Subsystem	Unified IP IVR	Unified CCX Enhanced	Unified CCX Premium
CMT Subsystem	X	X	X
Core RTR Subsystem	X	X	X
Database Subsystem	X		X
eMail Subsystem	X		X
HTTP Subsystem	X		X
Unified CM Telephony Subsystem	X	X	X
MRCP ASR Subsystem	X		X
MRCP TTS Subsystem	X		X
Outbound Subsystem[4]			X
RmCm Subsystem	X	X	X
Voice Browser Subsystem	X		X
RouteAndQueue Subsystem			X

[4] The Unified CCX Outbound Preview Dialer feature does not require an additional license and it comes as part of the Premium license package.

Unified CCX Services Availability by License Package

The following table lists the Unified CCX Services available with each license package:

Unified CCX Services	None[5]	Unified IP IVR	Unified CCX Enhanced	Unified CCX Premium
Unified CCX Cluster View Daemon	X	X	X	X
Unified CCX Administration	X	X	X	X
Unified CCX Engine		X	X	X
Cisco Unified CCX Database		X	X	X

[5] Available upon installation, before license package is activated.

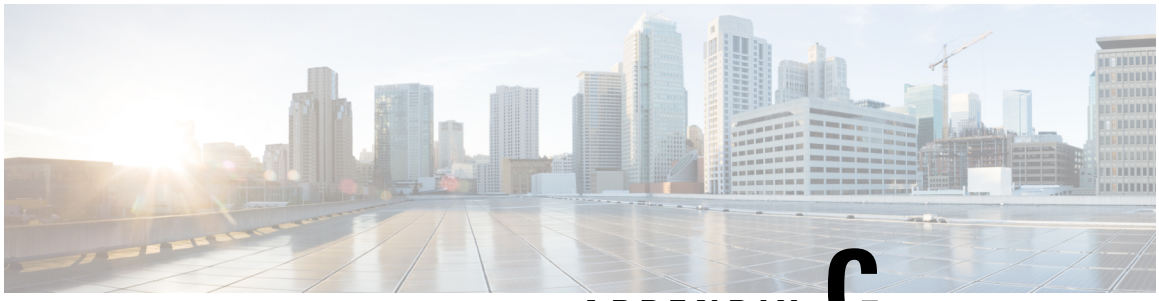
Unified CCX Component Availability by License Package

The following table lists the Unified CCX Component available with each license package:

Unified CCX Component	None[6]	Unified IP IVR	Unified CCX Enhanced	Unified CCX Premium
Unified CCX Cluster View Daemon (CVD)	X	X	X	X
Unified CCX Engine		X	X	X
Unified CCX Repository Datastore		X	X	X
Unified CCX Historical Datastore		X	X	X
Unified CCX Configuration Datastore		X	X	X
Unified CCX Recording			X	X
Unified CCX Monitoring				X

[6] Available upon installation, before license package is activated.

Unified CCX License Packages



APPENDIX C

Bubble Chat Experience

• Bubble Chat Experience, on page 693

Bubble Chat Experience

Bubble chat can be launched on any device and the display adapts to the screen size of the device used. For example, if you launch the bubble chat using a desktop, a small chat pop-over appears on the right-side bottom of the web page. If you use a mobile device, the bubble chat launches in the full-screen mode.

To use Bubble chat, ensure that:

- The browser cookies and third-party cookies are enabled.
- The Tracking Protection option in the browser is disabled.
- The Customer Collaboration Platform server and customer website are in the same domain so that the bubble chat works on various browsers.

Note For more information about cookies and Tracking Protection option, see your browser-specific documentation.

If you use a private certificate, your end customers must accept an untrusted certificate in their browser to initiate a chat. If you do not want your end customers to accept untrusted certificate, you must use CA-signed certificate.

The chat process is as follows:

1. The customer initiates the chat by clicking a text link, button, or icon.

   The chat form attempts to collect the details of the customer, such as, name, email, phone number etc. The form also presents a list of problem statements - from which the customer has to mandatorily select one.

2. The customer provides details in the chat form and submits it.
3. The chat pop-over opens with a welcome message, such as 'Thanks for contacting. We will be with you shortly'. If all the agents are busy, an appropriate message appears.

When the agent joins the chat, the customer is notified by a message, and the pop-over divides into a conversation area (where messages appear) and a typing area (where the customer can type messages for the agent).

4. The customer and agent chat - more than one agent can join the chat to create a group chat. While chatting, the agent's messages are displayed on the left of the conversation area and the customer's messages are displayed on the right. All messages are displayed with the timestamp below the message (in the 24-hour format); the agent's message will additionally have the agent's name before the timestamp.

   The chat pop-over can be minimized or maximized.

   The following indicators appear on the chat pop-over at appropriate times:

   - Agent typing indicator: This indicator, represented by three squiggly dots, appears above the typing area whenever the agent types.
   - New messages indicator: The pop-over blinks in a minimized stated whenever a new event occurs during the chat, such as the receipt of a new message, joining of another agent, connection problems etc.
   - Agent left/joined indicator: The customer is informed when an agent leaves or joins the chat.

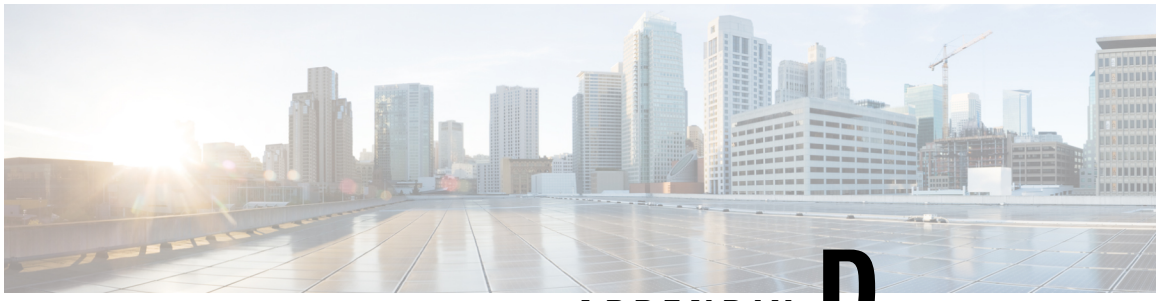
5. When the customer completes the chat and attempts to exit the chat, the following pop-ups are displayed in a sequence:

   a. A chat closure confirmation box.

   b. A chat transcript download box. The customer can choose to download the chat transcript.

   c. A chat rating box, if rating is enabled for the chat. The customer can choose to rate or skip rating by closing this box.

Note Any connectivity or technical problems that are encountered during the chat session are notified as banner messages at the top of the conversation area.



APPENDIX D

Reverse-Proxy Configuration

- Introduction, on page 695
- Prerequisites, on page 695
- Background Information, on page 696
- Reverse-Proxy Configuration, on page 698
- Verifying Reverse-Proxy Configuration, on page 717
- Brute Force Attack Prevention Configuration, on page 718
- Troubleshoot, on page 721

Introduction

This section describes how to configure a reverse-proxy and access the Cisco Finesse desktop without connecting to a VPN based on Unified CCX and Customer Collaboration Platform..

Note

- The content in this chapter is provided as a guidance for customers to install and configure reverse-proxy. Cisco does not support requests for reverse-proxy installation and configuration issues. Queries that are related to this subject can be discussed onCisco community forums.
- For 12.5(1) SU2 deployments of VPN-less Finesse, see the Cisco Finesse 12.6 ES04 Readme.

Note The OpenResty® Nginx configurations provided as part of Release 12.5(1) SU2 need to be manually edited and applied to match your deployment, along with requiring a manual install of the OpenResty® Nginx.

Prerequisites

Cisco recommends that you have knowledge of the following:

- Cisco Unified Contact Center Express Release
- Cisco Finesse

- Linux administration
- Network administration and Linux network administration

Components Used

The information in this document is based on these software and hardware versions:

- Unified CCX - 12.5(1) SU2
- Customer Collaboration Platform - 12.5(1) SU2
- IdS - 12.5(1) SU2

The information in this document was created from the devices in a specific lab environment. All the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

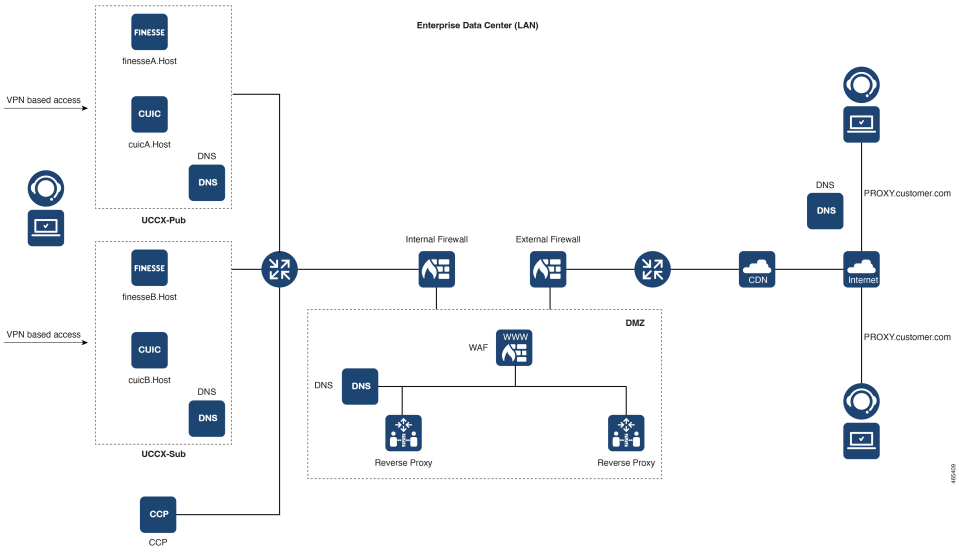
This deployment model is supported for Unified CCX and Customer Collaboration Platform.

Deployment of a reverse-proxy is supported (available from Release 12.5(1) SU2) as an option to access the Cisco Finesse desktop without connecting to a VPN. This feature provides the flexibility for agents to access the Finesse desktop from anywhere through the Internet.

To enable this feature, a reverse-proxy pair must be deployed in the Demilitarized Zone (DMZ).

Media access remains unchanged in reverse-proxy deployments. To connect to the media, agents and supervisors can use Cisco Jabber or Webex over Mobile and Remote Access solution (MRA). This diagram shows how the network deployment will look like when you access two Finesse clusters and two Unified IC nodes through a single high availability (HA) pair of reverse-proxy nodes.

Concurrent access from agents on the Internet and agents who connect from LAN is supported as shown in the following image:



Note See the Reverse-Proxy selection and configurations, on page 502 section to select an appropriate reverse-proxy that supports this deployment. The *Solution Design Guide for Cisco Unified Contact Center Express, Release 12.5(1) SU2* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-implementation-design-guides-list.html provides security configuration guidelines for the reverse-proxy deployment.

