THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.
CONTENTS

PREFACE

Preface xxv
Change History xxv
About This Guide xxvi
Audience xxvii
Conventions xxvii
Related Documents xxix
Documentation and Support xxix
Documentation Feedback xxx

CHAPTER 1

Unified CCX Introduction 1
Unified CCX Components 1
Unified CCX Product Family 3
Unified IP IVR 3
Unified Contact Center Express 3
Unified CCX Cluster Architecture 5
Unified CCX Active Server 5
Unified CCX Engine 6
Set Up Unified CCX 7
Provision Telephony and Media Subsystems 7
Configure Unified CCX Subsystems 8
Provision Unified CCX Subsystem 8
Provision Additional Unified CCX Subsystems 9
View License Information 9
Upload Licenses 10
Configure Unified CCX Applications 11
Available Applications 11
<table>
<thead>
<tr>
<th>Chapter 2: Unified CCX Administration Web Interface</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Unified CCX Administration Web Interface</td>
<td>13</td>
</tr>
<tr>
<td>Cisco Unified CCX Administration Menu Bar and Menus</td>
<td>15</td>
</tr>
<tr>
<td>Cisco Unified CCX Administration Navigation</td>
<td>16</td>
</tr>
<tr>
<td>Unified CCX Configuration Web Pages</td>
<td>17</td>
</tr>
<tr>
<td>Details for Advanced Configuration</td>
<td>18</td>
</tr>
<tr>
<td>Toolbar and Buttons</td>
<td>18</td>
</tr>
<tr>
<td>Application and RmCm Wizards</td>
<td>19</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 3: Unified CCX Provision Checklist</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified CCX</td>
<td>21</td>
</tr>
<tr>
<td>Provision Unified CCX</td>
<td>22</td>
</tr>
<tr>
<td>Change Licensing Packages</td>
<td>23</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 4: Provision Unified CM for Unified CCX</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Unified Communications Manager Information</td>
<td>25</td>
</tr>
<tr>
<td>Modify AXL Information</td>
<td>25</td>
</tr>
<tr>
<td>Modify Unified Communications Manager Telephony Information</td>
<td>27</td>
</tr>
<tr>
<td>Modify RmCm Provider Information</td>
<td>29</td>
</tr>
<tr>
<td>Unified Communications Manager for Unified CCX Configuration</td>
<td>30</td>
</tr>
<tr>
<td>Invoke Unified Communications Manager Administration</td>
<td>31</td>
</tr>
<tr>
<td>Unified Communications Manager Users as Unified CCX Agents</td>
<td>31</td>
</tr>
<tr>
<td>Guidelines for Agent Phone Configuration</td>
<td>33</td>
</tr>
<tr>
<td>Modify Existing Unified Communications Manager Users</td>
<td>34</td>
</tr>
<tr>
<td>Assign Unified Communications Manager Users as Cisco TelePresence Virtual Agents</td>
<td>37</td>
</tr>
<tr>
<td>Configure Tool for Auto-Registered Phones Support (TAPS)</td>
<td>38</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 5: Update Unified CM IP Address Change in Unified CCX</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Unified CM IP Address Change in Unified CCX</td>
<td>41</td>
</tr>
</tbody>
</table>
CHAPTER 6  
Cisco Applications Configuration 43
  - About Unified CCX Applications 43
  - Configure Script Applications 43
  - Add New Cisco Script Application 45
  - Configure Busy Application 46
  - Configure Ring-No-Answer Application 47

Application Triggers 48
  - 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
Contents

<table>
<thead>
<tr>
<th>Chapter 9</th>
<th>Provision of Additional Subsystems 111</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About Additional Subsystems 111</td>
</tr>
<tr>
<td></td>
<td>Provision of HTTP Subsystem 112</td>
</tr>
<tr>
<td></td>
<td>Configure HTTP Triggers 112</td>
</tr>
<tr>
<td></td>
<td>Provision of Database Subsystem 113</td>
</tr>
<tr>
<td></td>
<td>Database Subsystem Configuration 113</td>
</tr>
<tr>
<td></td>
<td>Add New Datasource 114</td>
</tr>
<tr>
<td></td>
<td>Datasource Configuration Web Page 114</td>
</tr>
<tr>
<td></td>
<td>Poll Database Connectivity 115</td>
</tr>
<tr>
<td></td>
<td>Provision eMail Subsystem 116</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 10</th>
<th>Management of Prompts, Grammars, Documents, and Custom Files 119</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Manage Prompt Files 119</td>
</tr>
<tr>
<td></td>
<td>Manage Grammar Files 121</td>
</tr>
<tr>
<td></td>
<td>Manage Document Files 122</td>
</tr>
<tr>
<td></td>
<td>Language Management 123</td>
</tr>
<tr>
<td></td>
<td>Create New Language 124</td>
</tr>
<tr>
<td></td>
<td>Rename Language 124</td>
</tr>
</tbody>
</table>
Contents

Delete Language  125
Upload Zip Files to Language Folder  125
Upload of Prompt Files  126
Record a Prompt  127
Add Spoken-Name Prompts  128
Management of Custom Files  129
  Specify Custom Classpath Entries  129
AAR File Management  130
  AAR File Creation  131
Upload AAR Files  131
META-INF Directory  132
Directories for Prompts, Grammars, Documents, and Scripts  132
  Prompts Directory  133
  Grammars Directory  133
  Documents Directory  133
  Scripts Directory  133
AAR Manifest  133
Attribute Types  135
  Main Attributes  135
  Per-entry Attributes  137
  META-INF Directory Attributes  137

CHAPTER 11
Unified CCX System Management  141
  Basic Terminology  141
  High Availability and Automatic Failover  142
    Network Partitions  143
Unified CCX CDS Information Management  143
Manage System Parameters  143
Unified CCX IP Address/hostname Management  144
  Prepare System for IP Address/hostname Change  144
  IP Address Modification  146
    Change IP Address for Server in Single-Node Deployment  146
    IP Address Modification in High-Availability (HA) Deployment  148
  Host Name Modification  152

Cisco Unified Contact Center Express Administration and Operations Guide, Release 11.6(1)
Chapter 12

Unified CCX Reporting 161

Reporting Administration on Unified CCX 161

Import of Stock Reports 161

Unified CCX Historical Reports 161

Unified CCX Historical Datastore 161

Historical Reporting Configuration 162

Purge of Historical Data 163

File Restore 166

Unified CCX Real-Time Reports 166

Available Unified CCX Real-Time Reports 167

Open Real-Time Reports 168

Run Reports 169

View Detailed Subreports 169

Print Reports 170

Reset Report Statistics 170

Clear Contact Option for Stuck Calls 170

Set Report Options 170

Set Report Appearance 171

Application Reporting User Interface 171

Reporting Administration on Unified Intelligence Center 204

Overview 204

Start Unified Intelligence Center 207

Administrator Overview 207

Security Overview 207

User List 208
Create a User 209
User Groups 210
   About User Groups 211
   Create a User Group 211
Manage User Permissions 212
   About Permissions 212
   User Roles and Permissions 213
   Assigned Group Permissions 214
   Assigned User Permissions 215
Run As 215
Audit Trail Logging in Cisco Unified Intelligence Center 216
   View Audit Trail Logging in Unified Intelligence Center 216
Audit Trail Report 216
Security Considerations 217

CHAPTER 13
Unified CCX Outbound Dialer Configuration 219
   Outbound Feature for Unified CCX 219
   Outbound Characteristics 219
   Unified CCX Requirements 220
   Outbound Components 222
Supported Dialers and Dialing Modes for Outbound 222
   Unified CCX Outbound Dialing Modes 223
   Direct Preview Dialing Mode 223
   Progressive Dialing Mode 223
   Predictive Dialing Mode 223
Configure Outbound Subsystem in Unified CCX 224
Configure General Outbound Properties 224
   Callbacks 227
   Outbound Area Code Functionality 228
   Configuration Updates 228
   CSQ Agent Pool Allocation 229
Configure Application and Trigger for Outbound Campaign 229
Add New Campaign 230
Import Contacts for Campaign 240
Custom File Configuration 268
Standalone Cisco Unified Intelligence Center Configuration 268
License Information 269
  Add Licenses 269
  Display Licenses 269
Language Information 270
Logout Menu 271

CHAPTER 16

Applications Menu 273
  Access Application Management Menu 273
  Manage Scripts 274
  Prompt Management 274
  Grammar Management 275
  Document Management 275
  AAR Management 276

CHAPTER 17

Subsystems Menu 277
  Unified CM Telephony Menu 278
    Unified CM Telephony Provider Configuration 278
    Unified CM Telephony Call Control Group Configuration 278
    Unified CM Telephony Triggers Configuration 279
    Synchronize Unified CM Telephony Data 279
    Unified CM Telephony Cisco JTAPI Resync 280
    Unified CM Telephony Advanced Settings 280
  RmCm Menu 281
    Skill Configuration 281
      Add New Skill 281
      Modify Skills 282
    Resources Configuration 282
      Modify Resource 282
    Resource Group Configuration 283
      Add New Resource Group 283
      Modify Existing Resource Groups 283
    Contact Service Queues Configuration 283
Administration Tools 344
Manage System Settings 351
  Context Service Settings 351
Manage Call Variables Layouts 353
  Call Variables Layouts 353
  Call Variables 354
  Configure Call Variables Layouts 354
  Add ECC Variables to Call Variables Layout 356
  Assign Call Variables Layouts 356
  Manipulate Call Variables Layouts with a Workflow 357
Manage Desktop Layout 357
  Finesse Desktop Layout XML 357
  Default Layout XML 358
  Update Default Desktop Layout 358
  XML Schema Definition 359
  Add Web Chat and Email to Finesse 361
Live Data Gadgets 368
Live Data Reports 373
Manage Phone Books 375
  Phone Books and Contacts 375
  Add Phone Book 376
  Edit Phone Book 376
  Delete Phone Book 377
  Import Contacts 377
  Export Contacts 378
  Add Contact 378
  Edit Contact 379
  Delete Contact 379
Manage Reasons 379
  Not Ready Reason Codes 380
  Sign Out Reason Codes 382
  Predefined System Reason Codes 385
  Manage Reason Code Conflicts During Upgrade 387
Wrap-Up Reasons 388
Manage Team Resources 390
  Team Resources 390
  Assign Phone Books and Reasons to Team 392
  Unassign Phone Books and Reasons from Team 392
  Assign Custom Desktop Layout to Team 393
  Assign Workflows to Team 393
  Unassign Workflows from Team 394
Manage Workflows 394
  Workflows and Workflow Actions 394
  Add Browser Pop Workflow Action 398
  Add HTTP Request Workflow Action 399
  Edit Workflow Action 400
  Delete Workflow Action 400
  Add Workflow 401
  Edit Workflow 401
  Delete Workflow 402
Manage Security 402
  HSTS 402
Manage Finesse IP Phone Agent 403
  Finesse IP Phone Agent 403
  One Button Sign In 403
  Finesse IP Phone Service Subscription Options 404
  Set Up Application User, Web Access, and HTTPS Server Parameters 405
  Configure Finesse IP Phone Service in Unified CM 406
  Add Service Parameters for One Button Sign In 408
  Subscribe Agent Phones to Manual Subscription Service 410
  Set Up Agent Access to the Self Care Portal 411
Backup and Restore 411
  Additional Language Support 412
Cisco Finesse Agent and Supervisor Desktop 412
Call Manager-Based Call Recording Using Cisco MediaSense 412
  Configure Cisco MediaSense with Unified CM 412
  Upload Cisco MediaSense Certificate to Unified CCX Server 413
  Upload MediaSense Recording License 413
CHAPTER 26
Backup and Restore 463
  Important Considerations 464
  SFTP Requirements 465
  Master and Local Agents 465
    Master Agent Duties 465
    Local Agent Duties 466
  Backup Tasks 466
    Manage Backup Devices 466
    Manage Backup Schedules 467
    Perform Manual Backup 467
    Check Backup Status 468
  Restore Scenarios 468
    Restore SA or HA Setup (Without Rebuild) 469
    Restore SA Setup (with Rebuild) 469
    Restore Only First Node in HA Setup (with Rebuild) 470
    Restore Second Node in HA Setup (with Rebuild) 471
    Restore Both Nodes in HA Setup (with Rebuild) 472
  Trace Files 473
Command Line Interface 473
  Command Line Interface Basics 475
    Start CLI Session 475
    Get Help with Commands 476
    Exit Command with Ctrl-C Key Sequence 477
    End CLI Session 477
    Additional CLI Commands 477
  Show commands 478
    show uccx version 478
    show uccx jtapi_client version 479
    show uccx components 479
    show uccx subcomponents 480

APPENDIX A
Command Line Interface 475
  Command Line Interface Basics 475
    Start CLI Session 475
    Get Help with Commands 476
    Exit Command with Ctrl-C Key Sequence 477
    End CLI Session 477
    Additional CLI Commands 477
  Show commands 478
    show uccx version 478
    show uccx jtapi_client version 479
    show uccx components 479
    show uccx subcomponents 480
set uccx provider ip axl 502
set uccx provider ip jtapi 503
set uccx provider ip rmcm 503
set uccx appadmin administrator 504
set authmode 505
run Commands 505
  run uccx hrdataexport 505
  run uccx sql database_name sql_query 506
  run uccx sp database_name sp_name 507
Utils Commands 508
  utils uccx notification-service log 508
  utils remote_account 509
  utils reset_application_ui_administrator_name 510
  utils reset_application_ui_administrator_password 511
  utils service 511
  utils system upgrade 512
  utils system switch-version 513
  utils uccx database dbserver integrity 514
  utils uccx list license 514
  utils uccx delete license licenseName 515
  utils uccx jtapi_client update 516
  utils uccx prepend custom_classpath 516
  utils uccx switch-version db-check 517
  utils uccx switch-version db-recover 517
  utils uccx syncusers 518
  utils uccx synctocuic 518
  utils uccx icd clid status 519
  utils uccx icd clid enable 519
  utils uccx icd clid disable 520
  utils uccx icd clid header 520
  utils uccx icd clid prefix 520
  utils uccx security_filter enable 521
  utils uccx security_filter disable 521
  utils uccx security_filter status 522
utils ucxx dbreplication dump configfiles 522
utils ucxx database healthcheck 523
utils ucxx database dbperf start 523
utils ucxx database dbperf stop 524
utils ids sync-security-config 524

File Commands 525
file ucxx view 525
file ucxx list custom_file 525
file ucxx list prompt_file 526
file ucxx get 527
file ucxx tail 528
file ucxx dump 528
file ucxx delete 529

High Availability Commands 530
show ucxx dbreplication tables 530
show ucxx dbreplication servers 531
utils ucxx modify remote_IPAddress 531
utils ucxx modify remote_hostname 532
utils ucxx database forcedataasync 533
utils ucxx setuppubrestore 533
utils ucxx dbreplication setup 534
utils ucxx dbreplication status 534
utils ucxx dbreplication templatestatus 535
utils ucxx dbreplication repair 536
utils ucxx dbreplication start 536
utils ucxx dbreplication stop 537
utils ucxx dbreplication reset 537
utils ucxx dbreplication teardown 538

Cisco Finesse Commands 538
utils reset_3rdpartygadget_password 538

Cisco Finesse Trace Logging 539
Cisco Finesse Toaster Notifications 540
Cisco Finesse IPPA Inactivity Timeout 540

Cisco Unified Intelligence Center Commands 541
Preface

- Change History, on page xxv
- About This Guide, on page xxvi
- Audience, on page xxvii
- Conventions, on page xxvii
- Related Documents, on page xxix
- Documentation and Support, on page xxix
- Documentation Feedback, on page xxx

Change History

This table lists changes made to this guide. Most recent changes appear at the top.
<table>
<thead>
<tr>
<th>Change</th>
<th>See</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Release of Document for Release 11.6(1)</td>
<td></td>
<td>August 2017</td>
</tr>
<tr>
<td>Unified CCX System Management</td>
<td>Manage System Parameters</td>
<td></td>
</tr>
<tr>
<td>Unified CCX Outbound Dialer Configuration</td>
<td>Import Contacts for Campaign</td>
<td></td>
</tr>
<tr>
<td>Subsystems &gt; Chat and Email Menu Options</td>
<td>Mail Server Configuration</td>
<td></td>
</tr>
<tr>
<td>Subsystems &gt; Chat and Email Menu Options</td>
<td>Wrap-Up Reason</td>
<td></td>
</tr>
<tr>
<td>Subsystems &gt; Chat and Email Menu Options</td>
<td>Email Signatures and Email Signature Configuration</td>
<td></td>
</tr>
<tr>
<td>Subsystems &gt; Chat and Email Menu Options &gt; List Chat form</td>
<td>Chat Web Form Configuration</td>
<td></td>
</tr>
<tr>
<td>Tools</td>
<td>Plug-ins</td>
<td></td>
</tr>
<tr>
<td>Tools</td>
<td>Real-Time Reporting Tool</td>
<td></td>
</tr>
<tr>
<td>Tools</td>
<td>Context Service Status</td>
<td></td>
</tr>
<tr>
<td>Command Line Interface</td>
<td>show ucxx livedata connections</td>
<td></td>
</tr>
<tr>
<td></td>
<td>show tls server min-version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>show tls client min-version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set tls server min-version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set tls client min-version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>utils cuic user make-admin</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified CCX Serviceability &gt; Tools</td>
<td>Network Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Context Service Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default Layout XML</td>
<td></td>
</tr>
</tbody>
</table>

**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 CCX Administration web interface.

This guide will help you to:

- Perform initial configuration tasks
- Administer applications such as the Unified CCX Engine and other components of the Cisco Unified Communications family of products
- Familiarize yourself with the menus and menu options of the Unified CCX Administration 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.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong> font</td>
<td>Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example:</td>
</tr>
<tr>
<td></td>
<td>• Choose <strong>Edit &gt; Find</strong></td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Finish</strong>.</td>
</tr>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><em>italic</em> font</td>
<td>Italic font is used to indicate the following:</td>
</tr>
<tr>
<td></td>
<td>• To introduce a new term. Example: <em>A skill group</em> is a collection of agents who share similar skills.</td>
</tr>
<tr>
<td></td>
<td>• For emphasis. Example: <em>Do not</em> use the numerical naming convention.</td>
</tr>
<tr>
<td></td>
<td>• An argument for which you must supply values. Example:</td>
</tr>
<tr>
<td></td>
<td>IF (<em>condition, true-value, false-value</em>)</td>
</tr>
<tr>
<td></td>
<td>• A book title. Example:</td>
</tr>
<tr>
<td></td>
<td>See the <em>Cisco Unified Contact Center Express Installation Guide</em>.</td>
</tr>
<tr>
<td><em>window</em> font</td>
<td>Window font, such as Courier, is used for the following:</td>
</tr>
<tr>
<td></td>
<td>• Text as it appears in code or information that the system displays. Example:</td>
</tr>
<tr>
<td></td>
<td><code>&lt;html&gt;&lt;title&gt; Cisco Systems,Inc. &lt;/title&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td></td>
<td>• File names. Example:</td>
</tr>
<tr>
<td></td>
<td>tserver.properties.</td>
</tr>
<tr>
<td></td>
<td>• Directory paths. Example:</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files\Adobe</td>
</tr>
<tr>
<td>string</td>
<td>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.</td>
</tr>
<tr>
<td>[]</td>
<td>Optional elements appear in square brackets.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Angle brackets are used to indicate the following:</td>
</tr>
<tr>
<td></td>
<td>• For arguments where the context does not allow italic, such as ASCII output.</td>
</tr>
<tr>
<td></td>
<td>• A character string that the user enters but that does not appear on the window such as a password.</td>
</tr>
</tbody>
</table>
### Convention

| ^ | 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

<table>
<thead>
<tr>
<th>Document or Resource</th>
<th>Link</th>
</tr>
</thead>
</table>

**Note**

From Unified CCX Release 12.5(1), CCP documents are available in the Cisco Unified CCX documentation folder.

<table>
<thead>
<tr>
<th>Document or Resource</th>
<th>Link</th>
</tr>
</thead>
</table>

### Documentation and Support


You can also subscribe to the *What's New in Cisco Product Documentation* RSS feed to deliver updates directly to an RSS reader on your desktop. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.
Documentation Feedback

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

contactcenterproducts_docfeedback@cisco.com
Unified CCX Introduction

Unified CCX provides a multimedia (voice, data, and web) IP-enabled customer-care application environment that enhances the efficiency of contact centers by simplifying business integration, easing agent administration, increasing agent flexibility, and enhancing network hosting.

All configuration values in Unified CCX must be entered in English language unless explicitly mentioned on the administration screen.

The following sections provide an overview of the configuration and management components of the Unified CCX product family:

- Unified CCX Components, on page 1
- Unified CCX Product Family, on page 3
- Unified CCX Cluster Architecture, on page 5
- Unified CCX Engine, on page 6
- Set Up Unified CCX, on page 7
- Manage Unified CCX, on page 12

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 CCX Engine 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. See the Cisco Unified Contact Center Express Serviceability Administration Guide.

- 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).

**Note**

If you are using Microsoft Internet Explorer Version 6.0 or later or Mozilla Firefox Version 2.0 or 3.0 browser, verify that the popup blocker is disabled.

- Cisco SocialMiner—Acts as the endpoint that hosts the widgets that end users and agents use during chat and email sessions. SocialMiner 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. SocialMiner 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 CCX Editor—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 IP 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.


- 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 CCX Engine and Unified CCX Editor.

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 scripted 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 Standard (designed for entry-level users)—Includes the steps necessary for creating basic Unified CCX applications, including Finesse IP Phone Agent (Finesse IPPA) and skills-based routing.

• Unified CCX Enhanced (designed for enterprise-level users)—Includes all functions of Unified CCX Standard, plus support for priority queuing. Includes a license to enable custom Java extensions.

• Unified CCX Enhanced—Includes the steps necessary for creating basic Unified CCX applications, including Finesse IP Phone Agent (Finesse IPPA), skills-based routing, and support for priority queuing.

• 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.

The Unified CCX Standard License is currently End of Sale.
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

Related Topics

Unified CCX IP Address/hostname Management, on page 144

Unified CCX Engine

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

The Unified CCX Engine 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 CCX Engine is implemented as a service that supports multiple applications.

You can use a web browser to administer the Unified CCX Engine 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 CCX Serviceability 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

If you are using Microsoft Internet Explorer Version 6.0 or later or Mozilla Firefox Version 2.0 or 3.0 browser, verify that the popup blocker is disabled.
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 CCX Engine and other features such as session management.

**Cisco Media**
Configures Cisco Media Termination (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 CCX Engine.

**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. You can assign skills to agents if you have a Unified CCX Standard license.

• **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**

  (Unified CCX Standard license) 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 CCX Administration 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 CCX Administration 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.
The number of In Use IVR ports and In Use agent seats are displayed only for the master node.

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 CCX Administration 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.

Configure Unified CCX Applications

After you provision the Unified CCX subsystems and view your license information, you need to configure Unified CCX applications to interact with contacts and perform a wide variety of functions.

To continue the Unified CCX system configuration process, connect to the Unified CCX Administration web interface and manage the following tasks:

- Available Applications, on page 11
- Manage Scripts Prompts, Grammars, and Documents, on page 11
- Wizards Menu, on page 315

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 Cisco script 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 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—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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Define the maximum number of database connections for report client sessions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Assign historical reporting capability to users.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure the Daily Purge Schedule and specify notification parameters.</td>
</tr>
</tbody>
</table>

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.
The Unified CCX provides a multimedia (voice, data, and web) IP-enabled customer-care application environment, using VoIP technology that allows your Cisco Unified Communications network to share resources with your data network.

You can then use a web browser located on any computer on the IP network to configure and administer your applications with the Unified CCX Administration web interface.

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

The Unified CCX Administration web interfaces (Cisco Unified CCX Administration and Cisco Unified CCX Serviceability) allows you to:

- Configure and monitor overall system functions, applications, and subsystems
- Access a wide variety of system tools
- Perform many other administrative tasks

The following sections provide more information about the Unified CCX Administration web interface:

- Access Unified CCX Administration Web Interface, on page 13
- Cisco Unified CCX Administration Menu Bar and Menus, on page 15
- Cisco Unified CCX Administration Navigation, on page 16
- Unified CCX Configuration Web Pages, on page 17

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.

• Verify that the popup blocker is disabled if you are using Microsoft Internet Explorer Version 6.0 or later or Mozilla Firefox Version 2.0 or 3.0 browser.

• Enable the compatibility mode if you are using Microsoft Internet Explorer Version 11.0.

Tip
Add the IP address of the Unified CCX server to the "Compatibility View Settings," to enable the compatibility mode in Microsoft Internet Explorer Version 11.0.

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 specified during installation of the Unified CCX. See the Cisco Unified Contact Center Express Install and Upgrade Guide for further instructions. The user ID is not case sensitive in Unified CCX 9.0(1).

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.
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.

---

### 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, Cisco Media, 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 end 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://FQDN:8445/cfadmin`, where `FQDN` is the fully-qualified domain name 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 CCX Administration 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.

<table>
<thead>
<tr>
<th>Icon/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy</td>
<td>Click this icon to copy the information in that specific row.</td>
</tr>
<tr>
<td>Note</td>
<td>When you click Copy, the web page displays the copied configuration so you can make changes, if desired.</td>
</tr>
<tr>
<td>Delete</td>
<td>Click this icon to delete the information in that specific row.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Click this icon to refresh the information in that specific row.</td>
</tr>
<tr>
<td>Refresh All</td>
<td>Click this button to refresh the information listed on this page.</td>
</tr>
</tbody>
</table>

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.

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. See the Cisco Unified Contact Center Enterprise installation and upgrade guides available at https://www.cisco.com/en/US/products/sw/custcsw/ps1844/prod_installation_guides_list.html for detailed information. 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 webpage 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**.
Unified CCX Provision Checklist

The Cisco Unified Communications Manager (CM) product supports both single-node and two-node (high availability) deployments available for the Cisco Unified Contact Center Express (CCX).

The deployment model is transparent to the Unified CCX installer as the clustering for Unified CM is performed through the Unified CCX Administration using the Unified CCX setup wizard. The high availability over WAN feature of Unified CCX is supported only for Unified CM deployments.

The following topics introduce the Unified CCX subsystem and explain how to modify the Unified CM information from Unified CCX.

- 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Unified CM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure Unified CM users who will be agents in your Unified CCX system.</td>
<td>Provision Unified CM for Unified CCX, on page 25</td>
</tr>
<tr>
<td>Step 2</td>
<td>Provision resources information for Unified CCX telephony and media.</td>
<td>Provision Unified CM Telephony Subsystem, on page 61</td>
</tr>
<tr>
<td>Step 3</td>
<td>Provision RmCm Provider to allow RmCm Subsystem to be in service.</td>
<td>RmCm Provider Configuration, on page 89</td>
</tr>
<tr>
<td>Step 4</td>
<td>Create resource groups.</td>
<td>Resource Groups, on page 91</td>
</tr>
<tr>
<td>Step 5</td>
<td>Create skills.</td>
<td>Skills Configuration, on page 92</td>
</tr>
<tr>
<td>Step 6</td>
<td>Assign agents to resource groups and assign skills to agents.</td>
<td>Agent Configuration, on page 94</td>
</tr>
<tr>
<td>Step 7</td>
<td>Create Contact Service Queues.</td>
<td>Contact Service Queue Configuration, on page 98</td>
</tr>
<tr>
<td>Step 9</td>
<td>Provision agent-based routing—if using Unified CCX Enhanced or Premium.</td>
<td>Configure Agent-Based Routing, on page 106</td>
</tr>
</tbody>
</table>
## Change Licensing Packages

The following three license upgrade options are available for Unified CCX system:

- Standard to Premium
- Standard to Enhanced
- Enhanced to Premium

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

- **Standard to Premium or Enhanced**—Only Enhanced and Premium package licenses support Recording. When you upgrade to Enhanced or Premium license package, you need to manually change the Recording Count to a desired value to enable the recording functionality.

- **Standard to Premium or Enhanced**—Only Enhanced and Premium package licenses support Recording.

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

- **Standard or 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.
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). 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.

Modify AXL Information

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AXL Service Provider Configuration</strong></td>
<td></td>
</tr>
</tbody>
</table>
| 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.  
**Note**  
If you deselect the AXL service provider from the Selected list box, a Microsoft Internet Explorer or Mozilla Firefox window opens, informing you about the (list of) deselected services. For security reasons (in case the service is being used by another AXL service provider), manually disable the AXL service only from the Unified Communications Manager. |
| 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. |
| 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.

---

**Note**

After regenerating the Unified Communications Manager certificates, restart the CTI Manager on Cisco Unified Communication Manager (CUCM) and the Unified CCX Engine on Unified CCX across all the clusters.

---

**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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unified CM Telephony Subsystem—Unified CM Telephony Provider Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Selected CTI Managers</td>
<td>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. <strong>Note</strong> If you deselect CTI Managers from the Selected list box, a Microsoft Internet Explorer or Mozilla Firefox window opens, informing you about the list of deselected CTI Managers. SRTP settings remain unchanged, even if the Selected CTI Managers are changed.</td>
</tr>
<tr>
<td>Available CTI Managers</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Cluster Wide Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>User Prefix</td>
<td>The syntax of the User ID is: <code>&lt;userprefix&gt;_&lt;nodeid&gt;</code> For example, if you set this field to <code>cti_user</code>, the User ID for Node 1 will be <code>cti_user_1</code>. This is a mandatory field.</td>
</tr>
<tr>
<td>Password</td>
<td>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.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Reenter the password that you provided in the Password field. This is a mandatory field.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RmCm Subsystems—RmCm Provider Configuration</strong></td>
<td></td>
</tr>
</tbody>
</table>
| 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**  
If you deselect CTI Managers from the Selected list box, a Microsoft Internet Explorer or Mozilla Firefox window opens, informing you about the (list of) deselected CTI Managers. |
### 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.

### 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 bytes.
**Attention**

Unified Communications Manager user ID should not exceed 31 bytes. If user ID exceeds 31 bytes, Unified CCX does not synchronize users from Unified Communications Manager.

### Agent Name

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

- English-based script (German, Spanish, English, etc)—50 bytes / 50 characters
- Non-English script (Arabic, Chinese, Cyrillic, etc)—48 bytes / 16 characters

**Attention**

Unified CCX truncates the name to 50 / 48 bytes and stores if the agent name exceeds the above limit.

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 have 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:

<table>
<thead>
<tr>
<th>System\Components</th>
<th>Reserved words</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified CCX Web Chat</td>
<td>admin</td>
</tr>
<tr>
<td>Cisco Finesse</td>
<td>admin</td>
</tr>
<tr>
<td></td>
<td>finesse</td>
</tr>
<tr>
<td></td>
<td>fippa</td>
</tr>
<tr>
<td></td>
<td>xmpprootowner</td>
</tr>
<tr>
<td></td>
<td>presencelistener</td>
</tr>
</tbody>
</table>
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.

  - 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.
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.

---

*Cisco Unified Contact Center Express Administration and Operations Guide, Release 11.6(1)*
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.

**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 Release 9.0(1) 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log into Cisco Unified Communications Manager Administration Release 9.0(1) and choose Application &gt; Plugins from the Cisco Unified Communications Manager Administration menu bar.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Find and List Plugins web page, search for “Cisco TAPS” and click Find.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Download the TAPS_AAR.aar file to your client PC, which is used for accessing Unified Communications Manager Administration and Unified CCX Administration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>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 (&lt;) 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.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Log into 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 &gt; 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.</td>
</tr>
</tbody>
</table>
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.
Configure Tool for Auto-Registered Phones Support (TAPS)
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.
Cisco Applications Configuration

The Unified CCX system uses applications to interact with contacts and perform a wide variety of functions, such as prompting callers for information, transferring calls, and providing information to callers.

To configure Unified CCX applications, you must complete the following tasks:

- Provision telephony and media resources (see Telephony and Media Provision, on page 59)
- Provision your Unified CCX subsystem, if required (see Provision of Unified CCX, on page 89)
- Provision additional subsystems, if required (see Provision of Additional Subsystems, on page 111)

The following sections describe how to configure applications and make them available to the Unified CCX system.

- About Unified CCX Applications, on page 43
- Application Triggers, on page 48
- 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 CCX Editor. These applications come with every Unified CCX system and execute scripts created in the Unified CCX Editor.
Use the Unified CCX Editor 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.

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.

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 CCX Editor 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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the Unified CCX Administration menu bar, choose Applications &gt; Application Management. The Application Management web page opens, displaying the details of any existing applications.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>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.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the Application Type drop-down menu, choose Cisco Script Application and click Next. The Cisco Script Application configuration Web page opens.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Specify the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the application. This is a mandatory field.</td>
</tr>
<tr>
<td>ID</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum Number Of Sessions</td>
<td>The maximum number of simultaneous sessions (instances) that the application can handle. This is a mandatory field.</td>
</tr>
<tr>
<td>Script</td>
<td>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</td>
</tr>
</tbody>
</table>
### 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 CCX Administration 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 toolbar 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the application. This is a mandatory field.</td>
</tr>
<tr>
<td>ID</td>
<td>Accept the automatically-generated ID, or enter a unique ID. This is a mandatory field.</td>
</tr>
<tr>
<td>Note</td>
<td>The Historical Reporting feature uses this ID to identify this application.</td>
</tr>
<tr>
<td>Maximum Number Of Sessions</td>
<td>The maximum amount of simultaneous sessions (instances) that the application can handle.</td>
</tr>
</tbody>
</table>

The following fields are displayed only on click of **Show More** button.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Use the Tab key to automatically populate this field.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Click the required radio button to accept - <strong>Yes</strong> (the default).</td>
</tr>
</tbody>
</table>

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

Procedure

Step 1
From the Unified CCX Administration 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the application. This is a mandatory field.</td>
</tr>
<tr>
<td>ID</td>
<td>Accept the automatically-generated ID, or enter a unique ID. This is a mandatory field.</td>
</tr>
<tr>
<td>Note</td>
<td>The Historical Reporting feature uses this ID to identify this application.</td>
</tr>
<tr>
<td>Maximum Number Of Sessions</td>
<td>The maximum amount of simultaneous sessions (instances) that the application can handle. This is a mandatory field.</td>
</tr>
</tbody>
</table>

The following fields are displayed only when you click the Show More button:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Use the Tab key to automatically populate this field.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Click the required radio button to accept - Yes (the default).</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>From the Trigger Type drop-down menu, choose Unified CM Telephony and click Next. The Unified CM Telephony Trigger Configuration window opens.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Follow the procedure described in Add Unified CM Telephony Trigger.</td>
</tr>
</tbody>
</table>

**Related Topics**

Add Unified CM Telephony Trigger, on page 70

**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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>From the Unified CCX Administration menu bar, choose Subsystems &gt; Unified CM Telephony &gt; Triggers. The Unified CM Telephony Trigger Configuration summary web page opens.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

Related Topics

Add Unified CM Telephony Trigger, on page 70

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 host name 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.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 CCX Administration 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>The relative URL. For example: /hello</td>
</tr>
<tr>
<td>Language</td>
<td>Perform one of the following actions:</td>
</tr>
<tr>
<td></td>
<td>• Choose a default language from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Edit</strong>, specify a default language in the dialog box that appears,</td>
</tr>
<tr>
<td></td>
<td>and click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Application Name</td>
<td>Choose the name of the application from the drop-down list.</td>
</tr>
<tr>
<td>Maximum Number Of Sessions</td>
<td>The maximum amount of simultaneous sessions that can be served by the HTTP subsystem for this trigger.</td>
</tr>
<tr>
<td>Idle Timeout (in ms)</td>
<td>Maximum amount of time (in milliseconds) that the system will wait to invoke the application before rejecting a contact.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Click the required radio button to accept - <strong>Yes</strong> (the default)</td>
</tr>
</tbody>
</table>

**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 and route calls to available agents, and place outbound calls.

The Script Management option of the Applications menu of the Unified CCX Administration web interface contains options for managing and refreshing Unified CCX scripts that are stored in the repository.
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. In Unified CCX Release 4.5 and later, uploaded scripts are stored in the Repository Datastore (RDS) database, along with prompts, grammars, and documents files. Prior to Release 4.5, the RDS database only contained the prompts, grammars, and documents files. The scripts can also be grouped into folders and subfolders. When user scripts are uploaded into repository, they get synchronized to local disk and are accessed from there.

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

### Procedure

**Step 1**

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

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder Path</td>
<td>The level of the directory that is currently selected in the folder drop-down list.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the script.</td>
</tr>
<tr>
<td>Note</td>
<td>Click the icon in front of the script name to download the script file.</td>
</tr>
<tr>
<td>Size</td>
<td>The size of the script file prefixed with <strong>KB</strong>. The file size is converted from bytes to KB.</td>
</tr>
<tr>
<td>Note</td>
<td>This column is usually blank on the root page as the items on this page are usually folders.</td>
</tr>
<tr>
<td>Date Modified</td>
<td>The date and time when the document was last uploaded or changed along with time zone.</td>
</tr>
<tr>
<td>Modified by</td>
<td>The user ID of the person who performed these modifications.</td>
</tr>
</tbody>
</table>
### Download Script File

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

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the Unified CCX Administration menu bar, choose <strong>Applications &gt; Script Management</strong>. The Script Management page opens to display the contents of the <strong>default</strong> folder.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the <strong>Download Script</strong> icon that appears before the Name of the script file you want to view or download. The File Download dialog box opens.</td>
</tr>
</tbody>
</table>
| 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. |

---

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.
The file is saved to the specified directory.

---

### Refresh Scripts

**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.

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 CCX Administration 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** icon.

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 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 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 CCX Administration 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 CCX Administration 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 CCX Editor 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.
Resource provisioning information for the Unified CCX telephony and media subsystems are provided in this chapter.

- 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 Cisco Media subsystem.
Cisco Media subsystem controls CMT media resources for Unified CCX system.

**Step 3** Provision the MRCP ASR subsystem.
MRCP ASR 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 CCX Engine 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.
In previous versions of Unified CCX, it was necessary to configure Unified CM Telephony information using Unified CM. In Unified CCX Release 4.0 and later, 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.

<table>
<thead>
<tr>
<th>Field Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Unified CM Telephony Provider</td>
<td>IP address of the Server, running Unified CM CTI Manager in the cluster. This is normally the first CTI Manager or Cisco Unified CM Telephony Provider selected by the Unified CCX user for Unified CM Telephony subsystem using System &gt; Cisco Unified CM Configuration web page.</td>
</tr>
</tbody>
</table>
### Field Heading | Description
--- | ---
Secondary Unified CM Telephony Provider | IP address of the second Server, running Unified CM CTI Manager in the cluster. This is normally 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 pool together a series of CTI ports, which the system uses to serve calls as they arrive or depart from the Unified CCX server. You can create multiple Unified CM Telephony call control groups to share and limit the resources to be 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 **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 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.

| The CTI ports should be created 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 displays 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 displays, 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 vice versa. 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.  
**Note** The existing call control groups will have this value as inbound after an upgrade from Unified CCX versions prior to 9.0(1). |
### Page Area | Field | Description
--- | --- | ---
Directory Number Information | Device Name Prefix | The Device Name Prefix (DNP) used in the name that will be given all of the CTI Ports in this group. This is a mandatory field. The CTI ports for this port group is 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.

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 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.

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 [https://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_implementation_design_guides_list.html](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.
<table>
<thead>
<tr>
<th>Page Area</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Number</td>
<td>Starting Directory Number</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Device Pool</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> The support for having multiple device pools associated with 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
</tbody>
</table>
### Page Area

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DN Calling Search Space</td>
<td>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. For more information, see the <a href="#">device documentation</a>.</td>
</tr>
<tr>
<td>Location</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Advanced Directory Number Information (only available if you click Show More)

<table>
<thead>
<tr>
<th>Directory Number (continued)</th>
<th>Alerting Name ASCII</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• If the device is not capable of handling the Unicode strings</td>
</tr>
<tr>
<td></td>
<td>• If the locals on endpoint devices do not match</td>
</tr>
<tr>
<td></td>
<td>• If the Unicode string is not specified</td>
</tr>
<tr>
<td>Redirect Calling Search Space</td>
<td>A collection of partitions that are searched to determine how a redirected call is routed.</td>
</tr>
<tr>
<td></td>
<td>Redirect Calling Search Space options:</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> DN Calling Search Space is deprecated. Use Calling Party or Redirect Party instead.</td>
</tr>
<tr>
<td></td>
<td>• DN Calling Search Space—This option enables the CTI Port to use its directory number CSS when performing a redirect / consult transfer.</td>
</tr>
<tr>
<td></td>
<td>• Calling Party—This option enables the CTI Port to use the calling party's CSS when performing a redirect / consult transfer.</td>
</tr>
<tr>
<td></td>
<td>• Redirect Party—This option enables the CTI Port to use the CTI Port's CSS to control the redirect.</td>
</tr>
<tr>
<td>Media Resource Group List</td>
<td>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 &lt;none&gt;, Unified CM uses the Media Resource Group that is defined in the device pool.</td>
</tr>
</tbody>
</table>
### 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 &lt;None&gt;, 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 &lt;None&gt; 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, .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).  
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
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.

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

**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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Directory Information</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Directory Number</strong></td>
<td>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 (*).</td>
</tr>
<tr>
<td></td>
<td>• Supports only route point directory numbers and Finesse agent and supervisor extensions.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>• +1234 and 1234 are two different directory numbers.</td>
</tr>
<tr>
<td></td>
<td>• The square brackets ([ ]) enclose a range of values.</td>
</tr>
<tr>
<td></td>
<td>• For more information, see the “Wildcards and Special Characters in Route Patterns and Hunt Pilots” section in the <em>System Configuration Guide for Cisco Unified Communications Manager</em>.</td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Valid directory numbers—+1223* or <em>#12#</em></td>
</tr>
<tr>
<td></td>
<td>• Invalid directory numbers—91X+ or +1-12345</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Trigger Information</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Language</strong></td>
<td>Choose the default language to associate with the incoming call when the application is started from this drop-down menu.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To add a Language option, click <strong>Edit</strong> button. The User Prompt dialog box opens. Enter a locale string value and click <strong>OK</strong>. 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.</td>
</tr>
<tr>
<td><strong>Application Name</strong></td>
<td>From the drop-down menu, choose the application to associate with the trigger.</td>
</tr>
<tr>
<td><strong>Device Name</strong></td>
<td>A unique identifier for this device, consisting of alphanumeric characters, dots, dashes, or underscores.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>A descriptive name for the CTI route point.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Call Control Group</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Advanced Configuration</strong> (available only if you click <strong>Show More</strong>).</td>
<td></td>
</tr>
<tr>
<td><strong>Advanced Trigger Information</strong></td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>Radio buttons to choose the required option:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Yes</strong>—enable the trigger (default)</td>
</tr>
<tr>
<td></td>
<td>• <strong>No</strong>—disable the trigger.</td>
</tr>
<tr>
<td>Maximum Number of Sessions</td>
<td>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.</td>
</tr>
<tr>
<td>Idle Timeout (in ms)</td>
<td>The number of milliseconds (ms) the system should wait before rejecting the Unified CM Telephony request for this trigger.</td>
</tr>
<tr>
<td>Override Media Termination</td>
<td>Radio buttons to choose the required options:</td>
</tr>
<tr>
<td></td>
<td><strong>Yes</strong>—Override media termination.</td>
</tr>
<tr>
<td></td>
<td><strong>No</strong>—Enable media termination (default).</td>
</tr>
<tr>
<td></td>
<td>If you select Yes, two panes open:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Selected Dialog Groups</strong> displays the default or selected group.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Available Dialog Groups</strong> lists the configured dialog.</td>
</tr>
<tr>
<td><strong>CTI Route Point Information</strong></td>
<td></td>
</tr>
<tr>
<td>Alerting Name ASCII</td>
<td>This information is automatically populated based on the configuration in the Unified CM setup and displays the ASCII name field used in one of the following situations:</td>
</tr>
<tr>
<td></td>
<td>• If the device is not capable of handling the Unicode strings</td>
</tr>
<tr>
<td></td>
<td>• If the locals on endpoint devices do not match</td>
</tr>
<tr>
<td></td>
<td>• If the Unicode string is not specified</td>
</tr>
<tr>
<td>Device Pool</td>
<td>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.</td>
</tr>
<tr>
<td>Location</td>
<td>The total bandwidth that is available for calls to/from this location. A location setting of <strong>HUB_NONE</strong> indicates that the locations feature does not keep track of the bandwidth used by this route point.</td>
</tr>
</tbody>
</table>
### Directory Number Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partition</td>
<td>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 <code>&lt;None&gt;</code> as the partition setting.</td>
</tr>
<tr>
<td>Voice Mail Profile</td>
<td>A list of profiles defined in the Voice Mail Profile Configuration. The first option is <code>&lt;None&gt;</code>, which is the current default Voice Mail Profile that is configured in the Voice Mail Profile Configuration.</td>
</tr>
<tr>
<td>Calling Search Space</td>
<td>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 .</td>
</tr>
</tbody>
</table>

### 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.

#### 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) 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.

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 forth)
- Creating any missing route points
- Modifying out-of-sync route points
- Associating route points to all the Unified CM Telephony users.

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.
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.

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.

Related Topics
Add CMT Dialog Control Group, on page 76

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GroupID</td>
<td>The unique Group ID associated with the media.</td>
</tr>
<tr>
<td>Description</td>
<td>CMT group description.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The ID in this field need not necessarily match the CMT group ID.</td>
</tr>
<tr>
<td>Channels</td>
<td>Number of channels associated with the group.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group ID</td>
<td>A Group ID value unique within all media group identifiers, including ASR group identifiers. This is a mandatory field.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Description for the Cisco Media Termination Dialog group.</td>
</tr>
<tr>
<td>Number of Licensed IVR ports</td>
<td>Number of licensed IVR ports. Display only.</td>
</tr>
<tr>
<td>Maximum Number Of Channels</td>
<td>Maximum number of channels associated with this group. This is a mandatory field.</td>
</tr>
</tbody>
</table>

**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. You can configure the speech software for Unified CCX in the same way as Unified CCX 7.0 (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 for details.).

• 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider Name</td>
<td>Enter the name of the MRCP ASR provider supported by Unified CCX.</td>
</tr>
<tr>
<td>Number of Provider Licenses</td>
<td>The number of ASR port licenses purchased from the ASR vendor.</td>
</tr>
</tbody>
</table>
Vendor-specific grammar setting. Valid options:
- Nuance Open Speech Recognizer servers version 9.0 and above (OSR 3.1.x)
- Nuance 8.5 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 INSERVICE 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:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
</table>

Cisco Unified Contact Center Express Administration and Operations Guide, Release 11.6(1)
Computer Name | Host name 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 host name 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
- 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Host name or IP address of the server where the MRCP ASR server software is installed.</td>
</tr>
<tr>
<td>Provider Name</td>
<td>Select the name of the MRCP ASR Provider to which this server is associated from this drop-down list.</td>
</tr>
</tbody>
</table>
| 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  
  - 2003 SISR—554  
  - Nuance—554 |
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group ID</td>
<td>Identifier for the group.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of this dialog group.</td>
</tr>
<tr>
<td>Provider</td>
<td>Name of the MRCP ASR provider.</td>
</tr>
<tr>
<td>Channels</td>
<td>Maximum number of sessions.</td>
</tr>
</tbody>
</table>

This web page also displays the Number ofLicensed 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group ID</td>
<td>Associated group ID.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of this dialog group.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> 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.</td>
</tr>
<tr>
<td>Number Of Provider Licenses</td>
<td>Display only.</td>
</tr>
<tr>
<td>Number Of Licensed IVR Ports</td>
<td>Display only.</td>
</tr>
<tr>
<td>Maximum Number Of sessions</td>
<td>Maximum number of sessions associated with this dialog group. <strong>Note</strong> 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. <strong>Caution</strong> 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.</td>
</tr>
<tr>
<td>Provider Name</td>
<td>Select a MRCP Provider name from the drop-down list that contains a list of all previously defined provider names.</td>
</tr>
<tr>
<td>Enabled Languages</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Step 4

Click **Add** to apply changes.

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

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>Host name or IP address of the server in which the TTS server software is installed.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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 host name or IP address that is local with the Unified CCX node while installing the TTS server software in this field.</td>
</tr>
<tr>
<td>Port</td>
<td>TCP port number used to connect to an MRCP server. Following are the different TCP Provider names:</td>
</tr>
<tr>
<td></td>
<td>• MRCP Server</td>
</tr>
<tr>
<td></td>
<td>• Nuance Vocalizer</td>
</tr>
<tr>
<td></td>
<td>• Scansoft Realspeak</td>
</tr>
<tr>
<td>Provider</td>
<td>The MRCP TTS Provider to which this server is associated.</td>
</tr>
<tr>
<td>Status</td>
<td>Status or state of the subsystem.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Host name or IP address of the server the MRCP TTS server software is installed.</td>
</tr>
<tr>
<td>Provider Name</td>
<td>Select the name of the MRCP TTS Provider to which this server is associated from this drop-down list.</td>
</tr>
</tbody>
</table>
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—554
- 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.
Provision MRCP TTS Default Genders
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 94
- Contact Service Queue Configuration, on page 98
- Configure Agent-Based Routing, on page 106
- Teams Configuration, on page 107

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 "Adding Users to a User Group" section in the Cisco Unified Communications Manager Administration Guide available here:


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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary RmCm Provider</td>
<td>The host name 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.</td>
</tr>
<tr>
<td>Secondary RmCm Provider</td>
<td>The host name or IP address of the secondary RmCm Provider.</td>
</tr>
<tr>
<td>User ID</td>
<td>The RmCm user ID.</td>
</tr>
</tbody>
</table>

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.
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.

**Related Topics**

- Modify Unified Communications Manager Telephony Information, on page 27

## 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**

1. **Step 1**
   - From the Unified CCX Administration menu bar, choose Subsystems > RmCm > Resource Groups.
   
   The Resource Group web page opens with a list of configured resource groups (if any).

2. **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.

3. **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”).

4. **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**

1. **Step 1**
   - From the Unified CCX Administration 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 CCX Administration 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 CCX Administration 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 toolbar 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).

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 CCX Administration 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.

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.
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 CCX Administration 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.

If you have the Unified CCX Standard license package, 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

---

\(^1\) Unified Communications users in a Unified CM deployment refers to a Unified CM user.
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 (~).

- 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 names now support the use of SPACE in the name.

**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 CCX Administration 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 CCX Administration 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Name</td>
<td>Name of the agent (display only).</td>
</tr>
<tr>
<td>Resource ID</td>
<td>Unique identifying number of the agent (display only). This is the alpha-numeric user id assigned in the Unified CM End User Configuration page.</td>
</tr>
<tr>
<td>Unified CCX Extension</td>
<td>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.</td>
</tr>
<tr>
<td>Resource Group</td>
<td>A resource group with which to associate the agent (optional).</td>
</tr>
</tbody>
</table>
| 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>From the Unified CCX Administration menu bar, select Subsystems &gt; RmCm &gt; Assign Skills. The Assign Skills summary web page opens. <strong>Tip</strong> Only agents or supervisors who have assigned Unified CCX extensions are displayed in the list of resources in the Resources area.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>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. <strong>Note</strong> You can check the Select All check box to select all agents. The Skill summary web page shows the total number of skills created.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Specify the following fields. <strong>Field</strong></td>
</tr>
<tr>
<td>Resource Group</td>
<td>To assign a resource group to all the selected agents, choose a resource group from the Resource Group drop-down menu.</td>
</tr>
<tr>
<td>Skills to Add</td>
<td>Select one or more skills from the Skills list and click &lt; to add the skills to the Skills to Add List. <strong>Note</strong> The Skills to Add list contains all skills, not just the skills that agents already have.</td>
</tr>
<tr>
<td>Skills</td>
<td>List of the available skills.</td>
</tr>
<tr>
<td>Competence Level</td>
<td>Select a skill from the Assigned Skills list and choosing a number from the Competence Level drop-down menu</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Click Update to apply the changes.</td>
</tr>
</tbody>
</table>
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 CCX Administration 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.


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 CCX Administration menu bar, choose Subsystems > RmCm > Contact Service Queues.

The Contact Service Queues web page opens.

Use this web page to view the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the resource or skill group.</td>
</tr>
<tr>
<td>Contact Queuing Criteria</td>
<td>Algorithm used to order the queued calls (contacts).</td>
</tr>
<tr>
<td>Resource Pool Selection Model</td>
<td>The resource selection criteria chosen for this CSQ.</td>
</tr>
<tr>
<td>Resource Pool</td>
<td>The skills or resource group used for this CSQ.</td>
</tr>
<tr>
<td>CSQ Type</td>
<td>The type of the CSQ.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the selected CSQ.</td>
</tr>
</tbody>
</table>

**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.
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.

### Related Topics

- [Contact Service Queue Configuration Web Page](#), on page 101

### Contact Service Queue Configuration Web Page

Contact Service Queue Configuration web page:

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Service Queue Name</td>
<td>Enter a meaningful name that is concise, yet easy to recognize (for example, Language Experts). This is a mandatory field.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Contact Service Queue Type</td>
<td>Display only. Voice—Agents in this CSQ can handle inbound and outbound voice calls.</td>
</tr>
<tr>
<td>Contact Queuing Criteria</td>
<td>Display only. Displays the criteria used for queuing the contacts. For example, First In, First Out (FIFO).</td>
</tr>
<tr>
<td>Automatic Work</td>
<td>Determines whether agents handling calls that are routed through this CSQ automatically enter the Work state when a call ends. This field is mandatory. Options are:</td>
</tr>
<tr>
<td></td>
<td>• Enabled—Agents associated to a CSQ that has the Automatic Work option enabled, enter the Work state automatically when on a call. CSQ ends. If agents are associated to a CSQ that has the Automatic Work option disabled handle transferred calls that were originally delivered by a CSQ that has Automatic Work enabled, they also enter the Work state automatically when a call ends.</td>
</tr>
<tr>
<td></td>
<td>• Disabled (default)—Agents enter Ready or Not Ready state when a call ends, depending on the Automatic Available setting.</td>
</tr>
<tr>
<td>Wrapup Time</td>
<td>Determines the length of the Work state for this CSQ when a call ends. Options are:</td>
</tr>
<tr>
<td></td>
<td>• Enabled button with Seconds field—The Seconds field specifies the length of the Work state phase.</td>
</tr>
<tr>
<td></td>
<td>• Disabled—No limit on how long the agent can stay in the Work state.</td>
</tr>
<tr>
<td>Resource Pool Selection Model</td>
<td>Select one of the following options from the drop-down menu:</td>
</tr>
<tr>
<td></td>
<td>• Resource Skills—To create a skills-based CSQ.</td>
</tr>
<tr>
<td></td>
<td>• Resource Group—To create a resource group-based CSQ.</td>
</tr>
<tr>
<td></td>
<td>This is a mandatory field.</td>
</tr>
<tr>
<td>Service Level</td>
<td>The target maximum number of seconds a call is queued before it is connected to an agent. This is a mandatory field.</td>
</tr>
<tr>
<td>Service Level Percentage</td>
<td>The target goal for percentage of contacts that meet the service level. This is a mandatory field.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
### 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 the script executes, 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.

### Related Topics
*Wrap-Up Reasons*, on page 388

---

**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 CCX Administration 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.
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 CCX Administration 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:

<table>
<thead>
<tr>
<th>Agent ID</th>
<th>Assigned Skills</th>
<th>Resource Group</th>
</tr>
</thead>
</table>
| 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 1: Agent Skill and Resource Group Settings**

<table>
<thead>
<tr>
<th>CSQ Name</th>
<th>Resource Pool Selection Model</th>
<th>Resource Selection Criteria</th>
<th>Skill/Competence</th>
<th>Available Agents</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSQ1</td>
<td>Resource Skills</td>
<td>Most Skilled</td>
<td>BankingMinimum competency: 5</td>
<td>Agent1, Agent2</td>
</tr>
<tr>
<td>CSQ2</td>
<td>Resource Skills</td>
<td>Most Skilled</td>
<td>CreditCardMinimum competency: 5</td>
<td>Agent1, Agent2</td>
</tr>
<tr>
<td>CSQ3</td>
<td>Resource Group</td>
<td>Longest Available</td>
<td>GeneralQueries</td>
<td>Agent1, Agent2, Agent3</td>
</tr>
</tbody>
</table>

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.

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 2: Resource Skill Selection Criteria

<table>
<thead>
<tr>
<th>Example</th>
<th>CSQ Skills</th>
<th>Agent Competency Levels</th>
<th>Sequence Agents Become Ready</th>
<th>Selection Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most skilled resource selection model</td>
<td>Technical Support</td>
<td>Agent A = 10</td>
<td>A, B C</td>
<td>A, B, C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Agent B = 10</td>
<td>C, A, B</td>
<td>A, B, C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Agent C = 5</td>
<td>A, C, B</td>
<td>A, B, C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C, B, A</td>
<td>B, A, C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Technical Support</td>
<td>A, B C</td>
<td>A, B, C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Agent A = 10</td>
<td>C, A, B</td>
<td>A, B, C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Agent B = 10</td>
<td>A, C, B</td>
<td>A, B, C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Agent C = 5</td>
<td>C, A, B</td>
<td>B, A, C</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Example</th>
<th>CSQ Skills</th>
<th>Agent Competency Levels</th>
<th>Sequence Agents Become Ready</th>
<th>Selection Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most skilled resource selection model</td>
<td>SalesSupport</td>
<td>Agent A = Sales (10) Support (5)</td>
<td>A, B C</td>
<td>A, B, C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Agent B = Sales (5), Support (10)</td>
<td>C, A, B</td>
<td>A, B, C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Agent C = Sales (5) Support (1)</td>
<td>A, C, B</td>
<td>A, B, C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C, B, A</td>
<td>B, A, C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SalesSupport</td>
<td>A, B C</td>
<td>A, B, C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Agent A = Sales (10) Support (5)</td>
<td>C, A, B</td>
<td>A, B, C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Agent B = Sales (5), Support (10)</td>
<td>A, C, B</td>
<td>A, B, C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Agent C = Sales (5) Support (1)</td>
<td>C, B, A</td>
<td>C, B, A</td>
</tr>
</tbody>
</table>

**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 CCX Administration 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Work</td>
<td>Determines whether agents handling calls that are routed through this CSQ automatically enter the Work state when a call ends.</td>
</tr>
<tr>
<td></td>
<td>• Enabled—Agents associated to a CSQ that has the Automatic Work option enabled enter the Work state automatically when on a call. If agents are associated to a CSQ that has the Automatic Work option disabled handle transferred calls that were originally delivered by a CSQ that has Automatic Work enabled, they also enter the Work state automatically when a call ends.</td>
</tr>
<tr>
<td></td>
<td>• Disabled (default)—Agents enter Ready or Not Ready state when a call ends, depending on the Automatic Available setting.</td>
</tr>
<tr>
<td>Wrapup Time</td>
<td>Determines if agents automatically enter Wrapup when a call ends.</td>
</tr>
<tr>
<td></td>
<td>• Enabled button with seconds field—Controls how long the agent can stay in the Work state if Automatic Work is enabled. The seconds field specifies the Wrapup time length.</td>
</tr>
<tr>
<td></td>
<td>• Disabled (default)—No limit of how long the agent can stay in the Work state if Automatic Work is enabled.</td>
</tr>
</tbody>
</table>

**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**
A team that accesses Live Data reports should be 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 Team Supervisor

Perform the following procedure to create team supervisor:

**Procedure**

**Step 1**
From the Unified CCX Administration menu, choose **Subsystems > RmCm > Teams**.

The Team page displays the list of all teams.

**Step 2**
Click the team for which you want to create a supervisor.

The Team Configuration page displays the configuration information about the team.
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 CCX Administration 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 that displays at the bottom of the window.
        The Team Configuration page appears.
Step 3  Click Add to apply changes.

Modify Agents on Teams

Use the Teams area to add agents or change agents on an existing Team.

Procedure

Step 1  From the Unified CCX Administration menu bar, choose Subsystems > RmCm > Teams.
        The Teams web page opens.
Step 2  Click a name in the Team Name column
        The Team Configuration page appears.
Step 3  Select an agent name in the Resources Assigned to other Teams list and use the arrow icon to move it into the Assigned Resources list if you want 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 Resources Assigned to other Teams list. This agent now belongs to the default team.
Step 4  Click Update to apply changes.

Delete a Team

Use the Teams area of the RmCm Configuration web page to delete an existing Team.
**Procedure**

**Step 1**  
From the Unified CCX Administration 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

To provision additional subsystems, you must complete the following tasks:

- Log into the Unified CCX Administration.
- Provision your telephony and media resources.
- Provision your Unified CCX subsystem, if required.

The following sections introduce the additional Unified CCX subsystems and explain how to provision them.

- About Additional Subsystems, on page 111
- Provision of HTTP Subsystem, on page 112
- Provision of Database Subsystem, on page 113
- Provision eMail Subsystem, on page 116

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

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.

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).

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.

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 CCX Administration menu bar, choose Subsystems > HTTP.
The HTTP Trigger Configuration web page opens.

Step 2
Specify the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>The relative URL. For example: /hello</td>
</tr>
</tbody>
</table>
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 execute 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

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 CCX Administration 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.

Related Topics

Datasource Configuration Web Page, on page 114

Datasource Configuration Web Page

Datasource Configuration web page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Source Name</td>
<td>Data source name for referring to the datasource. This is a mandatory field.</td>
</tr>
<tr>
<td>User Name</td>
<td>Username defined for connecting to the enterprise database. This is a mandatory field.</td>
</tr>
<tr>
<td>Password</td>
<td>Password defined for connecting to the enterprise database.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Re-enter the password that you provided in the Password field.</td>
</tr>
<tr>
<td>Maximum Number of Connections</td>
<td>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.</td>
</tr>
<tr>
<td>Driver</td>
<td>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.</td>
</tr>
</tbody>
</table>
### 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 theDatasource 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 not supported.

---

### Poll Database Connectivity

To poll connectivity to the database on a periodic basis, complete the following steps.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the Unified CCX Administration menu bar, choose <strong>Subsystems &gt; Database &gt; Parameters</strong>. The Parameters web page opens to display the parameter-related fields.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Specify the following fields:</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>RetryConnectInterval</td>
<td>Specifies the interval between two connection attempts when a data source is initialized. The default is 15,000 milliseconds.</td>
</tr>
<tr>
<td>NumAttempt</td>
<td>Specifies the number of attempts to establish connections to the database when a data source is initialized. The default is 3 attempts.</td>
</tr>
<tr>
<td>LoginTimeout</td>
<td>Sets the maximum time in seconds that a driver will wait while attempting to connect to a database. The default is 0 (disabled).</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Update</strong> to apply changes (or <strong>Reset to Default</strong> 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.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Server</td>
<td>A fully-qualified email server name. (Example: server.domain.com)</td>
</tr>
<tr>
<td>email Address</td>
<td>An existing fully qualified e-mail address for the administrative account.</td>
</tr>
<tr>
<td></td>
<td>Example: <a href="mailto:administrator@domain.com">administrator@domain.com</a></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Unified CCX supports alphanumeric IDs and special characters (only hyphen &quot;-&quot;, underscore &quot;.&quot;, and dot &quot;.&quot;).</td>
</tr>
</tbody>
</table>

Step 3
Click Update.

The Unified CCX system saves your changes and the Unified CCX Administration 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.
Provision eMail Subsystem
Management of Prompts, Grammars, Documents, and Custom Files

Unified CCX applications can make use of many auxiliary files that interact with callers, such as scripts, pre-recorded prompts, grammars, and custom Java classes.

To manage these auxiliary files, you must complete the following tasks:

- Provision telephony and media resources.
- Provision Unified CCX subsystem, if required.
- Provision additional subsystems, if required.
- Configure Cisco script applications.

Depending on your particular Unified CCX implementation, your applications might make use of some or all of the file types described in the following sections.

- Manage Prompt Files, on page 119
- Manage Grammar Files, on page 121
- Manage Document Files, on page 122
- Language Management, on page 123
- Upload of Prompt Files, on page 126
- Management of Custom Files, on page 129
- AAR File Management, on page 130

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.
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 CCX Administration menu bar, choose Application > Prompt Management.

**Step 2** The Prompt Management web page opens to display the following fields and buttons.

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>Lists the location of the items listed in the Name column.</td>
</tr>
<tr>
<td>Folder</td>
<td>Path of the current item selected in the Name column with respect to the root folder.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the language.</td>
</tr>
<tr>
<td>Size</td>
<td>The size of the prompt file prefixed with KB. The file size is converted from bytes to KB. &lt;br&gt;<strong>Note</strong> This column is usually blank on the root page because the items on this page are usually folders.</td>
</tr>
<tr>
<td>Date Modified</td>
<td>The date and time when the document was last uploaded or changed along with time zone.</td>
</tr>
<tr>
<td>Modified by</td>
<td>The user ID of the person who performed these modifications.</td>
</tr>
<tr>
<td>Delete</td>
<td>Click <strong>Delete</strong> icon to remove the folder and its contents from the repository.</td>
</tr>
<tr>
<td>Rename</td>
<td>Click <strong>Rename</strong> icon to rename the folder in the repository.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Click <strong>Refresh</strong> icon to refresh the folder in the repository.</td>
</tr>
<tr>
<td>Create Language</td>
<td>Displays a dialog box that lets you create a new language folder.</td>
</tr>
<tr>
<td>Upload Zip Files</td>
<td>Displays a dialog box that lets you locate and upload a zip file. &lt;br&gt;<strong>Note</strong> 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.</td>
</tr>
</tbody>
</table>

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 CCX Administration menu bar, choose **Applications > Grammar Management**.

**Step 2**

The Grammar Management web page opens to display the following fields and buttons.

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>Lists the location of the items listed in the Name column.</td>
</tr>
<tr>
<td>Folder</td>
<td>Path of the current item selected in the Name column with respect to the root folder.</td>
</tr>
<tr>
<td>Codec</td>
<td>The codec chosen during installation for this Unified CCX server. Display only.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the language folder.</td>
</tr>
<tr>
<td>Size</td>
<td>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.</td>
</tr>
<tr>
<td>Date Modified</td>
<td>The date and time when the document was last uploaded or changed along with time zone.</td>
</tr>
<tr>
<td>Modified by</td>
<td>The user ID of the person who performed these modifications.</td>
</tr>
<tr>
<td>Delete</td>
<td>Displays a dialog box that lets you delete an existing language folder.</td>
</tr>
</tbody>
</table>
### 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 CCX Administration menu bar, choose **Applications > Document Management**.
- **Step 2** The Document Management web page opens to display the following fields and buttons.
<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>Lists the location of the items listed in the Name column.</td>
</tr>
<tr>
<td>Folder</td>
<td>Path of the current item selected in the Name column with respect to the root folder.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the language folder.</td>
</tr>
<tr>
<td>Size</td>
<td>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.</td>
</tr>
<tr>
<td>Date Modified</td>
<td>The date and time when the document was last uploaded or changed along with time zone.</td>
</tr>
<tr>
<td>Modified by</td>
<td>The user ID of the person who performed these modifications.</td>
</tr>
<tr>
<td>Delete</td>
<td>Displays a dialog box that lets you delete an existing language folder.</td>
</tr>
<tr>
<td>Rename</td>
<td>Displays a dialog box that lets you rename an existing language folder.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Refreshes the specified folder in the repository.</td>
</tr>
<tr>
<td>Create Language</td>
<td>Displays a dialog box that lets you create a new language folder.</td>
</tr>
<tr>
<td>Upload Zip Files</td>
<td>Displays a dialog box that lets you locate and upload a zip file. <strong>Note</strong> 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.</td>
</tr>
</tbody>
</table>

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 CCX Administration 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.

Rename Language

Follow this procedure to rename a Prompt/Grammar/Document language folder in the Repository datastore:

**Procedure**

**Step 1**  
From the Unified CCX Administration 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 CCX Administration 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 CCX Administration 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.
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.

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 your own prompts to be used in applications.

• **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 your own prompts to be used in applications. The example provided in this section uses the Windows Sound Record option. This option is one of many possibilities for recording G711 prompts. G711 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.

The G729 codec is licensed and is not freely distributed. A white paper that describes the G729 prompt recording options is available on request. Send an email to apps-support@cisco.com to obtain a copy of this white paper. To record a prompt, complete the following steps.

The following procedure is an example of recording G.711 prompts with Microsoft Windows Sound Recorder, using a microphone plugged into your computer. If you are not using Microsoft Windows Sound Recorder, see the documentation provided with your audio application.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>From your Windows Start menu, choose <strong>Start &gt; Programs &gt; Accessories &gt; Entertainment &gt; Sound Recorder</strong>. The Sound Recorder dialog box opens.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click the <strong>Record</strong> button and speak your greeting into the microphone.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click the <strong>Stop</strong> button when you finish recording.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>To check your greeting, click the <strong>Rewind</strong> button or drag the slider back to the beginning of the recording. Then click the <strong>Play</strong> button.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>When you are satisfied with your greeting, choose <strong>File &gt; Save As</strong>. The Save As window opens.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Click <strong>Change</strong> to set the recording options. You can also set recording properties by choosing <strong>Properties</strong> from the Sound Recorder File menu. The Sound Selection dialog box opens.</td>
</tr>
</tbody>
</table>
| **Step 7** | From the Format drop-down menu, choose one of the following options based on the prompts selected during the installation of Unified CCX software:  
  • If you selected G711 prompts, **CCITT u-Law**. |
• If you selected G729 prompts, see your G.729 white paper.