Before you read this section, it is recommended to review the following sections:

- VPN-less Access to Finesse Desktop section in this guide
- Security Guidelines for Reverse-Proxy Deployment section in the *Solution Design Guide for Cisco Unified Contact Center Express, Release 12.5(1) SU2*

Validating unauthenticated static resources

All valid endpoints that can be accessed without any authentication are actively tracked in the Release 12.5(1) SU2. If invalid URIs are requested to these unauthenticated paths, they are rejected without sending the requests to the components' servers.

Brute Force Attack Prevention

Unified CCX Release 12.5(1) SU2 authentication scripts actively prevent brute force attacks that can be used to guess the user password. The scripts do this by blocking the IP address used to access the service, after a certain number of failed attempts in a short time. These requests will be rejected by **418 client error**. The number of failed requests, time interval, and blocking duration are configurable.

Caching CORS Headers

When the first options request is successful, the response headers **access-control-allow-headers, access-control-allow-origin, access-control-allow-methods, access-control-expose-headers,** and **access-control-allow-credentials** are cached at the proxy for five minutes. These headers are cached for each respective upstream server.

Reverse-Proxy Configuration

This section describes the configuration of OpenResty Nginx as the reverse-proxy to be used to enable VPN-less access to Finesse. The Unified CCX component, proxy, and OS versions used to verify the instructions are provided. The relevant instructions have to be adapted to the OS or proxy of your choice.

- OpenResty Nginx version used - OpenResty 1.19.9.1
- OS used for configuration - CentOS 7.4.1708

Any of the following Nginx versions can be used for this purpose, as long as they are based on Nginx 1.19+ and support Lua:

- Nginx Plus
- Nginx Open Source (Nginx open source must be compiled along with OpenResty-based Lua modules)
- OpenResty
- GetPageSpeed Extras

Note The OpenResty Nginx configuration described can be downloaded from the Software Download page.

Install OpenResty as a Reverse-Proxy in DMZ

This section details the OpenResty-based proxy installation steps. The reverse-proxy is typically configured as a dedicated device in the network demilitarized zone (DMZ) as shown in the deployment diagram in *Background Information*.

1. Install the OS of your choice with the required hardware specification. Kernel and IPv4 parameter tweaks might differ depending on the OS selected. Users are advised to reverify these aspects if the chosen OS version is different from CentOS 7.
2. Configure two network interfaces. One interface will be required for public access from the Internet clients and another to communicate with the servers in the internal network.
3. Install OpenResty.

Note The configuration provided has been tested with OpenResty 1.19 and is expected to work with other distributions with only minor updates, if any.

Install OpenResty

SUMMARY STEPS

1. Install OpenResty. See OpenResty Linux Packages.
2. Start or stop OpenResty Nginx

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	Install OpenResty. See OpenResty Linux Packages.	As part of the OpenResty installation, Nginx will be installed in this location. Add the OpenResty path to the ***PATH*** variable by adding the following line in the ***~/.bashrc*** file. `export PATH=/usr/local/openresty/bin:$PATH`
Step 2	Start or stop OpenResty Nginx	• To start OpenResty Nginx, enter **`openresty`**. • To stop OpenResty Nginx, enter **`openresty -s stop`**.

Configure OpenResty Nginx

The configuration is explained for an OpenResty-based Nginx installation. The default directories for OpenResty are:

- <nginx-install-directory> = /usr/local/openresty/nginx
- <Openresty-install-directory> = /usr/local/openresty

1. Download and extract the 12.5(1) SU2-reverse-proxy-config.zip that contains the reverse-proxy configuration for OpenResty Nginx. This file is available on the Software Download page.
2. Copy `nginx.conf`, `nginx/conf.d/`, and `nginx/html/` from the extracted reverse-proxy configuration directory to `<nginx-install-directory>/conf`, `<nginx-install-directory>/conf/conf.d/`, and `<nginx-install-directory>/html/` respectively.
3. Copy the `nginx/lua` directory from the extracted reverse-proxy configuration directory inside the `<nginx-install-directory>`.
4. Copy the contents of lualib to `<Openresty-install-directory>/lualib/resty`.
5. Configure OpenResty Nginx log rotation by copying the `nginx/logrotate/saproxy` file to the `<nginx-install-directory>/logrotate/` folder. Modify the file contents to point to the correct log directories if OpenResty Nginx defaults are not used.
6. OpenResty Nginx must be run with a dedicated non-privileged service account, which must be locked and have an invalid shell (or as applicable for the chosen OS).

7. Find the **Must-change** string in the files under the extracted folders named `html` and `conf.d` and replace the indicated values with the appropriate entries.
8. Ensure that all mandatory replacements are done, which are described with the **Must-change** comments in the config files.
9. Make sure that the cache directories configured for Cisco Unified Intelligence Center and Finesse are created under `<nginx-install-directory>/cache` along with these temporary directories.
   - <nginx-install-directory>/cache/client_temp
   - <nginx-install-directory>/cache/proxy_temp

Note The configuration provided is for a sample 400 agent deployment and has to be expanded appropriately for a larger deployment.

Configure OpenResty Nginx Cache

By default, the proxy cache paths are stored in the file system. We recommend changing them to in-memory drives by creating a cache location in tmpfs as shown here.

1. Create directories for the different proxy cache paths under /home.

   As an example, these directories must be created for the primary Unified CCX and Customer Collaboration Platform servers. The same steps should be followed for the secondary Unified CCX server.

```
mkdir -p /home/primaryCCX/rest
mkdir -p /home/primaryCCX/desktop
mkdir -p /home/primaryCCX/shindig
mkdir -p /home/primaryCCX/openfire
mkdir -p /home/CCP/ccp
mkdir -p /home/CCP/ccpopenfire
mkdir -p /home/primaryCUIC/cuic
mkdir -p /home/primaryCUIC/cuicdoc
mkdir -p /home/client_temp
mkdir -p /home/proxy_temp

echo "tmpfs /home/primaryFinesse/rest tmpfs
size=1510M,rw,auto,noexec,nodev,nosuid,gid=root,uid=root,mode=1700 0 0" >> /etc/fstab
echo "tmpfs /home/primaryFinesse/desktop tmpfs
size=20M,rw,auto,noexec,nodev,nosuid,gid=root,uid=root,mode=1700 0 0" >> /etc/fstab echo
 "tmpfs /home/primaryFinesse/shindig tmpfs
size=500M,rw,auto,noexec,nodev,nosuid,gid=root,uid=root,mode=1700 0 0" >>
/etc/fstab echo "tmpfs /home/primaryFinesse/openfire tmpfs
size=10M,rw,auto,noexec,nodev,nosuid,gid=root,uid=root,mode=1700 0 0" >> /etc/fstab echo
 "tmpfs /home/primaryCUIC/cuic tmpfs
size=100M,rw,auto,noexec,nodev,nosuid,gid=root,uid=root,mode=1700 0 0" >> /etc/fstab
echo "tmpfs /home/primaryCUIC/cuicdoc tmpfs
size=100M,rw,auto,noexec,nodev,nosuid,gid=root,uid=root,mode=1700 0 0" >> /etc/fstab
echo "tmpfs /home/client_temp tmpfs
size=2048M,rw,auto,noexec,nodev,nosuid,gid=root,uid=root,mode=1700 0 0" >> /etc/fstab
echo "tmpfs /home/proxy_temp tmpfs
size=2048M,rw,auto,noexec,nodev,nosuid,gid=root,uid=root,mode=1700 0 0" >> /etc/fstab
```

Note Increase the client and proxy_temp caches by 1 GB for each new Finesse cluster added to the configuration.

2. Mount the new mount points with the `mount -av` command.
3. Validate that the file system has mounted the new mount points with the `df -h` command.
4. Change the proxy_cache_path locations in the Unified CCX and Customer Collaboration Platform cache configuration files. For example, to change the paths for the Finesse primary, go to `to<nginx-installdirectory>/conf.d/finesse/caches` and change the existing cache location `/etc/nginx/cache/<ccx_server_name>/` to the newly created filesystem location `/home/primaryCCX`.

```
##Must-change /etc/nginx/cache/ location would change depending on folder extraction ##
 Nginx config file to cache the desktop/shindig and notification service related static
 files.
proxy_cache_path /home/primaryCCX/desktop levels=1:2 use_temp_path=on
keys_zone=desktop_cache_primary:10m max_size=15m inactive=3y use_temp_path=off;
proxy_cache_path /home/primaryCCX/shindig levels=1:2 use_temp_path=on
keys_zone=shindig_cache_primary:10m max_size=500m inactive=3y use_temp_path=off;
proxy_cache_path /home/primaryCCX/openfire levels=1:2 use_temp_path=on
keys_zone=openfire_cache_primary:10m max_size=10m inactive=3y use_temp_path=off;
proxy_cache_path /home/primaryCCX/rest levels=1:2 use_temp_path=on
keys_zone=rest_cache:10m max_size=1500m inactive=40m use_temp_path=off;
```

5. Follow the same steps for the Unified CCX secondary server.

Note Ensure that sum of all the tmpfs drive sizings created in all the previous steps is added to the final memory sizing for the deployment. This is because these drives are memory blocks that are configured to look like disks to the application and they consume that much memory space.

Use Self-Signed Certificates—Test Deployments

Use self-signed certificates until the reverse-proxy is ready to be rolled out into production. On a production deployment, use only a Certificate Authority-signed (CA-signed) certificate.

1. Generate OpenResty Nginx certificates for SSL folder content. Before you generate certificates, you must create a folder called **ssl** under `/usr/local/openresty/nginx`. Generate two certificates (one for `<reverseproxy_primary_fqdn>` and another for `<reverseproxy_secondary_fqdn>`) with the help of the following commands:
   a. `sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /usr/local/openresty/nginx/ssl/nginx.key -out /usr/local/openresty/nginx/ssl/nginx.crt` (pass hostname as: <reverseproxy_primary_fqdn>)
   b. `sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /usr/local/openresty/nginx/ssl/nginxnode2.key -out /usr/local/openresty/nginx/ssl/nginxnode2.crt` (pass hostname as: <reverseproxy_secondary_fqdn>)
   c. Ensure that the certificate path is `/usr/local/openresty/nginx/ssl/nginx.crt` and `/usr/local/openresty/nginx/ssl/nginxnode2.crt`.
2. Change the permission of the private key **400 (r--------)**.

3. Configure the firewall and iptables on the reverse-proxy to enable the firewall to communicate with the ports that are configured to listen to the OpenResty Nginx server.
4. Add the IP address and hostname of all the configured servers in the `/etc/hosts` file of the reverse-proxy server.