Note  The instructions in this procedure assume that, during Unified CCX installation, you configured Unified CCX to use the G.711 codec for prompts. If this assumption is incorrect, and you specified the G.729 codec instead, you would choose a G.729 option from this menu. For more information about recording prompts with G.729, see your G.729 documentation.

When a custom prompt is uploaded to CCX, the prompt is saved in both the formats CCITT u-Law and CCITT a-Law.

**Step 8**  From the Attributes drop-down menu, choose 8.000 kHz, 8 Bit, Mono 7 kb/sec.

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

The Save As dialog box opens.

**Step 10**  Enter a name for this format, and then click **OK**.

The Save As Dialog Box closes.

**Step 11**  In the Sound Selection dialog box, click **OK**.

The Sound Selection dialog box closes.

**Step 12**  In the Save As window, navigate to the directory of your choice, preferably a directory that you have set aside for prompts.

**Step 13**  Select the file name, and click **Save**.

The Save As dialog box closes.

You are now ready to add this prompt to the Unified CCX system.

---

### 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 CCX Administration menu bar, choose **Tools > User Management > Spoken Name Upload**.

**Step 2**  The Spoken Name Prompt Upload web page opens with the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Id</td>
<td>Unique identifier of the user for which the spoken name is to be uploaded. This is a mandatory field.</td>
</tr>
<tr>
<td>Codec</td>
<td>The codec chosen during installation for this Unified CCX server. Display only.</td>
</tr>
</tbody>
</table>
Management of Custom Files

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 CCX Administration 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

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: 1.1
Created-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: 1.1
Created-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 CCX Administration menu bar, choose **Applications > AAR Management**.

The AAR Management web page opens to display the following fields and buttons.

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter a Valid AAR File to Upload</td>
<td>You can either enter the name of the AAR file or click <strong>Browse</strong> button next to this field to navigate to the directory in which the file is located. This is a mandatory field.</td>
</tr>
<tr>
<td>Overwrite existing files</td>
<td>Enable this checkbox in case you want to overwrite the existing files.</td>
</tr>
<tr>
<td>Upload</td>
<td>Click this button to upload the AAR file.</td>
</tr>
<tr>
<td>Clear</td>
<td>Click this button to clear the selected file.</td>
</tr>
</tbody>
</table>

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.

**Related Topics**

[Main Attributes](#), on page 135

**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).

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>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>section:</td>
<td>*header +newline</td>
</tr>
<tr>
<td>nonempty-section:</td>
<td>+header +newline</td>
</tr>
<tr>
<td>newline:</td>
<td>CR LF</td>
</tr>
<tr>
<td>header:</td>
<td>name: value</td>
</tr>
<tr>
<td>name:</td>
<td>alphanum *headerchar</td>
</tr>
<tr>
<td>value:</td>
<td>SPACE *otherchar newline *continuation</td>
</tr>
</tbody>
</table>
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 4: Syntax for AAR Files

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>manifest-file</td>
<td>main-section newline *individual-section</td>
</tr>
<tr>
<td>main-section</td>
<td>version-info newline *main-attribute</td>
</tr>
<tr>
<td>version-info</td>
<td>Manifest-Version: version-number</td>
</tr>
<tr>
<td>version-number</td>
<td>digit+{.digit+}*</td>
</tr>
<tr>
<td>main-attribute</td>
<td>(any legitimate main attribute) newline</td>
</tr>
<tr>
<td>individual-section</td>
<td>Name: value newline *perentry-attribute</td>
</tr>
<tr>
<td>perentry-attribute</td>
<td>(any legitimate perentry attribute) newline</td>
</tr>
<tr>
<td>newline</td>
<td>CR LF</td>
</tr>
<tr>
<td>digit</td>
<td>{0-9}</td>
</tr>
</tbody>
</table>

Note: To prevent corruption of files sent through email, do not use “From” to start a header.
### 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 5: General Main Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manifest-Version</td>
<td>The manifest file version. The value is a legitimate version number.</td>
</tr>
<tr>
<td>Created-By</td>
<td>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.</td>
</tr>
<tr>
<td>Cisco Unified CCX-Version</td>
<td>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.</td>
</tr>
<tr>
<td>Class-Path</td>
<td>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.</td>
</tr>
<tr>
<td>Application-List</td>
<td>The application configuration files from the META-INF/applications/ directory to be installed. Entries are separated by one or more spaces.</td>
</tr>
</tbody>
</table>
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 6: Implementation Category in Main Attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementation-Title</td>
<td>The title of the extension implementation.</td>
</tr>
<tr>
<td>Implementation-Version</td>
<td>The version of the extension implementation.</td>
</tr>
<tr>
<td>Implementation-Vendor</td>
<td>The organization that maintains the extension implementation.</td>
</tr>
<tr>
<td>Implementation-Vendor-Id</td>
<td>The ID of the organization that maintains the extension implementation.</td>
</tr>
<tr>
<td>Implementation-URL</td>
<td>The URL from which the extension implementation is downloaded.</td>
</tr>
<tr>
<td>Sealed</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 6: Implementation Category in Main Attributes, on page 136 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 7: Application Subdirectory Manifest File Syntax

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>application-file</td>
<td>version-info newline *application-attribute</td>
</tr>
<tr>
<td>version-info</td>
<td>Application-Version: version-number</td>
</tr>
<tr>
<td>Name</td>
<td>Value</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>version-number</td>
<td>digit+ {.digit+}*</td>
</tr>
<tr>
<td>application-attribute</td>
<td>(any legitimate application attribute) newline</td>
</tr>
<tr>
<td>newline</td>
<td>CR LF</td>
</tr>
<tr>
<td>digit</td>
<td>{0-9}</td>
</tr>
</tbody>
</table>

The application attributes fall into the following groups:

**Table 8: Application Attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application-Version</td>
<td>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.</td>
</tr>
<tr>
<td>Application-Name</td>
<td>The unique name of the application (see Unified CCX Application Management).</td>
</tr>
<tr>
<td>Application-Type</td>
<td>The type of the application (Cisco Script Application, Busy, Ring-No-Answer).</td>
</tr>
<tr>
<td>Application-Description (optional)</td>
<td>The description for the application (see Unified CCX Application Management).</td>
</tr>
<tr>
<td>Application-Id</td>
<td>A unique identifier for the application (see Unified CCX Application Management).</td>
</tr>
<tr>
<td>Max-Sessions</td>
<td>The maximum number of sessions for the application (see Unified CCX Application Management).</td>
</tr>
<tr>
<td>Enabled</td>
<td>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.</td>
</tr>
<tr>
<td>Script</td>
<td>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.</td>
</tr>
<tr>
<td>Default-Script</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Attribute Subdirectory Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial-Script</td>
<td>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.</td>
</tr>
</tbody>
</table>

- 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 135.
Unified CCX System Management

Unified CCX administration provides options to configure, control, and monitor Unified CCX component activities and information across a cluster.

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

See the Cisco Unified Contact Center Express Install and Upgrade Guide for instructions about tasks that significantly change your Unified CCX deployment, such as:

- Changing from a single-server deployment to a multiple-server deployment.
- Removing a Unified CCX Software component from a server.
- Moving a Unified CCX Software component to another server.
- Changes to a Unified CCX cluster (adding, removing, or replacing a server).

The following sections describe the day-to-day management of Unified CCX components.

- Basic Terminology, on page 141
- High Availability and Automatic Failover, on page 142
- Unified CCX CDS Information Management, on page 143
- Manage System Parameters, on page 143
- Unified CCX IP Address/hostname Management, on page 144
- Set Up Certificates, on page 159
- Exit Unified CCX Administration, on page 160

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.

---

**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.
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 > System Parameters** from the Unified CCX Administration 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.

Related Topics

- [System Parameters](#), on page 261

**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 Host Name is 24 characters.

**Prepare System for IP Address/hostname Change**

Perform the following tasks to ensure that your system is prepared for a successful IP address/host name 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/host name 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 host names.

- 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 host names and capture this list of servers for later reference. Ensure that you have saved an inventory of both the host name 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:

```bash
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
   ** WARNING **
   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**

Once the Unified CCX IP address change takes effect, when the Cloud Connect services are enabled, run the following CLI command:

```bash
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 publisher server in a HA 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 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 by using 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 new IP of the publisher server in subscriber, enter the following CLI command on the subscriber server:

```bash
utils uccx modify remote_IPAddress <Old_IP_of_Publisher> <New_IP_of_Publisher>
```

The following output displays:
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 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)?

Caution Ensure that the server is moved to 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 displays:

```
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)?

*** WARNING ***
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)?

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.

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.

If you change the IP address, License MAC will also change. Rehost the new license for the new LicenseMAC. 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 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 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 other nodes by using 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 new IP of the subscriber in 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 displays:
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 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)?
```

Caution  Ensure that the server is moved to 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 displays:

```
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)?
*** WARNING ***
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)?
```

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.

**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.

---

**Host Name Modification**

This section describes how to change the host name.

**Caution**

Changing the host name on any node in a Cisco CRS cluster can interrupt call processing and other system functions. Also, changing the host name 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 host name changes during a planned maintenance window.

**Note**

As a prerequisite ensure that the DNS is reachable and the DNS record exists for the server.

**Change Host Name for Server in a Single-Node Deployment**

Use this procedure to change the hostname of the server in a single-node deployment.

**Note**

The character limit for Host Name is 24 characters.

Ensure Single Sign-On is disabled before performing the change in Host Name.

**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 Communications Operating System Administration interface. To change the host name using CLI command, go to step 3 or to change the host name using Cisco Unified Communications Operating System 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.
```

*** WARNING ***
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 Communications Operating System 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 SocialMiner:

**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.

**Host Name Modification in High-Availability (HA) Deployment**

The character limit for Host Name is 24 characters.

**Related Topics**

Single Sign-On (SSO), on page 266

**Change Host Name for Publisher Server in HA Deployment**

Use this procedure to change the hostname of publisher server in a HA deployment.

**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 Unified Communications Operating System 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 Communications Operating System Administration interface:**

From **Cisco Unified Communications Operating System Administration** Cisco Unified OS Administration 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:

```bash
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
- Cisco Unified Communications Operating System Administration interface

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 Communications Operating System Administration interface:
Change the hostname using Cisco Unified Communications Operating System 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 SocialMiner:

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 Host Name 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 Communications Operating System 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
*** WARNING ***
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 Communications Operating System Administration interface:**

Change the hostname using Cisco Unified Communications Operating System 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 reset up 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 SocialMiner.

a) Choose **Subsystems > Chat and Email > SocialMiner Configuration**.
b) Click **Save** and verify that the SocialMiner **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/host name Change, on page 144 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 SocialMiner 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.
Set Up Certificates

Deploy Root Certificate for Internet Explorer

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

Note

To avoid certificate warnings, each user must use the fully-qualified domain name (FQDN) of the Unified CCX server.

Set Up CA Certificate for Internet Explorer Browser

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

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

Procedure

Step 1
In Windows Explorer, double-click the ca_name.cer file (in which ca_name is the name of your certificate) and then click Open.

Step 2
Click Install Certificate > Next > Place all certificates in the following store.

Step 3
Click Browse and select Trusted Root Certification Authorities.

Step 4
Click OK.

Step 5
Click Next.

Step 6
Click Finish.

A message appears that states you are about to install a certificate from a certification authority (CA).

Step 7
Click Yes.

A message appears that states the import was successful.

Step 8
To verify the certificate was installed, open Internet Explorer. From the browser menu, select Tools > Internet Options.

Step 9
Click the Content tab.

Step 10
Click Certificates.

Step 11
Click the Trusted Root Certification Authorities tab.

Step 12
Ensure that the new certificate appears in the list.

Step 13
Restart the browser for certificate installation to take effect.
Set Up CA Certificate for Firefox Browser

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

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

**Procedure**

**Step 1** From the Firefox browser menu, select **Options**.

**Step 2** Click **Advanced**.

**Step 3** Click the **Certificates** tab.

**Step 4** Click **View Certificates**.

**Step 5** Click **Authorities**.

**Step 6** Click **Import** and browse to the *ca_name*.cer file (in which *ca_name* is the name of your certificate).

**Step 7** Check the **Validate Identical Certificates** check box.

**Step 8** Restart the browser for certificate installation to take effect.

Exit Unified CCX Administration

To exit Unified CCX Administration without closing your web browser, you can do either of the following:

**Note** You can also exit Unified CCX Administration 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 CCX Administration 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 161
- Reporting Administration on Unified Intelligence Center, on page 204

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 the “Command line interface” section of the Cisco Unified Contact Center Express Administration and Operations Guide, located at https://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html.

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.
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. **Database Server Configuration**, on page 325
2. **Configure Automatic Purging**, on page 163

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 CCX Administration menu bar, choose **Tools > Historical Reporting > Database Server Configuration**.

The Database Server Configuration web page opens with the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>The host name or IP Address of the database server.</td>
</tr>
<tr>
<td>Maximum DB Connections for Report Clients Sessions</td>
<td>The maximum number of client and scheduler connections that can access the Historical Reports Database server.</td>
</tr>
<tr>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• Standalone Setup—1 to 8 instances</td>
</tr>
<tr>
<td></td>
<td>• High Availability Setup—1 to 16 instances</td>
</tr>
</tbody>
</table>

**Step 2**
Enter a value in the **Maximum DB Connections for Report Client Sessions** field next to a Server Name.

**Step 3**
Click **Update**.

---

**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*. 

---

Cisco Unified Contact Center Express Administration and Operations Guide, Release 11.6(1)
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 a large number of records. This leads to calls not being written to the database.

---

**Configure Automatic Purging**

The Unified CCX Engine 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 CCX Administration menu bar, choose **Tools > Historical Reporting > Purge Schedule Configuration**.

The Purge Schedule Configuration area opens. The following fields are displayed in the Purge Schedule Configuration area.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purge Schedule</strong></td>
<td></td>
</tr>
<tr>
<td>Daily purge at</td>
<td>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.</td>
</tr>
<tr>
<td>Purge data older than</td>
<td>Data can persist for a number of months before being purged.</td>
</tr>
<tr>
<td>Purge run time</td>
<td>The total duration for which the purge process should run.</td>
</tr>
</tbody>
</table>

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.
### Field

<table>
<thead>
<tr>
<th>Description</th>
<th>Percentage of the maximum database size at which an automatic purge is initiated (as compared to the total available size).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiate automatic purge when database exceeds</td>
<td>Percentage of the maximum extents size of any table above which an automatic purge is initiated.</td>
</tr>
<tr>
<td>Auto purge data for the oldest</td>
<td>Age of data to be purged.</td>
</tr>
</tbody>
</table>

### 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 CCX Administration menu bar, choose Tools > Historical Reporting > 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.

---

**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 CCX Administration web interface.

To access Real-Time Reporting tools, you must configure the DNS client on your local machine.

If your local machine is not in the domain where Unified CCX resides, enter the hostnames in the local host file for the machines that house Unified CCX nodes.

You must be logged into the Unified CCX Administration web interface to run Unified CCX real-time reports.

The following sections provide more information about real-time Unified CCX data.

---

**Note**

Real-Time Reporting for Unified CCX is not supported with Chrome. Use Microsoft Internet Explorer or Mozilla Firefox for accessing the RTR page.
# 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.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Tasks</td>
<td>Provides information about currently active applications.</td>
</tr>
<tr>
<td>Application Tasks Summary</td>
<td>Provides a summary of specific application activity.</td>
</tr>
<tr>
<td>Applications</td>
<td>Provides a list of all applications loaded on the Unified CCX server.</td>
</tr>
<tr>
<td>Contacts Summary</td>
<td>Provides information for call contacts, email contacts, and HTTP contacts. Also provides the total number of contacts.</td>
</tr>
<tr>
<td>Contacts</td>
<td>Provides information about currently active contacts.</td>
</tr>
<tr>
<td>Chat CSQ Cisco Unified Contact Center Express Stats</td>
<td>Provides information about Chat CSQ activity. This report is available only if Unified CCX has been configured.</td>
</tr>
<tr>
<td>Chat Resource Cisco Unified Contact Center Express Stats</td>
<td>Provides information about Chat Unified CCX resources activity.</td>
</tr>
<tr>
<td>CSQ Cisco Unified Contact Center Express Stats</td>
<td>Provides information about CSQ activity. This report is available only if Unified CCX has been configured.</td>
</tr>
<tr>
<td>Data Source Usage</td>
<td>Provides information about configured data source names (DSNs).</td>
</tr>
<tr>
<td>Engine Tasks</td>
<td>Provides information about currently active Engine tasks.</td>
</tr>
<tr>
<td>Preview Outbound Campaign Cisco Unified Contact Center Express Stats</td>
<td>Provides information about real-time Unified CCX information for the Outbound preview dialer.</td>
</tr>
<tr>
<td>Outbound Campaign Stats</td>
<td>Provides real-time statistics on IVR and agent based progressive and predictive Outbound campaigns since the statistics were last reset.</td>
</tr>
</tbody>
</table>

**Note** Calls made by the Outbound subsystem will not be displayed in the Contacts Summary Real-Time Report.

**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.
### Open Real-Time Reports

Real-Time reporting is available from the Unified CCX Administration 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**

• Use Mozilla Firefox and Internet Explorer for Real Time Reporting.

• If you are using Mozilla Firefox, you must manually install the correct version of JRE to use real-time reports.

---

The Application Reporting web page is a stand-alone component of the Unified CCX Administration interface. It has its own menu bar, which replaces the Unified CCX Administration 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 CCX Administration 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 CCX Administration 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 CCX Administration 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
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 CCX Administration 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**

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

When you choose Tools > Real-Time Reporting from the Unified CCX Administration 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 173
- Application Tasks Summary, on page 175
- Application Tasks Real-Time Report, on page 175
- Engine Tasks Real-Time Report, on page 176
- Contacts Report, on page 176
- Applications Report, on page 181
- Sessions Report, on page 181
- Data Source Usage Report, on page 182
- Overall Cisco Unified Contact Center Express Stats Report, on page 182
- CSQ Cisco Unified Contact Center Express Stats Report, on page 186
- Preview Outbound Campaign Cisco Unified Contact Center Express Stats Report, on page 188
- Outbound Campaign Stats Report, on page 193
- Overall Outbound Stats Report, on page 196
- Resource Cisco Unified Contact Center Express Stats Report, on page 197
- Failover Behavior for Unified CCX Stats, on page 199

**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.
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.

<table>
<thead>
<tr>
<th>Failover Scenario</th>
<th>Connection Status</th>
<th>Node 1 Status</th>
<th>Node 2 Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both nodes are up</td>
<td>Fully Connected</td>
<td>Node ID current/start-time</td>
<td>Node ID current/start-time</td>
</tr>
<tr>
<td>Node 1 is up</td>
<td>Partially Connected</td>
<td>Node ID current/start-time</td>
<td>Node ID Not Connected</td>
</tr>
<tr>
<td>Node 2 is down</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node 1 is down</td>
<td>Partially Connected</td>
<td>Node ID Not Connected</td>
<td>Node ID current/start-time</td>
</tr>
<tr>
<td>Node 2 is up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Both nodes are down</td>
<td>Not Connected</td>
<td>Node ID Not Connected</td>
<td>Node ID Not Connected</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Active contacts that are currently running.</td>
</tr>
<tr>
<td>Inbound</td>
<td>Number of inbound contacts since the statistics were last reset.</td>
</tr>
<tr>
<td>Outbound</td>
<td>Number of outbound contacts since the statistics were last reset.</td>
</tr>
</tbody>
</table>
### Contacts Summary Real-Time Report

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>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).</td>
</tr>
</tbody>
</table>
| Terminated  | Number of terminated contacts since the statistics were last reset. This row reports contacts that are ended normally by the application (for example, a caller hangs up 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.                                                                                                                                                                                                                               |
| 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  
  **Note** 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.                       |
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Handled</td>
<td>Number of handled contacts since the statistics were last reset.</td>
</tr>
<tr>
<td></td>
<td>This row reports contacts that are explicitly marked “Handled” by the application (typically when the application connects the contact to a Unified CCX agent).</td>
</tr>
<tr>
<td>Abandoned</td>
<td>Number of abandoned contacts since the statistics were last reset.</td>
</tr>
<tr>
<td></td>
<td>This row reports contacts that end without being marked “Handled” by the application.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>Names of the applications that are running or have run.</td>
</tr>
<tr>
<td>Running</td>
<td>Currently running applications.</td>
</tr>
<tr>
<td>Completed</td>
<td>Applications that have stopped running.</td>
</tr>
<tr>
<td>Total</td>
<td>Number of times an application was invoked since the statistics were last reset.</td>
</tr>
<tr>
<td>DTMF VB and AA</td>
<td>Application names configured from the Unified CCX Administration.</td>
</tr>
<tr>
<td>Status</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Unique identifier of the engine task.</td>
</tr>
<tr>
<td>Parent ID</td>
<td>Unique identifier for the parent of the engine task (if any).</td>
</tr>
<tr>
<td>Node ID</td>
<td>Unique identifier for a server in the cluster.</td>
</tr>
<tr>
<td>Server IP Address</td>
<td>IP address identifying the server in the cluster.</td>
</tr>
<tr>
<td>Script</td>
<td>Name of the script that is running the task (if the task is running a Unified CCX script).</td>
</tr>
<tr>
<td>Start Time</td>
<td>Time that the task started.</td>
</tr>
<tr>
<td>Duration</td>
<td>Length of time the task has been active.</td>
</tr>
</tbody>
</table>

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.

Contacts Report

Use the Contacts real-time report to view information for all the active contacts for all servers across clusters.
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 178
- Email Detailed Info Report, on page 178
- HTTP Detailed Info Report, on page 179

The following fields are displayed on the Contacts report.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Unique identifier representing a contact.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of contact: Unified CM Telephony call, Cisco agent call, or</td>
</tr>
<tr>
<td>Impl ID</td>
<td>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.</td>
</tr>
<tr>
<td>Node ID</td>
<td>Unique identifier for a server in the cluster.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Time stamp when the contact was created.</td>
</tr>
<tr>
<td>Duration</td>
<td>Length of time that the contact is active.</td>
</tr>
<tr>
<td>Handled</td>
<td>If True, the contact is handled; if False, the contact is not handled.</td>
</tr>
<tr>
<td>Aborting</td>
<td>If True, the contact is aborted with a default treatment; if False, the contact is not aborted.</td>
</tr>
<tr>
<td>Application</td>
<td>Name of the application currently managing the contact.</td>
</tr>
<tr>
<td>Task</td>
<td>Unique identifier of the application task that is currently responsible for the contact.</td>
</tr>
<tr>
<td>Session</td>
<td>Unique identifier of the session currently managing the contact (if any).</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Current state of the contact.</td>
</tr>
<tr>
<td>Inbound</td>
<td>If True, this call was received by the Unified CCX server; if False, this call was placed as an outbound call by an application.</td>
</tr>
<tr>
<td>Language</td>
<td>The selected language context of the call.</td>
</tr>
<tr>
<td>Application ID</td>
<td>Unique identifier of the associated application.</td>
</tr>
<tr>
<td>Called Number</td>
<td>Called number for this call leg from the perspective of the called party.</td>
</tr>
<tr>
<td>Dialed Number</td>
<td>Dialed number for this call leg from the perspective of the calling party.</td>
</tr>
<tr>
<td>Calling Number</td>
<td>Calling number of the originator of this call.</td>
</tr>
<tr>
<td>ANI</td>
<td>Automatic number identification.</td>
</tr>
<tr>
<td>DNIS</td>
<td>Dialed number identification service.</td>
</tr>
<tr>
<td>CLID</td>
<td>Caller ID.</td>
</tr>
<tr>
<td>Arrival Type</td>
<td>Information on how the call contact arrived in the system.</td>
</tr>
<tr>
<td>Last Redirected Number</td>
<td>Number from which the last call diversion or transfer was invoked.</td>
</tr>
<tr>
<td>Original Called Number</td>
<td>Originally called number.</td>
</tr>
<tr>
<td>Original Dialed Number</td>
<td>Originally dialed number.</td>
</tr>
<tr>
<td>ANI Digits</td>
<td>Automatic Number Identification information indicator digit codes.</td>
</tr>
<tr>
<td>CED</td>
<td>Entered digits that were gathered by the network before the call was received.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Current state of the contact.</td>
</tr>
<tr>
<td>Inbound</td>
<td>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.</td>
</tr>
<tr>
<td>Language</td>
<td>Selected language context of the email message.</td>
</tr>
<tr>
<td>Application ID</td>
<td>Unique identifier of the associated application.</td>
</tr>
<tr>
<td>From</td>
<td>Sender of this email message.</td>
</tr>
<tr>
<td>To</td>
<td>All the recipients of this email message.</td>
</tr>
<tr>
<td>Subject</td>
<td>“Subject” field of this email message.</td>
</tr>
<tr>
<td>Attachments</td>
<td>List of all attachments (file names) associated with this email message.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Current state of the contact.</td>
</tr>
<tr>
<td>Inbound</td>
<td>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.</td>
</tr>
<tr>
<td>Language</td>
<td>Language currently associated with the HTTP request.</td>
</tr>
<tr>
<td>Application ID</td>
<td>Unique identifier of the associated application.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Name of the authentication scheme used to protect the servlet; for example, “BASIC” or “SSL.”</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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. |
| 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name of the currently loaded application.</td>
</tr>
<tr>
<td>ID</td>
<td>Application ID.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of application that is currently running (for example, a Cisco Script Application).</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the application as entered on the Unified CCX Administration web site.</td>
</tr>
<tr>
<td>Enabled</td>
<td>If True, the application is enabled; if False, the application is disabled.</td>
</tr>
<tr>
<td>Max. Sessions</td>
<td>Maximum number of simultaneous task instances that can run simultaneously on the Unified CCX server.</td>
</tr>
<tr>
<td>Valid</td>
<td>If True, the application is valid; if False, the application is invalid.³</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Session ID.</td>
</tr>
<tr>
<td>Note</td>
<td>This identifier is guaranteed to remain unique for a period of 12 months.</td>
</tr>
<tr>
<td>Mapping ID</td>
<td>User- or system-defined identifier that maps to this session.</td>
</tr>
<tr>
<td>Node ID</td>
<td>Unique identifier for a server in the cluster.</td>
</tr>
<tr>
<td>Parent</td>
<td>Sessions that were created as a result of consult calls propagated in the system.</td>
</tr>
<tr>
<td>Creation Time</td>
<td>Creation time of the session.</td>
</tr>
</tbody>
</table>
Current state of the session. 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Source Name</td>
<td>Name of the data source, as configured through the Unified CCX Administration web interface.</td>
</tr>
<tr>
<td>Available Connections</td>
<td>Number of connections available.</td>
</tr>
<tr>
<td>Busy Connections</td>
<td>Number of busy connections.</td>
</tr>
<tr>
<td>Checkouts Granted</td>
<td>Number of times the database connections have been used up since the statistics were last reset.</td>
</tr>
<tr>
<td>Checkouts Denied</td>
<td>Number of times the Database connections have been denied since the statistics were last reset.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resource Information</strong></td>
<td></td>
</tr>
<tr>
<td>CSQs</td>
<td>Number of CSQs currently configured. If a CSQ is added or removed, this statistic reflects that change.</td>
</tr>
<tr>
<td>Logged-in Resources</td>
<td>Number of resources currently logged in.</td>
</tr>
<tr>
<td>Talking Resources</td>
<td>Number of resources currently talking. <em>Note</em> This number includes resources in Talking, Work, and Reserved states.</td>
</tr>
<tr>
<td>Ready Resources</td>
<td>Number of resources currently ready.</td>
</tr>
<tr>
<td>Not Ready Resources</td>
<td>Number of resources currently not ready.</td>
</tr>
<tr>
<td><strong>Call Information — Inbound</strong></td>
<td></td>
</tr>
<tr>
<td>Total Contacts</td>
<td>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.</td>
</tr>
<tr>
<td>Contacts Waiting</td>
<td>Number of contacts waiting to be connected to a resource. <em>Note</em> 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.</td>
</tr>
<tr>
<td>Oldest Contact in Queue</td>
<td>Displays the wait time for the oldest contact in the queue.</td>
</tr>
<tr>
<td>Contacts Handled</td>
<td>Number of contacts that have been handled by a resource.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Contacts Abandoned</td>
<td>Number of contacts that have arrived and disconnected before being connected to a resource.</td>
</tr>
<tr>
<td>Avg Talk Duration</td>
<td>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.</td>
</tr>
<tr>
<td>Avg Wait Duration</td>
<td>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.</td>
</tr>
<tr>
<td>Longest Talk Duration</td>
<td>Longest talk duration (in seconds) of a contact. Talk duration does not include hold time.</td>
</tr>
<tr>
<td>Longest Wait Duration</td>
<td>Longest wait (in seconds) for a contact to be connected to a resource. Wait duration does not include hold time.</td>
</tr>
</tbody>
</table>

**Call Information — Preview Outbound**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Total number of preview outbound calls currently previewed or connected to agents.</td>
</tr>
<tr>
<td>Preview</td>
<td>Total number of preview outbound calls currently previewed but have not been accepted, rejected, or closed by the agents.</td>
</tr>
<tr>
<td>Connected</td>
<td>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.</td>
</tr>
<tr>
<td>Offered</td>
<td>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.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Accepted</td>
<td>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.</td>
</tr>
<tr>
<td>Rejected</td>
<td>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.</td>
</tr>
<tr>
<td>Closed</td>
<td>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.</td>
</tr>
<tr>
<td>Timed-Out</td>
<td>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.</td>
</tr>
<tr>
<td>Invalid Number</td>
<td>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. <strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Voice</td>
<td>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.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Answering Machine</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Requested Callback</td>
<td>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.</td>
</tr>
<tr>
<td>Avg Outbound Talk Duration</td>
<td>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.</td>
</tr>
<tr>
<td>Longest Outbound Talk Duration</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the CSQ.</td>
</tr>
<tr>
<td>Talking/Ready Resources/Not Ready Resources/Logged-In Resources</td>
<td>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. <strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Total Contacts</td>
<td>Number of total contacts since the statistics were last reset for this CSQ.</td>
</tr>
<tr>
<td>Contacts Waiting</td>
<td>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.</td>
</tr>
<tr>
<td>Contacts [oldest contact in queue]</td>
<td>Duration of longest currently waiting contact.</td>
</tr>
<tr>
<td>Contacts Handled</td>
<td>Number of contacts that have been handled by this CSQ.</td>
</tr>
<tr>
<td>Contacts Abandoned</td>
<td>Number of contacts that have been abandoned by this CSQ.</td>
</tr>
<tr>
<td>Contacts Dequeued</td>
<td>Number of contacts that have been dequeued from this CSQ.</td>
</tr>
<tr>
<td>Avg Talk Duration</td>
<td>Average time (in seconds) agents in this CSQ spent talking to contacts.</td>
</tr>
<tr>
<td>Avg Wait Duration</td>
<td>Average wait time (in seconds). It begins when the call was queued (when you execute 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.</td>
</tr>
<tr>
<td>Longest Talk Duration</td>
<td>Longest time (in seconds) agents in this CSQ spend talking to contacts.</td>
</tr>
</tbody>
</table>
Longest wait (in seconds) for a contact to be connected to a resource.

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Longest Wait Duration</td>
<td>Longest wait (in seconds) for a contact to be connected to a resource.</td>
</tr>
<tr>
<td>Campaign</td>
<td>The name of the preview outbound campaign.</td>
</tr>
<tr>
<td>Status</td>
<td>The current activation state of the preview outbound campaign:</td>
</tr>
<tr>
<td></td>
<td>• Running: an active preview outbound campaign</td>
</tr>
<tr>
<td></td>
<td>• Stopped: an inactive preview outbound campaign</td>
</tr>
<tr>
<td>Active</td>
<td>Total number of outbound calls currently previewed by or connected to agents for this preview outbound campaign. Active Calls = Previewed + Connected.</td>
</tr>
<tr>
<td>Preview</td>
<td>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.</td>
</tr>
<tr>
<td>Connected</td>
<td>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.</td>
</tr>
<tr>
<td>Offered</td>
<td>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.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Accepted</td>
<td>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.</td>
</tr>
<tr>
<td>Rejected</td>
<td>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.</td>
</tr>
<tr>
<td>Closed</td>
<td>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.</td>
</tr>
<tr>
<td>Timed-Out</td>
<td>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.</td>
</tr>
<tr>
<td>Invalid Number</td>
<td>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. <strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Voice</td>
<td>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.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Answering Machine</td>
<td>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.</td>
</tr>
<tr>
<td>Requested Callback</td>
<td>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.</td>
</tr>
<tr>
<td>Avg Talk Duration</td>
<td>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.</td>
</tr>
<tr>
<td>Longest Talk Duration</td>
<td>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.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the chat CSQ</td>
</tr>
<tr>
<td>Busy Resources/Ready Resources/Not Ready Resources/Logged-In Resources</td>
<td>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. <strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Total Contacts</td>
<td>Number of total contacts presented to this queue since last reset of statistics.</td>
</tr>
<tr>
<td>Contacts Waiting [Oldest Contact in Queue]</td>
<td>Number of contacts waiting in this queue with the duration of longest waiting contact in this queue.</td>
</tr>
<tr>
<td>Contacts Handled</td>
<td>Number of contacts that have been handled by this queue since last reset of statistics.</td>
</tr>
<tr>
<td>Contacts Abandoned</td>
<td>Number of contacts that have been abandoned in this queue since last reset of statistics.</td>
</tr>
<tr>
<td>Avg Contact Handling Duration</td>
<td>Average time (in HH:MM:SS) agents in this CSQ spent chatting with contacts.</td>
</tr>
<tr>
<td>Avg Wait Duration</td>
<td>Average wait time (in HH:MM:SS) a contact spent in queue waiting for an agent.</td>
</tr>
<tr>
<td>Longest Contact Handling Duration</td>
<td>Longest time (in HH:MM:SS) agents in this CSQ spent chatting with contacts.</td>
</tr>
<tr>
<td>Longest Wait Duration</td>
<td>Longest wait (in HH:MM:SS) for a contact to be connected to an agent.</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name (ID)</td>
<td>Unique identifier of the resource.</td>
</tr>
<tr>
<td>State</td>
<td>Current state of the resource.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Current Active Contacts</td>
<td>Number of active contacts that the agent is handling.</td>
</tr>
<tr>
<td>Duration in State</td>
<td>Length of time (in HH:MM:SS) the resource has remained in the current state.</td>
</tr>
<tr>
<td>Avg Resource Busy Duration</td>
<td>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.</td>
</tr>
<tr>
<td>Longest Resource Busy Duration</td>
<td>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.</td>
</tr>
<tr>
<td>Contacts Presented</td>
<td>Number of contacts that have been presented to this resource.</td>
</tr>
<tr>
<td>Contacts Handled</td>
<td>Number of contacts that have been handled by this resource.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resource Information</strong></td>
<td></td>
</tr>
<tr>
<td>CSQs</td>
<td>Number of chat CSQs currently configured. If a chat CSQ is added or removed, this statistic reflects that change.</td>
</tr>
<tr>
<td>Logged-in Resources</td>
<td>Number of resources currently logged in.</td>
</tr>
<tr>
<td>Busy Resources</td>
<td>Number of resources currently busy.</td>
</tr>
<tr>
<td>Ready Resources</td>
<td>Number of resources currently ready.</td>
</tr>
<tr>
<td>Not Ready Resources</td>
<td>Number of resources currently not ready.</td>
</tr>
<tr>
<td><strong>Contact Information</strong></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Total Contacts</td>
<td>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.</td>
</tr>
<tr>
<td>Contacts Waiting</td>
<td>Number of contacts waiting to be connected to a resource.</td>
</tr>
<tr>
<td>Note</td>
<td>A contact is shown as waiting until the contact is answered by the agent.</td>
</tr>
<tr>
<td>Oldest Contact in Queue</td>
<td>Displays the wait time for the oldest contact in the queue.</td>
</tr>
<tr>
<td>Contacts Handled</td>
<td>Number of contacts that have been handled by a resource.</td>
</tr>
</tbody>
</table>
| 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.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Campaign Name</td>
<td>The name of the IVR-based or agent-based progressive or predictive campaign.</td>
</tr>
</tbody>
</table>
| 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 executing 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. |
<p>| Answering Machine | The total number of calls that reached an answering machine. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid Number</td>
<td>The total number of calls that reached an invalid number:</td>
</tr>
<tr>
<td></td>
<td>• A failed call when the gateway returns an invalid or not found error.</td>
</tr>
<tr>
<td>Fax/Modem</td>
<td>The total number of calls that reached fax or modem.</td>
</tr>
<tr>
<td>No Answer</td>
<td>The total number of calls that were not answered within the time configured for the No Answer Ring</td>
</tr>
<tr>
<td></td>
<td>Limit field in the Add New Campaign web page.</td>
</tr>
<tr>
<td>Busy</td>
<td>The total number of calls that reached a busy destination.</td>
</tr>
<tr>
<td>Failed</td>
<td>The total number of calls that failed due to any one of the following reasons:</td>
</tr>
<tr>
<td></td>
<td>• Dialer asked the Gateway to cancel a call that was dialed out, but not connected.</td>
</tr>
<tr>
<td></td>
<td>• Gateway has declined the call.</td>
</tr>
<tr>
<td></td>
<td>• Gateway failure or configuration issues at the Gateway.</td>
</tr>
<tr>
<td></td>
<td>• Gateway is down.</td>
</tr>
<tr>
<td>Active</td>
<td>The total number of calls that were connected to IVR ports or agents.</td>
</tr>
<tr>
<td></td>
<td>All the voice calls that will be connected to Outbound IVR ports or agents will be marked as active.</td>
</tr>
<tr>
<td></td>
<td>If you have selected Answering Machine Treatment or Abandoned Call Treatment as &quot;Transfer to IVR,&quot; the</td>
</tr>
<tr>
<td></td>
<td>answering machine calls and abandoned calls that are getting transferred to Outbound IVR ports will</td>
</tr>
<tr>
<td></td>
<td>also be marked as active.</td>
</tr>
<tr>
<td>Customer Abandoned</td>
<td>The total number of calls that were disconnected by the customer or agent within the Abandoned Call</td>
</tr>
<tr>
<td></td>
<td>Wait Time configured in Add New Campaign web page.</td>
</tr>
<tr>
<td>System Abandoned</td>
<td>The total number of calls that were abandoned due to any of the following reasons:</td>
</tr>
<tr>
<td></td>
<td>• Non-availability of ports or agents.</td>
</tr>
<tr>
<td></td>
<td>• Any issues at system level.</td>
</tr>
<tr>
<td>Abandon Rate (in %)</td>
<td>Abandon Rate = (System Abandoned/Voice)*100</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Attempted</td>
<td>The total number of attempted Outbound calls.</td>
</tr>
<tr>
<td>Voice</td>
<td>The total number of Outbound calls that were connected to live voice.</td>
</tr>
<tr>
<td>Answering Machine</td>
<td>The total number of Outbound calls that reached answering machine.</td>
</tr>
<tr>
<td>Invalid Number</td>
<td>The total number of Outbound calls that reached an invalid number.</td>
</tr>
<tr>
<td>Fax/Modem</td>
<td>The total number of Outbound calls that reached fax or modem.</td>
</tr>
<tr>
<td>No Answer</td>
<td>The total number of Outbound calls that were not answered.</td>
</tr>
<tr>
<td>Busy</td>
<td>The total number of Outbound calls that reached a busy destination.</td>
</tr>
<tr>
<td>Failed</td>
<td>The total number of failed Outbound calls for all IVR and agent based Outbound campaigns.</td>
</tr>
<tr>
<td>Active</td>
<td>The total number of Outbound calls that were connected to Outbound IVR ports or agents.</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name (ID)</td>
<td>Unique identifier of the agent.</td>
</tr>
<tr>
<td>State</td>
<td>Current state of the agent.</td>
</tr>
<tr>
<td>Duration in State</td>
<td>Amount of time (in seconds) the agent has remained in the current state.</td>
</tr>
<tr>
<td>Contacts Presented</td>
<td>Number of contacts presented to the agent.</td>
</tr>
<tr>
<td>Contacts Handled</td>
<td>Number of contacts handled by the agent.</td>
</tr>
<tr>
<td>Avg Talk Duration</td>
<td>Average time (in seconds) the agent spent in talking state.</td>
</tr>
<tr>
<td>Avg Hold Duration</td>
<td>Average time (in seconds) the agent keeps calls on hold.</td>
</tr>
<tr>
<td>Longest Talk Duration</td>
<td>Longest time (in seconds) the agent spent in talking state.</td>
</tr>
<tr>
<td>Longest Hold Duration</td>
<td>Longest time (in seconds) the agent keeps a call on hold.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Outbound Offered</td>
<td>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.</td>
</tr>
<tr>
<td>Outbound Accepted</td>
<td>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 Agent AutoAnswer is disabled).</td>
</tr>
<tr>
<td>Outbound Rejected</td>
<td>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.</td>
</tr>
<tr>
<td>Outbound Closed</td>
<td>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.</td>
</tr>
<tr>
<td>Outbound Timed-Out</td>
<td>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.</td>
</tr>
<tr>
<td>Outbound Voice</td>
<td>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.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Outbound Avg Talk Duration</td>
<td>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.</td>
</tr>
<tr>
<td>Outbound Avg Hold Duration</td>
<td>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.</td>
</tr>
<tr>
<td>Outbound Longest Talk Duration</td>
<td>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.</td>
</tr>
<tr>
<td>Outbound Longest Hold Duration</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.

**Procedure**

Choose **Tools > Reset All Statistics** from the Application Reporting menu bar.

**Note**

The Unified CCX system automatically resets all statistics each day at midnight.

**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 Contacts Real-Time Report

To clear stuck calls or contacts from the Unified CCX system:
Procedures

**Clear Stuck Calls from Overall Cisco Unified CCX Stats**

To clear stuck calls/contacts from the Unified CCX system:

1. Choose **Reports > Overall Cisco Unified Contact Center Express Stats**.
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.
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**.
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.
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:

1. Choose **Reports > CSQ Cisco Unified Contact Center Express Stats**.
2. Choose the contact from **Views** and click **CSQ Waiting Contacts Info**.
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**.
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.
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polling Interval</td>
<td>Time between two requests to the server for new statistics by the client.</td>
</tr>
<tr>
<td>Server Connect Retry Count</td>
<td>The number of times that the Unified CCX Administration web interface should attempt to reconnect to the Unified CCX server.</td>
</tr>
</tbody>
</table>

**Note** If an error occurs, an Error dialog box opens to alert you that the server is not communicating with the web interface.
Reporting Administration on Unified Intelligence Center

Overview

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:


**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.

**Related Topics**

- Introduction, on page 343
- Cisco Finesse Administration Console, on page 343
- Getting Started, on page 343
- Administration Tools, on page 344
- Cisco Finesse Administration Console, on page 344
- Sign In to Cisco Finesse Administration Console, on page 344
- Account Locked After Five Failed Sign In Attempts, on page 345
- Manage System Settings, on page 351
- Context Service Settings, on page 351

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Logged Off Resources</td>
<td>Specifies whether logged off agents appear in reports.</td>
</tr>
</tbody>
</table>

Click **Apply** to submit configuration changes.
Overview

Edit Wrap-Up Reason, on page 389
Delete Wrap-Up Reason, on page 390
Manage Team Resources, on page 390
Team Resources, on page 390
Assign Phone Books and Reasons to Team, on page 392
Unassign Phone Books and Reasons from Team, on page 392
Assign Custom Desktop Layout to Team, on page 393
Assign Workflows to Team, on page 393
Unassign Workflows from Team, on page 394
Manage Workflows, on page 394
Workflows and Workflow Actions, on page 394
Workflow Triggers and Outbound Calls, on page 397
Add Browser Pop Workflow Action, on page 398
Add HTTP Request Workflow Action, on page 399
Edit Workflow Action, on page 400
Delete Workflow Action, on page 400
Add Workflow, on page 401
Edit Workflow, on page 401
Delete Workflow, on page 402
Manage Security, on page 402
HSTS, on page 402
Trust Self-Signed Certificate, on page 348
Obtain and Upload CA Certificate, on page 347
Add Certificate for HTTPS Gadget, on page 350
Add Certificate for Multi-session Chat and Email, on page 350
Manage Finesse IP Phone Agent, on page 403
Finesse IP Phone Agent, on page 403
One Button Sign In, on page 403
Finesse IP Phone Service Subscription Options, on page 404
Set Up Application User, Web Access, and HTTPS Server Parameters, on page 405
Configure Finesse IP Phone Service in Unified CM, on page 406
Add Service Parameters for One Button Sign In
Subscribe Agent Phones to Manual Subscription Service, on page 410
Set Up Agent Access to the Self Care Portal, on page 411
CTI Failover
Finesse IP Phone Agent Failover
Backup and Restore, on page 411
Additional Language Support, on page 412
Cisco Finesse Agent and Supervisor Desktop, on page 412
Call Manager-Based Call Recording Using Cisco MediaSense, on page 412
Configure Cisco MediaSense with Unified CM, on page 412
Upload Cisco MediaSense Certificate to Unified CCX Server, on page 413
Upload MediaSense Recording License, on page 413
Configure MediaSense as a Recording Server, on page 414
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 multi-layered 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 9: Fields on User List Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only show currently active users</td>
<td>Check the check box to display users who are currently active.</td>
</tr>
<tr>
<td>Name Contains</td>
<td>Use this filter field to narrow the list of names or to move to a specific name.</td>
</tr>
<tr>
<td>User Name</td>
<td>The domain and user name (domain\name).</td>
</tr>
<tr>
<td>First Name</td>
<td>The user's first name.</td>
</tr>
<tr>
<td>Last Name</td>
<td>The user's last name.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Navigate to Security &gt; User List.</td>
</tr>
</tbody>
</table>
| **Step 2** | Under the General Information tab, perform the following:  
  a) In the User Name field, enter the domain and user name (domain\username).  
  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 execute 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 10: Fields on the User Groups Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the group.</td>
</tr>
<tr>
<td>Name Contains</td>
<td>Use this filter field to narrow down the list of group names or to move to a specific name.</td>
</tr>
</tbody>
</table>
| 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.                                              |

You 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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Navigate to Security &gt; User Groups.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Under the General Information tab, perform the following:</td>
</tr>
<tr>
<td></td>
<td>a) In the Group Name field, enter the name of the group. This field is available only when you create a new group.</td>
</tr>
<tr>
<td></td>
<td>b) In the Description field, enter or modify text to describe this group</td>
</tr>
</tbody>
</table>
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 can 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.
- A user can only Edit or Save an entity even if the immediate parent category has no WRITE permissions.
- 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 11: Fields on the Group Members Tab**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permissions For panel (top left)</td>
<td>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.</td>
</tr>
<tr>
<td>All Groups panel (top right)</td>
<td>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.</td>
</tr>
<tr>
<td>All Users for the Selected Group panel (bottom right)</td>
<td>This panel shows all members in the group that is highlighted in the All Groups panel above.</td>
</tr>
<tr>
<td>Set Permissions button</td>
<td>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.</td>
</tr>
<tr>
<td>Group Permissions for the selected item</td>
<td>This panel shows the groups that have already been assigned permission for the selected object, and their permission level.</td>
</tr>
</tbody>
</table>
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 username 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permissions For panel (top left)</td>
<td>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.</td>
</tr>
<tr>
<td>User List panel (top right)</td>
<td>This panel shows current users. Filter the list and select one or many user names.</td>
</tr>
<tr>
<td>Show Groups button</td>
<td>Click this option to show the All Groups for the selected user panel.</td>
</tr>
<tr>
<td>All Groups for the selected User (bottom right)</td>
<td>This panel shows all groups to which the highlighted username in the User List panel above is a member.</td>
</tr>
<tr>
<td>Set Permissions button</td>
<td>Click this option to open a dialog box where you select the permission level for the object (Execute, Write).</td>
</tr>
<tr>
<td>All Permissions for the selected item</td>
<td>This panel shows users who have permission for the object, and the level of permissions they have.</td>
</tr>
</tbody>
</table>

**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.
• 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.
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 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.

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.

---

**Note**

In this guide, the underscore character linking each word differentiates the national do_not_call list from the Outbound subsystem's 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

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 Cisco Finesse 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.

Related Topics
- Configure General Outbound Properties, on page 224
- Add New Area Code, on page 304
- Configure SIP Gateway, on page 305
- Add New Campaigns, on page 303

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)

**Outbound Call Timeout (seconds)**

If an agent does not respond to the Outbound preview call on Cisco Finesse 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 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**

- This field is used only when Agent AutoAnswer is disabled for agent-based progressive and predictive outbound campaigns.
- If the Unified CCX Engine or Finesse restarts when a 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'.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
| 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. |
| Agent AutoAnswer              | 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. This check box is checked by default.  
**Note**  
- Either check this option in Unified CCX, or set Auto Answer to 'yes' in Unified Communications Manager. Do not select both of these options.  
- Enable Agent Autoanswer so that the call presented to the agent is automatically answered. A beep tone notifies the agent that the call has been answered.  
- If the workflow is enabled, it will be executed irrespective of the status (Checked/unchecked) of the AutoAnswer 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.

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.

Related Topics
  About Unified CCX Applications, on page 43
  Configure Script Applications, on page 43
  Add New Cisco Script Application, on page 45
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select the type of the campaign</strong></td>
<td></td>
</tr>
</tbody>
</table>
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.
### Add New Campaign

**Field** | **Description**
---|---
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.

<table>
<thead>
<tr>
<th><strong>Fields displayed only if you have selected IVR-based campaign type</strong></th>
</tr>
</thead>
</table>
| 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.

<p>| <strong>Fields displayed only if you have selected Agent-based campaign type</strong> |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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**
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Records</td>
<td>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.</td>
</tr>
<tr>
<td>Cache Size</td>
<td>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</td>
</tr>
<tr>
<td>Answering Machine</td>
<td>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</td>
</tr>
<tr>
<td>Retry</td>
<td></td>
</tr>
</tbody>
</table>

The following fields in Dialing Options are displayed if you have selected IVR-based campaign type
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 220 to know how the licensed IVR ports are distributed between the inbound and outbound IVR calls in different scenarios.
**Field** | **Description**
---|---
**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** If you change this value in the middle, the predictive algorithm will take the updated value in this field during the next iteration.

This is a mandatory field.

Default value = 1.5; Range = 1 to 3.

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** If you change this value in the middle, the predictive algorithm will take the updated value in this field during the next iteration.

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
### Field | Description
--- | ---
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.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
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. |
### Unified CCX Outbound Dialer Configuration

#### Add New Campaign

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following field in Dialing Options is displayed only if you have selected Predictive dialer type for an Agent-based campaign</td>
<td></td>
</tr>
</tbody>
</table>
| 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 remain 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. |
The timeduration (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 than the value set for the Callback Time Limit.

The timeduration (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

If the dialer abandons a call, the time duration (in minutes) after which the dialer should call back the customer.

Default value = 0

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.
When you import contact that have agent extension numbers, ensure that the agents are not logged in when the campaigns are executed.

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).
- The maximum limit of contacts in the contacts file is 1 million.
- 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
  - The number of contacts present in the contacts file being imported
- After the import of contacts, ensure that a maximum of 20,000 contacts remaining (yet to be dialed) to be imported for a campaign.
- 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 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 1 million.

- 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 1 million 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 failover, then 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.
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.
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the campaign.</td>
</tr>
<tr>
<td>Start Time/End Time (hh:mm) AM/PM</td>
<td>Start Time and End Time fields indicate the time range during which the campaign runs.</td>
</tr>
<tr>
<td>Remaining Contacts</td>
<td>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.</td>
</tr>
<tr>
<td>Enabled</td>
<td>The Enabled field indicates to the Outbound subsystem whether this campaign is currently active.</td>
</tr>
<tr>
<td>Campaign Type</td>
<td>Denotes whether a specific campaign is IVR-based or Agent-based. The existing campaigns will be marked as Agent-based after an upgrade.</td>
</tr>
<tr>
<td>Delete</td>
<td>Click Delete icon next to the name of the campaign that you want to delete.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Caution</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Call Status</th>
<th>Value (stored in database)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending</td>
<td>1</td>
<td>The call is pending. This is the initial state for all records.</td>
</tr>
<tr>
<td>Active</td>
<td>2</td>
<td>The record was retrieved by the Outbound subsystem for dialing.</td>
</tr>
<tr>
<td>Closed</td>
<td>3</td>
<td>The record is closed (not dialed).</td>
</tr>
<tr>
<td>Callback</td>
<td>4</td>
<td>The record is closed (not dialed).</td>
</tr>
<tr>
<td>Max Calls</td>
<td>5</td>
<td>Maximum attempts have been reached for this record (considered closed).</td>
</tr>
<tr>
<td>Retry</td>
<td>6</td>
<td>The record is redialed immediately whenever there is any miss in the callbacks for Retries with Delay.</td>
</tr>
<tr>
<td>Unknown</td>
<td>7</td>
<td>If the Outbound subsystem was restarted with records in the Active (2) state, they are moved to this state.</td>
</tr>
<tr>
<td>Retries with Delay</td>
<td>8</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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. |

• Dialing list records with a call result of Do Not Call are not deleted, as these records are exported to a text file.

• 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:

<table>
<thead>
<tr>
<th>Call Result</th>
<th>Value (stored in database)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>1</td>
<td>Customer answered and was connected to agent.</td>
</tr>
<tr>
<td>Fax</td>
<td>2</td>
<td>Fax machine or modem detected.</td>
</tr>
<tr>
<td>Answering machine</td>
<td>3</td>
<td>Answering machine detected.</td>
</tr>
<tr>
<td>Call Result</td>
<td>Value (stored in database)</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Invalid</td>
<td>4</td>
<td>Number reported as invalid by the network.</td>
</tr>
<tr>
<td>Wrong Number</td>
<td>6</td>
<td>Number successfully contacted but wrong number.</td>
</tr>
<tr>
<td>Customer Not Home</td>
<td>7</td>
<td>Number successfully contacted but reached the wrong person.</td>
</tr>
<tr>
<td>Callback</td>
<td>8</td>
<td>Customer requested callback.</td>
</tr>
<tr>
<td>Agent Rejected</td>
<td>9</td>
<td>Agent skipped or rejected the preview call.</td>
</tr>
<tr>
<td>Agent Closed</td>
<td>10</td>
<td>Agent skipped or rejected the preview call with the close option (not dialed).</td>
</tr>
<tr>
<td>Busy</td>
<td>11</td>
<td>Busy tone detected.</td>
</tr>
<tr>
<td>Ring No Answer</td>
<td>12</td>
<td>Agent did not respond to the preview call within the time out duration.</td>
</tr>
<tr>
<td>Callback Failed</td>
<td>13</td>
<td>This value should not be written to the database; this is for internal use only.</td>
</tr>
<tr>
<td>Callback Missed</td>
<td>14</td>
<td>Callback missed and marked for Retry.</td>
</tr>
<tr>
<td>Timeout</td>
<td>15</td>
<td>Customer phone timed out either due to Ring No Answer (RNA) or Gateway failure.</td>
</tr>
<tr>
<td>Call Abandoned</td>
<td>16</td>
<td>Call was abandoned because IVR port was unavailable or Unified CCX failed due to transfer the call to the IVR port.</td>
</tr>
</tbody>
</table>

**Note** You can configure the time out duration using the Preview Call Timeout field detailed in the Configure General Outbound Properties.
Call Result | Value (stored in database) | Description |
---|---|---|
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 callback, 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.

<table>
<thead>
<tr>
<th>Call Result</th>
<th>Call Status</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice (1)</td>
<td>Closed (3)</td>
<td>This contact is not dialed again.</td>
</tr>
<tr>
<td>Fax (2)</td>
<td>Retry (6)</td>
<td>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.</td>
</tr>
<tr>
<td>Answering machine (3)</td>
<td>Retry (6)</td>
<td>This contact is retried, with the same phone number as before.</td>
</tr>
</tbody>
</table>
The call status is set to 5 (Closed) when the Outbound contact is no longer dialed for this campaign. This happens when a call was successfully placed (call result is voice) and also when an agent selects Skip-Closed, Reject-Closed, or Do Not Call. 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 is 15 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).

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.
Cisco Unified Contact Center Express Supervisor and User Options Plug-Ins

The following sections provide detailed information on the additional plug-in options provided by the Unified CCX.

- About User Management, on page 253
- About Unified CCX User Capabilities, on page 253
- Unified CCX Supervisor Web Interface, on page 255
- Unified CCX User Options Web Interface, on page 256

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.

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

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 cannot 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.

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the Unified CCX Administration, enter https://&lt;Cisco Unified CCX IP address&gt;/appuser.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>If prompted to do so, enter your UserID and Password. The Unified CCX User Options web page appears.</td>
</tr>
<tr>
<td>Note</td>
<td>Only Unified CM users are allowed to log in.</td>
</tr>
<tr>
<td>Step 3</td>
<td>When finished, click Logout.</td>
</tr>
</tbody>
</table>

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.
Cisco Unified Contact Center Express Supervisor and User Options Plug-Ins

Access Unified CM User Options Page
System Menu

The System menu of the Unified CCX Administration system provides options for performing system-related tasks. Depending on the product package you purchased, the System menu contains some or all of the following menu options:

- Access Server Menu, on page 259
- Unified CM Configuration, on page 261
- System Parameters, on page 261
- Recording Configuration, on page 266
- Single Sign-On (SSO), on page 266
- Custom File Configuration, on page 268
- Standalone Cisco Unified Intelligence Center Configuration, on page 268
- License Information, on page 269
- Language Information, on page 270
- Logout Menu, on page 271

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, IPv6 Address (for dual IPv4/IPv6), 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name/IP Address</td>
<td>Hostname or IP address of the server that you want to add.</td>
</tr>
<tr>
<td>IPv6 Address (for dual IPv4/IPv6)</td>
<td>IPv6 address of the server that you want to add.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address of the server that you want to add.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the server that you want to add.</td>
</tr>
</tbody>
</table>

Note
- This field is required only when IPv6 is enabled on the Unified CCX server.

Step 3
Click Add to add details of the new server.

Configure IPv6 Address

Follow this procedure to configure IPv6 addressing.

Procedure

Step 1
On the List Servers page, click on the server name link to edit the server details.

The Server Configuration web page opens.

Step 2
Enter the IPv6 address or remove it in the IPv6 Address (for dual IPv4/IPv6) field.

Step 3
Click Save to add the IPv6 address.
What to do next

Login to Cisco Unified CCX Serviceability page and click Tools>Control Center - Network Services. Restart the Cisco Unified Intelligence Center Reporting service.

Note

Eventhough the CTI ports are registered with dual stack or only with IPv6, this is displayed as IPv4 in the Call Manager.

Unified CM Configuration

Choose System > Unified CM Configuration from the Unified CCX Administration 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.

Related Topics

Configure Unified Communications Manager Information, on page 25

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 12: System Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic System Parameters</td>
<td></td>
</tr>
<tr>
<td>System Time Zone</td>
<td>The system or primary time zone will be 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you have changed the primary time zone, you need to reboot both the nodes in the Unified CCX cluster.</td>
</tr>
<tr>
<td>Network Deployment Parameters</td>
<td>(displayed only in a HA over WAN deployment)</td>
</tr>
</tbody>
</table>
### System Parameters

#### Network Deployment Type
Displays the network deployment type as LAN or WAN only if we have more than one node. Display only.

#### Internationalization Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizable Locales</td>
<td>Use to specify a unique locale. Default value is blank.</td>
</tr>
<tr>
<td>Default Currency</td>
<td>Default currency, such as American dollars (USD), Euros, and so on. This is a mandatory field. The system uses the default currency for converting currency amounts in a playable format when no currency designator is specified. Default: American Dollar [USD]</td>
</tr>
</tbody>
</table>

#### Media Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Codec</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> After changing the Codec, ensure that you restart Unified CCX Engine on all nodes for the settings to take effect.</td>
</tr>
<tr>
<td>Default TTS Provider</td>
<td>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.</td>
</tr>
<tr>
<td>User Prompts override System Prompts</td>
<td>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.</td>
</tr>
</tbody>
</table>

#### 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 will be able to see the teams 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.

## Max Number of Executed Steps
The maximum number of steps an application can execute 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 continues to be 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).*

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor Access</td>
<td>The Administrator uses this option to allow certain privileges to supervisors (all supervisors have the same privilege). The options are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>No access to teams</strong>—The supervisor logs into the Supervisor page, but will not be able to see any team information (No RmCm info).</td>
</tr>
<tr>
<td></td>
<td>- <strong>Access to all teams</strong>—The supervisor logs into the Supervisor page, and will be able to see all the teams (RmCm information).</td>
</tr>
<tr>
<td></td>
<td>- <strong>Access to supervisor teams only</strong>—The supervisor logs into the Supervisor page, and will be able to see the teams 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.</td>
</tr>
<tr>
<td></td>
<td><em>Default: No access to teams</em></td>
</tr>
<tr>
<td></td>
<td><em>Note</em> A supervisor who does not have administrator privileges can add, modify, or remove skills from an agent.</td>
</tr>
<tr>
<td>Max Number of Executed Steps</td>
<td>The maximum number of steps an application can execute before the Unified CCX Engine terminates the script or application. This is a mandatory field.</td>
</tr>
<tr>
<td></td>
<td>This limitation is intended to prevent a script from running indefinitely.</td>
</tr>
<tr>
<td></td>
<td><em>Default value is 1000.</em></td>
</tr>
<tr>
<td></td>
<td><em>Note</em> Do not change the default value.</td>
</tr>
<tr>
<td>Additional Tasks</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><em>Default value is 0.</em></td>
</tr>
<tr>
<td>Default Session Timeout</td>
<td>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 continues to be 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.</td>
</tr>
<tr>
<td></td>
<td>The default value is 30 minutes. If you reduce this number, you also reduce the system memory usage comparatively.</td>
</tr>
<tr>
<td></td>
<td>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 <em>Cisco Unified Contact Center Express Getting Started with Scripts</em> for more information.</td>
</tr>
<tr>
<td>Enterprise Call Info Parameter Separator</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>*Default value is</td>
</tr>
</tbody>
</table>

---

Cisco Unified Contact Center Express Administration and Operations Guide, Release 11.6(1)
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
| 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. |
| 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 the 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| RMI Port | The port number used by the Unified CCX CVD 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RmCm TCP Port</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Context Service Parameters

If there are any changes made in the Context Service Parameters, validate that the change is successfully reflected in the **Context Service Status** page before making any subsequent changes. The changes in the Request Timeout can be validated in the exported file from the **Context Service Status** page.

### Mode

Radio button to select the connection mode to connect with Context Service.
- Lab
- Production

Default value is Production.

**Note** Context Service in the Lab mode will create the data in the lab work group. When Context Service switches to the production mode, the data created in the lab work group will no longer be available in the production mode and vice versa. Lab mode is a work group created for test and debug.

### Request Timeout

The number of milliseconds (ms) the system should wait before rejecting the Context Service cloud connectivity.

Default value is 5000 milliseconds. Range is from 200 to 5000 milliseconds.

### Proxy Type

Determines if the Http proxy is used for Context Service connectivity.

Default value is None.

### 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.
Recording Configuration

Use the Recording Configuration web page to configure the host names, user name, and password to connect to the recording server such as Cisco MediaSense.

You must configure recording server details in Unified CCX so that supervisors can search and play recordings based on various filter criteria.

Choose System > Recording Configuration from the Unified CCX Administration menu bar to access the Recording Configuration web page.

This web page displays currently configured recording server details.

Note
User name must be a MediaSense API user. API user name is a Unified CM end user, who is configured in Cisco MediaSense as a MediaSense API user.


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.


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.

Related Topics

Manage System Parameters, on page 143
If Cisco Identity Service is configured, it displays the status as 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 executed operation. A green color icon indicates success in executed operation. A grey color icon indicates the inability to capture the status of the executed operation.

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 execute CLI command utilscui 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.
• 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 normal 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.

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 CCX Administration 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 Configuration

To access the Cisco Unified Intelligence Center standalone configuration webpage, perform the following steps:

Procedure

Step 1 Click System > Standalone CUIC configuration for configuring standalone CUIC.

Step 2 Enter FQDN (Fully Qualified Domain Name), DataSource Name, Username, and Password of standalone CUIC.

Step 3 Click Save. A Status message will be displayed.
Asterisk (*) indicates the required fields.

If the configuration is successful, a status message will be displayed. If the configuration is not successful, an error message will be displayed. This can be due to:

- An error in input validation (DataSource Name, Username or Password).
- A failure in connectivity between the CUIC and the Unified CCX servers.

License Information

Use the License Information web pages to display the cluster licensing information and to upload additional licenses.

Choose System > License Information > Add License(s) or Display License(s) from the Cisco Unified CCX Administration menu bar to access the License Information web pages.

Add Licenses

From the Unified CCX Administration menu bar:

Procedure

**Step 1** Choose System > License Information > Add License(s).

The License Information web page displays.

**Step 2** In the License File field, enter the path for the license file or click Browse to locate the license file. Select the required license file and click Open.

Use this page to specify a license file and upload it to Unified CCX.

**Step 3** Click Upload to upload the license file to Unified CCX.

Display Licenses

From the Unified CCX Administration menu bar:

Procedure

Choose System > License Information > Display License(s).

The License Information web page opens, displaying the details of the Configured License such as the license type, number of IVR ports, number of seats, maximum number of agents, and so on.
The License Information page displayed on click of **Display License(s)** menu option will also specify the expiry date in case of time-bound licenses.

For Unified CCX, if you have a premium license with an outbound license, this web page will display:

- The number of licensed IVR ports and dedicated IVR ports for IVR outbound.
- The number of licensed agent seats and concurrent 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.

---

**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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Choose IVR Language</strong></td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td>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 <strong>Set IVR Language</strong> option. The chosen language doesn't get automatically set and the value is not persisted after it is chosen.</td>
</tr>
<tr>
<td><strong>Set IVR Language</strong></td>
<td></td>
</tr>
<tr>
<td>IVR Language</td>
<td>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 <strong>Edit</strong> button. This is a mandatory field and you can choose from the drop-down list. Click <strong>Edit</strong> to add a new Language option. Default: English (United States) [en_US]</td>
</tr>
</tbody>
</table>
Logout Menu

To exit Unified CCX Administration without closing your web browser, you can perform one of the following:

- Choose **System > Logout** from the Unified CCX Administration 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 CCX Administration by closing your web browser.
CHAPTER 16

Applications Menu

The Applications menu on the top contains the following menu options:

- **Application Management**—to add, configure, copy, delete, or refresh a specific application
- **Script Management**—to add a new script and to view, refresh, upload, or delete an existing script
- **Prompt Management**—to display, modify, or delete existing prompts, and to add new prompts
- **Grammar Management**—to display, modify, or delete existing grammars, and to add new grammars
- **Document Management**—to display, modify, or delete existing documents, and to add new documents
- **AAR Management**—to upload AAR files to Unified CCX

The following sections describe the menu options:

- **Access Application Management Menu, on page 273**
- **Manage Scripts, on page 274**
- **Prompt Management, on page 274**
- **Grammar Management, on page 275**
- **Document Management, on page 275**
- **AAR Management, on page 276**

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 CCX Administration 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.
**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 the [Manage Prompt Files](#) section to know more about the different fields in this page and how to rename, refresh, or delete existing prompts.

**Related Topics**

- [Manage Prompt Files](#), on page 119

### 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 CCX Administration menu bar. The AAR Management web page appears.
Subsystems Menu

The Subsystems menu of the Unified CCX Administration web interface provides access to the subsystems that are licensed for your Unified CCX system.

The Unified CCX system uses subsystems for communicating with other services. Depending on the Unified CCX package you have installed, the Subsystems menu may contain some or most of the following menu options:

- **Cisco Unified CM Telephony**—to enter Unified CM Telephony provider information, Computer Telephony Interface (CTI) port group information, Unified CM Telephony trigger information, and to resynchronize Unified CM Telephony information.
- **RmCm**—to set up your Unified CCX resources.
- **Chat / Chat and Email**—allows Unified CCX to configure and manage chat and email CSQs, configure mail server and SocialMiner, predefined responses for chat and email, channel parameters, chat widget list, and teams.
- **Outbound**—to configure contact centers for automated outbound activities.
- **Database**—to configure the Unified CCX system to communicate with database servers.
- **HTTP**—to configure the Unified CCX Engine to respond to requests from a variety of web clients, including computers and IP phones.
- **eMail**—to configure the Unified CCX Engine to communicate with your email server and enable your applications to create and send email.
- **Cisco Media**—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.
- **MRCP ASR**—to configure the MRCP Automated Speech Recognition (ASR) subsystem, which allows users to navigate through a menu of options using spoken responses to prompts.
- **MRCP TTS**—to configure the MRCP Text-to-Speech (TTS) subsystem, which converts plain text (UNICODE) into spoken words to provide a user with information or to prompt a user to respond to an action.