Note The provided configuration is for a sample 400 agent deployment and must be expanded appropriately for larger deployments.

Use CA-Signed Certificate—Production Deployments

A CA-signed certificate can be installed on the reverse-proxy with these steps:

1. Generate the certificate signing request (CSR).

   To generate the CSR and private key, enter `openssl req -new -newkey rsa:4096 -keyout nginx.key -out nginx.csr` after you log in to the proxy. Follow the prompt, and provide the details. This generates the CSR (nginx.csr in the example) and the RSA private key (nginx.key in the example) of 4096 bits.

   For example:

```
[root@reverseproxyhost.companyname.com ssl]# openssl req -new -newkey rsa:4096 -keyout
nginx.key -out nginx.csr
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'nginx.key'
Enter PEM pass phrase:passphrase
Verifying - Enter PEM pass phrase:passphrase
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:CA
Locality Name (eg, city) [Default City]:Orange County
Organization Name (eg, company) [Default Company Ltd]:CompanyName
Organizational Unit Name (eg, section) []:BusinessUnit
Common Name (eg, your name or your server's hostname)
[]:reverseproxyhostname.companydomain.com
Email Address []:john.doe@comapnydomain.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:challengePWD
An optional company name []:CompanyName
```

   Write down the PEM passphrase. This is used to decrypt the private key during the deployment.

2. Obtain the signed certificate from the CA.

   Send the CSR to the certificate authority and obtain the signed certificate.

Note If the certificate received from the CA is not a certificate chain containing all the respective certificates, compose all the relevant certificates into a single certificate chain file.

3. Deploy the certificate and key.

   Decrypt the key generated in the first step with the `openssl rsa -in nginx.key -out nginx_decrypted.key` command. Place the CA-signed certificate and the decrypted key inside the folder `/usr/local/openresty/nginx/ssl` in the reverse-proxy machine. Update or add the following SSL configurations related to the certificate in the OpenResty Nginx configurations in the following file: `/usr/local/openresty/nginx/conf/conf.d/ssl/ssl.conf`:

   ```
   ssl_certificate /usr/local/openresty/nginx/ssl/ca_signed_cert.crt;
   ssl_certificate_key/usr/local/openresty/nginx/ssl/nginx_decrypted.key;
   ```

4. Configure permissions for the certificates.

   Enter `chmod 400 /usr/local/openresty/nginx/ssl/ca_signed_cert.crt` and `chmod 400 /usr/local/openresty/nginx/ssl/nginx_decrypted.key`, so that the certificate has read-only permission and is restricted to the owner.

5. Reload OpenResty Nginx.

Create Custom Diffie-Hellman Parameter

1. Create a custom Diffie-Hellman parameter by using the following commands:

   ```
   openssl dhparam -out /usr/local/openresty/nginx/ssl/dhparam.pem 2048
   chmod 400 /usr/local/openresty/nginx/ssl/dhparam.pem
   ```

2. Modify the server configuration to use the new parameters in the file `/usr/local/openresty/nginx/conf/conf.d/ssl/ssl.conf` by using the following command:

   ```
   ssl_dhparam /usr/local/openresty/nginx/ssl/dhparam.pem;
   ```

Enable OCSP Stapling

Note To enable the Online Certificate Status Protocol (OCSP) stapling, the server should be using a CA-signed certificate. Also, the server should have access to the CA which signed the certificate.

Add or update the following configuration in the file: `/usr/local/openresty/nginx/conf/conf.d/ssl/ssl.conf`:

- `ssl_stapling on;`
- `ssl_stapling_verify on;`

Modify the Common OpenResty Nginx Configuration

The default OpenResty Nginx configuration file `(/usr/local/openresty/nginx/conf/nginx.conf)` has to be modified to contain these entries to enforce security and enhance performance. This content should be used to modify the default configuration file which is created during the OpenResty Nginx installation.

```
#user  nobody;
# Increasing number of worker processes will not increase the processing the request. The
number of worker process will be same as number of cores
# in system CPU. Nginx provides "auto" option to automate this, which will spawn one worker
 for each CPU core.
worker_processes  auto;

# Process id file location
pid /usr/local/openresty/nginx/logs/nginx.pid;

# Binds each worker process to a separate CPU
worker_cpu_affinity auto;

#Defines the scheduling priority for worker processes. This should be calculated by "nice"
 command. In our proxy set up the value is 0
worker_priority 0;


error_log  /usr/local/openresty/nginx/logs/error.log info;
error_log  /usr/local/openresty/nginx/logs/blocking.log emerg;

#user root root;
#user nginxuser nginxuser;
# current limit on the maximum number of open files by worker processes, keeping 10 times
of worker_connections
worker_rlimit_nofile 102400;

events {
    multi_accept on;

    # Sets the maximum number of simultaneous connections that can be opened by a worker
process.
    # This should not be more the current limit on the maximum number of open files i.e.
hard limit of the maximum number of open files for the user (ulimit -Hn)
    # The appropriate setting depends on the size of the server and the nature of the
traffic, and can be discovered through testing.
    worker_connections  10240;
    #debug_connection 10.78.95.21;
}


http {
    include       mime.types;

    default_type  text/plain;

    ## Must-change Change with DNS resolver ip in deployment
    ;
    resolver X.X.X.X;
    lua_package_path
"/usr/local/openresty/lualib/resty/?.lua;/usr/local/openresty/nginx/lua/?.lua;;";


    ## Must-change change proxy_temp folder as per cache directory configurations
    proxy_temp_path /usr/local/openresty/nginx/cache/proxy_temp 1 2;
```

```
    ## Must-change change client_temp folder as per cache directory configurations
    client_body_temp_path /usr/local/openresty/nginx/cache/client_temp 1 2;


    lua_shared_dict userlist 50m;
    lua_shared_dict credentialsstore 100m;
    lua_shared_dict userscount 100k;
    lua_shared_dict clientstorage 100m;
    lua_shared_dict blockingresources 100m;
    lua_shared_dict tokencache_ccxproxy 10M;
    lua_shared_dict tokencache_ccxproxy99 10M;
    lua_shared_dict ipstore 10m;
    lua_shared_dict desktopurllist 10m;
    lua_shared_dict desktopurlcount 100k;
    lua_shared_dict thirdpartygadgeturllist 10m;
    lua_shared_dict thirdpartygadgeturlcount 100k;
    lua_shared_dict corsheadersstore 100k;
    lua_shared_dict timerthreadsstore 100k;

    init_worker_by_lua_block {
        local UsersListManager = require('users_list_manager')
        local UnauthenticatedDesktopResourcesManager =
require("unauthenticated_desktopresources_manager")
        local UnauthenticatedResourcesManager =
require("unauthenticated_thirdpartyresources_manager")
        --  Must-change Replace saproxy.cisco.com with reverseproxy fqdn
       -- This is done so that all the apis required are prepopulated with data before the
 first request by starting required timers.
        if  ngx.worker.id() == 0 then
        UsersListManager.getUserList("ccx-rproxy-finesse.cisco.com",
"https://ccx-rproxy-finesse.cisco.com:8445/finesse/api/Users")

UnauthenticatedDesktopResourcesManager.getDesktopResources("ccx-rproxy-finesse.cisco.com",
 "https://ccx-rproxy-finesse.cisco.com:8445/desktop/api/ResourceURLs?type=desktop")

UnauthenticatedResourcesManager.getThirdPartyGadgetResources("ccx-rproxy-finesse.cisco.com",
 "https://ccx-rproxy-finesse.cisco.com:8445/desktop/api/ResourceURLs?type=3rdParty")
        end
    }


    include conf.d/*.conf;

    sendfile        on;

    tcp_nopush     on;

    server_names_hash_bucket_size 512;

}
```

Configure Reverse Proxy Port

By default, the OpenResty Nginx configuration listens on port 8445 for Unified CCX requests. At a time, only one port can be enabled from a reverse proxy to support finesse requests e.g., 8445. If 443 port needs to be supported, then check the `<NGINX_HOME>/conf.d/finesse`.conf in order to enable listening on 443 and disable listening on 8445.

Configure mutual TLS authentication between reverse-proxy and components

To enable client SSL certificate authentication for connections from reverse-proxy hosts on Unified CCX and Customer Collaboration Platform, use the new CVOS CLI option `utils system reverse-proxy client-auth enable/disable/status`.

By default, this is disabled and has to be enabled by the administrator by running the CLI on each upstream server independently. After this option is enabled, the Cisco Web proxy service running on the upstream host will start authenticating client certificates in a TLS handshake. It's authenticated for connections originating from trusted reverse-proxy hosts that are added by using the CLI `utils system reverse-proxy allowed-hosts add <proxy-host>`.

The following is the configuration block for the same in proxy configuration files named **ssl.conf** and **ssl2.conf**.

```
#Must-change /usr/local/openresty/nginx/ssl/nginx.crt change this location accordingly
proxy_ssl_certificate /usr/local/openresty/nginx/ssl/nginx.crt;
#Must-change /usr/local/openresty/nginx/ssl/nginx.key change this location accordingly
proxy_ssl_certificate_key /usr/local/openresty/nginx/ssl/nginx.key;
```

The SSL certificate used for outbound traffic (proxy to upstream) can be the same as the SSL certificate that is configured for inbound traffic (SSL connector for component server blocks). If a self-signed certificate is used as **proxy_ssl_certificate** and has to be authenticated successfully, it has to be uploaded to the tomcat trust store of the upstream components (Finesse/IdS/Cisco Unified Intelligence Center/Livedata).

Upstream server certificate validation by reverse-proxy is optional and is disabled by default. If you want to achieve full TLS mutual authorization between reverse-proxy and upstream hosts, the following configuration must be uncommented in the **ssl.conf** and **ssl2.conf** files:

```
#Enforce upstream server certificate validation at proxy ->
#this is not mandated as per CIS buit definitely adds to security.
#It requires the administrator to upload all upstream server certificates to the proxy
certificate store
#Must-Change Uncomment below lines IF need to enforce upstream server certificate validation
 at proxy
#proxy_ssl_verify on;
#proxy_ssl_trusted_certificate /usr/local/openresty/nginx/ssl/finesse25.crt;
proxy_ssl_trusted_certificate: This file should contain the all upstream certificate enteries
 concatenated together
```

The **mutual TLS (mTLS)** is a standard security requirement for connections established from DMZ into the data center. For more information, see Nginx CIS benchmarks-https://www.cisecurity.org/benchmark/nginx

For mTLS, both the server and client must be pre-configured with mutual information about each other. Also, the mutual certificates must be properly verified. So the term **"mutual TLS (mTLS)"**. A properly configured proxy server will be able to circumvent TCP rate limits and provide the client IP to the server for logging purposes. As a result, it's critical to verify the proxy identity before connecting as a reverse-proxy. For security reasons, it is recommended that this feature be used and turned on.

This requires the upstream component certificates to be made available to the proxy and vice-versa. By default, reverse-proxy establishes verified TLS connections to the upstream server and it's the proxy verification at the client which is optional. So, this must be enabled at the upstream client server.

Enabling mutual TLS

The mTLS must be enabled at the upstream component servers using the provided CLI.

Use the **utils system reverse-proxy client-auth enable** CLI to enable proxy certificate verification at the upstream component server.

After running the CLI, upload the proxy SSL certificate corresponding to the reverse-proxy hostname that is used to connect to the same server. This can be used to verify TLS connections when the reverse-proxy attempts to establish an upstream connection.

Clear Cache

The reverse-proxy cache can be cleared with the `<NGINX_HOME>/clearCache.sh` command.

Standard Guidelines

This section briefly describes the standard guidelines that must be followed when you set up OpenResty Nginx as a proxy server. The guidelines for the OpenResty Nginx server software is derived from the Center for Internet Security.

1. Use the latest stable versions of OpenResty and OpenSSL version.
2. Install OpenResty Nginx in a separate disk mount.
3. The OpenResty Nginx process id must be owned by the root user (or as applicable for the chosen OS) and must have permission **644 (rw-------)** or stricter.
4. OpenResty Nginx must block requests for unknown hosts. Ensure that each server block contains the server_name directive explicitly defined. To verify, search all server blocks in the `nginx.conf` and `nginx/conf.d` files and verify that all server blocks contain the server_name.
5. OpenResty Nginx must listen only on the authorized ports. Search all server blocks in the `nginx.conf` and `nginx/conf.d` files and check for the `listen` directives to verify that only the authorized ports are open for requests.
6. Block the proxy server HTTP port, because Cisco Finesse does not support HTTP.
7. The OpenResty Nginx SSL protocol must be TLS 1.2. Remove support for legacy SSL protocols. Disable weak SSL ciphers.
8. Send the OpenResty Nginx error and access logs to the remote syslog server.
9. Install the **mod_security** module that works as a web application firewall. See the ModSecurity manual for more information. Note that OpenResty Nginx load has not been verified within the **mod_security** module in place.

Configure the Mapping File

Refer to the *Host Mapping File for Network Translation* section in the *Solution Design Guide for Cisco Unified Contact Center Express* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-implementation-design-guides-list.html.

Use reverse-proxy as the Mapping File server

The following steps are required only if the reverse-proxy is also used as the proxy mapping file host:

1. Configure the reverse-proxy hostname in the domain controller used by the Unified CCX and Customer Collaboration Platform hosts such that its IP address can be resolved.

2. Upload the generated OpenResty® Nginx signed certificates on both the nodes under tomcat-trust of `cmplatform` and restart the server.
3. Update the **Must-change** values in `<NGINX_HOME>/html/proxymap.txt`.
4. Reload OpenResty® Nginx configurations with the following commands:
   - `openresty -s stop`
   - `openresty`
5. Use the `curl` command to validate if the configuration file is accessible from another network host.

CentOS 7 Kernel Hardening

If the operating system is Cent OS 7 and the installations use a dedicated server for hosting the proxy, harden the kernel by using these `sysctl` configurations:

```
## Configurations for kernel hardening - CentOS 7. The file path is /etc/sysctl.conf
## Note that the commented configurations denote that CentOS 7's default value matches
## the recommended/tested value, and are not security related configurations.


# Avoid a smurf attack
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Turn on protection for bad icmp error messages
net.ipv4.icmp_ignore_bogus_error_responses = 1

# Turn on syncookies for SYN flood attack protection
net.ipv4.tcp_syncookies = 1


# Turn on and log spoofed, source routed, and redirect packets
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1

# Turn off routing
net.ipv4.ip_forward = 0
net.ipv4.conf.all.forwarding = 0
net.ipv6.conf.all.forwarding = 0

net.ipv4.conf.all.mc_forwarding = 0
net.ipv6.conf.all.mc_forwarding = 0

# Block routed packets
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
net.ipv6.conf.all.accept_source_route = 0
net.ipv6.conf.default.accept_source_route = 0


# Block ICMP redirects
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
```

```
# Filter routing packets with inward-outward path mismatch(reverse path filtering)
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1


# Router solicitations & advertisements related.
net.ipv6.conf.default.router_solicitations = 0
net.ipv6.conf.default.accept_ra_rtr_pref = 0
net.ipv6.conf.default.accept_ra_pinfo = 0
net.ipv6.conf.default.accept_ra_defrtr = 0
net.ipv6.conf.default.autoconf = 0
net.ipv6.conf.default.dad_transmits = 0
net.ipv6.conf.default.max_addresses = 1
net.ipv6.conf.all.accept_ra = 0
net.ipv6.conf.default.accept_ra = 0

# Backlog - increased from default 1000 to 5000.
net.core.netdev_max_backlog = 5000

# Setting syn/syn-ack retries to minimum value, so that they don't stay in the queue.
net.ipv4.tcp_syn_retries = 1
net.ipv4.tcp_synack_retries = 0

# Max tcp listen backlog. Setting it to 511 to match nginx config
net.core.somaxconn = 511


# Reduce the duration of connections held in TIME_WAIT(seconds)
net.ipv4.tcp_fin_timeout = 6


# Maximum resources allotted
# fs.file-max = 2019273
# kernel.pid_max = 4194304
# net.ipv4.ip_local_port_range = 32768 60999

# TCP window size tuning
# net.ipv4.tcp_window_scaling = 1
# net.core.rmem_default = 212992
# net.core.rmem_max = 212992
# net.ipv4.tcp_rmem = 4096 87380 6291456
# net.ipv4.udp_rmem_min = 4096
# net.core.wmem_default = 212992
# net.core.wmem_max = 212992
# net.ipv4.tcp_wmem = 4096 16384 4194304
# net.ipv4.udp_wmem_min = 4096
# vm.lowmem_reserve_ratio = 256 256 32 0 0
# net.ipv4.tcp_mem = 236373 315167 472746

# Randomize virtual address space
kernel.randomize_va_space = 2


# Congestion control
# net.core.default_qdisc = fq_codel
# net.ipv4.tcp_congestion_control = cubic

# Disable SysReq
kernel.sysrq = 0

# Controls the maximum size of a message, in bytes
kernel.msgmnb = 65536

# Controls the default maximum size of a message queue
```

```
kernel.msgmax = 65536

# Controls the eagerness of the kernel to swap.
vm.swappiness = 1
```

Reboot after you make the recommended changes.

IPtables Hardening

IPtables is an application that allows a system administrator to configure the IPv4 and IPv6 tables, chains, and rules provided by the Linux kernel firewall.

The IPtables rules are configured to secure the proxy application from brute force attacks by restricting the access in the Linux kernel firewall.

The comments in the configuration indicate which service is being rate-limited by using the rules.

Note If administrators use a different port or expand access to multiple servers using the same ports, they must do appropriate sizing for these ports accordingly.