- Unified CM Telephony Menu, on page 278
- RmCm Menu, on page 281
- Chat and Email Menu Options, on page 285
- Outbound Menu, on page 302
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 CCX Administration 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 CCX Administration 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**

From Unified CCX Release 9.0(1), 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 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 are in synchronize, without any inconsistency.

**Data Check** option displays if the selected data components are in synchronization 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 CCX Administration menu bar, choose **Subsystems > Cisco Unified CM Telephony > Data Synchronization**.

The Cisco Unified CM Telephony Data Synchronization page appears.

**Step 2**

Select one or more of the following three components by checking the corresponding check boxes:

- Call Control Group(s)
- Trigger(s)
• CM Telephony User(s)

Step 4  Click **Data Check** or **Data Resync**. Once 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**  Once you click **OK** in the confirmation message for Data Check or Data Resync, you will not be allowed to cancel the process.

Step 5  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 adjacent 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 would merge 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.

---

**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 CCX Administration 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 CCX Administration 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 CCX Administration 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 CCX Administration 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 CCX Administration menu bar.

Related Topics

Skills Configuration, on page 92

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 CCX Administration 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 CCX Administration 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 CCX Administration 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 CCX Administration menu bar to access this configuration area.
Add New Team

Click the Add New icon or button on the Teams summary web page. The Team Configuration page appears. Click the Open Printable Report of this Team Configuration icon in the Teams web page to open the report in a new window and send it to a printer.

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:

• SocialMiner Customer Collaboration Platform Configuration—Choose this option to configure the SocialMiner parameters. This page also displays the overall health of SocialMiner.

• 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.

SocialMiner Configuration

Use the SocialMiner Configuration web page to configure Cisco SocialMiner. 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 SocialMiner administration page.

This option is available only with the Unified CCX Premium license package. The email feature support for Unified CCX depends on the SocialMiner 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 SocialMiner Administration interface is not supported.
On a high availability setup, after the Add to Cluster operation is successful, the following message is displayed:

**Note**

In case of HA, configure the SocialMiner 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:

- **SocialMiner XMPP Service**
  Unified CCX checks the connectivity with the SocialMiner XMPP service. If the XMPP service is down, the following message is displayed:
  
  SocialMiner XMPP service is not accessible. Check the logs for more details.

- **SocialMiner Runtime Service**
  Unified CCX checks the connectivity with the SocialMiner runtime service. If the runtime service is down, the following message is displayed:
  
  SocialMiner runtime service is not accessible. Check the logs for more details.

- **SocialMiner Tomcat Service**
  Unified CCX checks the connectivity with the SocialMiner Tomcat service. If the Tomcat service is down, the following message is displayed:
  
  Unable to communicate to the SocialMiner on the IP address(Hostname) provided. Please verify whether SocialMiner is running on this IP address(Hostname) or check the network connection and make sure that SocialMiner is reachable from CCX.

- **SocialMiner Status**
  - **Feeds**
    Unified CCX validates the status of the intended chat and email feeds in SocialMiner.
    
    - ✓—All the feeds are operating normally in SocialMiner.
    
    - ┤—One or more feeds mismatches with SocialMiner.
    
    - ×—All the feeds are missing in SocialMiner.

  - **Campaigns**
    Unified CCX validates the status of the intended chat and email campaigns in SocialMiner.
    
    - ✓—All the campaigns are operating normally in SocialMiner.
• 😞—One or more campaigns mismatches with SocialMiner.
• ❌—All the campaigns are missing in SocialMiner.

• Notifications
Unified CCX validates the status of the intended chat and email notifications in SocialMiner.
• ✔️—All the notifications are operating normally in SocialMiner.
• 😞—One or more notifications mismatches with SocialMiner. 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 SocialMiner.

• Email Server
Unified CCX checks the connectivity with the email server.
• ✔️—Email server is operating normally.
• 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.
  • SocialMiner version is incompatible with the Email feature.
• ❌—Unable to reach the email server.

Procedure

Step 1
From the Unified CCX Administration menu bar, choose Subsystems > Chat > CCP Configuration OR Subsystems > Chat and Email > SocialMiner Configuration as applicable.
The Configuration web page appears.

Step 2
Complete or modify the following fields for SocialMiner:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address / Host Name</td>
<td>IP address or fully qualified domain name of the SocialMiner server. For example, 192.168.1.5 or host.example.com.</td>
</tr>
<tr>
<td>User Name</td>
<td>Username of the SocialMiner administrator.</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the SocialMiner administrator.</td>
</tr>
</tbody>
</table>
Note When the SocialMiner application password is reset, ensure that the new password is first updated in Unified CCX and then reset the password in SocialMiner. 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

• If you see an error message, click Save to re-create feeds, campaigns, and notifications for chat and email in SocialMiner.
• When Unified CCX hostname is changed or when a new Unified CCX node is added, the SocialMiner Configurations must be saved again. This enables the change to take effect to re-create all the notifications for email and chat in SocialMiner.
• The Classic Chat Web Forms will not work if the feed is deleted from SocialMiner Administration interface. To revive this chat web form, save the SocialMiner configuration in the Unified CCX. A new Feed ID will then be created in the Unified CCX database. Download the Classic Chat Web Form code snippet again from the Chat Widget section of UCCX Administration and redeploy on the website to reflect the new feed ID.

Reinject Email Contacts

Emails may be parked in SocialMiner 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 SocialMiner Configuration > Reinject.

Note The SocialMiner 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 SocialMiner User Guide or the SocialMiner 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 SocialMiner interface or see the Cisco SocialMiner User Guide, located at:
Mail Server Configuration

Use the **Mail Server Configuration** web page to configure the mail server. This web page is available on the Unified CCX node with a premium license.

**Before you begin**

- Execute the commands *set-service msExchangeIMAP4* `-startuptype automatic`, and *start-service msExchangeIMAP4* on Microsoft Exchange to set the Microsoft Exchange IMAP4 service to start automatically.

- Execute the command *set-service msExchangeIMAP4BE* `-startuptype automatic`, and execute *start-service msExchangeIMAP4BE* (for Microsoft Exchange 2013) on Microsoft Exchange to set the Microsoft Exchange IMAP4 Back End service to start automatically.

  These commands are specific to the local Exchange server.

- Create accounts and email addresses to be used for CSQ creation.

**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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Server Settings</td>
<td></td>
</tr>
<tr>
<td>Mail Server</td>
<td>Choose the mail server that is required to be configured from the listed options:</td>
</tr>
<tr>
<td></td>
<td>• MS Exchange Server / Office 365</td>
</tr>
<tr>
<td></td>
<td>• Gmail</td>
</tr>
</tbody>
</table>

**IMAP Folder Structure**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drafts Folder Name</td>
<td>The name of the drafts folder of the respective mail sever that is configured.</td>
</tr>
</tbody>
</table>
| Outbox Folder Name   | The name of the outbox folder of the MS Exchange Server / Office 365 email sever that is configured.  
|                      | This folder is not available for the **Gmail** mail server.                   |
| Sent Items Folder Name | The name of the sent items folder of the respective mail sever that is configured.  
| **Note**             | All the listed mail servers have the default folder names pre-populated for all the IMAP folders in English locale. These folder names can be edited and can have custom values. |
### Contact Service Queues

**Before you begin**

- 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 > Contact Service Queues** or **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.

---

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incoming (Secure IMAP)</strong></td>
<td></td>
</tr>
<tr>
<td>Host Name</td>
<td>Fully qualified domain name (FQDN) of the incoming (IMAP) server. Do not enter the IP address.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Port number that is used to connect to the IMAP server. The default port number is 993.</td>
</tr>
<tr>
<td><strong>Outgoing (Secure SMTP)</strong></td>
<td></td>
</tr>
<tr>
<td>Host Name</td>
<td>FQDN of the outgoing (SMTP) server. Do not enter the IP address.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Port number that is used to connect to the SMTP server. The default port number is 587.</td>
</tr>
<tr>
<td><strong>Proxy Settings</strong></td>
<td></td>
</tr>
<tr>
<td>SOCKS</td>
<td>Choose the radio button to enable/disable usage of socks proxy for Mail Server connectivity.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To enable socks, configure socks proxy in system parameters.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Description of the mail server.</td>
</tr>
</tbody>
</table>
Step 3

Specify the following fields:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSQ Name</td>
<td>Name for the CSQ.</td>
</tr>
<tr>
<td>Resource Selection</td>
<td>Resource selection criteria chosen for the chat CSQ.</td>
</tr>
<tr>
<td>Criteria</td>
<td></td>
</tr>
<tr>
<td>Longest Available</td>
<td>Selects the agent who has been in the Available state for the longest amount of time.</td>
</tr>
</tbody>
</table>
| 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: If two agents score equal in the primary selection criteria, the agent who was updated first is assigned to the incoming chat.

Table 13: CSQ Type—Chat

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSQ Type</td>
<td>Choose Chat.</td>
</tr>
</tbody>
</table>

Table 14: CSQ Type—Email

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSQ Type</td>
<td>Choose Email.</td>
</tr>
<tr>
<td>Note</td>
<td>You can create up to 100 email CSQs. If you exceed the limit, the following error is displayed:</td>
</tr>
</tbody>
</table>

Cisco Unified CCX supports a maximum of 100 Email CSQs. Exceeded maximum limit for Email CSQs.

<table>
<thead>
<tr>
<th>Mail Server</th>
<th>Fully Qualified Domain Name (FQDN) of email server. This field displays the mail server that you configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email username</td>
<td>The email address to which emails are sent or retrieved.</td>
</tr>
<tr>
<td>Email password</td>
<td>Password for email account.</td>
</tr>
</tbody>
</table>
### Field Name | Description
--- | ---
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

Drafts Folder Name | The folder to which SocialMiner will save the drafts of the emails when agent composes the response.

Outbox Folder Name | The folder to which SocialMiner will move the response email to when it is being sent.  
This folder doesn't exist for **Gmail** mail server. The email response being sent will be moved to the drafts folder instead.

Sent Items Folder Name | The folder to which SocialMiner will move the response email to when it is sent.

Poll Interval (Seconds) | Frequency in seconds to fetch emails from the server.  
Default value = 600, Range 10 to 86400

Snapshot Age (Minutes) | Specify the time in minutes from when the emails are to be fetched.  
Default value = 120, Range 10 to 43200  
For example, if you specify 120 minutes, this field fetches the emails from the last two hours.

Test Configuration | This checks the following:  
• Connectivity from SocialMiner to the configured mail server using the user credentials specific in the Contact Service Queue (CSQ) configuration  
• Presence of and permissions to the Inbox, Drafts, Outbox, and Sent Items folder for the user, specific in the CSQ configuration.

---

**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.
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Unique identifier of the predefined response.</td>
</tr>
<tr>
<td>Note</td>
<td>The special characters angle brackets (&lt;&gt;), parentheses ( ), double quotation marks ( &quot; &quot; ), and pipe symbol (</td>
</tr>
<tr>
<td>Type</td>
<td>Types of media.</td>
</tr>
<tr>
<td>Response Description</td>
<td>Description for the predefined response.</td>
</tr>
<tr>
<td></td>
<td>• Rich Text Editor is available to create an HTML-based email predefined response.</td>
</tr>
<tr>
<td></td>
<td>Use the supported tags as provided in the Rich Text Editor for formatting purpose.</td>
</tr>
<tr>
<td></td>
<td>• Plain Text Editor is available to create a chat predefined response.</td>
</tr>
<tr>
<td>Note</td>
<td>The special characters angle brackets (&lt;&gt;), parentheses ( ), double quotation marks (&quot;&quot;), and pipe symbol (</td>
</tr>
<tr>
<td></td>
<td>The maximum characters limit for predefined response for chat and email is 1500.</td>
</tr>
<tr>
<td></td>
<td>In case of email, rich text is supported and includes the HTML tag characters for representing rich text.</td>
</tr>
</tbody>
</table>
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:
### 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name of the email signature.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The name can have a maximum of 100 characters.</td>
</tr>
<tr>
<td>Content</td>
<td>The email signature content.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The email signature can have a maximum of 1500 characters. You</td>
</tr>
<tr>
<td></td>
<td>may format the text of the email signature content, add images, add URL to</td>
</tr>
<tr>
<td></td>
<td>the email signature, and add the Agent alias information.</td>
</tr>
<tr>
<td></td>
<td>The Agent alias variable appears by default when any new email</td>
</tr>
<tr>
<td></td>
<td>signature is created. If it is removed from the email signature it can be</td>
</tr>
<tr>
<td></td>
<td>reinserted at the cursor location in the email signature by clicking on the</td>
</tr>
<tr>
<td></td>
<td>Agent alias variable icon.</td>
</tr>
<tr>
<td></td>
<td>When there is no alias configured for an agent, the Agent ID is</td>
</tr>
<tr>
<td></td>
<td>presented in the email signature by default.</td>
</tr>
<tr>
<td>Tags</td>
<td>Choose a tag for the email signature.</td>
</tr>
<tr>
<td></td>
<td><strong>Global for all CSQs</strong>: The email signature is available to all the agents</td>
</tr>
<tr>
<td></td>
<td>that are associated with all the CSQs.</td>
</tr>
<tr>
<td></td>
<td><strong>Customize (Maximum 10 CSQs)</strong>: The email signature is available only to</td>
</tr>
<tr>
<td></td>
<td>the agents that are associated with the selected CSQs.</td>
</tr>
<tr>
<td></td>
<td>If you choose this option, select the CSQs from the Available CSQs pane,</td>
</tr>
<tr>
<td></td>
<td>and then click the left arrow to assign them.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Only one (1) email signature can be tagged as Global for all CSQs.</td>
</tr>
<tr>
<td></td>
<td>A CSQ can be tagged with only one (1) email signature.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Answer Timeout (Seconds)</td>
<td>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. <strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Join Timeout (Minutes)</td>
<td>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 <strong>Chat Web Form Configuration</strong> 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.</td>
</tr>
<tr>
<td>Inactivity Timeout (Minutes)</td>
<td>The customer inactivity time after which, the system ends the chat. This timeout is on the customer side only. The agent gets a message &quot;<strong>You are alone in the chat room. Click End to close the chat interface.</strong>&quot;. The customer gets a message &quot;<strong>Warning: the server connection was lost due to an inactivity timeout or connection failure.</strong>&quot;. 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 &quot;<strong>Sorry, the chat service is currently not available. Please try again later.</strong>&quot;</td>
</tr>
</tbody>
</table>
Click Yes if agents are allowed to handle a chat session during a voice call. 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.

**Note**

Offer Chat Contact When On Voice Call

Click Yes if agents are allowed to handle a voice call during a chat session. 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.

**Note**

Offer Voice Call When On Chat

Number of chat sessions (ranging from 1 to 5) that an agent is allowed to handle. This includes the group chat sessions also.

**Note**

Maximum Number Of Chat Sessions Per Agent

Number of Email sessions (ranging from 1 to 5) that an agent is allowed to handle.

**Note**

Maximum Number Of Email Sessions Per Agent

Specify the amount of time for which an email message waits in a specific agent CSQ.

Sticky Email Timeout (Hours)

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**

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.
List Chat Web Forms

Use the chat widgets to generate HTML code that can be hosted on the customer website. Use the List Chat Web Forms page to configure and manage chat web forms. To access the chat web forms, choose Subsystems > Chat > Chat Widget List OR Subsystems > Chat and Email > Chat Widget List as applicable.

Chat Web Form Configuration

You can add, modify, and delete chat web forms. You can schedule business hours in the chat web form for week days, custom business days, holidays, and configure messages after business hours.

Note

To modify an existing chat web form, click the web form. To delete an existing chat web form, click the delete icon.

Procedure

Step 1

From the Unified CCX Administration menu bar, choose Subsystems > Chat > Chat Widget List OR Subsystems > Chat and Email > Chat Widget List as applicable.

The List Chat Web Forms web page opens, displaying the information for existing Chat Web Forms, if any.

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 create a new chat web form.

The Chat Web Form Configuration web page opens.

Step 3

Specify the following information:

<table>
<thead>
<tr>
<th>Page Area</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Widget Details</td>
<td>Name</td>
<td>Unique identifier of the chat widget.</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Chat widget description.</td>
</tr>
<tr>
<td>Context Service</td>
<td>Fieldsets</td>
<td>Valid fieldsets that will be entered by the Admin while configuring the chat widgets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fieldsets are comma separated strings in the format fieldset1, fieldset2 (for example: cisco.base.pod,cisco.ccx.pod). A maximum number of 10 fieldsets can be entered.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• All the Selected User Form Fields except Name and Email should be part of the FieldSets specified, otherwise Context Service operations for chat will fail.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To perform Context Service Lookup Customer for chat, the Email field is mandatory in the chat form.</td>
</tr>
<tr>
<td>Page Area</td>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Logo URL</td>
<td>Location of the logo file that is displayed in the widget.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> The custom logo size will be resized to 300 x 300 pixel by default.</td>
</tr>
<tr>
<td></td>
<td>Widget Wait Message</td>
<td>Message that is displayed to the customer when the customer starts a chat session.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default message: “Welcome. Please wait while we connect you to a customer care representative.”</td>
</tr>
<tr>
<td></td>
<td>Join Time-out Message</td>
<td>Message that is displayed to the customer when a chat request is not handled within the set time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default message: “All customer care representatives are busy. Please wait or try again later.”</td>
</tr>
<tr>
<td></td>
<td>Error Message</td>
<td>Message that is displayed to the customer when Unified CCX or chat service is not available to handle chat requests.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default message: “Sorry, the chat service is currently not available. Please try again later.”</td>
</tr>
</tbody>
</table>

**Step 4**  
In the User Form Fields area, select the desired fields from the **Available Fields** and move it to the **Selected Fields**.

**Step 5**  
To create new field(s) in addition to the list of available fields, click **Add Custom Field**. The Explorer User Prompt dialog box opens.

**Step 6**  
Enter the name of the new custom field in the text box and click **OK**. The new custom field appears in the list of **Selected Fields**.

**Step 7**  
Click **Next**.  
The **Add problem Statement CSQ mapping** area opens.

**Step 8**  
Enter the problem statement for the chat web form and map the same with an existing chat CSQ from the **CSQ List** drop down list.

**Step 9**  
To add more problem statements and associate the same with the Chat CSQs, click **Add More**. Click the delete icon beside the CSQ List drop down to delete the newly created problem statement.

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

**Step 11**  
In the **Schedule Business Hours** area, select one of the following options to configure the Business Days.

- 24 hours x 7 days
- Custom Business Hours

**Note**  
- The **Chat Schedule Configuration** is based on the Unified CCX server time zone.
- Ensure that the moment.js library is accessible in the client environment. If this is not accessible, reference to the correct location where the moment.js is available
- During an upgrade to Unified CCX 11.6(1), by default the **24 hours x 7 days** is selected as the **Business Days**.
Step 12  
In the **Schedule Holidays** area, configure holidays.  
a)  To add more holidays, click **Add More**. Click the delete icon to delete a configured holiday.

Step 13  
In the **Schedule Custom Business Days** area, 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 14  
In the **Off Hours Details** area, enter a message in the **Off Hours Message** text box.

Step 15  
Click **Next**.

The Web Form Preview area displays a preview of the chat web form as per the schedule configured. It displays all the fields that you had selected for the user form and problem statements along with CSQ mapping.

Step 16  
Click any of the following:  
- Click the **Back** button if you want to modify the configuration of the chat web form.  
- Click the **Finish** button if you want to generate the web form code.

**Note**  
The Chat Web Form that is generated uses JavaScript. The web page where this is loaded must be accessed using a JavaScript enabled browser. The default Chat Web Form, displays a warning message to the user if JavaScript is not enabled on the browser where it is loaded.

During an upgrade of Unified CCX from version 11.0(1) or any earlier version to 11.6(1), the Chat Web Form must be regenerated and redeployed on the website.

---

**Teams**

Choose **Subsystems > Chat > Teams** OR **Subsystems > Chat and Email > Teams** as applicable from the Unified CCX Administration menu bar to access this configuration area.

---

**Note**  
The team configuration for chat is the same as it is for voice.

**Related Topics**  
**Teams Configuration**, on page 107

---

**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.

Related Topics
Configure General Outbound Properties, on page 224

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.

Note
The existing campaigns will be marked as Agent-based after an upgrade from Unified CCX versions prior to 9.0(1).

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.

Related Topics
Unified CCX Requirements, on page 220
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

Related Topics
- Manual Import of Contacts for Campaign, on page 242
- Schedule Import of Contacts Using SFTP or HTTPS, on page 244

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.

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 CCX Administration 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gateway Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Gateway Hostname/IP Address</td>
<td>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.</td>
</tr>
<tr>
<td>Gateway Port</td>
<td>Destination port used by Unified CCX to communicate with SIP gateway. The default value is 5060.</td>
</tr>
<tr>
<td>Local CCX Port</td>
<td>Destination port to be used by SIP gateway to communicate with Unified CCX. Default: 5065, Range: 1025-32767 or 61001-65535</td>
</tr>
</tbody>
</table>
### Local User Agent

This read-only field provides a description of the owner for this connection. The default value is Cisco-UCCX/8.5.

### 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)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Silence Period (10-1000)</td>
<td>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</td>
</tr>
<tr>
<td>Analysis Period (1000 - 10000)</td>
<td>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</td>
</tr>
<tr>
<td>Maximum Time Analysis (1000-10000)</td>
<td>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</td>
</tr>
<tr>
<td>Minimum Valid Speech Time (50-500)</td>
<td>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</td>
</tr>
<tr>
<td>Maximum Term Tone Analysis (1000-60000)</td>
<td>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</td>
</tr>
</tbody>
</table>

---

**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.


**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.

**Related Topics**

Poll Database Connectivity, on page 115

---

**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 CCX Administration 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.

**Related Topics**

Specify Custom Classpath Entries, on page 129
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.

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 CCX Administration 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
Provision MRCP TTS Servers, on page 84

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

Provision MRCP TTS Default Genders, on page 86
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 315
- RmCm Wizard, on page 316

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.

**Related Topics**
- Configure Unified CCX Applications, on page 11
- Script Management, on page 52
- Manage Prompt Files, on page 119
- Manage Grammar Files, on page 121
- Manage Document Files, on page 122
- About Unified CCX Applications, on page 43
- Application Triggers, on page 48

**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 CCX Administration 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 284
  - **Unified Communications Manager for Unified CCX Configuration**, on page 30

- **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.
Tools Menu

The Tools menu of the Unified CCX Administration web interface provides access to system tools you can use to perform a variety of administrative tasks and contains the following menu options:

- **Plug-ins**—to download plug-ins that you can use to enhance the Unified CCX Engine.
- **Real-Time Reporting**—to generate reports that provide detailed information about the status of your Unified CCX system.
- **Real-Time Snapshot Config**—to configure the Unified CCX database connection to a wallboard display.
- **Historical Reporting**—to perform Historical Reporting tasks, including configuring the database server, synchronizing data, configuring users, installing client software, and purging your database.
- **User Management**—to assign access levels to administrators and supervisors.
- **Password Management**—to reset passwords for external database access users like workforce management, historical reporting user and so on.
- **W1 Upgrade**—to show if you have selected "Upgrade from a previous Unified CCX release" option during initial Appadmin setup in a single-node or high availability deployment.

The following sections describe the various menu options.

- Plug-Ins Menu, on page 319
- Real-Time Reporting Tool, on page 320
- Real-Time Snapshot Config Menu, on page 321
- Historical Reporting Menu, on page 325
- User Management Menu, on page 327
- Password Management, on page 331

Plug-Ins Menu

The Unified CCX system includes software components called **plug-ins** that you can use to enhance the Unified CCX Engine. 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 CCX Administration 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—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 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.
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.

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.

## 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.

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Writing Enable</td>
<td>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.</td>
</tr>
</tbody>
</table>
### 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](https://www-01.ibm.com/marketing/iwm/iwm/web/pickUrxNew.do?source=ifxdl). Download the IBM Informix Client Software Development Kit (CSDK) Version 3.0.0 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/](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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>This is the instance name of the Informix database.</td>
</tr>
<tr>
<td></td>
<td>Informix database instance name can be formed using Host Name of the Unified</td>
</tr>
<tr>
<td></td>
<td>CCX server by following these conventions:</td>
</tr>
<tr>
<td></td>
<td>• Convert all upper case letters to lower case.</td>
</tr>
<tr>
<td></td>
<td>• Replace hyphens with underscore.</td>
</tr>
<tr>
<td></td>
<td>• Add the letter “i” as a prefix to the instance name, if the hostname starts with a number.</td>
</tr>
<tr>
<td></td>
<td>• Append the letters “_uccx” to the instance name.</td>
</tr>
<tr>
<td></td>
<td>For example, if the hostname is “802UCCX-Ha-Node1”, enter “i802uccx_ha_node1_uccx” in the Server Name field.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter the hostname of the primary Unified CCX server.</td>
</tr>
<tr>
<td>Service</td>
<td>Enter 1504.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Enter onsoctcp.</td>
</tr>
<tr>
<td>Options</td>
<td>Leave blank.</td>
</tr>
<tr>
<td>Database Name</td>
<td>Enter db_cra.</td>
</tr>
<tr>
<td>User ID</td>
<td>Enter uccxwallboard. This is the user id of the Unified CCX database created for wallboard.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the wallboard user that has been configured. You can change the password by going to <strong>Tools &gt; Password Management</strong> submenu option from the Unified CCX Administration menu bar.</td>
</tr>
</tbody>
</table>

Step 9  Click **Apply**.

Step 10 Click the **Environment** tab and enter the values for the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Locale</td>
<td>Enter en_US.UTF8.</td>
</tr>
<tr>
<td>Database Locale</td>
<td>Enter en_US.UTF8.</td>
</tr>
</tbody>
</table>
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 master 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://<UnifiedCCX 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host/IP Address</td>
<td>The host name or IP address of the SMTP server</td>
</tr>
<tr>
<td>From email address</td>
<td>The email address that is to appear in the From field of emails sent by the Scheduler</td>
</tr>
<tr>
<td>Note</td>
<td>Unified CCX supports alphanumeric IDs and special characters (only hyphen &quot;-&quot;, underscore &quot;.&quot;, and dot &quot;.&quot;).</td>
</tr>
<tr>
<td>Use Email Proxy</td>
<td>Check this if you use a proxy server to reach your SMTP server. Only HTTPS is supported as an email proxy type. SOCKS proxy is not supported.</td>
</tr>
<tr>
<td>Email Proxy Hostname</td>
<td>The hostname or IP address of the proxy server used to reach the SMTP server</td>
</tr>
<tr>
<td>Email Proxy Port</td>
<td>The port used to connect to the SMTP proxy server</td>
</tr>
<tr>
<td>Use SMTP Authentication</td>
<td>Check this if your SMTP server expects to receive username/password credentials</td>
</tr>
<tr>
<td>SMTP Username</td>
<td>If you check the Authenticate checkbox, enter the username that is to be authenticated</td>
</tr>
<tr>
<td>SMTP Password</td>
<td>If you check the Authenticate checkbox, enter the password that is to be authenticated</td>
</tr>
</tbody>
</table>

You will not be able to save the SMTP configuration if Cisco Unified Intelligence Center service on the publisher node is down.

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 CCX Administration 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.

**Note**
- Only administrators can update the Unified CCX system. You must select at least one administrator, so that someone is available to perform updates.
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.

Procedure

Choose **Tools > User Management** and click any of the following submenu options from the Unified CCX Administration menu bar to assign administrative privileges to administrators and supervisors:

- User Configuration, on page 328
- Name Grammar Generator Configuration, on page 328
- Spoken Name Upload Submenu, on page 329
- Administrator Capability View Menu, on page 330
- Supervisor Capability View Menu, on page 330
- Reporting Capability View Menu, on page 331
- Agent Capability View Menu, on page 331

User Configuration

From the Unified CCX Administration 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 userID that contain Agent1.

All the columns are hyperlinked to the user configuration page.

Note

This search bar will search the users only by last name or user ID. Do not use the first name for searching.

Name Grammar Generator Configuration

Use the Name Grammar Generator Configuration web page to define scheduling information for the Name Grammar Generator.
From the Unified CCX Administration 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>How often Name Grammar Generator is automatically run. Valid options: Never, Daily, and Weekly. This is a mandatory field.</td>
</tr>
<tr>
<td>Run task on (hrs of day)</td>
<td>Time of day to run the task. This is a mandatory field.</td>
</tr>
<tr>
<td>Run task on (day of week)</td>
<td>Day of week to run the task. This is a mandatory field.</td>
</tr>
<tr>
<td>Last Completed on</td>
<td>Date of last generation of name grammar.</td>
</tr>
<tr>
<td>Last Completion Result</td>
<td>The status after the last name grammar generation. (Display only.)</td>
</tr>
<tr>
<td>Grammar Variant</td>
<td>Select one or more grammar variants to generate from the check box next to the following three options:</td>
</tr>
<tr>
<td></td>
<td>• OSR 3.1.x</td>
</tr>
<tr>
<td></td>
<td>• 2003 SISR</td>
</tr>
<tr>
<td></td>
<td>• Nuance</td>
</tr>
<tr>
<td>Current Status</td>
<td>Running status of the Name Grammar Generator. (Display only.)</td>
</tr>
</tbody>
</table>

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 CCX Administration web interface.

To access the Spoken Name Prompt Upload web page, choose **Tools > User Management > Spoken Name Upload** from the Unified CCX Administration 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 CCX Administration 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. Execute 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 Menu**

From the Unified CCX Administration menu bar, choose **Tools > User Management > Supervisor Capability View** to access the capability view for the Supervisor User Management area.

This web page contains a pane for users identified as the Unified CCX Supervisor 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**

For a supervisor to access Unified Intelligence Center Live Data reports, an extension should be assigned to the supervisor.

---

**Note**

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. If you assign Supervisor capability to such a user ID, an error appears.
Reporting Capability View Menu

From the Unified CCX Administration 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:

<table>
<thead>
<tr>
<th>Roles</th>
<th>Access</th>
<th>Available reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application administrator</td>
<td>Super user</td>
<td>• Historical reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Live Data reports</td>
</tr>
<tr>
<td>Reporting user</td>
<td>Unified CCX administrator must assign this role to a user.</td>
<td>• Historical reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Live Data reports</td>
</tr>
<tr>
<td>Supervisor</td>
<td>Unified CCX administrator must assign this role to a user.</td>
<td>Live Data reports</td>
</tr>
<tr>
<td>Agent</td>
<td>Unified CCX administrator must assign this role to a user.</td>
<td>Agent-specific Live Data reports</td>
</tr>
</tbody>
</table>

Agent Capability View Menu

From the Unified CCX Administration 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 Permissions

<table>
<thead>
<tr>
<th>User</th>
<th>Username</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wallboard</td>
<td>uccxwallboard</td>
<td>This user can connect to Configuration and Historical databases and has read-only access to RtICDStatistics and RtCSQsSummary tables.</td>
</tr>
<tr>
<td>Recording SFTP</td>
<td>uccxrecording</td>
<td></td>
</tr>
<tr>
<td>Workforce Management</td>
<td>uccxworkforce</td>
<td></td>
</tr>
<tr>
<td>Historical Reporting</td>
<td>uccxhruser</td>
<td>This user can connect to Configuration, Historical and Repository databases and has the following privileges:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• read-only access to Historical, Configuration, and Repository tables</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• execute stored procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• create new stored procedures.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This user is used by coresident Unified Intelligence Center and Standalone Unified Intelligence Center (if configured) to connect to Unified CCX Database and execute historical reports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This user is also used during initialization of Live Data gadgets in Finesse and Live Data reports in Unified Intelligence Center.</td>
</tr>
<tr>
<td>System Call Tracking</td>
<td>uccxsct</td>
<td></td>
</tr>
</tbody>
</table>

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.
Help Menu

The Help Menu of the Unified CCX Administration web interface provides access to online help for the Unified CCX system.

Use the Help menu to access configuration procedures and descriptions of Unified CCX components.

The Help menu contains the following menu options:

- **Contents and Index**—Choose this option to view the entire Unified CCX Administrator Guide online help system and index.

- **For this page**—Choose this option to view context-sensitive help.

- **Unified CCX Documentation on Cisco.com**—Choose this option to view the documentation index page.

- **About**—Choose this option to view Unified CCX version information.

The following sections describe the Help menu options.

- Contents and Index, on page 335
- For This Page Menu, on page 336
- Unified CCX Documentation Link, on page 336
- About Menu, on page 336

Contents and Index

To view the entire Unified CCX Administration Guide online help system and index, choose Help > Contents and Index from the Unified CCX Administration 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.

<table>
<thead>
<tr>
<th>Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back</td>
<td>Returns you to the previous page.</td>
</tr>
<tr>
<td>Forward</td>
<td>Leads you to the next page.</td>
</tr>
<tr>
<td>Menu Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Print</td>
<td>Prints the help document.</td>
</tr>
<tr>
<td>View PDF</td>
<td>Opens a PDF version of the Cisco Unified CCX Administration Guide.</td>
</tr>
<tr>
<td>Contents and Index</td>
<td>Displays the index and contents of the Unified CCX Administrator Guide online help files in a separate webpage.  The index is displayed in the left pane while the contents are displayed in the right pane in the online help page.</td>
</tr>
</tbody>
</table>

### 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 CCX Administration 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:


### About Menu

To access Unified CCX version information, choose **Help > About** from the Unified CCX Administration menu bar. The Unified CCX Administration web page opens, displaying version information and package information.
Cisco Mobile Skill Manager

The Unified CCX supervisor can use the Cisco Mobile Skill Manager on a smartphone to remotely manage the skill data of all associated agents. This application is not a native one and can run on smartphone browsers.

The devices with the following operating systems are supported:

- For Apple devices using iOS-5.x and above with Safari browser
- For Android devices - 2.x and above with default browser

The following sections provide procedures to allow you to access Cisco Mobile Skill Manager, such as modify the team; add and delete new skills, add, delete and update skills of agents; and view skills and agents.