A sample IPtable is as follows:

```
# Configuration for iptables service
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]

# Ensure loopback traffic is configured
-A INPUT -i lo -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A INPUT -s 127.0.0.0/8 -j DROP

# Ensure ping openeded only for the particular source and blocked for rest
# Must-Change: Replace the x.x.x.x with valid ip address
-A INPUT -p ICMP --icmp-type 8 -s x.x.x.x -j ACCEPT

# Ensure outbound and established connections are configured
-A INPUT -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -p tcp -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT

# Block ssh for external interface
# Must-Change: Replace the ens224 with valid ethernet interface
-A INPUT -p tcp -i ens224 --dport 22 -j DROP
# Open inbound ssh(tcp port 22) connections
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT

# Configuration to allow connection from CDN without any limiting
# Must-Change: Uncomment and replace the x.x.x.x/xx and  ens224 with valid IP address and
ethernet interface respectively.
# Add similar lines for all CDN IP addresses
# iptables -A INPUT -i ens224 -s x.x.x.x/xx -j ACCEPT

# Configuration for finesse 8445 port
-A INPUT -p tcp -m tcp --dport 8445 --tcp-flags SYN SYN -m connlimit --connlimit-above 10
--connlimit-mask 32 --connlimit-saddr -m limit --limit 1/min --limit-burst 1 -j LOG
--log-prefix " Connections to 8445 exceeded connlimit "
-A INPUT -p tcp -m tcp --dport 8445 --tcp-flags SYN SYN -m connlimit --connlimit-above 10
--connlimit-mask 32 --connlimit-saddr -j DROP
 -A INPUT -p tcp -m tcp --dport 8445 --tcp-flags SYN SYN -m hashlimit --hashlimit-upto 6/sec
```

```
 --hashlimit-burst 8 --hashlimit-mode srcip,dstport --hashlimit-name TCP_8445_DOS -j ACCEPT
-A INPUT -p tcp -m tcp --dport 8445 --tcp-flags SYN SYN -m limit --limit 1/min --limit-burst
 1 -j LOG --log-prefix " Exceeded 8445 hashlimit "
-A INPUT -p tcp -m tcp --dport 8445 --tcp-flags SYN SYN -j DROP

# Configuration for finesse 8442 port
-A INPUT -p tcp -m tcp --dport 8442 --tcp-flags SYN SYN -m connlimit --connlimit-above 10
--connlimit-mask 32 --connlimit-saddr -m limit --limit 1/min --limit-burst 1 -j LOG
--log-prefix " Connections to 8442 exceeded connlimit "
-A INPUT -p tcp -m tcp --dport 8442 --tcp-flags SYN SYN -m connlimit --connlimit-above 10
--connlimit-mask 32 --connlimit-saddr -j DROP
 -A INPUT -p tcp -m tcp --dport 8442 --tcp-flags SYN SYN -m hashlimit --hashlimit-upto 6/sec
 --hashlimit-burst 8 --hashlimit-mode srcip,dstport --hashlimit-name TCP_8445_DOS -j ACCEPT
-A INPUT -p tcp -m tcp --dport 8442 --tcp-flags SYN SYN -m limit --limit 1/min --limit-burst
 1 -j LOG --log-prefix " Exceeded 8442 hashlimit "
-A INPUT -p tcp -m tcp --dport 8442 --tcp-flags SYN SYN -j DROP

# Configuration for IdS 8553 port
-A INPUT -p tcp -m tcp --dport 8553 --tcp-flags SYN SYN -m connlimit --connlimit-above 6
--connlimit-mask 32 --connlimit-saddr -m limit --limit 1/min --limit-burst 1 -j LOG
--log-prefix " IdS connection limit exceeded"
-A INPUT -p tcp -m tcp --dport 8553 --tcp-flags SYN SYN -m connlimit --connlimit-above 6
--connlimit-mask 32 --connlimit-saddr -j DROP
-A INPUT -p tcp -m tcp --dport 8553 --tcp-flags SYN SYN -m hashlimit --hashlimit-upto 2/sec
 --hashlimit-burst 4 --hashlimit-mode srcip,dstport --hashlimit-name TCP_8553_DOS -j ACCEPT
-A INPUT -p tcp -m tcp --dport 8553 --tcp-flags SYN SYN -m limit --limit 1/min --limit-burst
 1 -j LOG --log-prefix " Exceeded 8553 hashlimit "
-A INPUT -p tcp -m tcp --dport 8553 --tcp-flags SYN SYN -j DROP

# Configuration for IdP 443 port
-A INPUT -p tcp -m tcp --dport 443 --tcp-flags SYN SYN -m connlimit --connlimit-above 8
--connlimit-mask 32 --connlimit-saddr -m limit --limit 1/min --limit-burst 1 -j LOG
--log-prefix " IdP connection limit exceeded"
-A INPUT -p tcp -m tcp --dport 443 --tcp-flags SYN SYN -m connlimit --connlimit-above 8
--connlimit-mask 32 --connlimit-saddr -j DROP
-A INPUT -p tcp -m tcp --dport 443 --tcp-flags SYN SYN -m hashlimit --hashlimit-upto 4/sec
 --hashlimit-burst 6 --hashlimit-mode srcip,dstport --hashlimit-name TCP_443_DOS -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 --tcp-flags SYN SYN -m limit --limit 1/min --limit-burst
 1 -j LOG --log-prefix " Exceeded 443 hashlimit "
-A INPUT -p tcp -m tcp --dport 443 --tcp-flags SYN SYN -j DROP


# Must-Change: A2A file transfer has not been considered for below IMNP configuration.
# For A2A for support, these configuration must be recalculated to cater different file
transfer scenarios.

# Configuration for IMNP 5280 port
-A INPUT -p tcp -m tcp --dport 5280 --tcp-flags SYN SYN -m connlimit --connlimit-above 30
--connlimit-mask 32 --connlimit-saddr -m limit --limit 1/min --limit-burst 1 -j LOG
--log-prefix " IMNP connection limit exceeded"
-A INPUT -p tcp -m tcp --dport 5280 --tcp-flags SYN SYN -m connlimit --connlimit-above 30
--connlimit-mask 32 --connlimit-saddr -j DROP
-A INPUT -p tcp -m tcp --dport 5280 --tcp-flags SYN SYN -m hashlimit --hashlimit-upto 20/sec
 --hashlimit-burst 25 --hashlimit-mode srcip,dstport --hashlimit-name TCP_5280_DOS -j ACCEPT
-A INPUT -p tcp -m tcp --dport 5280 --tcp-flags SYN SYN -m limit --limit 1/min --limit-burst
 1 -j LOG --log-prefix " Exceeded 5280 hashlimit "
-A INPUT -p tcp -m tcp --dport 5280 --tcp-flags SYN SYN -j DROP

# Configuration for IMNP 15280 port
-A INPUT -p tcp -m tcp --dport 15280 --tcp-flags SYN SYN -m connlimit --connlimit-above 30
 --connlimit-mask 32 --connlimit-saddr -m limit --limit 1/min --limit-burst 1 -j LOG
--log-prefix " IMNP connection limit exceeded"
-A INPUT -p tcp -m tcp --dport 15280 --tcp-flags SYN SYN -m connlimit --connlimit-above 30
 --connlimit-mask 32 --connlimit-saddr -j DROP
```

```
-A INPUT -p tcp -m tcp --dport 15280 --tcp-flags SYN SYN -m hashlimit --hashlimit-upto
20/sec --hashlimit-burst 25 --hashlimit-mode srcip,dstport --hashlimit-name TCP_15280_DOS
-j ACCEPT
-A INPUT -p tcp -m tcp --dport 15280 --tcp-flags SYN SYN -m limit --limit 1/min --limit-burst
 1 -j LOG --log-prefix " Exceeded 15280 hashlimit "
-A INPUT -p tcp -m tcp --dport 15280 --tcp-flags SYN SYN -j DROP


# Configuration for IMNP 25280 port
-A INPUT -p tcp -m tcp --dport 25280 --tcp-flags SYN SYN -m connlimit --connlimit-above 30
 --connlimit-mask 32 --connlimit-saddr -m limit --limit 1/min --limit-burst 1 -j LOG
--log-prefix " IMNP connection limit exceeded"
-A INPUT -p tcp -m tcp --dport 25280 --tcp-flags SYN SYN -m connlimit --connlimit-above 30
 --connlimit-mask 32 --connlimit-saddr -j DROP
-A INPUT -p tcp -m tcp --dport 25280 --tcp-flags SYN SYN -m hashlimit --hashlimit-upto
20/sec --hashlimit-burst 25 --hashlimit-mode srcip,dstport --hashlimit-name TCP_25280_DOS
-j ACCEPT
-A INPUT -p tcp -m tcp --dport 25280 --tcp-flags SYN SYN -m limit --limit 1/min --limit-burst
 1 -j LOG --log-prefix " Exceeded 25280 hashlimit "
-A INPUT -p tcp -m tcp --dport 25280 --tcp-flags SYN SYN -j DROP


# Configuration for CUIC 8444 port
-A INPUT -p tcp -m tcp --dport 8444 --tcp-flags SYN SYN -m connlimit --connlimit-above 6
--connlimit-mask 32 --connlimit-saddr -m limit --limit 1/min --limit-burst 1 -j LOG
--log-prefix " CUIC connection limit exceeded"
-A INPUT -p tcp -m tcp --dport 8444 --tcp-flags SYN SYN -m connlimit --connlimit-above 6
--connlimit-mask 32 --connlimit-saddr -j DROP
-A INPUT -p tcp -m tcp --dport 8444 --tcp-flags SYN SYN -m hashlimit --hashlimit-upto 2/sec
 --hashlimit-burst 4 --hashlimit-mode srcip,dstport --hashlimit-name TCP_8444_DOS -j ACCEPT
-A INPUT -p tcp -m tcp --dport 8444 --tcp-flags SYN SYN -m limit --limit 1/min --limit-burst
 1 -j LOG --log-prefix " Exceeded 8444 hashlimit "
-A INPUT -p tcp -m tcp --dport 8444 --tcp-flags SYN SYN -j DROP

# Configuration for CUIC 8447 port
-A INPUT -p tcp -m tcp --dport 8447 --tcp-flags SYN SYN -m connlimit --connlimit-above 6
--connlimit-mask 32 --connlimit-saddr -m limit --limit 1/min --limit-burst 1 -j LOG
--log-prefix " CUIC connection limit exceeded"
-A INPUT -p tcp -m tcp --dport 8447 --tcp-flags SYN SYN -m connlimit --connlimit-above 6
--connlimit-mask 32 --connlimit-saddr -j DROP
-A INPUT -p tcp -m tcp --dport 8447 --tcp-flags SYN SYN -m hashlimit --hashlimit-upto 2/sec
 --hashlimit-burst 4 --hashlimit-mode srcip,dstport --hashlimit-name  TCP_8447_DOS -j ACCEPT
-A INPUT -p tcp -m tcp --dport 8447 --tcp-flags SYN SYN -m limit --limit 1/min --limit-burst
 1 -j LOG --log-prefix " Exceeded 8447 hashlimit "
-A INPUT -p tcp -m tcp --dport 8447 --tcp-flags SYN SYN -j DROP

# Configuration for LiveData 12005  port
-A INPUT -p tcp -m tcp --dport 12005 --tcp-flags SYN SYN -m connlimit --connlimit-above 10
 --connlimit-mask 32 --connlimit-saddr -m limit --limit 1/min --limit-burst 1 -j LOG
--log-prefix " LD connection limit exceeded"
-A INPUT -p tcp -m tcp --dport 12005 --tcp-flags SYN SYN -m connlimit --connlimit-above 10
 --connlimit-mask 32 --connlimit-saddr -j DROP
-A INPUT -p tcp -m tcp --dport 12005 --tcp-flags SYN SYN -m hashlimit --hashlimit-upto 6/sec
 --hashlimit-burst 8 --hashlimit-mode srcip,dstport --hashlimit-name TCP_12005_DOS -j ACCEPT
-A INPUT -p tcp -m tcp --dport 12005 --tcp-flags SYN SYN -m limit --limit 1/min --limit-burst
 1 -j LOG --log-prefix " Exceeded 12005 hashlimit "
-A INPUT -p tcp -m tcp --dport 12005 --tcp-flags SYN SYN -j DROP

# Configuration for LiveData 12008  port
-A INPUT -p tcp -m tcp --dport 12008 --tcp-flags SYN SYN -m connlimit --connlimit-above 10
 --connlimit-mask 32 --connlimit-saddr -m limit --limit 1/min --limit-burst 1 -j LOG
--log-prefix " LD connection limit exceeded"
-A INPUT -p tcp -m tcp --dport 12008 --tcp-flags SYN SYN -m connlimit --connlimit-above 10
 --connlimit-mask 32 --connlimit-saddr -j DROP
```

```
-A INPUT -p tcp -m tcp --dport 12008 --tcp-flags SYN SYN -m hashlimit --hashlimit-upto 6/sec
 --hashlimit-burst 8 --hashlimit-mode srcip,dstport --hashlimit-name  TCP_12008_DOS -j
ACCEPT
-A INPUT -p tcp -m tcp --dport 12008 --tcp-flags SYN SYN -m limit --limit 1/min --limit-burst
 1 -j LOG --log-prefix " Exceeded 12008 hashlimit "
-A INPUT -p tcp -m tcp --dport 12008 --tcp-flags SYN SYN -j DROP

# Block all other ports
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited

COMMIT
```

Note The rules that are provided block the DNS resolution at the proxy. So, all the hostnames of the components that are configured in the proxy must be explicitly added to the host resolution file `/etc/hosts`.

Interface level rules must be added to restrict access to only users accessing via LAN and to block public access to port 10000, which is used for accessing the proxy map file. For example,

```
-A INPUT -p tcp -m tcp -i <PRIVATE_INTERFACE> --dport 10000 --tcp-flags SYN SYN -m hashlimit
--hashlimit-upto 35/sec --hashlimit-burst 2000 --hashlimit-mode srcip,dstport --hashlimit-name
TCP_10000_DOS -j ACCEPT -A INPUT -p tcp -m tcp -i <PRIVATE_INTERFACE> --dport 10000
--tcp-flags SYN SYN -m limit --limit 1/min --limit-burst 1 -j LOG --log-prefix " Exceeded
hashlimit " -A INPUT -p tcp -m tcp -i <PRIVATE_INTERFACE> --dport 10000 --tcp-flags SYN SYN
-j DROP
```

These rules could be applied directly by editing the `/etc/sysconfig/iptables` file manually. Alternatively, save the configuration into a file such as `iptables.conf` and run cat `iptables.conf >>/etc/sysconfig/iptables` to apply the rules.