- Access Mobile Skill Manager, on page 337
- Adding Skills Using Cisco Mobile Skill Manager, on page 338
- Searching Skills Using Cisco Mobile Skill Manager, on page 338
- View Details of Resources Assigned to Supervisor, on page 339
- View Resources Assigned to Supervisor, on page 339
- Search Resources Using Cisco Mobile Skill Manager, on page 339
- Modify Resource Team, on page 340
- Assign Skill Competency to Resource, on page 340
- Unassign Skill Competency of Resource, on page 341

Access Mobile Skill Manager

Pre-requisites

Cisco Mobile Skill Manager allows you as the supervisor to manage the skill data associated with an agent. You can also modify the agent team, and add and delete new skills. Before you access the Cisco Mobile Skill Manager, make sure

- the supervisor capability is assigned to you. To know more on supervisor options, see sections Supervisor Privileges and User View submenu option, in this guide.
- Cisco Tomcat and Cisco Unified Cluster View Daemon services are up and running.

Follow the steps below to login to Cisco Mobile Skill Manager from your smartphone:

1. Open Cisco Mobile Skill Manager home page from your mobile smart phone browser and enter the following case-sensitive URL: https://<ipaddress>/mobileskillmanager
In this example, replace <ipaddress> with the IP address of the required Unified CCX server.

2. In the Security Alert dialog box that displays, click the appropriate button.

3. In the Cisco Mobile Skill Manager authentication page, enter the supervisor credentials, and click Sign In.

   A window with the Resources and Skills links is displayed.
   - **Resources:** This link is used to access the Resources page. This page displays the resources assigned to you.
   - **Skills:** This link is used to access the Skills page. You can add a new skill or delete an existing skill from this page.

4. Select either depending on what you want to do. Individual tasks related to these two choices are provided separately.

### Adding Skills Using Cisco Mobile Skill Manager

**Procedure**

**Step 1** Login to Cisco Mobile Skill Manager using supervisor credentials.

**Step 2** Click **Skills**.

**Step 3** In the Skills page, enter the name of the skill in the edit box and click the **Add** button.

   A dialog box confirming the successful addition of skill is displayed.

**Step 4** Click **OK**.

   The dialog box closes and the Skills page refreshes to display the updated list of skills.

### Searching Skills Using Cisco Mobile Skill Manager

**Procedure**

**Step 1** Login to Cisco Mobile Skill Manager using supervisor credentials.

**Step 2** Click **Skills**.

**Step 3** In the Skills page, enter the skill to be searched in the search filter box.

**Step 4** If the skill exists, the same will be displayed.
View Details of Resources Assigned to Supervisor

Procedure

Step 1 Log into Cisco Mobile Skill Manager using supervisor credentials.

Step 2 Click Resources. The Resources page launches to display all resources assigned to the supervisor.

Step 3 Click the selected resource name. The Resource details page launches and lists the following details of the selected resource.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Name</td>
<td>Displays the full name of the resource.</td>
</tr>
<tr>
<td>User Id</td>
<td>Displays the user id of the resource.</td>
</tr>
<tr>
<td>IPCC Extension</td>
<td>Displays the IPCC extension of the resource.</td>
</tr>
<tr>
<td>Team</td>
<td>Link to launch the Teams page which displays the team to which the resource is assigned.</td>
</tr>
<tr>
<td>Skills</td>
<td>Link to launch the Assigned skills page which displays the skills assigned to the resource.</td>
</tr>
</tbody>
</table>

View Resources Assigned to Supervisor

Procedure

Step 1 Log into Cisco Mobile Skill Manager using supervisor credentials.

Step 2 Click Resources. The Resources page launches to display all resources assigned to the supervisor.

Search Resources Using Cisco Mobile Skill Manager

Procedure

Step 1 Log into Cisco Mobile Skill Manager using supervisor credentials.
**Modify Resource Team**

**Procedure**

**Step 1** Login to Cisco Mobile Skill Manager using supervisor credentials.

**Step 2** Click **Resources**.

The Resource page launches and all resources assigned to the supervisor are displayed.

**Step 3** Click the resource name to launch the Resource details page.

**Step 4** In the Resource details page, click **Teams**.

The Teams page launches to display all the teams configured in the Cisco CCX system.

**Step 5** Click the team name, then in the confirmation box click **OK**.

A window displays the successful modification of the team.

**Step 6** To return back to the Agents Details page, click **OK**.

---

**Assign Skill Competency to Resource**

**Procedure**

**Step 1** Login to Cisco Mobile Skill Manager using supervisor credentials.

**Step 2** Click **Resources**.

The Resource page displays all the resources assigned to the supervisor.

**Step 3** Click the resource name to display the Resource details window.

**Step 4** Click **Skill**.

All skills configured in Unified CCX are displayed.

**Step 5** To set the competency level for a particular skill, select the value from the drop down list displayed against each skill.

**Step 6** Click the **Update** button located at the top of the window.

A dialog box displays the successful assignment of a skill to a resource.
Step 7 Click OK to be redirected to the Resources Details page.

---

Unassign Skill Competency of Resource

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Login to Cisco Mobile Skill Manager using supervisor credentials.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click Resources.</td>
</tr>
</tbody>
</table>

**Example:**
The Resources page launches displaying names of all resources assigned to the supervisor.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Click on a resource name to launch the Resources details page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>Click Skills.</td>
</tr>
</tbody>
</table>

The skills page with all skills configured in Unified CCX is displayed.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>To unassign the competency level for a particular skill, select the value NA from the drop-down list for that resource.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>Click the Update button that displays at the top of the window.</td>
</tr>
</tbody>
</table>

**Example:**
A dialog box shows the success of the task, that is unassigning a skill.

| Step 7          | Click OK to return to the Resource Details page.                                                                 |
Unassign Skill Competency of Resource
Cisco Finesse

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 that you click to access the various administration features. The tab names and the tasks that you can perform on each tab are as follows:

- **Settings**: IP Phone Agent Settings, and Context Service Management.
- **Call Variables Layout**: Manage the call variables and ECC variables that appear on the agent desktop call control gadget.
- **Desktop Layout**: Make changes to the default desktop layout for agents and supervisors.
- **Phone Books**: Add, edit, or delete phone books or phone book contacts.
- **Reasons**: Add, edit, or delete Not Ready reason codes, Sign Out reason codes, or Wrap-Up reasons.
- **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.

**Sign In to Cisco Finesse Administration Console**

You can access the Cisco Finesse administration console only through HTTPS.

When you sign in to Finesse, always use the fully qualified domain name (FQDN) of the Finesse server in the URL, not the server IP address or hostname.

**Procedure**

**Step 1**
Direct your browser to https://FQDN:8445/cfadmin, where FQDN is the fully qualified domain name of your primary server.

**Step 2**
The first time 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you use Internet Explorer:</td>
<td>a. A page appears that states there is a problem with the website's security certificate. Click <strong>Continue to this website (not recommended)</strong>. This action opens the sign in page for the administration console. A certificate error appears in the address bar of your browser.</td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>Certificate Error</strong>, and then click <strong>View Certificates</strong> to open the Certificate dialog box.</td>
</tr>
</tbody>
</table>

**Note**
If you are using HTTP to access the administration console, this step is not required.
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 the .
In the Certificate dialog box, click **Install Certificate**. This action opens the Certificate Import Wizard.

c. Click **Next**.

d. Select **Place all certificates in the following store**, and then click **Browse**.

e. Select **Trusted Root Certification Authorities**, and then click **OK**.

f. Click **Next**.

g. Click **Finish**.

h. If a Security Warning dialog box appears that asks if you want to install the certificate, click **Yes**.

A Certificate Import dialog box appears that states the import was successful.

i. Click **OK**.

If you use 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 the **Permanently store this exception** check box is checked.

d. Click **Confirm Security Exception**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>c.</td>
<td>In the Certificate dialog box, click <strong>Install Certificate</strong>. This action opens the Certificate Import Wizard.</td>
</tr>
<tr>
<td>d.</td>
<td>Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>e.</td>
<td>Select <strong>Place all certificates in the following store</strong>, and then click <strong>Browse</strong>.</td>
</tr>
<tr>
<td>f.</td>
<td>Select <strong>Trusted Root Certification Authorities</strong>, and then click <strong>OK</strong>.</td>
</tr>
<tr>
<td>g.</td>
<td>Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>h.</td>
<td>Click <strong>Finish</strong>.</td>
</tr>
<tr>
<td>i.</td>
<td>If a Security Warning dialog box appears that asks if you want to install the certificate, click <strong>Yes</strong>. A Certificate Import dialog box appears that states the import was successful.</td>
</tr>
<tr>
<td>j.</td>
<td>Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

**Step 3**

On the Sign-In page, in the ID field, enter the Application User ID that was established during the installation.

**Step 4**

In the Password field, enter the Application User password that was established during the installation.

**Step 5**

Click **Sign In**.

A successful sign-in launches an interface with defined administration gadgets and a Sign Out link.

---

**Note**

After 30 minutes of inactivity, Finesse automatically signs you out of the administration console and you must sign in again.

---

**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 in a row, Finesse blocks access to that user account for a period up to 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 in a row with the wrong password, Finesse blocks access to that user account. However, in this case, the lockout period is only 5 minutes. This restriction also applies when agents and supervisors sign in using the mobile agent or Finesse IP Phone Agent (IPPA).
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 whether a user account is locked, enter the following CLI command:

```
file get activelog desktop recurs compress
```

Then 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>"
```

### Sign In to Cisco Unified Communications Operating System Administration

#### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Direct your browser to <code>https://FQDN:8443/cmplatform</code>, where <code>FQDN</code> is the fully-qualified domain name of your server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Sign in with the username and password for the Administrator User account.</td>
</tr>
</tbody>
</table>

**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 you can use or you can 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, 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 hostname in the certificate, a warning message is displayed in the IE browser about certificate address mismatch. The certificate must be re-generated so that the hostname in the certificate matches the server hostname before importing to Finesse. If there is a valid reason for the mismatch, you can 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

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

To eliminate browser security warnings each time you sign in, obtain Finesse certificate signed by a Certificate Authority (CA). Use the Certificate Management utility from Cisco Unified Communications Operating System Administration.

To open Cisco Unified Communications Operating System Administration, enter the following URL in your browser:

https://hostname of primary UCCX server/cmplatform

Sign in using the username and password for the Application User account created during the installation of Unified CCX.

Procedure

Step 1 Generate a CSR.
   a) Select Security > Certificate Management > Generate CSR.
   b) From the Certificate Name drop-down list, select tomcat.
   c) Click Generate CSR.
      You must not download the ECDSA certificate.

Step 2 Download the CSR.
   a) Select Security > Certificate Management > Download CSR.
   b) From the Certificate Name drop-down list, select tomcat.
   c) Click Download CSR.

Step 3 Generate and download a CSR for the secondary Unified CCX server.
   To open Cisco Unified Operating System Administration for the secondary server, enter the following URL in the address bar of your browser:

https://hostname of secondary UCCX server/cmplatform

Step 4 Use the CSRs to obtain the CA root certificate, intermediate certificate, and signed application certificate from the Certificate Authority.

Note To set up the certificate chain correctly, you must upload the certificates in the order described in the following steps.

Step 5 When you receive the certificates, select Security > Certificate Management > Upload Certificate.

Step 6 Upload the root certificate.
   a) From the Certificate Purpose drop-down list, select tomcat-trust.
   b) In the Upload File field, click Browse and browse to the root certificate file.
   c) Click Upload File.

Step 7 Upload the intermediate certificate.
a) From the Certificate Purpose drop-down list, select tomcat-trust.
b) In the Upload File field, click Browse and browse to the intermediate certificate file.
c) Click Upload File.

Step 8
Upload the application certificate.
a) From the Certificate Purpose drop-down list, select tomcat.
b) In the Upload File field, click Browse and browse to the application certificate file.
c) Click Upload File.

Step 9
After the upload is complete, restart the Cisco Unified CCX server on the primary node.

Note
Delete the self-signed certificates from the clients certificate store. Then close the browser, relaunch, and reauthenticate.

Step 10
Upload the application certificate to the secondary Cisco Unified CCX server.

You do not need to upload the root and intermediate certificates to the secondary Unified CCX server. After you upload these certificates to the primary server, they are replicated to the secondary server.

Step 11
Restart the Cisco Unified CCX server on the secondary node.

Client-Side Certificate Acceptance
The procedures that agents must perform to accept certificates the first time they sign in depends on the method you choose to manage certificates and the browser used by the agents.

Related Topics
Set Up Certificates, on page 159

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 uploaded a CA certificate, you can skip this procedure.

Procedure

Step 1
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).

Step 2
Perform the steps in the following table for the browser you are using.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you use Internet Explorer:</td>
<td>a. A page appears that states there is a problem with the website's security certificate. Click <strong>Continue to this website (not recommended)</strong>. This action opens the sign in page for the administration console (or agent desktop). A certificate error appears in the address bar of your browser.</td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>Certificate Error</strong>, and then click <strong>View Certificates</strong> to open the Certificate dialog box.</td>
</tr>
</tbody>
</table>
In the Certificate dialog box, click Install Certificate. This action opens the Certificate Import Wizard.

**Note** If you use Internet Explorer 11, you must add Finesse to your trusted sites before the Install Certificate option appears (Internet Options > Security > Trusted Sites > Sites).

After you click Install Certificate, under Store Location, select Current User to install the certificate for the current user only, or select Local Machine to install the certificate for all Windows users who use this computer.

d. Click Next.
e. Select Place all certificates in the following store, and then click Browse.
f. Select Trusted Root Certification Authorities, and then click OK.
g. Click Next.
h. Click Finish.
i. If a Security Warning dialog box appears that asks if you want to install the certificate, click Yes.

A Certificate Import dialog box that states the import was successful appears.
j. Click OK.
k. Enter your credentials, and then click Sign In.

If you use 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 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 then 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 allow the gadget to load into 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 that 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 a fully qualified domain name) as the name with which the certificate is signed. If the certificate name and the name in the gadget URL do not match, the connection is not trusted and the gadget does not 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 that was entered during installation. To verify that Finesse can resolve the name, run the CLI command “utils network ping <hostname>”.

Procedure

Step 1  Download the tomcat.pem certificate from the third-party gadget host.
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 SocialMiner certificate to the Finesse servers to allow communication between SocialMiner and Finesse. After you complete this procedure, agents must accept certificates in the Finesse desktop before they can use this gadget.

If SocialMiner is deployed with private certificates, agents cannot join chat rooms or reply to email messages until they accept the SocialMiner 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 SocialMiner server.

Related Topics

Add Certificate for HTTPS Gadget, on page 350

Manage System Settings

Note

For information about Finesse IP Phone Agent Settings, see Manage Finesse IP Phone Agent.

Related Topics

Manage Finesse IP Phone Agent, on page 403

Context Service Settings

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

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

For more information about Context Service and to check service availability, see https://help.webex.com/community/context-service.

Context Service Network Connectivity Requirements

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

Context Service uses port 443 (HTTPS).

The following URLs must be whitelisted in your firewall so that your contact center components can connect to, and receive data from Context Service.

- *.webex.com
- *.wbx2.com
- *.ciscoccservice.com
Register and Configure Context Service

Registering applications with Context Service is easy if your Cisco Webex Control Hub account has been entitled for Context Service.

For Cisco Context Center on-premise applications, simply use the built-in registration process. A browser window displays and prompts you to log in to Cisco Webex Control Hub. Log in and follow the on-screen instructions to authorize the application to connect to Context Service.

Use the Context Service Management gadget to register Unified CCX with the Context Service.

Before you begin

Ensure that your web browser allows popups.

When your organization is entitled for Cisco Context Service, you must have received an email requesting a sign-in and a password change. Sign in using the registration email, and change the password. Now your organization is entitled to use Context Service.

If the browser requires a proxy to connect to internet, configure the browser to use proxy. See the browser documentation about configuring proxy.

Procedure

Step 1  Verify the Context Service parameters as specified on the System Parameters Configuration Web Page. If Unified CCX server has to access Context Service via HTTP proxy, configure the proxy parameters and select proxy type as HTTP.

Step 2  If you are not already signed in, sign in to the Cisco Finesse Administration console.

Step 3  To register Unified CCX with the Context Service, in the Context Service Management gadget, click Register. For more information about Context Service registration, see https://help.webex.com/community/context-service.

   Note  If the Unified CCX FQDN is not added as an exception in the blocked popup window settings of the browser, the opened registration and deregistration popup windows do not close automatically. You must manually close the popup windows.

Step 4  You are prompted to log in and enter your Cisco Webex Control Hub admin credentials to complete the registration.

   Note  If you encounter any issues with the Context Service connectivity and would want to reregister or troubleshoot the issue, click Deregister.

   During the Registration process, at any time if you wish to cancel the registration, click Cancel. If registration fails or context service cannot be reached, you can reregister by clicking the Register button.
In case of Context Service failures, you will receive RTMT alerts.

**Note** If using Firefox, enable the `dom.allow_scripts_to_close_windows` config to ensure that any additional tabs opened for context service registration close as expected. To do this:

a. Enter `about:config` in the Firefox browser.

b. Click *I accept the risk*.

c. Search for `dom.allow_scripts_to_close_windows` config.

d. Double click to change the value field to *True*.

e. Restart your browser.

---

**What to do next**

If context service registration is done by enabling the proxy setting option, configure the browser proxy with the URL specified in the Context Service Management gadget.

### 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 layout and 199 custom layouts). As part of this functionality:

- Each layout has a name (required) and description (optional).
- After an upgrade from a release earlier than Cisco Finesse Release 11.0, Finesse migrates the previously configured default layout and assigns it the default name (Default Layout) and description (Layout used when no other layout matches the user layout Custom/ECC Variable).
- You can change the name and description of the default Call Variables Layout.
- You cannot delete the default Call Variables Layout.
- Finesse appends *(Default)* to the name of the default Call Variables Layout.
- To display a custom Call Variables Layout, in the Unified 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
- BASStatus
- BADialedListID
- BATimeZone
- BABuddyName
- BACustomerNumber

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
- wrapUpReason

To enable Outbound Option data to appear in Cisco Finesse, the administrator must edit the Default layout to include some or all Outbound Option variables.

Configure Call Variables Layouts

Procedure

Step 1 From the Manage Call Variables Layouts gadget:

- To create a new Call Variables Layout, click New.
- To modify an existing Call Variables Layout, choose a layout from the list, and click Edit (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 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 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 6 To view the latest configured Call Variables Layout, click Refresh from the Manage Call Variables Layouts gadget.
Add ECC Variables to Call Variables Layout

Note
Cisco Finesse only supports Latin1 characters for ECC variables. Other Unicode characters are not supported. For example, if you add an ECC variable that contains Chinese characters to the call variable layout, it may not appear correctly on the agent desktop.

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.

The Custom/ECC Variable Entry dialog box appears.

![Custom/ECC Variable Entry](image)

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 the CCX Editor's Expanded Call Variables tab, create an ECC variable called `user.layout` in the Set Enterprise Call Info Step used in the CCX routing script.

Note
If both a user.layout and a user.Layout are specified, Finesse will prioritize user.layout over user.Layout. If the layout specified in the user.Layout or user.layout is not found, Finesse will use the Default layout.
Step 2

Set the value of user.layout to the name of the call variables layout that should be used. The layout name should match the name of a call variables layout that was created on the Call Variables Layout tab in Finesse Administration.

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 executed, see Workflows and Workflow Actions.

For more details, see the section, "Adding an HTTP Request Workflow Action" in the white paper Cisco Finesse: How to Create a Screen-Pop Workflow.

Related Topics

Workflows and Workflow Actions, on page 394

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

Finesse Desktop Layout XML

The Finesse Layout XML defines the layout of the Finesse desktop, including tab names and the gadgets that appear on each tab.

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:

• Finesse Default Layout XML: Expands to show the layout XML for the default Finesse desktop.

• Restore Default Layout: Restores the Finesse desktop to the default layout.

• Save: Saves your configuration changes.

• Revert: Retrieves and applies the most recently saved desktop layout.
Default Layout XML

Update Default Desktop Layout

When you modify the layout of the Finesse desktop, the changes you make take effect on the desktop after 10 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 the desktop.

Note

The call control gadget is only supported at the page level. You must ensure that the call control gadget (<gadget>/desktop/gadgets/CallControl.jsp</gadget>) is placed within the <page></page> tag for it to work correctly. Do not place this gadget within a <tab></tab> tag.

Procedure

Step 1

In the Finesse Layout XML area, make changes to the XML as required.

Example:

If you want to add a new tab called Reports, add the following XML within the tabs tags under the <role>Agent</role> tag.

```
<tab>
  <id>reports</id>
  <label>Reports</label>
</tab>
```

If you want to add this tab to the supervisor desktop, add the XML within the tabs tags under the <role>Supervisor</role> tag.

To add a gadget to a tab, add the XML for the gadget within the gadgets tag for that tab.

```
<gadgets>
  <gadget>http://<ipAddress>/gadgets/<gadgetname>.xml</gadget>
</gadgets>
```

Replace <ipAddress> with the IP address of the server where the gadget resides.

If you want to add multiple columns to a tab on the Finesse desktop, add the gadgets for each column within the columns tags for that tab. You can have up to four columns on a tab.

```
<tab>
  <id>tab-id</id>
  <label>Tab Label</label>
  <columns>
    <column>
      <gadgets>
        <gadget>/gadget/1/url.xml</gadget>
        <gadget>/gadget/2/url.xml</gadget>
      </gadgets>
    </column>
    <column>
      <gadgets>
        <gadget>/gadget/3/url.xml</gadget>
      </gadgets>
    </column>
  </columns>
</tab>
```
Step 2

Click Save.

Finesse validates the XML file to ensure that it is valid XML syntax and conforms to the Finesses schema.

Step 3

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 will be not be updated. You need to click on Restore Default Layout to get the latest changes.

---

**XML Schema Definition**

You must ensure the XML you upload conforms to the XML schema definition for Finesse. The XML schema definition for Finesses is as follows:

```xml
<?xml version="1.0" encoding="ISO-8859-1" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  targetNamespace="http://www.cisco.com/vtg/finesse"
  xmlns="http://www.cisco.com/vtg/finesse"
  elementFormDefault="qualified">

<!-- 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:restriction>
  </xs:simpleType>
</xs:element>

<xs:element name="gadget">
  <xs:simpleType>
    <xs:restriction base="xs:anyURI">
      <xs:minLength value="1" />
    </xs:restriction>
  </xs:simpleType>
</xs:element>

</xs:schema>
```

---
<xs:schema>
  <xs:element name="role" type="role"/>
  <xs:element name="gadgets"> <!-- Grouping of a set of gadgets -->
    <xs:complexType>
      <xs:sequence 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="page"> <!-- Grouping of a set of persistent gadgets -->
    <xs:complexType>
      <xs:sequence 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"> <!-- Grouping of a set of persistent gadget URLs -->
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="id"/> <!-- Id of the tab selector in the desktop -->
        <xs:element ref="label"/> <!-- Label of the tab selector -->
        <xs:element ref="gadgets" minOccurs="0" maxOccurs="1"/> <!-- URI of the gadget xml -->
      </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"/> <!-- URI of the gadget xml -->
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="layout"> <!-- Type of the role -->
    <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 maxOccurs="3"> <!-- only support 3 roles for now -->
        <xs:element ref="layout" /> <!-- URI of the gadget xml -->
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
Add Web Chat 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/agentdesktop/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.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>When to use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Web Chat and Email to the default desktop layout.</td>
<td>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.</td>
</tr>
<tr>
<td>Add Web Chat and Email to a custom desktop layout.</td>
<td>Follow this procedure if you want to add Web Chat and Email and have customized the desktop layout.</td>
</tr>
<tr>
<td>Add Web Chat and Email to a team layout.</td>
<td>Follow this procedure if you want to add Web Chat and Email to the desktop only for specific teams.</td>
</tr>
</tbody>
</table>

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  
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/agentdesktop/gadgets/NonVoiceControl.xml</gadget>
-->

Step 3  
Remove the comments and comment characters (<!-- and -->) that surround the gadget, leaving only the gadget (<gadget>https://localhost/agentdesktop/gadgets/NonVoiceControl.xml</gadget>).
Step 4  
To add the Manage Chat and Email tab and gadget to the agent desktop, look for the following within the `<tabs></tabs>` tag:

```xml
<tab>
  <id>manageNonVoiceMedia</id>
  <label>finesse.container.tabs.agent.manageNonVoiceMediaLabel</label>
  <columns>
    <column>
      <gadgets>
        <gadget>https://my-socialminer-server/multisession/ui/gadgets/multisession-reply-gadget.jsp?gadgetHeight=430</gadget>
      </gadgets>
    </column>
  </columns>
</tab>
```

Step 5  
Remove the comments and comment characters (`<!--` and `-->`) that surround the tab.

Step 6  
Replace `my-socialminer-server` in the gadget URL with the fully-qualified domain name (FQDN) of your SocialMiner server.

Step 7  
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:

```xml
<gadget>https://my-socialminer-server/multisession/ui/gadgets/multisession-reply-gadget.jsp?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 8  
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:

```xml
<gadget>https://localhost/agentdesktop/gadgets/NonVoiceControl.xml</gadget>
```

Step 9  
Remove the comments and comment characters (`<!--` and `-->`), leaving only the gadget (`<gadget>https://localhost/agentdesktop/gadgets/NonVoiceControl.xml</gadget>`).

Step 10  
To add the Live Data report for Agent Chat Statistics to the supervisor desktop, look for the following:

```xml
<gadget>https://localhost:8444/cucic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId=F2F1FC171000001440000014E0A4E5D48&filterId=ChatAgentStats.agentId=CL</gadget>
```

Step 11  
Remove the comments and comment characters (`<!--` and `-->`), leaving only the gadget.

Step 12  
To add the Live Data report for Chat Queue Statistics to the supervisor desktop, look for the following:

```xml
<gadget>https://localhost:8444/cucic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310</gadget>
```
Add Web Chat and Email to a Custom Desktop Layout

Procedure

Step 1
In the Finesse administration console, click the Desktop Layout tab.

Step 2
Click Finesse Default Layout XML to show the default layout XML.

Step 3
Copy the XML code for the Chat and Email Control gadget for the agent desktop.

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:

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:

Step 6
Copy the code for the agent Manage Chat and Email tab and gadget from the default layout XML.
Step 7 Paste the code within the `<tabs></tabs>` tag for the agent role after the Manage Call tab:

```xml
<tab>
  <id>manageNonVoiceMedia</id>
  <label>finesse.container.tabs.agent.manageNonVoiceMediaLabel</label>
  <columns>
    <column>
      <gadgets>
        <gadget>https://my-socialminer-server/multisession/ui/gadgets/multisession-reply-gadget.jsp?gadgetHeight=430</gadget>
      </gadgets>
    </column>
  </columns>
</tab>
```

Step 8 Replace `my-social-miner-server` with the FQDN of your SocialMiner 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:

```xml
<gadget>https://my-socialminer-server/multisession/ui/gadgets/multisession-reply-gadget.jsp?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.

```xml
<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId=F2F1FC17100001440000148EA4E5D48&filterId=ChatAgentStats.agentId=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.

Step 13 Paste the code within the <tabs></tabs> tag for the supervisor role after the Manage Call tab:

Step 14 Replace my-social-miner-server with the FQDN of your SocialMiner 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 Click Finesse Default Layout XML to show the default layout XML.
Step 3 Copy the XML code for the Chat and Email Control gadget for the agent desktop and paste it into a text file.

Step 4 Copy the code for the agent Manage Chat and Email tab and gadget and paste it into your text file.
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.

Step 6  Copy the code for the supervisor Manage Chat and Email tab and gadget and paste it into your text file.

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  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:

Step 12  To add the gadget to the supervisor desktop, paste the code within the <page></page> tags under the Call Control gadget as follows:
Step 13
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>
      </gadgets>
    </column>
  </columns>
</tab>
```

Step 14
Replace my-social-miner-server with the FQDN of your SocialMiner server.

Step 15
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-socialminer-server/multisession/ui/gadgets/multisession-reply-gadget.jsp?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 16
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 17
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>
```

---

Note: The example code provided is for illustration purposes and may need to be modified based on your specific environment and requirements.
Step 18 Replace my-social-miner-server with the FQDN of your SocialMiner server.
Step 19 Optionally, change the height of the gadget.
Step 20 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.

<table>
<thead>
<tr>
<th>Users</th>
<th>Reports</th>
<th>Report View</th>
<th>Is the Report Available in Default Layout?</th>
<th>Tab</th>
<th>Gadget URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>Agent CSQ Statistics Report</td>
<td>Agent CSQ Statistics Report</td>
<td>Yes</td>
<td>Home</td>
<td>&lt;gadget&gt;<a href="https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=76D964AD10000140000000830A4E5E6F&amp;filterId=AgentCSQStats.csqName=CL&amp;compositeFilterId=AgentCSQStats.AgentIds.agentId=loginId">https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=76D964AD10000140000000830A4E5E6F&amp;filterId=AgentCSQStats.csqName=CL&amp;compositeFilterId=AgentCSQStats.AgentIds.agentId=loginId</a>&lt;/gadget&gt;</td>
</tr>
<tr>
<td>Agent</td>
<td>Agent State Log Report</td>
<td>Agent State Log Report</td>
<td>Yes</td>
<td>My Statistics</td>
<td>&lt;gadget&gt;<a href="https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=420&amp;viewId=5D411E8A10000140000000230A4E5E6B&amp;filterId=AgentStateDetailStats.agentId=loginId">https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=420&amp;viewId=5D411E8A10000140000000230A4E5E6B&amp;filterId=AgentStateDetailStats.agentId=loginId</a>&lt;/gadget&gt;</td>
</tr>
<tr>
<td>Users</td>
<td>Reports</td>
<td>Report View</td>
<td>Is the Report Available in Default Layout?</td>
<td>Tab</td>
<td>Gadget URLs</td>
</tr>
<tr>
<td>---------</td>
<td>------------------</td>
<td>----------------------</td>
<td>-------------------------------------------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Agent</td>
<td>Agent Statistics</td>
<td>Agent Statistics</td>
<td>Yes</td>
<td>My Statistics</td>
<td>&lt;gadget&gt;<a href="https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=150&amp;viewId=67D4371110000140000001080A4E5E6E&amp;filterId=ResourceIAQStats.resourceId=loginId">https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=150&amp;viewId=67D4371110000140000001080A4E5E6E&amp;filterId=ResourceIAQStats.resourceId=loginId</a>&lt;/gadget&gt;</td>
</tr>
<tr>
<td></td>
<td>Report</td>
<td>Report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent</td>
<td>Agent Team</td>
<td>Agent Team</td>
<td>Yes</td>
<td>Home</td>
<td>&lt;gadget&gt;<a href="https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=5C626F9C1000014000000060A4E5B33&amp;filterId=ResourceIAQStats.resourceId=CL">https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=5C626F9C1000014000000060A4E5B33&amp;filterId=ResourceIAQStats.resourceId=CL</a>&lt;/gadget&gt;</td>
</tr>
<tr>
<td></td>
<td>Summary Report</td>
<td>Summary Report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisor</td>
<td>Agent Outbound</td>
<td>Report since midnight</td>
<td>No</td>
<td>Team Data</td>
<td>&lt;gadget&gt;<a href="https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=FD919FB9100001440000001470A4E5B29&amp;filterId=ResourceIAQStats.resourceId=CL">https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=FD919FB9100001440000001470A4E5B29&amp;filterId=ResourceIAQStats.resourceId=CL</a>&lt;/gadget&gt;</td>
</tr>
<tr>
<td></td>
<td>Team Summary</td>
<td>Report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisor</td>
<td>Agent Outbound</td>
<td>Short and long term</td>
<td>No</td>
<td>Team Data</td>
<td>&lt;gadget&gt;<a href="https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=FD919FB510000144000000470A4E5B29&amp;filterId=ResourceIAQStats.resourceId=CL">https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=FD919FB510000144000000470A4E5B29&amp;filterId=ResourceIAQStats.resourceId=CL</a>&lt;/gadget&gt;</td>
</tr>
<tr>
<td></td>
<td>Team Summary</td>
<td>Report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisor</td>
<td>Chat Agent</td>
<td>Chat Agent</td>
<td>No</td>
<td>Team Data</td>
<td>&lt;gadget&gt;<a href="https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=120&amp;viewId=F2F1FC17100001440000014E0A4E5D48&amp;filterId=ChatAgentStats.agentId=CL">https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=120&amp;viewId=F2F1FC17100001440000014E0A4E5D48&amp;filterId=ChatAgentStats.agentId=CL</a>&lt;/gadget&gt;</td>
</tr>
<tr>
<td></td>
<td>Statistics Report</td>
<td>Statistics Report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisor</td>
<td>Chat CSQ</td>
<td>Chat CSQ</td>
<td>No</td>
<td>Queue Data</td>
<td>&lt;gadget&gt;<a href="https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=120&amp;viewId=E42ED788100001440000007B0A4E5CA1&amp;filterId=ChatQueueStatistics.queueName=CL">https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=120&amp;viewId=E42ED788100001440000007B0A4E5CA1&amp;filterId=ChatQueueStatistics.queueName=CL</a>&lt;/gadget&gt;</td>
</tr>
<tr>
<td></td>
<td>Summary Report</td>
<td>Summary Report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisor</td>
<td>Email Agent</td>
<td>Email Agent</td>
<td>No</td>
<td>Team Data</td>
<td>&lt;gadget&gt;<a href="https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=BCC5767B1000014F000000580A4D3FA7&amp;filterId=EmailAgentStats.agentId=CL">https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=BCC5767B1000014F000000580A4D3FA7&amp;filterId=EmailAgentStats.agentId=CL</a>&lt;/gadget&gt;</td>
</tr>
<tr>
<td></td>
<td>Statistics Report</td>
<td>Statistics Report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisor</td>
<td>Email CSQ</td>
<td>Email CSQ</td>
<td>No</td>
<td>Queue Data</td>
<td>&lt;gadget&gt;<a href="https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=13970B4E100001500000021C0A4D3FA7&amp;filterId=EmailQueueStatistics.queueName=CL">https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=13970B4E100001500000021C0A4D3FA7&amp;filterId=EmailQueueStatistics.queueName=CL</a>&lt;/gadget&gt;</td>
</tr>
<tr>
<td></td>
<td>Summary Report</td>
<td>Summary Report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td>Reports</td>
<td>Report View</td>
<td>Is the Report Available in Default Layout?</td>
<td>Tab</td>
<td>Gadget URLs</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------</td>
<td>-------------------------------------------------</td>
<td>-------------------------------------------</td>
<td>-----------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Supervisor</td>
<td>Team State Report</td>
<td>Team State Report</td>
<td>No</td>
<td>—</td>
<td>&lt;gadget&gt;<a href="https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=5c90012f100001400000000830a4e5b33&amp;filterId=ResourceIAQStats.resourceId=CL">https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=5c90012f100001400000000830a4e5b33&amp;filterId=ResourceIAQStats.resourceId=CL</a>&lt;/gadget&gt;</td>
</tr>
<tr>
<td>Supervisor</td>
<td>Team Summary Report</td>
<td>Report since midnight</td>
<td>Yes</td>
<td>Team Data</td>
<td>&lt;gadget&gt;<a href="https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=728283c210000140000000530a4e5b33&amp;filterId=ResourceIAQStats.resourceId=CL">https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=728283c210000140000000530a4e5b33&amp;filterId=ResourceIAQStats.resourceId=CL</a>&lt;/gadget&gt;</td>
</tr>
<tr>
<td>Supervisor</td>
<td>Team Summary Report</td>
<td>Short and long term average</td>
<td>Yes</td>
<td>Team Data</td>
<td>&lt;gadget&gt;<a href="https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=7291dc310000140000000890a4e5b33&amp;filterId=ResourceIAQStats.resourceId=CL">https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=7291dc310000140000000890a4e5b33&amp;filterId=ResourceIAQStats.resourceId=CL</a>&lt;/gadget&gt;</td>
</tr>
<tr>
<td>Supervisor</td>
<td>Voice CSQ Agent Detail Report</td>
<td>Voice CSQ Agent Detail Report</td>
<td>Yes</td>
<td>Queue Data</td>
<td>&lt;gadget&gt;<a href="https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=9a7a14ce1000014000000e0a4e5e6b&amp;filterId=VoiceCSQDetailsStats.agentId=CL&amp;compositeFilterId=VoiceCSQDetailsStats.AgentVoiceCSQNames.agentVoiceCSQName=CL">https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=9a7a14ce1000014000000e0a4e5e6b&amp;filterId=VoiceCSQDetailsStats.agentId=CL&amp;compositeFilterId=VoiceCSQDetailsStats.AgentVoiceCSQNames.agentVoiceCSQName=CL</a>&lt;/gadget&gt;</td>
</tr>
<tr>
<td>Supervisor</td>
<td>Voice CSQ Summary</td>
<td>Snapshot</td>
<td>Yes</td>
<td>Queue Data</td>
<td>&lt;gadget&gt;<a href="https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=C82e2db161000014000000a60a4e5e6b&amp;filterId=VoiceIAQStats.esdName=CL">https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=C82e2db161000014000000a60a4e5e6b&amp;filterId=VoiceIAQStats.esdName=CL</a>&lt;/gadget&gt;</td>
</tr>
<tr>
<td>Supervisor</td>
<td>Voice CSQ Summary</td>
<td>Short and long term average</td>
<td>Yes</td>
<td>Queue Data</td>
<td>&lt;gadget&gt;<a href="https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=C8e24191000014000000c30a4e5e6b&amp;filterId=VoiceIAQStats.esdName=CL">https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=C8e24191000014000000c30a4e5e6b&amp;filterId=VoiceIAQStats.esdName=CL</a>&lt;/gadget&gt;</td>
</tr>
<tr>
<td>Supervisor</td>
<td>Voice CSQ Summary</td>
<td>Report since midnight</td>
<td>No</td>
<td>Queue Data</td>
<td>&lt;gadget&gt;<a href="https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=C8ef51081000014000000e0b0a4e5e6b&amp;filterId=VoiceIAQStats.esdName=CL">https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&amp;viewId=C8ef51081000014000000e0b0a4e5e6b&amp;filterId=VoiceIAQStats.esdName=CL</a>&lt;/gadget&gt;</td>
</tr>
</tbody>
</table>

**Gadgets Customization**

You can use optional query parameter to adjust height of the gadgets.
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  Click Finesse Default Layout XML to show the default layout XML.
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.jsp?gadgetHeight=150&viewId=67D4371110000140000001080A4E5E6B&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.jsp</gadget>
    </page>
    <tabs>
      <tab>
        <id>home</id>
        <label>finesse.container.tabs.agent.homeLabel</label>
        <gadgets>
          <gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId=5C626F9C10000140000000600A4E5E63&filterId=ResourceIAQStats.resourceId=CL</gadget>
        </gadgets>
      </tab>
      <tab>
        <id>myStatistics</id>
        <label>finesse.container.tabs.agent.myStatisticsLabel</label>
        <gadgets>
          <gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=150&viewId=67D4371110000140000001080A4E5E6B&filterId=ResourceIAQStats.resourceId=loginId</gadget>
        </gadgets>
      </tab>
    </tabs>
  </layout>
</finesseLayout>
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.