Restart the IPtables service after you apply the rules. To restart the IPtables service, enter `systemctl restart iptables`.

Restrict Client Connections

In addition to the previous IPtables configuration, installations that know the address range for clients who use the proxy must use this knowledge to secure the proxy access rules. This helps to secure the proxy from malicious botnets which are often created in the IP address range of countries that have more lax rules with regards to online security. Restrict the IP address ranges to country-based, state-based, or ISP-based IP ranges if you are sure of the access patterns.

Block Client Connections

Block the specific range of addresses when an attack is identified to be made from an IP address or a range of IP addresses. In such cases, the requests from those IP addresses can be blocked with **iptable** rules.

Block Distinct IP Addresses

To block multiple distinct IP addresses, add a line to the **IPTables** configuration file for each IP address.

For example, to block the addresses 192.0.2.3 and 192.0.2.4, enter:

```
iptables -A INPUT -s 192.0.2.3 -j DROP iptables -A INPUT -s 192.0.2.4 - j DROP.
```

Block a Range of IP Addresses

Block multiple IP addresses in a range and add a single line to the **IPTables** configuration file with the IP address range.

For example, to block the addresses from 192.0.2.3 to 192.0.2.35, enter:

```
iptables -A INPUT -m iprange --src-range 192.0.2.3-192.0.2.35 -j DROP.
```

Block All IP Addresses in a Subnet

Block all IP addresses in an entire subnet by adding a single line to the **IPTables** configuration file by using the classless inter-domain routing notation for the IP address range. For example, to block all class **C addresses**, enter:

```
iptables -A INPUT -s 192.0.0.0/16 -j DROP.
```

SELinux

Security-Enhanced Linux (SELinux) is a platform security framework integrated as an enhancement into the Linux OS. The procedure to install and add SELinux policies to run OpenResty as the reverse-proxy is provided next.

1. Stop the process with the `openresty -s stop` command.
2. Configure and start or stop OpenResty Nginx server with the `systemctl` command so that during boot up the OpenResty process will start automatically. Enter these commands as root user.
   a. Go to `/usr/lib/systemd/system`.
   b. Open the file called `openresty.service`.
   c. Update the content of the file as per `PIDFile` location.

```
[Unit]
Description=The OpenResty Application Platform
After=syslog.target network-online.target remote-fs.target nss-lookup.target
Wants=network-online.target

[Service]
Type=forking
PIDFile=/usr/local/openresty/nginx/logs/nginx.pid
ExecStartPre=/usr/local/openresty/nginx/sbin/nginx -t
ExecStart=/usr/local/openresty/nginx/sbin/nginx
ExecReload=/bin/kill -s HUP $MAINPID
ExecStop=/bin/kill -s QUIT $MAINPID
PrivateTmp=true

[Install]
WantedBy=multi-user.target
```

   d. As root user, enter `sudo systemctl enable openresty`.
   e. Start or stop the OpenResty service with the `systemctl start openresty / systemctl stop openresty` command and ensure that the process starts or stops as root user.

1. **Install SElinux**
   - By default, only some SELinux packages will be installed in CentOS.

- The **policycoreutils-devel** package and its dependencies must be installed in order to generate the SELinux policy.
- Enter the following command to install **policycoreutils-devel**

```
yum install policycoreutils-devel
```

- Ensure that after you install the package, the `sepolicy` command works.

```
usage: sepolicy [-h] [-P POLICY]


{booleans,communicate,generate,gui,interface,manpage,network,transition}
                ...

SELinux Policy Inspection Tool
```

2. **Create a New Linux User and Map with SElinux User**

   a. Enter `semanage login -l` to view the mapping between Linux users and SELinux users.

```
[root@loadproxy-cisco-com ~]# semanage login -l

Login Name           SELinux User         MLS/MCS Range        Service

__default__          unconfined_u         s0-s0:c0.c1023       *              *
root                 unconfined_u         s0-s0:c0.c1023       *
```

   b. As root, create a new Linux user (**nginx** user) that is mapped to the SELinux **user_u** user.

```
useradd -Z user_u nginxuser
[root@loadproxy-cisco-com ~]# passwd nginxuser
Changing password for user nginxuser.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

   c. In order to view the mapping between **nginxuser** and **user_u**, enter this command as root:

```
[root@loadproxy-cisco-com ~]# semanage login -l

Login Name           SELinux User         MLS/MCS Range        Service

__default__          unconfined_u         s0-s0:c0.c1023       *
nginxuser            user_u               s0                   *
root                 unconfined_u         s0-s0:c0.c1023       *
```

   d. SELinux **__default__** login is by default mapped to the SELinux **unconfined_u** user. By default, it is required to confine **user_u** by using the following command:

```
semanage login -m -s user_u -r s0 __default__
```

   In order to check if the command worked properly, enter `semanage login -l`. It should produce this output:

```
Login Name           SELinux User         MLS/MCS Range        Service

__default__          user_u               s0                   *
nginxuser            user_u               s0                   *
root                 unconfined_u         s0-s0:c0.c1023       *
```

464783

   e. Modify nginx.conf and perform change ownership for nginxuser.

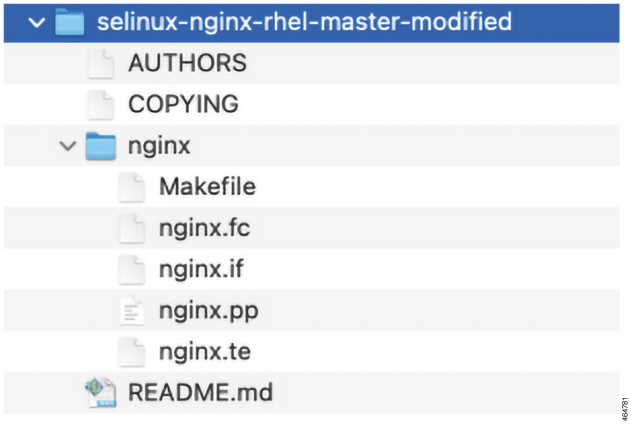
1. Enter `chown -R nginxuser:nginxuser *` in the `<Openresty-install-directory>` directory.
2. Modify the **nginx.conf** file to include nginxuser as the user for running worker processes.

```
........

user nginxuser nginxuser;

..........
```

3. **Write the SELinux Policy for OpenResty Nginx**

   a. Instead of generating a new default custom policy for OpenResty Nginx with the `sepolicy generate --init /usr/bin/nginx` command, start with an existing policy.

   The **nginx.fc** file (File Contexts file) and **nginx.te** (Type Enforcement file) files, that are downloaded from the following location, are modified for reverse-proxy usage:



   This modified version can be used as a reference because it is updated for a particular use case.

   b. Download the **selinux-nginx-rhel-master-modified.tar** file from the Software Download page.

   c. Extract the **.tar** file and navigate to the **nginx** directory within it.

   d. Open the **.fc** file and verify the required file paths of **Nginx installer**, **cache**, and **pid** files.

   e. Compile the configuration with the `make` command.

   f. The **nginx.pp** file is generated.

   g. Load the policy with the `semodule` command.

```
semodule -i nginx.pp
```

   h. Go to **/root** and create an empty file called `touch /.autorelabel`.

   i. Reboot the system.

   j. Enter the following command to verify that the policy is loaded successfully:

```
semodule --list-modules=full
```

```
[root@loadproxy-cisco-com ~]# semodule --list-modules=full
400 nginx               pp
200 container           pp
200 flatpak             pp
100 abrt                pp
100 accountsd           pp
100 acct                pp
100 afs                 pp
100 aiccu               pp
100 aide                pp
100 ajaxterm            pp
100 alsa                pp
```

464782

k. OpenResty Nginx should run without any violation. (Violation logs will be available in **/var/log/messages** and **/var/log/audit/audit.log**).

l. Enter the following command to check the status of OpenResty Nginx:

```
ps -aefZ | grep nginx
```

```
[root@loadproxy-cisco-com ~]# ps -aefZ |grep nginx
system_u:system_r:nginx_t:s0    root        1686       1  0 16:14 ?        00:00:00 nginx: master process /usr/bin/nginx
system_u:system_r:nginx_t:s0    nginxus+    1687    1686  0 16:14 ?        00:00:00 nginx: worker process
system_u:system_r:nginx_t:s0    nginxus+    1688    1686  0 16:14 ?        00:00:00 nginx: worker process
system_u:system_r:nginx_t:s0    nginxus+    1689    1686  0 16:14 ?        00:00:00 nginx: worker process
system_u:system_r:nginx_t:s0    nginxus+    1690    1686  0 16:14 ?        00:00:00 nginx: worker process
system_u:system_r:nginx_t:s0    nginxus+    1691    1686  0 16:14 ?        00:00:00 nginx: worker process
system_u:system_r:nginx_t:s0    nginxus+    1692    1686  0 16:14 ?        00:00:00 nginx: worker process
system_u:system_r:nginx_t:s0    nginxus+    1693    1686  0 16:14 ?        00:00:00 nginx: worker process
system_u:system_r:nginx_t:s0    nginxus+    1694    1686  0 16:14 ?        00:00:00 nginx: worker process
system_u:system_r:nginx_t:s0    nginxus+    1695    1686  0 16:14 ?        00:00:00 nginx: cache manager process
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 2543 2252  0 16:17 pts/0 00:00:00 grep --color=auto nginx
```

464784

m. Now the Finesse agent desktop or supervisor desktop should be accessible.

Verifying Reverse-Proxy Configuration

Finesse

Procedure

Step 1 From the DMZ, open *https://<reverseproxy:port>/finesse/api/SystemInfo* and check if it's reachable.

Step 2 Check if the **<host>** values in both **<primaryNode>** and **<secondaryNode>** are valid in the reverse-proxy hostnames. It shouldn't be the Finesse hostnames.

Note

- If CORS status is **enabled**, you must explicitly add the reverse-proxy domain name to the list of CORS trusted domain names.

- Reverse-proxy supports a maximum of 8000 folders (including sub-directories) in the `finesse/3rdpartygadget` folder.

Unified CCX and Customer Collaboration Platform

1. If the Unified CCX hostnames are seen in the response instead of the reverse-proxy hostnames, validate proxy-mapping configurations and check if allowed hosts are added in the Unified CCX servers as described in the Populate Network Translation Data, on page 494 section.
2. If MSC, NV and ASC gadgets load properly in Finesse Desktop, then the Unified CCX and Customer Collaboration Platform proxy configurations are correct.

Cisco Identity Service

To validate the Cisco IdS configuration, perform the following steps:

Procedure

Step 1 Log in to the Cisco IdS Admin interface at **https://<ids_LAN_host:ids_port>:8553/idsadmin** from the LAN because the admin interface isn't exposed over reverse-proxy.

Step 2 Choose **Settings** > **IdS Trust**.

Step 3 Verify that the proxy cluster publisher node is listed on the Download SP metadata page, and click **Next**.

Step 4 Verify that the IDP proxy is correctly displayed (if configured on the Upload IDP metadata page) and click **Next**.

Step 5 Initiate test SSO through all proxy cluster nodes from the Test SSO page and validate that all are successful. This requires client system connectivity to reverse-proxy nodes.

Brute Force Attack Prevention Configuration

Unified CCX Release 12.5(1) SU2 authentication scripts actively prevent brute force attacks that can be used to guess the user password. The scripts do this by blocking the IP address used to access the service, after a certain number of failed attempts in a short time. These requests will be rejected by **418 client error**. The number of failed requests, time interval, and blocking duration are configurable.

Attack Detection Parameters

Configurations are present in the **<nginx-install-directory>/conf/conf.d/maps.conf** file.