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.jsp?gadgetHeight=310&viewId=5C626F9C100001400000000600A4E5B33&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.htm?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.

```html
gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?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 Finesses desktop and check the report.

---

**Related Topics**

- Live Data Gadgets, on page 368

---

**Live Data Reports**

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

**Configure Live Data Reports with Multiple Views**

Cisco Finesses 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 Finesses 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.

Finesses 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 Finesses 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.
Configure Live Data Reports with Multiple Views

Example:
Copy the viewId, which is underlined in this example, from the permalink for the report.

https://<Server Name>:8444/cuic/permalink/PermalinkViewer.htmx?
viewId=5C90012F10000140000000830A4E5B33&linkType=htmlType&viewType=Grid

Step 2 From the Finesse default layout XML, copy the gadget URL for one of the Live Data reports and paste it into a text editor.

Example:
Copy the URL for the Agent Skill Group for HTTPS from the default layout XML and paste it into a text editor:

<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&
viewId_1=9AB7848B10000141000001C50A0006C4&filterId_1=agent.id=CL\ teamName</gadget>

Step 3 To update the URL to refer to a different report view, populate the viewId_1 value (after the equal sign) with the desired viewId obtained in step 1.

Example:
The following shows the URL updated with the example viewId copied from step 1.

<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL\ teamName</gadget>

Step 4 For each additional view you want to include:

a) At the end of the URL, copy and paste the viewId_1 and agentId_1 strings with a leading ampersand.

Example:

<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%teamName&
viewId_2=5C90012F10000140000000830A4E5B33&filterId_2=agent.id=CL%teamName</gadget>

b) Update the copied viewId_1 and filterId_1 in the URL to the next available integer (in this example, viewId_2 and filterId_2).

Example:

<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%teamName&
viewId_2=5C90012F10000140000000830A4E5B33&filterId_2=agent.id=CL%teamName</gadget>

c) Populate the copied viewId value (after the equal sign) with the value defined in the permalink for the desired report (in this example, 99E6C8E210000141000000D80A0006C4).

Example:

<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%teamName&
viewId_2=99E6C8E210000141000000D80A0006C4&filterId_2=agent.id=CL%teamName</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
Step 5
Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

Step 6
Add the customized gadget URL to the desktop layout XML in the Manage Desktop Layout gadget and click Save.

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

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

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 1500.

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the phone book. The name must be unique, and can be a maximum length of 64 alphanumeric characters.</td>
</tr>
<tr>
<td>Assign To</td>
<td>Indicates if the phone book is global (All Users) or team (Teams).</td>
</tr>
<tr>
<td>Last Name</td>
<td>The last name of a contact. The last name can be a maximum length of 128 characters. This field is optional.</td>
</tr>
</tbody>
</table>
### Add Phone Book

**Procedure**

**Step 1**
In the Manage Phone Books gadget, click **New**.

The Manage Phone Books area appears.

**Step 2**
In the Name box, enter a name for the phone book.

**Note**
Phone book names can be a maximum length of 64 characters.

**Step 3**
In the Assign To box drop-down list, 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**.

The Edit Phone Books area appears.
**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**.

A question appears asking you to confirm that you want to delete the selected phone book.

**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 1500 contacts. Import lists that contain more than 1500 contacts are rejected with an error message.

The CSV file contains the fields described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Max Length</th>
<th>Can Be Blank?</th>
<th>Permitted Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>128</td>
<td>Yes</td>
<td>Alphanumeric characters</td>
</tr>
<tr>
<td>Last Name</td>
<td>128</td>
<td>Yes</td>
<td>Note: The CSV file that contains the contacts to import must use Latin encoding.</td>
</tr>
<tr>
<td>Phone Number</td>
<td>32</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td>128</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

The following is an example of a phone book CSV file:

"First Name","Last Name","Phone Number","Notes"
"Amanda","Cohen","651-123-4",""
"Nicholas","Knight","612-555-122","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.
Exported CSV files always show each field enclosed in double quotes, as in the preceding example, to ensure that any commas or double quotes that are part of the actual fielded 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**.

The Import Contacts area appears.

**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**.

A message is displayed asking if you want to open or save the file.

*Note*  
The default name for an export file is *PhoneBookContacts.csv*.

**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**, as desired.

**Step 4**
A message appears that gives you the option to view the downloaded file, open the folder into which the download was saved, view the Internet Explorer View Downloads window, or dismiss the message without viewing the file.

---

**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.  
The New Contact area appears.

**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.  
The Edit Contact area appears.

**Step 4**  
Edit the fields that you want to change. 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 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.  
A question appears asking you to confirm that you want to delete the selected contact.

**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.
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. 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. Click the Type header to sort and display system or custom reason codes. 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).

Finesse supports a total of 200 Not Ready reason codes. This includes a maximum of 100 global Not Ready reason codes, and 100 Not Ready 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 (Not Ready) gadget.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason Label</td>
<td>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. Both alphanumeric and special characters are supported.</td>
</tr>
<tr>
<td>Type</td>
<td>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.</td>
</tr>
<tr>
<td>Reason Code</td>
<td>A code for the Not Ready reason. The value of the code must be between 1 and 999 and must be unique.</td>
</tr>
<tr>
<td>Global?</td>
<td>Yes/No. Indicates if the reason code is available globally to all agents (Yes) or to specific teams of agents (No).</td>
</tr>
</tbody>
</table>

**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
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).

During a PG or CTI server failover, the pending state of an agent will not be retained.

Add Not Ready Reason Code

Perform the following procedure to add a new Not Ready reason code.

Procedure

**Step 1** In the Manage Reason Codes (Not Ready) gadget, click **New**.
The New Reason Code area appears.

**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 pre populated 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**.
The Finess server removes leading or trailing spaces before saving the Reason Label in the database.

Edit Not Ready Reason Code

Perform the following procedure to edit the label or code for an existing 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.
The Edit Reason Code area appears.
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

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.

Perform the following procedure to delete a Not Ready reason code.

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.
A question appears asking you to confirm that you want to delete the selected reason code.
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).

Finesse supports a total of 200 Sign Out reason codes. This includes a maximum of 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason Label</td>
<td>The label for the Sign Out reason code.</td>
</tr>
<tr>
<td></td>
<td>The label has a maximum length of 40 characters and should be unique for each Sign Out reason code. Both alphanumeric and special characters are supported.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of reason code (System or Custom).</td>
</tr>
<tr>
<td></td>
<td>The column is default and can be sorted to display both System reason codes and Custom reason codes.</td>
</tr>
<tr>
<td>Reason Code</td>
<td>A code for the Sign Out reason.</td>
</tr>
<tr>
<td></td>
<td>The code must be between 1 and 999 and must be unique.</td>
</tr>
<tr>
<td>Global?</td>
<td>Yes/No. Indicates if the reason code is available globally to all agents (Yes) or to specific teams of agents (No).</td>
</tr>
</tbody>
</table>

**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

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 back in 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 then choose the code that represents why that agent is signing out.

**Add Sign Out Reason Code**

Perform the following procedure to add a new Sign Out reason code.
Procedure

Step 1  In the Manage Reason Codes (Sign Out) gadget, click **New**.
       The New Reason Code area appears.

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 pre populated 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

Perform the following procedure to edit the label or code for an existing 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**.
       The Edit Reason Code area appears.

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.

Perform the following procedure to delete a Sign Out reason code.
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.

A question appears asking you to confirm that you want to delete the selected reason code.

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:

<table>
<thead>
<tr>
<th>System Reason Code</th>
<th>Reason Label</th>
<th>Reason Label Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>32767</td>
<td>Logged Out - Device Conflict</td>
<td>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.</td>
</tr>
<tr>
<td>32765</td>
<td>Logged Out - System Disconnect</td>
<td>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.</td>
</tr>
<tr>
<td>32764</td>
<td>Logged Out - System Standby</td>
<td>The system issues this reason code when the active server becomes the standby server and the agent loses connection to the Unified CCX Platform.</td>
</tr>
<tr>
<td>Code</td>
<td>Reason Code</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>32763</td>
<td>Not Ready - Call Not Answered</td>
<td>The system issues this reason code when the agent fails to answer a Unified CCX call within the specified timeout period.</td>
</tr>
<tr>
<td>32762</td>
<td>Not Ready - Offhook</td>
<td>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.</td>
</tr>
<tr>
<td>32761</td>
<td>Not Ready - Non ACD Busy</td>
<td>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.</td>
</tr>
<tr>
<td>32760</td>
<td>Not Ready - Log On</td>
<td>The system issues this reason code when an agent logs in and is automatically placed in the Not Ready state.</td>
</tr>
<tr>
<td>32759</td>
<td>Not Ready - Phone Failure</td>
<td>The system issues this reason code if the agent’s phone crashes and that agent is placed in the unavailable state.</td>
</tr>
<tr>
<td>32758</td>
<td>Not Ready - Wrap Up Timer Expiry</td>
<td>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.</td>
</tr>
<tr>
<td>32757</td>
<td>Not Ready - CUCM Failover</td>
<td>The system issues this reason code when the Unified CM fails over and the agent is moved to the Not Ready state.</td>
</tr>
<tr>
<td>32756</td>
<td>Not Ready - Phone Working</td>
<td>The system issues this reason code when the agent’s phone comes up after it has been through a Phone Down state.</td>
</tr>
<tr>
<td>32755</td>
<td>Not Ready - Call Ended</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>32749</td>
<td>Not Ready - Call Cancel</td>
<td>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.</td>
</tr>
<tr>
<td>32754</td>
<td>Not Ready - Restricted Device</td>
<td>The system issues this reason code if the agent device is flagged as a restricted device by the Unified CM Administrator.</td>
</tr>
<tr>
<td>Code</td>
<td>Reason Code Conflicts During Upgrade</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>32753</td>
<td>Not Ready - Restricted Line</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The system issues this reason code if the agent’s phone line is flagged as a restricted device by the Unified CM Administrator.</td>
<td></td>
</tr>
<tr>
<td>32752</td>
<td>Not Ready - Cancel Reservation Preview Call</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The system issues this reason code when an agent receives a preview outbound call and decides to cancel the reservation by pressing &quot;Decline&quot; button on Cisco Finesse desktop.</td>
<td></td>
</tr>
<tr>
<td>32751</td>
<td>Not Ready - Skip Preview Call</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The system issues this reason code when an agent receives a preview outbound call and skips the call.</td>
<td></td>
</tr>
<tr>
<td>32748</td>
<td>Log Out - Agent Deleted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>32750</td>
<td>Not Ready - Extension Modified</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>32742</td>
<td>Not Ready - Non ACD Offhook</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>32741</td>
<td>Logged Out - Extension Conflict</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>32740</td>
<td>Logout - System Initiated Relogin</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The system logs out the agent from one session when the agent tries to log in with the same credentials in another session.</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>Not Ready - Supervisor Initiated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The system issues this reason code when the Supervisor changes an agent’s state to Not Ready state.</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Logged Out - Supervisor Initiated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The system issues this reason code when the Supervisor changes an agent’s state to log out.</td>
<td></td>
</tr>
<tr>
<td>255</td>
<td>Logged Out - Connection Failure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

**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) or higher versions. 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

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.

### Note

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason Label</td>
<td>The label for the Wrap-Up reason.</td>
</tr>
</tbody>
</table>
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 back in to see those changes reflected on their desktops.

**Related Topics**
- [Contact Service Queue Configuration Web Page](#), on page 101

---

**Add Wrap-Up Reason**
Perform the following procedure to add a new Wrap-Up reason.

**Procedure**

**Step 1**
In the Manage Wrap-Up Reasons gadget, click **New**.

The New Wrap-Up Reason area appears.

**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**
Perform the following procedure to edit an existing 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

Perform the following procedure to delete a 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.

---

## 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.

<table>
<thead>
<tr>
<th>Tab Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Layout</td>
<td>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.</td>
</tr>
<tr>
<td>Phone Books</td>
<td>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.</td>
</tr>
<tr>
<td>Reason Codes (Not Ready)</td>
<td>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.</td>
</tr>
<tr>
<td>Reason Codes (Sign Out)</td>
<td>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.</td>
</tr>
<tr>
<td>Wrap-Up Reasons</td>
<td>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.</td>
</tr>
<tr>
<td>Workflows</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.
Tabs for each available resource appear.

**Step 2**
Click the tab for the resource you want to assign for the selected team.
The List of `<resource>` area appears.

**Step 3**
Click **Add**.
The Add `<resource>` popup appears.

**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 has finished 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.
Tabs for each available resource appear.

**Step 2**
Click the tab for the resource you want to unassign from the selected team.
Assign Custom Desktop Layout to Team

Perform the following procedure to create and assign a custom desktop layout to a team.

**Procedure**

**Step 1**
In the Manage Team Resources gadget, select a team. Tabs for each available resource appear.

**Step 2**
Click the Desktop Layout tab.
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**
Edit the XML as desired.

**Step 5**
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 go into 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.

---

**Assign Workflows to Team**

**Procedure**

**Step 1**
In the Manage Team Resources gadget, select a team. Tabs for each available resource appear.

**Step 2**
Click the Workflows tab.
The List of Workflows area appears.

**Step 3**  
Click **Add**.

The Add Workflow popup appears.

**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 executed in the order in which 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 have 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 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.

Tabs for each available resource appear.

**Step 2**  
Click the Workflow tab.

The List of Workflows area appears.

**Step 3**  
Click the red X next to the workflow you want 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.

Finesse supports the following number of workflows and workflow actions:
• 100 workflows per Finesses system
• 100 actions per Finesses system
• 20 workflows per team
• 5 conditions per workflow
• 5 actions per workflow
• 5 variables per action

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the workflow. The name must be unique and can be a maximum length of 40 characters.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the workflow. The description can be a maximum length of 128 characters.</td>
</tr>
</tbody>
</table>

The following table describes the fields on the Manage Workflow Actions gadget.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the workflow action. The name must be unique and can be a maximum length of 64 characters.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of workflow. Possible values are Browser Pop, HTTP Request.</td>
</tr>
</tbody>
</table>

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 Finesses desktop or in a third-party gadget. A third-party gadget can be designed to handle the action differently than Finess does.

Each workflow must contain only one trigger. Triggers are based on Finesses dialog events. Dialog events include the following:

• When a call arrives
• When a call is answered

**Note**

If you set a workflow to trigger when a call is answered, the workflow runs when an agent answers an incoming call or makes an outgoing call, or when a customer answers an Outbound Option call.
• When a call ends
• When making a call
• While previewing a Direct Preview Outbound call.

The workflow engine uses the following simple logic to determine whether to execute a workflow:

• To determine whether a workflow should execute, 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.

**Note**

Outbound Preview calls are an exception to this rule. You can have a workflow run while the agent previews the call as well as when the agent accepts the call.

• After a workflow for a particular trigger type (for example, Call Arrives) executes, 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**

Workflows that trigger when a call arrives, when a call is answered, or when making a call run whenever the browser is refreshed. When an agent refreshes the browser, the workflow engine sees 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. Otherwise, undesired results may occur.

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 execute if any conditions are met or if all conditions are met.

Individual conditions consist of the following:

• A piece of event data to be examined, for example, DNIS or call variables
• A comparison between the event data and entered values (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 executed. The actions execute in the order in which they are listed.

Workflows run only for agents and supervisors who are Finesse users. The Workflow Engine is a JavaScript library that runs client-side on a per-user basis within the Finesse desktop application. The desktop retrieves the workflows to execute for a user from the server when the user signs in or refreshes the browser.
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 the event and the workflow conditions evaluate to true, then that workflow is the one used and 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 used in workflow conditions from the dialog that triggered the workflow. If a variable is not found in the dialog, then its value is assumed to be empty.

The Workflow Engine executes the actions associated with the matched workflow in the order in which they are listed. The Workflow Engine executes actions in a workflow even if the previously executed action fails. Failed actions are logged.

The Finesse server controls which calls are displayed to the 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 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 the user has a call when 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 the user has multiple calls when the user refreshes the browser, the Workflow Engine treats the first dialog received from the Finesse server as the first displayed call. This call is not necessarily the same call that was the first displayed call before the browser refresh. Dialogs received for any other call are ignored because they are not considered first displayed calls. If dialogs for more than one call are received before the Workflow Engine is loaded after the browser refresh, no dialogs are evaluated because none are considered first displayed calls.

Workflows run for both 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. You may want to 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.
### 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.

<table>
<thead>
<tr>
<th>Workflow Trigger</th>
<th>Direct Preview Outbound Call</th>
<th>Progressive or Predictive Outbound Call</th>
</tr>
</thead>
<tbody>
<tr>
<td>While previewing a call</td>
<td>When the agent previews the call (before the agent accepts or rejects the call).</td>
<td>Does not trigger.</td>
</tr>
<tr>
<td>When a call arrives</td>
<td>When the agent accepts the call.</td>
<td>Does not trigger.</td>
</tr>
<tr>
<td>When a call is answered</td>
<td>When the customer answers the call.</td>
<td>When the customer answers the call.</td>
</tr>
<tr>
<td></td>
<td>If the agent conferences in another agent or transfers the call, the workflow triggers for the agent who is the recipient of the conference or transfer.</td>
<td>If the agent conferences in another agent or transfers the call, the workflow triggers for the agent who is the recipient of the conference or transfer.</td>
</tr>
<tr>
<td>When a call is made</td>
<td>When the customer call is initiated.</td>
<td>When the customer call is initiated or when failover occurs during the call.</td>
</tr>
<tr>
<td>When a call ends</td>
<td>When the customer call ends.</td>
<td>When the customer call ends.</td>
</tr>
</tbody>
</table>

---

**Note**

Whether the action opens a new window or tab on the desktop depends on the target user's browser settings.

**Procedure**

1. **Step 1**
   
   In the Manage Workflow Actions gadget, click **New**.
   
   The New Action area appears.

2. **Step 2**
   
   In the Name box, enter a name for the action.
   
   **Note**
   
   Workflow action names are limited to 64 characters.

3. **Step 3**
   
   From the Type drop-down list, select **Browser Pop**.

4. **Step 4**
   
   From the Handled By drop-down list, select what will execute the action, either the Finesse Desktop or Other (a third-party gadget).

5. **Step 5**
   
   In the Window Name box, enter the name that serves as the ID 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 to open, and then click the tag icon at the right of the box and select one or more variables from the drop-down list to add tags.

**Example:**

http://www.google.com/search?q=callVariable1&callVariable2

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**.

The New Action area appears.

**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 execute 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.

**Note** The drop-down list contains variables from all the media channels.

**Example:**
The preceding example is the URL for a Finesse API. 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:

```xml
<Dialog>
  <requestedAction>START_RECORDING</requestedAction>
  <targetMediaAddress>extension</targetMediaAddress>
</Dialog>
```

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**.

The Edit Action area appears.

**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.

The Delete Action area appears.
Step 2  Click **Delete**.

A question appears asking you to confirm that you want to delete the selected action.

Step 3  Click **Yes** to confirm the deletion of the selected action.

---

**Add Workflow**

**Procedure**

Step 1  In the Manage Workflows gadget, click **New**.

The New Workflow area appears.

Step 2  In the Name box, enter the name of the workflow.

**Note**  The name is limited to 40 characters.

Step 3  In the Description box, enter a description of the workflow.

**Note**  The description is limited to 128 characters.

Step 4  In the When to perform Actions drop-down list, select the event that triggers the workflow.

Step 5  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.

**Example:**

For example, you can specify that the action is taken when CallVariable 1 is equal to 123 and CallVariable 2 begins with 2.

Step 6  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 7  Use the up and down arrows next to the Ordered List of Actions to move actions into the order in which they should be performed.

Step 8  Click **Save**.

Step 9  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**.

The Edit Workflow area appears.
Delete Workflow

Procedure

Step 1 In the Manage Workflows gadget, select the workflow that you want to delete.

The Delete Workflow area appears.

Step 2 Click Delete.

A question appears asking you to confirm that you want to delete the selected workflow.

Step 3 Click Yes to confirm the deletion of the selected workflow.

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.

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.
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 codes 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.

HTTP Only

Finesse IPPA phone clients communicate with the Finesse server using HTTP only, whether or not HTTPS access is enabled on Finesse.

Failure Behavior

Unlike the Finesse desktop, the Finesse IP Phone Agent does not automatically failover to the alternate Finesse server. To resume normal 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 Finesseservice 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.

<table>
<thead>
<tr>
<th>Example Set Up</th>
<th>Prepopulated in Unified CM Administration (by Administrator)</th>
<th>Prepopulated in Self Care Portal (by Agent)</th>
<th>Entered at Sign-In (by Agent)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator populates the extension only</td>
<td>extension</td>
<td>-</td>
<td>id</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>password</td>
</tr>
<tr>
<td>Administrator populates the ID and extension</td>
<td>id</td>
<td>extension</td>
<td>password</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agents enter password only using Self Care Portal</td>
<td>id</td>
<td>extension</td>
<td>password</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agents enter all credentials using Self Care Portal</td>
<td>-</td>
<td>id</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>extension</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>password</td>
<td></td>
</tr>
<tr>
<td>Agents enter ID and extension only using Self Care Portal</td>
<td>-</td>
<td>id</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>extension</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 themselves.

The following table lists the Finesse IPPA configuration procedures and indicates which procedures are required depending on the subscription option you choose.
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. And for proper Finesse IPPA operation, you must also set the Web Access and HTTPS Server parameters in Unified CM.

These 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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Set the following parameters in Unified CM:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Set the <strong>Web Access</strong> parameter to <strong>Enabled</strong>.</td>
<td></td>
</tr>
<tr>
<td>• Set the <strong>HTTPS Server</strong> parameter to <strong>HTTP and HTTPS Enabled</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

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 userID 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/host name Change**.

**Note** For Finesse IP Phone Agent (FIPPA) from 11.0 (1) onwards, the User Device Profile (UDP) must be associated with the FIPPA Application User along with the physical phones for agents using Extension Mobility. The Finesse Service URL must use the complete FQDN of the UCCX server.

---

**Related Topics**

- Prepare System for IP Address/host name Change, on page 144

---

**Configure Finesse IP Phone Service in Unified CM**

The following procedure describes the steps required for both manual and enterprise subscription.

**Procedure**

**Step 1** Log in to the Cisco Unified Communications Manager Administration using administrator credentials.

**Step 2** From the Communications Manager menu, select **Device > Device Settings > Phone Services**.
Step 3  On the IP Phone Services page, 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#

where Finesse FQDN is the fully qualified domain name (FQDN) of your primary Finesses server.
Step 6  Ensure that the Service Category is set to XML Service, and the Service Type is set to Standard IP Phone Service.
Step 7  Check the Enable check box.
Step 8  Do one of the following:

- To automatically subscribe all phones in the cluster to the Finesses service, check the Enterprise Subscription check box, and click Save. Agents and supervisors can now access Cisco Finesses by selecting it from the Services menu on subscribed IP phones.

  Note  One Button Sign In is not supported with enterprise subscriptions.

  Figure 3: Finesses Service Configuration with Enterprise Subscription

- To subscribe only the desired phones to the Finesses service manually, leave the Enterprise Subscription check box unchecked and click Save.
Step 9  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, in the Service URL field, replace Finesse FQDN with the FQDN of the secondary server.

Note  Since Finesse IPPA works only over HTTP, avoid using Secured Phone URL Parameters in Unified CM.

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.
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.
The Configure Cisco IP Phone Service Parameter page displays.

**Step 3**
Set up service parameters for the agent id, extension, and password credentials in accordance with 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 additional parameters, click Add New and enter the required values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter Name</td>
<td>Enter one of the following parameter names as follows:</td>
</tr>
<tr>
<td></td>
<td>• Id</td>
</tr>
<tr>
<td></td>
<td>• extension</td>
</tr>
<tr>
<td></td>
<td>• password</td>
</tr>
<tr>
<td>Parameter Display Name</td>
<td>Enter a descriptive parameter name; for example, id, extension, and password.</td>
</tr>
<tr>
<td>Default Value</td>
<td>Leave the default value blank for all parameters.</td>
</tr>
<tr>
<td>Parameter Description</td>
<td>Enter a description of the parameter. The user can access this text when they subscribe to the service.</td>
</tr>
<tr>
<td>Parameter is Required</td>
<td>If the administrator will prepopulate the parameter in Unified CM Administration, check the Parameter is Required check box.</td>
</tr>
<tr>
<td></td>
<td>However, if the agent will prepopulate the parameter in the Self Care Portal, two options are available:</td>
</tr>
<tr>
<td></td>
<td>• If the agents will prepopulate all defined parameters, check the Parameter is Required check box for each parameter.</td>
</tr>
<tr>
<td></td>
<td>• If the agent and administrator will share the responsibility of prepopulating the parameters, set only the administrator-defined parameters as required.</td>
</tr>
<tr>
<td></td>
<td>This configuration ensures that the administrator can save the subscription without prepopulating all parameters.</td>
</tr>
<tr>
<td></td>
<td>In this case, the administrator first prepopulates the required parameters, and then the agents prepopulate the nonrequired parameters.</td>
</tr>
<tr>
<td>Parameter is a Password (mask contents)</td>
<td>Check this box for the password only.</td>
</tr>
<tr>
<td></td>
<td>This check box masks the password entries in the Self Care Portal, to display asterisks rather than the user entry.</td>
</tr>
</tbody>
</table>
When you save the last parameter, click **Save and Close**.

![Configure Cisco IP Phone Service Parameter](image)

**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 Finessse service as a manual subscription, you can subscribe the agent phones to the Finessse service in Unified CM and optionally define agent credentials for One Button Sign In.

If you prefer to allow the agents subscribe to the Finessse 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 Finessse 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 Finessse**.

**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 Finessse service.

The Cisco Finessse 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 Finesses setup (primary and secondary Finesses servers), perform this procedure again to also subscribe the phones to the secondary Finesses service that points to the secondary Finesses 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 Finesses 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 Finesses service and enter their own credentials under **Phones > Phone Settings > Services**.

**Note**

In a two-node Finesses setup with two services configured, the agents must enter their credentials on both the primary and secondary Finesses services.

---

**Backup and Restore**

The Unified CCX backup and restore component also backs up and restores Finesses configurations and data.

Additional Language Support

For the list of languages that are supported by Finesse, see the Unified CCX Compatibility related information, located at:


If you want to use the Finesses 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:


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.


Call Manager-Based Call Recording Using Cisco MediaSense

Cisco Finesse in Unified CCX supports call recording using Cisco MediaSense. MediaSense is the media-capture platform for Cisco Unified Communications.

To use MediaSense, perform the following procedures:

1. Configure Cisco MediaSense with Unified CM, on page 412
2. Upload Cisco MediaSense Certificate to Unified CCX Server, on page 413
3. Upload MediaSense Recording License, on page 413
4. Configure MediaSense as a Recording Server, on page 414
5. Call Recording Through Workflow, on page 414
6. Configure MediaSense Search and Play Gadget, on page 415

Note

After performing all of the procedures, restart the Unified CCX server. In high availability deployment, restart both of the nodes.

Configure Cisco MediaSense with Unified CM

Upload Cisco MediaSense Certificate to Unified CCX Server

To establish connection with Cisco MediaSense securely, you must upload the Cisco MediaSense certificate to Unified CCX server.

Procedure

**Step 1**
Download the tomcat.pem certificate from the Cisco MediaSense server.

a) Sign in to Cisco Unified Operating System Administration on the Cisco MediaSense host (https://host or IP address/cmplatform/showHome.do, where host or IP address is the hostname or IP address of the Cisco MediaSense server).

b) Select **Security > Certificate Management**.

The **Certificate List** screen appears.

c) Click **Find**.

A list of certificates appears.

d) In the **Common Name** column, click the link of the certificate you want to download.

   **Note**  
   The Certificate Name must be tomcat-trust and the Certificate Type must be trusts-cert. The Certificate Details pop-up window appears.

e) Click **Download .PEM File**.

A pop-up window appears.

f) Select **Save File** radio button and Click **OK**.

The file gets saved on your system.

**Step 2**
Upload the certificate to the designated Unified CCX server.

a) Sign in to Cisco Unified Operating System Administration on the primary Unified CCX node (http://host or IP address/cmplatform, where host or IP address is the hostname or IP address of the Unified CCX node).

b) Choose **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**.


Upload MediaSense Recording License

To use the MediaSense recording feature, you must purchase the Unified CCX recording license and upload it to the Unified CCX server.
For information about how to upload the license, see Upload Licenses.

Related Topics
Upload Licenses, on page 10

Configure MediaSense as a Recording Server

For information about configuring MediaSense as a recording server, see Recording Configuration.

Related Topics
Recording Configuration, on page 266

Call Recording Through Workflow

Use the HTTP Request action to invoke the Finesse Recording API after the call is answered.

Procedure

Step 1
Create an HTTP Request Recording action:

a) In the Manage Workflow Actions area, click New.
b) In the Name box, enter a name for the action.
c) From the Type drop-down list, select HTTP Request.
d) From the Handled By drop-down list, select Finesse Desktop.
e) From the Method drop-down list, select PUT.
f) From the Location drop-down list, select Finesse.
g) In the Content Type box, enter application/xml.
h) In the URL box, enter the following:
   
   /finesse/api/Dialog/

i) Click the tag icon at the right of the box and select dialogId to add it to the URL.
j) In the Body box, enter the following:

   <Dialog>
   <requestedAction>START_RECORDING</requestedAction>
   <targetMediaAddress>extension</targetMediaAddress>
   </Dialog>

To add the extension, click the tag icon and select extension.

Example:
Step 2  Click Save to save workflow action.

Step 3  Add a Call Answered Workflow that executes the HTTP Request Recording action that you created in the previous step.

**Note**  The Call Answered Workflow can be used to trigger an HTTP Request Recording action for inbound calls, agent-initiated outbound calls, and Predictive, Progressive, and Direct Preview outbound calls.

Step 4  Assign the workflow to the teams that you would like to record.

---

**Configure MediaSense Search and Play Gadget**

**Before you begin**

In the MediaSense server, you must have already configured Unified CM, Cisco Finesse, and MediaSense API.

**Procedure**

Step 1  Sign in to the Cisco Finesse administration console.

Step 2  Click the Desktop Layout tab.

Step 3  Find the MediaSense tab and gadget in the layout XML. Update the layout according to the comments in the layout.