```
## These two constants indicate five auth failures from a client can be allowed in thirty
seconds.
## if the threshold is crossed,client ip will be blocked.
map $host $auth_failure_threshold_for_lock {
```

```
## Must-change Replace below two parameters as per requirement
default 5 ;
}
map $host $auth_failure_counting_window_secs {
## Must-change Replace below two parameters as per requirement
default 30;
}
## This indicates duration of blocking a client to avoid brute force attack
map $host $ip_blocking_duration {
## Must-change Replace below parameter as per requirement
default 1800;
}
```

Logging

The details of the blocked IP addresses can be accessed from the files **<nginx-install-directory>/logs/blocking.log** and **<nginx-install-directory>/logs/error.log**. To find the IP addresses that are blocked, run the following commands from the directory **<nginx-install-directory>/logs.**

```
grep "will be blocked for" blocking.log
grep "IP is already blocked." error.log
2021/10/29 17:30:59 [emerg] 1181750#1181750: *19 [lua] block_unauthorized_users.lua:153:
_redirectAndSendError(): 10.68.218.190
will be blocked for 30 minutes for exceeding retry limit., client: 10.68.218.190, server:
saproxy.cisco.com, request: "GET
/finesse/api/SystemInfo?nocache=1636456574482 HTTP/2.0", host: "saproxy.cisco.com:8445",
referrer:
"https://saproxy.cisco.com:8445/desktop/container/?locale=en_US&"

2021/10/29 19:21:00 [error] 943068#943068: *43 [lua] block_unauthorized_users.lua:53:
10.70.235.30 :: IP is already blocked...,
client: 10.70.235.30, server: saproxy.cisco.com, request: "GET
/finesse/api/SystemInfo?nocache=1635591686497 HTTP/2.0", host:
"saproxy.cisco.com:8445", referrer:
"https://saproxy.cisco.com:8445/desktop/container/?locale=en_US"
```

It is recommended that customers integrate with **Fail2ban** or a similar intrusion prevention system to add the blocked IP addresses to the IPtable or firewall rules.

Install and Configure Fail2ban

Fail2ban can be configured to monitor the `blocking.log` to identify the IP addresses that are blocked by OpenResty Nginx on detecting brute force attacks, and ban the IP addresses for a configurable duration. Do the following to install and configure Fail2ban on a CentOS reverse-proxy:

SUMMARY STEPS

1. Install Fail2ban using yum
2. Create a local jail
3. Configure a filter
4. Start Fail2ban

DETAILED STEPS

Procedure

Step 1 Install Fail2ban using yum

```
yum update && yum install epel-release yum install fail2ban
```

Step 2 Create a local jail

Jail configurations allow the administrator to configure various properties such as the ports that are to be banned from being accessed by any blocked IP address, the duration for which the IP address stays blocked, the filter configuration used for identifying the blocked IP address from the log file monitored, and so on. Steps to add a custom configuration for banning IP addresses that are blocked from accessing the upstream servers are as follows:

a. Go to Fail2ban installation directory (in this example /etc/fail2ban)

```
cd /etc/fail2ban
```

b. Make a copy of jail.conf into jail.local to keep the local changes isolated.

```
cp jail.conf jail.local
```

c. Add the following jail configurations to the end of the file jail.local, and substitute the ports in the template with the actual ones. Update ban time configurations as required.

```
# Jail configurations for HTTP connections.
[finesse-http-auth]
enabled = true
# The ports to be blocked. Add any additional ports.
port = http,https,<finesse-ports>,<cuic-ports>,<any-other-ports-to-be-blocked>
# Path to nginx blocking logs.
logpath = /usr/local/openresty/nginx/logs/blocking.log
# The filter configuration.
filter = finesseban
# Block the IP from accessing the port, once the IP is blocked by lua.
maxretry= 1
# Duration for retry set to 3 mins. Doesn't count as the maxretry is 1
findtime= 180
# Lock time is set to 3 mins. Change as per requirements.
bantime = 180
```

Step 3 Configure a filter

A filter tells Fail2ban what to look for in the logs to identify the host to be banned. The steps to create a filter is as follows:

a. Create filter.d/finesseban.conf

```
touch filter.d/finesseban.conf
```

b. Add the following lines into the file filter.d/finesseban.conf

```
[Definition] # The regex match that would cause blocking of the host. failregex = <HOST> will be
blocked for
```

Step 4 Start Fail2ban

Run the following command to start fail2ban:

```
fail2ban-client start
```

Open fail2ban log files and verify that there are no errors. By default, logs for fail2ban go into the file `/var/log/fail2ban.log`.

Troubleshoot

Troubleshoot SELinux

Procedure

Step 1 If OpenResty Nginx is not started by default or the Finesse Agent Desktop is not accessible, set SELinux to **permissive** mode with this command:

```
setenforce 0
```

Step 2 Try to restart OpenResty Nginx with the **`systemctl restart nginx`** command.

Step 3 All the violations will be available in **/var/log/messages** and **/var/log/audit/audit.log**.

Step 4 You are required to regenerate the **.te** file with allow rules for addressing those violations by executing any one of the following commands:

- `cat /var/log/audit/audit.log | audit2allow -m nginx1 > nginx1.te. # this will create nginx1.te file`
- `ausearch -c 'nginx' --raw | audit2allow -M  my-nginx  # this will create my-nginx.te file`

Step 5 Update the original **nginx.te** file present in the **selinux-nginx-rhel-master-modified/nginx** directory with the newly generated allow rules.

Step 6 Compile the **nginx.te** file by using the **`make`** command.

Step 7 The **nginx.pp** file is regenerated.

Step 8 Load the policy by using the **semodule** command.

```
semodule -i nginx.pp
```

Step 9 Change SELinux to **enforce** mode by using the **setenforce** command.

Step 10 Reboot the system.

Step 11 Repeat this procedure until all the violations are fixed.

INDEX

A

AAR 132, 134, 281
  files 132
  management 281
  uploading files 134
active server 5, 143–144
administrator privileges 250
Administrator User Group 209
agent 34, 225, 249, 251
  capabilities 249
  configuring 34
  handling callbacks 225
  user privileges 251
alarm settings 512, 535–536
alarms 512–513
  alarms 513
    destinations 513
  configuration overview 512
  configuration settings 513
  Event Level 513
  overview 512
  viewing information 512
All Users Group 209
alternative pronunciation 252
  Call by Name window 252
  Call by Name window, how to add 252
application 2, 6, 49, 179–180, 184, 279, 689
  by package license 689
  management 279
  report 179–180, 184
  server 2
  subsystem 6
  triggers 49
architecture, cluster 4
ASR 77–78
  overview 77
  provisioning 78
automatic failover 5, 143–144
Automatic Speech Recognition, *See* ASR

B

best practices 216
  security 216
busy application 46
  about 46
  provisioning 46

C

cache size 227
  contact records 227
call control channel 60
call waiting 221
  disabling in Unified CM 221
calling search space 70
  ignore setting 70
  restrict users 70
  Unified CM Telephony trigger setting 70
  usage 70
campaigns 220, 226
  Outbound subsystem 220
  time changes 226
capabilities 249
  users 249
channels 60
  provisioning 60
Cisco IP Agent and Supervisor desktops 1
  about 1
Cisco Media subsystem 6, 75
  about 6
  provisioning 75
Cisco Script Application 43–44, 49
  adding 43–44
  adding a trigger 49
Cisco Security Agent 218
  usage 218
Cisco TelePresence application 36
Cisco Unified CCX Administration web interface 1, 16, 19–20
  about 1
  configuration web pages 19
  menu bar and menus 16
  using navigation bars 20
Cisco Unified CCX applications 43
  configuration overview 43
Cisco Unified CCX cluster 143
  profile 143
Cisco Unified CCX component availability 690
  by package license 690

Cisco Unified CCX components 1
Cisco Unified CCX Editor, about 1
Cisco Unified CCX Engine 6
about 6
Cisco Unified CCX Engine subsystems 6
Applications 6
Cisco Media 6
Core Reporting 6
Database 6
eMail 6
HTTP 6
MRCP ASR 6
RmCm 6
TTS 6
Unified CM Telephony 6
Cisco Unified CCX product family 2–3, 6
about 2
Unified CCX 3
Unified IP IVR 3, 6
Cisco Unified CCX Server, about 1
Cisco Unified CCX supervisor web interface 251
Cisco Unified CCX user options web interface 252
Cisco Unified Communications components 1
about 1
Cisco IP Agent and Supervisor desktops 1
Cisco Unified CCX Admnistration web interface 1
Cisco Unified CCX Editor 1
Cisco Unified CCX Server 1
Cisco Unified Gateway 1
historical reports database server 1
MRCP ASR server 1
MRCP TTS 1
Unified CM 1
Cisco Unified IP IVR, about 6
Cisco Unified Real-Time Monitoring Tool., *See* RTMT
CLI 531
starting services 531
stopping services 531
cluster 4–5
active server 5
architecture 4
cluster manager 5
cluster view daemon 5
cluster, definition 143
CM Telephony 286
Call Control group configuration 286
provider configuration 286
triggers 286
CMT dialog channels, about 75
CMT dialog group 75
about 75
CMT dialog interactions, about 75
component, definition 143
Computer Telephony Interface, *See* CTI
configuration 1
datastore server 1
Configuration datastore, contents 532
configuration updates 226
Outbound subsystem 226
configuring, definition 7
Contact Service Queues 99, 104–105
about 99
creating 99
deleting 105
modifying 104
contact summary report 217
Outbound 217
contacts report 181
Control Center 528, 530
network services 528
overview 528
starting services 530
stopping services 530
viewing status 530
Core Reporting subsystem, about 6
CPU utilization 52
and VRU scripts 52
CSQ 3, 99, 226, 291
about 3
creating 291
Outbound percentage 226
resource based 99
skill based 99
CSQ Cisco Unified CCX Stats report 189
CTI 6, 70
managing clusters 6
port device and route point 70
custom 267
classpaths for custom classes, steps, subsystems 267
custom file configuration 267
custom file configuration (System menu) 132

D

daily purge schedule 168
about 168
configuring 168
database 117–118, 329
maximum connections 117–118
parameter 329
password 117–118
username 117–118
Database 218
in service 218
database connectivity 119
polling 119
Database subsystem 6, 115, 117–118, 341
about 6, 115, 117
adding JDBC datasource 117
configuration overview 117
configuration web page 118

Database subsystem *(continued)*
configuring 117
defining ODBC datasource 341
supported Enterprise Databases 117
datasource usage report 185
datasource, adding 328
datastore 531
failover support and high availability 531
Datastore 532
Control Center, overview 532
Daylight Savings Time, *See* DST
db_cra database 225
area code mapping 225
default time zone 243
devices 690
by package license 690
dialing functionality 217
dialing mode 217, 221
direct preview 217, 221
Directory Number 31
associations 31
Directory Number information 70
Do Not Call list 218
Outbound subsystem 218
do_not_call list 218
national 218
document file 129
unzipping after upload 129
documents 126
about 126
DST 242
Outbound subsystem 242

E

eMail subsystem 6, 115, 120
about 6, 115, 120
configuring 120
enabling campaigns 242
engine tasks report 180
execute permission 211

F

failover 5
automatic 5
failover support 531
feature, definition 143
files 129
adding zip 129

G

general properties 222
Outbound subsystem 222
geographic region 218
Outbound support 218
grammars 124
about 124
Group 209

H

handling callbacks 225
Help menu 357–358
About 358
Contents and Index 357
For this Page 358
high availability 144, 531
Historical datastore, contents 532
historical report user capabilities 249
historical report user privileges 250
historical reporting 1, 13
client 1
configuration overview 13
historical reporting database 166, 168, 170
configuring daily purge schedule 168
configuring database server 166
file restore 170
purge configuration 168
historical reports database 169
purging manually 169
historical reports database server 1
about 1
HTTP subsystem 6, 115
about 6, 115
configuration overview 115
HTTP triggers, adding 51

I

Integrated Service Router, *See* ISR
international area codes 218
mapping 218
invalid number 225
handling callbacks 225

J

JDBC datasource 117–118
adding 117–118

L

LDAP server information (System menu) 145
license 10, 70, 115, 117, 120, 689–690
adding components 10
application availability 689
Cisco Unified CCX component availability 690
database subsystem 117

license *(continued)*
eMail subsystem 120
HTTP subsystem 115
product 70
service availability 690
subsystem availability 689
trigger availability 689
logging alarms 512, 535–536
logout 278
logout (System menu) 164

M

manage scripts 279
managing users 249
master service, definition 143
media channel 60
missed callback 225
MRCP ASR 78–79, 81
groups configuration 81
provider configuration 78
provisioning 78
server configuration 79
MRCP ASR server, about 1
MRCP ASR subsystem 6, 78
about 6
configuration overview 78
provisioning 78
MRCP TTS 83, 86
locals configuration 86
provider configuration 83
provisioning 83
MRCP TTS server, about 1
MRCP TTS subsystem 6, 83
about 6, 83
provisioning 83
multiple time zones 243

N

national do_not_call list 218
network services 529
Control Center 529
overview 529
starting 529
stopping 529
viewing status 529
nickname 252
node, definition 143

O

ODBC datasource 117, 341
about 117
defining 341
Outbound 221
licensed seat 221
Outbound subsystem 218
Do Not Call list 218
Outbound Subsystem 218
in service 218
output settings for trace 523
Overall Unified CCX Stats report 186
overview 529
network services 529

P

pending records 242
Outbound subsustem 242
pending state 226
Permissions 211
and User Groups 211
plug-ins 337
point system for provisioning channels 60
product 70
licenses 70
product license 115, 117, 120
database subsystem 117
eMail subsystem 120
HTTP subsystem 115
profile, cluster 143
prompts 123, 130–131
about 123, 130
adding spoken name prompt 131
provisioning checklist 61
telephony and media resources 61
provisioning, definition 7
publisher 5, 531
cluster manager 5
database 531
purge configuration 168
parameters 168
purging 168
automatic 168
manual 168
purging, manually 169

Q

queuing calls 74
with Unified CCX 74

R

read permission 211
real-time reports 171, 173–175, 178–181, 185–186, 189–190, 198
application tasks 180
application tasks summary 179
available reports 171

real-time reports *(continued)*
contact summary 178
contacts 181
CSQ Cisco Unified CCX Stats 189
datasource usage 185
engine tasks 180
Overall Unified CCX Stats 186
printing reports 174
resetting statistics 174–175
Resource Unified CCX Stats 190, 198
running reports 173
sessions 185
setting appearance 175
setting options 175
viewing subreports 174
Refresh All button 20
Repository datastore, contents 532
Resource based CSQ 99
resource groups 91–92, 290–291
creating 91, 290–291
deleting 92
modifying name 91
Resource Manager, about 3
Resource pool selection criteria 105–106
between skills and groups 105
within a CSQ 106
Resource Unified CCX Stats report 190, 198
resources 96–98, 290
assigning to resource groups and skills in bulk 97
assigning to resource groups and skills individually 96
modifying 290
removing skills from individual agents 98
resynchronizing 62, 75
Cisco JTAPI Client 62
Unified CM Telephony data 62
Unified CM Telephony information 75
Ring-No-Answer application 47
about 47
provisioning 47
RmCm provider 89
about 89
provisioning 89
RmCm subsystem 218
in service 218
RmCm subsystem, about 6
RNA application 47
about 47
provisioning 47
RTMT, using to collect and view alarms 512
Run As 214

S

scheduling callbacks 242
Outbound subsystem 242
script application 43–44
about 43–44
configuration overview 43–44
script management 52, 279
script repository 43–44
scripts 52, 54–57
about 52
deleting 57
refreshing 55
renaming 56
viewing or downloading 54
scripts, uploading 53
security 216
best practices 216
servers 143–144
active and standy 143–144
service 528–529
Control Center overview 528
network services 529
starting services 528
stopping services 528
service, definition 143
Session Initiation Protocol, *See* SIP
sessions report 185
SIP 6
router integration 6
Skill based CSQ 99
skills 92–94, 98, 292
creating 92, 292
deleting 94
modifying name 93
removing 292
removing from individual agents 98
spoken name prompt 131
adding 131
standby server 143–144
standby service, definition 143
subscriber 5, 531
cluster manager 5
database 531
subsystems 689
by package license 689
Subsystems menu 76, 285–286, 289–292, 328, 330–332
Add a New Dialog Control Group 76
adding HTTP triggers 330
agent-based routing 292
assigning skills 292
Cisco Media 331
CM Telephony 285
CM Telephony Call Control group configuration 286
CM Telephony provider configuration 286
CM Telephony triggers configuration 286
database configuration 328
eMail 330
HTTP 330
MRCP ASR 331

Subsystems menu *(continued)*
MRCP TTS 332
resource group 290
resources 290
RmCm provider 291
skills configuration 289
teams 292
Unified CCX 289
supervisor capabilities 249
supervisor privileges 250
System menu 132, 145, 164, 259, 267, 278
custom file configuration 132, 267
LDAP Information 145
logout 164, 278
system parameters 145, 259
systems parameters (System menu) 145, 259

T

team 110–111, 113, 293–294, 296
creating a team 110, 293
deleting a team 113, 296
making changtes to agents on a team 111, 294
Text-to-speech, *See* TTS
time zone 225, 242
determining local time 242
handling callbacks 225
toolbar 20
using 20
Tools menu 176, 178–181, 185–186, 189–190, 198, 200–202, 204, 337, 339, 343, 345, 347–348
application task summary 179
application tasks 180
Clear Contact 201
contact summary report 178
contacts 181
CSQ Unified CCX Stats 189
datasource usage 185
engine tasks 180
file restore 345
historical reporting 343
Open Printable Report 201
Options 204
overall Unified CCX Stats 186
plug-ins 337
purge now 345
purge schedule 345
real-time snapshot config 339
Refresh Connections 201
report 176
Reset All Stats 200
Resource Unified CCX Stats 190, 198
sessions 185
Tools 200
user configuration 345
user management, Name Grammar Generation 347
Tools menu *(continued)*
user management, Spoken Name Upload 348
Views 202
Tools meny 204
Settings 204
trace 514, 523
configuration overview 514
output settings 523
trace files 514, 518, 523
facilities 518
interpreting 523
level options 518
subfacilities 518, 523
viewing and interpreting 523
triggers 689
by package license 689
triggers and applications 49
TTS 77, 83–84
default provider 84
overview 77
provisioning 83
VXML applications 84

U

UNICODE 83
Unified CCX 3
about 3
Unified CCX components 3
CSQ 3
Resource Manager 3
Unified CCX Enhanced with CTI Option, about 3
Unified CCX Enhanced, about 3
Unified CCX Standard, about 3
Unified CM 30, 253
connecting to web interface 30
users 253
Unified CM telephony 61
configuration 61
Unified CM Telephony 70
trigger information 70
Unified CM Telephony information, resynchronizing 75
Unified CM Telephony subsystem 6, 61, 63, 70, 218
about 6
configuration overview 61
configuring Unified CM Telephony providers 63
in service 218
provisioning Unified CM Telephony trigger 70
Unified CM Telephony trigger 49
adding 49
Unified CM Telephony triggers 74
using with Unified CCX 74
Unified CM User Options page 253
Unified Communications Manager 31
configure users 31

Unified ICME 6
about 6
Unified ICME subsystem 115
about 115
Unified IP IVR, about 3
uploading licenses 10
uploading scripts 53
User Groups 209, 211
Administrator User Group 209
and Permissions 211
Child Groups 209
Groups 209
User Permissions 211
write, read, and execute 211
user roles 249
users 31, 214
configuring in Unified Communications Manager 31
Run As 214

V

viewing alarm information 512
virtual agents 36
virtual infrastructure 36
voice gateways 1
VRU scripts 52
uploading time 52
VXML applications 84
default TTS provider 84

W

wizards 20
using 20
Wizards menu 333–334
Application 333
RmCm 334
wrap-up data 108
usage 108
write permission 211

Z

zip files, uploading 129