```xml
<Dialog>
  <requestedAction>START_RECORDING</requestedAction>
  <targetMediaAddress>extension</targetMediaAddress>
</Dialog>
```

The following Tab and Gadget are for MediaSense. They are *ONLY* supported with MediaSense.

If you are not using MediaSense, then remove them. If you are using MediaSense and wish to show Recording Management, then do the following:

1) Remove these comments leaving the tab and gadget
2) Replace all instances of "my-mediasense-server" with the Fully Qualified Domain...
Name of your MediaSense Server.

IMPORTANT NOTE:
- In order for this Gadget to work, you must have performed all documented prerequisite steps.

```xml
<tab>
  <id>manageRecordings</id>
  <label>finesse.container.tabs.supervisor.manageRecordingsLabel</label>
  <gadgets>
    <gadget>https://my-mediasense-server:8440/ora/gadget/MediaSenseGadget.xml</gadget>
  </gadgets>
</tab>
```

Replace all instances of `my-mediasense-server` with `https://<Fully Qualified Domain Name of your MediaSense Server>/ora/gadget/MediaSenseGadget.xml`.

**Example:**
https://abcd-ef-gh102.abc.com:8440/ora/gadget/MediaSenseGadget.xml

**Step 4** Click Save.

**Note** The supervisor must log out and log in again to Cisco Finesse Supervisor Desktop to access MediaSense.

**Step 5** Sign in to Cisco Finesse desktop as a supervisor and confirm that MediaSense gadget is accessible.
Extend and Connect

Overview

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 more information about the Extend and Connect feature, see [https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/9_1_1/ccmfeat/CUCM_BK_C3E0EFA0_00_cucm-features-services-guide-91/CUCM_BK_C3E0EFA0_00_cucm-features-services-guide-91_chapter_0110010.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/9_1_1/ccmfeat/CUCM_BK_C3E0EFA0_00_cucm-features-services-guide-91/CUCM_BK_C3E0EFA0_00_cucm-features-services-guide-91_chapter_0110010.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.

**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**.


**Step 3** Install Cisco IM and Presence as a Call Manager subscriber.


**Step 4** Activate and start all the Cisco IM and Presence services in *Cisco Unified Serviceability*.


**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.


**Step 6** Create UC services for CTI and IM Presence services in Call Manager.

**Note** You must select CTI and IM Presence services.


**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.


**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 UserID that you want to set up and then choose Assign Selected Users.

Step 9
Set up the trunk in Call Manager.

Step 10
Add the route pattern in Call Manager to route the calls to the remote device.

Step 11
Configure the Presence Gateway configuration on IM and Presence.

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.
Cisco Unified CCX Serviceability

Access Cisco Unified CCX Serviceability

When you complete the AppAdmin initial 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 and Operations Guide for detailed instructions on initial AppAdmin setup and how to assign administrator capability to end users.

To access Cisco Unified CCX Serviceability:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>By using a supported web browser, open a browser session.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Go to https://&lt;server name or IP address&gt;/uccxservice/.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter an applicable username and password, and click Login.</td>
</tr>
</tbody>
</table>

**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.
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.


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 422
- Alarm Configuration Settings, on page 423

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 CCX Serviceability 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local Syslogs</strong></td>
<td></td>
</tr>
<tr>
<td>Enable Alarm</td>
<td>Use the check box next to Enable Alarm field to enable or disable the alarms for local syslog.</td>
</tr>
<tr>
<td>Alarm Event Level</td>
<td>Lists the alarm severity level.</td>
</tr>
<tr>
<td><strong>Remote Syslogs</strong></td>
<td></td>
</tr>
<tr>
<td>Enable Alarm</td>
<td>Use the check box next to Enable Alarm field to enable or disable the alarms for remote syslog.</td>
</tr>
<tr>
<td>Alarm Event Level</td>
<td>Lists the alarm severity level.</td>
</tr>
<tr>
<td>Server Name</td>
<td>IP address or host name of the Syslog server to which system should send the alarm messages. If you are using CiscoWorks, enter the IP address or the host name of the CiscoWorks server.</td>
</tr>
</tbody>
</table>

**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:
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Alarm for Local Syslogs</td>
<td>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 <em>Cisco Unified Real-Time Monitoring Tool Administration Guide for Cisco Unified Contact Center Express and Cisco Unified IP IVR.</em></td>
</tr>
<tr>
<td>Enable Alarm for Remote Syslogs</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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 Intelligence Center Services
- Cisco Unified CCX Socket.IO Service

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 15: Debug Levels for Different Unified CCX Subfacilities

<table>
<thead>
<tr>
<th>Cisco Unified CCX Components</th>
<th>Subfacilities or Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified CCX Administration</td>
<td>Libraries</td>
</tr>
<tr>
<td></td>
<td>Managers</td>
</tr>
<tr>
<td></td>
<td>Miscellaneous</td>
</tr>
<tr>
<td>Cisco Unified CCX Cluster View Daemon</td>
<td>Libraries</td>
</tr>
<tr>
<td></td>
<td>Managers</td>
</tr>
<tr>
<td></td>
<td>Miscellaneous</td>
</tr>
<tr>
<td>Cisco Unified CCX Editor</td>
<td>Libraries</td>
</tr>
<tr>
<td></td>
<td>Managers</td>
</tr>
<tr>
<td></td>
<td>Miscellaneous</td>
</tr>
<tr>
<td></td>
<td>Steps</td>
</tr>
<tr>
<td>Cisco Identity Service</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td>Debugging</td>
</tr>
<tr>
<td>Cisco Unified CCX Engine</td>
<td>Libraries</td>
</tr>
<tr>
<td></td>
<td>Managers</td>
</tr>
<tr>
<td></td>
<td>Miscellaneous</td>
</tr>
<tr>
<td></td>
<td>Steps</td>
</tr>
<tr>
<td>Cisco Unified CM Telephony Client or JTAPI Debug Levels</td>
<td>Subsystems</td>
</tr>
</tbody>
</table>
## Configure Trace Parameters

### Cisco Unified CCX Components

<table>
<thead>
<tr>
<th>Subfacilities or Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning</td>
</tr>
<tr>
<td>Information</td>
</tr>
<tr>
<td>Debugging</td>
</tr>
</tbody>
</table>

### Cisco Unified CCX Socket.IO Service

<table>
<thead>
<tr>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
</tr>
<tr>
<td>DataProcessing</td>
</tr>
<tr>
<td>Communication</td>
</tr>
</tbody>
</table>

### Cisco Unified Intelligence Center Services

<table>
<thead>
<tr>
<th>Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUIC</td>
</tr>
<tr>
<td>CUIC MODEL OBJECTS</td>
</tr>
<tr>
<td>CUIC SECURITY</td>
</tr>
<tr>
<td>CUIC JSP</td>
</tr>
<tr>
<td>CUIC DISPLAY</td>
</tr>
<tr>
<td>CUIC REALTIME</td>
</tr>
<tr>
<td>CUIC DATA PROCESSING</td>
</tr>
</tbody>
</table>

### Note

By default, the Cisco Unified Intelligence Center service is not activated. To use this service, see *Cisco Unified Contact Center Express Administration and Operations Guide*, available at: https://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html.

### 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.
### 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum No. of Files</td>
<td>The maximum number of trace files to be retained by the system.</td>
</tr>
<tr>
<td></td>
<td>This field specifies the total number of trace files for a given service.</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified CCX Serviceability automatically appends a sequence number to</td>
</tr>
<tr>
<td></td>
<td>the file name to indicate which file it is; for example, Cisco001MADM14.log.</td>
</tr>
<tr>
<td></td>
<td>When the last file in the sequence is full, the trace data begins writing</td>
</tr>
<tr>
<td></td>
<td>over the first file. The default value varies by service.</td>
</tr>
<tr>
<td>Maximum File Size</td>
<td>This field specifies the maximum size of the trace file in kilobytes or</td>
</tr>
<tr>
<td></td>
<td>megabytes depending on the selected service. The default value varies by</td>
</tr>
<tr>
<td></td>
<td>service.</td>
</tr>
</tbody>
</table>

**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.

**Note** You will not be able to save the Trace configuration if Cisco Unified Intelligence Center service on the publisher node is down.

**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 433
Table 16: Trace File Subfacilities

<table>
<thead>
<tr>
<th>Component Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC_CLUSTER</td>
<td>Archive Cluster Component</td>
</tr>
<tr>
<td>AC_CONFIG</td>
<td>Archive Configuration Component</td>
</tr>
<tr>
<td>AC_DATABASE</td>
<td>Archive Database Component</td>
</tr>
<tr>
<td>AC_JTAPI</td>
<td>JTAPI Archive Component</td>
</tr>
<tr>
<td>AC_OS</td>
<td>Archive Operating System Component</td>
</tr>
<tr>
<td>ADM</td>
<td>Administration Client</td>
</tr>
<tr>
<td>ADM_CFG</td>
<td>Administration Configuration</td>
</tr>
<tr>
<td>APP_MGR</td>
<td>Applications Manager</td>
</tr>
<tr>
<td>ARCHIVE_MGR</td>
<td>Archive Manager</td>
</tr>
<tr>
<td>AW_CFG</td>
<td>Restore Administration Configuration</td>
</tr>
<tr>
<td>BARBI_CLI</td>
<td>Backup and Restore Client Interface</td>
</tr>
<tr>
<td>BOOTSTRAP_MGR</td>
<td>Cisco Unified CCX Bootstrap Manager</td>
</tr>
<tr>
<td>CFG_MGR</td>
<td>Configuration Manager</td>
</tr>
<tr>
<td>CHANNEL_MGR</td>
<td>Channel Manager</td>
</tr>
<tr>
<td>CLUSTER_MGR</td>
<td>Cluster Manager</td>
</tr>
<tr>
<td>CONTACT_MGR</td>
<td>Contact Manager</td>
</tr>
<tr>
<td>CONTACT_STEPS</td>
<td>Contact Steps</td>
</tr>
<tr>
<td>CRA_CMM</td>
<td>Cisco Unified CCX ClusterMsgMgr Component</td>
</tr>
<tr>
<td>CONTEXT_SERVICE</td>
<td>Context Service</td>
</tr>
<tr>
<td>CRA_HRDM</td>
<td>Cisco Unified CCX Historical Reporting Data Manager</td>
</tr>
<tr>
<td>CVD</td>
<td>Cluster View Daemon</td>
</tr>
<tr>
<td>DB</td>
<td>Database</td>
</tr>
<tr>
<td>DBPURGE_MGR</td>
<td>Database Purge Manager</td>
</tr>
<tr>
<td>DESKTOP</td>
<td>Cisco Unified CCX Editor Desktop</td>
</tr>
<tr>
<td>DOC_MGR</td>
<td>Document Manager</td>
</tr>
<tr>
<td>EDT</td>
<td>Cisco Unified CCX Editor general</td>
</tr>
<tr>
<td>Component Code</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>ENG</td>
<td>Cisco Unified CCX Engine</td>
</tr>
<tr>
<td>EXECUTOR_MGR</td>
<td>Executor Manager</td>
</tr>
<tr>
<td>EXPR_MGR</td>
<td>Expression Manager</td>
</tr>
<tr>
<td>FILE_MGR</td>
<td>File Manager</td>
</tr>
<tr>
<td>GENERIC</td>
<td>Generic catalog for a facility</td>
</tr>
<tr>
<td>GRAMMAR_MGR</td>
<td>Grammar Manager</td>
</tr>
<tr>
<td>GRP_CFG</td>
<td>Group Configuration</td>
</tr>
<tr>
<td>HOLIDAY_MGR</td>
<td>Holiday Manager</td>
</tr>
<tr>
<td>HR_MGR</td>
<td>Historical Reports Manager</td>
</tr>
<tr>
<td>ICD_CTI</td>
<td>Cisco Unified CCX CTI Server</td>
</tr>
<tr>
<td>ICD_HDM</td>
<td>IPCC Express Historical Data Manager</td>
</tr>
<tr>
<td>ICD_RTDM</td>
<td>Cisco Unified CCX ICD Real-Time Data Manager</td>
</tr>
<tr>
<td>IVR_RTDM</td>
<td>Cisco Unified CCX IP IVR Real-Time Data Manager</td>
</tr>
<tr>
<td>IO_ICM</td>
<td>Cisco Unified ICME Input/Output</td>
</tr>
<tr>
<td>JASMIN</td>
<td>Java Signaling and Monitoring Interface</td>
</tr>
<tr>
<td>LIB_APPADMININTERCEPTOR</td>
<td>Cisco Unified CCX Administration Interceptor Library</td>
</tr>
<tr>
<td>LIB_AXL</td>
<td>AXL Library</td>
</tr>
<tr>
<td>LIB_CFG</td>
<td>Configuration Library</td>
</tr>
<tr>
<td>LIB_CLUSTER_CFG</td>
<td>Configuration Library for the cluster</td>
</tr>
<tr>
<td>LIB_CRTP</td>
<td>CRTP Library</td>
</tr>
<tr>
<td>LIB_DATABASE</td>
<td>Database Library</td>
</tr>
<tr>
<td>LIB_DIRECTORY</td>
<td>Directory Access Library</td>
</tr>
<tr>
<td>LIB_EVENT</td>
<td>Event Message Library</td>
</tr>
<tr>
<td>LIB_ICM</td>
<td>Cisco Unified ICME Library</td>
</tr>
<tr>
<td>LIB_JASPER</td>
<td>Jasper Tomcat Library</td>
</tr>
<tr>
<td>LIB_JCUP</td>
<td>JavaCup Library to parse expressions</td>
</tr>
<tr>
<td>LIB_JDBC</td>
<td>JDBC Library</td>
</tr>
<tr>
<td>Component Code</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>LIB_JINI</td>
<td>JINI Services</td>
</tr>
<tr>
<td>LIB_JMAIL</td>
<td>Java Mail Library</td>
</tr>
<tr>
<td>LIB_JLEX</td>
<td>JLEX Library used to parse expressions</td>
</tr>
<tr>
<td>LIB_LICENSE</td>
<td>License Library</td>
</tr>
<tr>
<td>LIB_MEDIA</td>
<td>Media Library</td>
</tr>
<tr>
<td>LIB_RMI</td>
<td>Java Remote Method Invocation Library</td>
</tr>
<tr>
<td>LIB_SERVLET</td>
<td>Servlet Library</td>
</tr>
<tr>
<td>LIB_TC</td>
<td>Tomcat Library</td>
</tr>
<tr>
<td>LOG_MGR</td>
<td>Log Manager</td>
</tr>
<tr>
<td>MRCP_CFG</td>
<td>MRCP Configuration</td>
</tr>
<tr>
<td>MGR_MGR</td>
<td>Manager Manager</td>
</tr>
<tr>
<td>NODE_MGR</td>
<td>Node Manager</td>
</tr>
<tr>
<td>PALETTE</td>
<td>Editor Palette</td>
</tr>
<tr>
<td>PROMPT_MGR</td>
<td>Prompt Manager</td>
</tr>
<tr>
<td>PURGING</td>
<td>Purging</td>
</tr>
<tr>
<td>RPT</td>
<td>Reporting</td>
</tr>
<tr>
<td>RTPPORT_MGR</td>
<td>RTP Manager</td>
</tr>
<tr>
<td>SCRIPT_MGR</td>
<td>Script Manager</td>
</tr>
<tr>
<td>SESSION_MGR</td>
<td>Session Manager</td>
</tr>
<tr>
<td>SIP_STACK</td>
<td>SIP Stack logging</td>
</tr>
<tr>
<td>SOCKET_MGR</td>
<td>Socket Manager</td>
</tr>
<tr>
<td>SS_APP</td>
<td>Application Subsystem</td>
</tr>
<tr>
<td>SS_CHAT</td>
<td>Chat Subsystem</td>
</tr>
<tr>
<td>SS_CM</td>
<td>Contact Manager Subsystem</td>
</tr>
<tr>
<td>SS_CMT</td>
<td>Cisco Media Termination Subsystem</td>
</tr>
<tr>
<td>SS_DB</td>
<td>Database Subsystem</td>
</tr>
<tr>
<td>SS_EMAIL</td>
<td>Email Subsystem</td>
</tr>
<tr>
<td>SS_HTTP</td>
<td>HTTP Subsystem</td>
</tr>
<tr>
<td>Component Code</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SS_ICM</td>
<td>Cisco Unified ICME Subsystem</td>
</tr>
<tr>
<td>SS_MRCP_ASR</td>
<td>MRCP ASR Subsystem</td>
</tr>
<tr>
<td>SS_MRCP_TTS</td>
<td>MRCP TTS Subsystem</td>
</tr>
<tr>
<td>SS_OUTBOUND</td>
<td>Outbound Dialer Express Subsystem (uses MIVR log file)</td>
</tr>
<tr>
<td>SS_RM</td>
<td>Resource Manager Subsystem</td>
</tr>
<tr>
<td>SS_RMCM</td>
<td>Resource Manager Contact Manager Subsystem</td>
</tr>
<tr>
<td>SS_ROUTEANDQUEUE</td>
<td>Route and Queue Subsystem</td>
</tr>
<tr>
<td>SS_RTR</td>
<td>Real-Time Reporting Subsystem</td>
</tr>
<tr>
<td>SS_SIP</td>
<td>SIP Subsystem</td>
</tr>
<tr>
<td>SS_TEL</td>
<td>JTAPI Subsystem (Telephony)</td>
</tr>
<tr>
<td>STEP_CALL_CONTROL</td>
<td>Call Control Steps</td>
</tr>
<tr>
<td>STEP_CONTEXT_SERVICE</td>
<td>Context Service Steps</td>
</tr>
<tr>
<td>STEP_MEDIA_CONTROL</td>
<td>Media Control Steps</td>
</tr>
<tr>
<td>STEP_SESSION</td>
<td>Sessions Steps</td>
</tr>
<tr>
<td>STEP_SESSION_MGMT</td>
<td>Session Management Steps</td>
</tr>
<tr>
<td>STEP_USER</td>
<td>User Steps</td>
</tr>
<tr>
<td>STEP_CALL_CONTACT</td>
<td>Call Contact Steps</td>
</tr>
<tr>
<td>STEPS_CONTACT</td>
<td>Contact Steps</td>
</tr>
<tr>
<td>STEPS_DB</td>
<td>Database Steps</td>
</tr>
<tr>
<td>STEPS_DOCUMENT</td>
<td>Document Steps</td>
</tr>
<tr>
<td>STEPS_EMAIL</td>
<td>E-mail Steps</td>
</tr>
<tr>
<td>STEPSGENERAL</td>
<td>General Steps</td>
</tr>
<tr>
<td>STEPS_GRAMMAR</td>
<td>Grammar Steps</td>
</tr>
<tr>
<td>STEPS_HTTP</td>
<td>HTTP Steps</td>
</tr>
<tr>
<td>STEPS_ICM</td>
<td>Cisco Unified ICME Steps</td>
</tr>
<tr>
<td>STEPS_IPCC_EXP</td>
<td>Cisco Unified CCX Steps</td>
</tr>
<tr>
<td>STEPS_JAVA</td>
<td>Java Steps</td>
</tr>
<tr>
<td>Component Code</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>STEPS_PROMPT</td>
<td>Prompt Steps</td>
</tr>
<tr>
<td>STEPS_SESSION</td>
<td>Session Steps</td>
</tr>
<tr>
<td>UCCX_WEB SERVICES</td>
<td>Chat Subsystem</td>
</tr>
<tr>
<td>USR_MGR</td>
<td>User Manager</td>
</tr>
<tr>
<td>WEB STEPS</td>
<td>HTTP Contact Steps</td>
</tr>
</tbody>
</table>

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_RMC.M.

**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 CCX Serviceability 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 17: System Log Profiles**

<table>
<thead>
<tr>
<th>Name</th>
<th>Scenario in which this profile must be activated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Activate this profile once an issue is resolved.</td>
</tr>
<tr>
<td>Outbound</td>
<td>For issues with Unified CCX Outbound Dialer AppAdmin.</td>
</tr>
<tr>
<td>AppAdmin</td>
<td>For issues with web administration through AppAdmin, Unified CCX Serviceability, and other web pages.</td>
</tr>
<tr>
<td>Media</td>
<td>For issues with media setup or media transmission.</td>
</tr>
<tr>
<td>HRDM ( Historical Reporting Data Manager)</td>
<td>For issues with historical data that is written to the database.</td>
</tr>
<tr>
<td>StuckSession</td>
<td>For issues with application sessions, sessions that are not being deleted when appropriate and appearing stuck in AppAdmin Real Time Reports.</td>
</tr>
<tr>
<td>Database</td>
<td>For issues with Unified CCX Informix database.</td>
</tr>
<tr>
<td>EDBS (Enterprise Database Subsystem)</td>
<td>For issues with external database connectivity and integration.</td>
</tr>
<tr>
<td>CallsStuckInQueue</td>
<td>For issues with calls in queue that are not being allocated to available agents or appearing stuck in queue in reports.</td>
</tr>
<tr>
<td>Serviceability</td>
<td>For issues with the functionality in Unified CCX Serviceability Administration Interface.</td>
</tr>
<tr>
<td>RealTimeDataProblems</td>
<td>For issues with Real Time Reports in AppAdmin.</td>
</tr>
</tbody>
</table>

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.
Create Profile

To create a log profile for a specific trace, perform the following steps:

**Procedure**

**Step 1**  
From the Unified CCX Serviceability 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 438
- Enable Profile, on page 436
- Save Current Trace Settings, on page 437

Save as Another Profile

To save an existing profile as another profile, perform the following steps:
Procedure

Step 1  From the Unified CCX Serviceability 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 438
- Enable Profile, on page 436
- Save Current Trace Settings, on page 437

Enable Profile

To enable or activate a log profile, perform the following steps:

Procedure

Step 1  From the Unified CCX Serviceability 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 435
- Update Profile, on page 438

Delete Profile

To delete an existing log profile, perform the following steps:
**Procedure**

**Step 1**
From the Unified CCX Serviceability 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 438
- **Enable Profile**, on page 436

**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 CCX Serviceability 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 438
- **Enable Profile**, on page 436
Upload Profile

To upload a log profile, perform the following steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the Unified CCX Serviceability menu bar, choose Trace &gt; Profile. The Log Profiles Management web page displays.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>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.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Upload to upload the profile.</td>
</tr>
<tr>
<td>Step 4</td>
<td>You should be able to view the uploaded profile along with the existing profiles in the Log Profiles Management web page.</td>
</tr>
</tbody>
</table>

**Related Topics**

- [Update Profile](#), on page 438
- [Enable Profile](#), on page 436
- [Save Current Trace Settings](#), on page 437

Update Profile

You can update only custom log profiles. To view and update an existing log profile, perform the following steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the Unified CCX Serviceability menu bar, choose Trace &gt; Profile. The Log Profiles Management web page displays.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>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.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click MIVR, MCVD, and MADM tabs to view and modify the trace settings.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Save to save the updated profile settings or <strong>Save and Enable</strong> 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.</td>
</tr>
</tbody>
</table>

**Related Topics**

- [Create Profile](#), on page 435
- [Upload Profile](#), on page 438
- [Enable Profile](#), on page 436
- [Save Current Trace Settings](#), on page 437
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 CCX Serviceability 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 Contact Center Express Serviceability Administration Guide available at: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.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 440
• DB Services, on page 441

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

---

**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 CCX Serviceability menu bar.

**Step 2**
From the **Server** drop-down list box, choose the server 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 through the Command Line Interface (CLI). For a list of services that you can start and stop through 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 9.0(1) 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 443
- **Datastores**, on page 444

The following table describes the datastores available and what they contain.

<table>
<thead>
<tr>
<th>Datastore Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Historical</td>
<td>This datastore contains Historical Report data.</td>
</tr>
<tr>
<td>Repository</td>
<td>This datastore contains user prompts tables, grammar tables, and document tables.</td>
</tr>
<tr>
<td>Configuration</td>
<td>This datastore contains Unified CCX system configuration information.</td>
</tr>
</tbody>
</table>

### 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 CCX Serviceability menu bar.

The Replication Servers web page opens displaying the list of servers and the following fields in a High Availability deployment:

<table>
<thead>
<tr>
<th>Datastore Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Host name of the server.</td>
</tr>
<tr>
<td>Node ID</td>
<td>Node ID of the server in the Unified CCX cluster.</td>
</tr>
<tr>
<td>State</td>
<td>The current connectivity status of the node in the replication network, which can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td><strong>DROPPED/TIMED OUT</strong></td>
</tr>
<tr>
<td></td>
<td>The server cannot be reached and is not available in the replicated network.</td>
</tr>
<tr>
<td></td>
<td><strong>ACTIVE/CONNECTED</strong></td>
</tr>
<tr>
<td></td>
<td>The server is connected in the replication network and sends or receives updates.</td>
</tr>
<tr>
<td>Job Status</td>
<td>The current state of this database.</td>
</tr>
<tr>
<td>Last Changed</td>
<td>The time the connection state was last changed.</td>
</tr>
</tbody>
</table>

**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 444
- Datastore Replication Status, on page 443

**Datastores**

**Procedure**

**Step 1** Choose **Tools > Datastore Control Center**.
Step 2 Click **Datastores** from the Unified CCX Serviceability 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 443
- [Datastore Replication Status](#), on page 443
- [Datastore Control Center contents](#), on page 445

**Datastore Control Center contents**

The following table describes the Datastore Control Center contents common to all the Unified CCX datastores.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server machine name.</td>
</tr>
<tr>
<td>Replication Type</td>
<td>One of the following Enterprise Replication (ER) values in a High Availability deployment:</td>
</tr>
<tr>
<td></td>
<td>• ER—Publication</td>
</tr>
<tr>
<td></td>
<td>• ER—Subscription</td>
</tr>
<tr>
<td>Node ID</td>
<td>Node ID of server/node in Unified CCX cluster.</td>
</tr>
<tr>
<td>Read Access</td>
<td>Indicates whether data can be read from the datastore. Options: Yes, No.</td>
</tr>
<tr>
<td>Write Access</td>
<td>Indicates whether data can be written to the datastore. Options: Yes, No.</td>
</tr>
<tr>
<td>Replicate Status</td>
<td>Can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td><strong>RUNNING</strong></td>
</tr>
<tr>
<td></td>
<td>All the necessary database services are up and the datastore is functioning as expected.</td>
</tr>
<tr>
<td></td>
<td><strong>RETRYING</strong></td>
</tr>
<tr>
<td></td>
<td>The datastore is in partial service and might be in the state of restart.</td>
</tr>
<tr>
<td></td>
<td><strong>SHUTDOWN</strong></td>
</tr>
<tr>
<td></td>
<td>The datastore is shutdown.</td>
</tr>
<tr>
<td></td>
<td><strong>UNKNOWN</strong></td>
</tr>
<tr>
<td></td>
<td>Unable to determine the current status of the datastore. This value is shown in a single-node deployment only.</td>
</tr>
<tr>
<td>Last Update Time</td>
<td>Indicates the last action the replication agent was performing.</td>
</tr>
<tr>
<td>Info</td>
<td>Use these icons to view further information in a new window:</td>
</tr>
<tr>
<td></td>
<td><strong>Check Details</strong></td>
</tr>
<tr>
<td></td>
<td>Click this icon to view information about data synchronization or repair jobs that might have been initiated.</td>
</tr>
<tr>
<td></td>
<td><strong>History</strong></td>
</tr>
<tr>
<td></td>
<td>Click this icon to view information about the replication latency (the time it takes to replicate transactions).</td>
</tr>
</tbody>
</table>
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 CCX Serviceability 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.
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 CCX Serviceability 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.

---

**Context Service Status**

The **Context Service Status** web page from the **Tools** menu in the Cisco Unified CCX Serviceability displays the status of Context Service for all the listed components of the Unified CCX solution.

The Context Service parameters for all the components like, Finesse, SocialMiner, Unified CCX, and Fusion Management Connector (FMC) are displayed.

The following parameters are displayed with their respective values for a particular **Component:Host Name**.

**Table 18: Context Service Parameters**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>The state of the component is displayed. The state can be, <strong>Registered</strong> or <strong>Not Registered</strong> or <strong>Unknown</strong> or <strong>Stopped</strong> for Context Service.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the component is displayed. The status can be, <strong>Online</strong> or <strong>Offline</strong> or <strong>Unknown</strong> or <strong>No Connectivity</strong> or <strong>Ready to Register</strong>.</td>
</tr>
<tr>
<td>Mode</td>
<td>This displays whether the component is connected to the Context Service in Lab mode or in Production mode. <strong>Note</strong> This parameter is not applicable for Fusion Management Connector.</td>
</tr>
<tr>
<td>Last Fetched At</td>
<td>The time stamp when the last connectivity status is identified.</td>
</tr>
<tr>
<td>Action</td>
<td>This provides an option, <strong>Initialize</strong>, to reinitialize the Context Service connector of Unified CCX component that is in <strong>Stopped</strong> state.</td>
</tr>
<tr>
<td>Static SDK Version</td>
<td>The static SDK library version used by the component to connect to the Context Service is displayed.</td>
</tr>
<tr>
<td>Extension SDK Version</td>
<td>The dynamic SDK library version used by the component to connect to the Context Service is displayed.</td>
</tr>
<tr>
<td>Proxy</td>
<td>This displays the HTTP proxy configured in Unified CCX for the connectivity to Context Service.</td>
</tr>
</tbody>
</table>

The possible scenarios for the parameter values are:

- When the state of the component is **Registered** the status can be **Online**, **Offline**, or **No Connectivity**.
- When the state of the component is **Not Registered** the status can be **Offline**, **Ready to Register**, or **No Connectivity**.
- When the state of the component is **Unknown** the status also is **Unknown**.
When the status is **Online** it indicates that the connectivity of the component with Context Service is successful. When the status is **Offline** it indicates that one or more critical services of Context Service is not working or there is an issue with network connectivity.

For troubleshooting purpose, you may click **Export** to download the data required for troubleshooting that can be shared with Cisco Support.
Real-Time Monitoring

The Cisco Unified Real-Time Monitoring Tool (RTMT), which runs as a client-side application, uses HTTPS and TCP to monitor system performance. Unified RTMT can connect directly to devices through HTTPS to troubleshoot system problems.

Unified RTMT allows you to perform the following tasks:

- Monitor a set of predefined management objects that monitor the health of the system.
- Generate alerts in the form of email messages, for objects when values go above or below user-configured thresholds.
- Collect and view traces in default viewers that exist in RTMT.
- View syslog messages in SysLog Viewer.
- Work with performance-monitoring counters.

Even when Unified RTMT is not running as an application on your desktop, tasks such as alarm and performance monitoring updates continue to take place on the server in the background.

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:

Performance Monitoring

Unified CCX provides performance counters (called perfmon counters) for application performance monitoring. The perfmon counters help expose various performance values and enable 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:


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

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.

## 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 well as event (alarms) notifications.

### Unified CCX Alerts

The following list contains preconfigured Unified CCX alerts:

**Table 19:**

<table>
<thead>
<tr>
<th>Alert Name</th>
<th>Syslog Alarm Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>DB CRA % Space Used</td>
<td>The percentage of used space in the Unified CCX database, db_cra. The database, db_cra, contains the Unified CCX historical and configuration data.</td>
<td></td>
</tr>
<tr>
<td>DBReplicationStopped</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>HistoricalDataWrittenToFiles</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Intelligence Center</td>
<td>This alert occurs when the Intelligence Center event gets generated. This indicates the system detected critical error with database.</td>
<td></td>
</tr>
<tr>
<td>Intelligence Center</td>
<td>This alert occurs when the Intelligence Center event gets generated. This indicates the Database replication failed.</td>
<td></td>
</tr>
<tr>
<td>Alert Description</td>
<td>Event Code</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Intelligence Center CUIC_REPORT_EXECUTION_FAILED</td>
<td>CUIC_REPORT_EXECUTION_FAILED</td>
<td>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.</td>
</tr>
<tr>
<td>Intelligence Center CUIC_UNRECOVERABLE_ERROR</td>
<td>CUIC_UNRECOVERABLE_ERROR</td>
<td>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.</td>
</tr>
<tr>
<td>CCXToCUICAadminSyncFailed</td>
<td>UCCX_TO_CUIC_SYNC_FAILED</td>
<td>This alert occurs when the Unified CCX has failed to notify CUIC on any resource change.</td>
</tr>
<tr>
<td>CCXToCUICCVDSyncFailed</td>
<td>UCCX_TO_CUIC_SYNC_FAILED</td>
<td>This alert occurs when the Unified CCX has failed to notify CUIC on any resource change.</td>
</tr>
<tr>
<td>CCXToCUICEngineSyncFailed</td>
<td>UCCX_TO_CUIC_SYNC_FAILED</td>
<td>This alert occurs when the Unified CCX has failed to notify CUIC on any resource change.</td>
</tr>
<tr>
<td>Alert Description</td>
<td>Alert Code</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MediasenseStatusDown</td>
<td>MEDIASENSE_STATUS_DOWN</td>
<td>One or more Mediasense nodes configured with this CCX are down or unreachable. This will impact CUCM-based call recording and CCX subscriptions to Mediasense for recording events.</td>
</tr>
<tr>
<td>PurgeInvoked</td>
<td>AUTO_PURGE_COMPLETE</td>
<td>This alert occurs when the Unified CCX Auto Purging has completed.</td>
</tr>
<tr>
<td>UnifiedCCXEngineMemoryUsageHigh</td>
<td>UnifiedCCXEngineMemoryUsageHigh</td>
<td>This alert occurs when the percentage of JVM heap memory used by Cisco Unified CCX Engine process is greater than the configured threshold value.</td>
</tr>
<tr>
<td>EMAIL_SERVER_DOWN</td>
<td>EMAIL_SERVER_DOWN</td>
<td>This alert occurs when the email server is not reachable.</td>
</tr>
<tr>
<td>SocialMinerTomcatServiceDown</td>
<td>SS_PARTIAL_SERVICE_SOCIALMINER_TOMCAT_DOWN</td>
<td>This alert occurs when SocialMiner Tomcat is not reachable.</td>
</tr>
<tr>
<td>SOCIALMINER_XMPP_ServiceDown</td>
<td>SOCIALMINER_XMPP_SERVICE_DOWN</td>
<td>This alert occurs when the Unified CCX has failed to contact SocialMiner runtime server (XMPP).</td>
</tr>
<tr>
<td>ContextServiceInitializationFailed</td>
<td>CONTEXT_SERVICE_INITIALIZATION_FAILED</td>
<td>Context Service failed to initialize.</td>
</tr>
<tr>
<td>ContextServiceFMCPushURLFailed</td>
<td>ContextServiceFMCPushURLFailed</td>
<td>Push URL Registration with Fusion Management Connector Failed.</td>
</tr>
<tr>
<td>Alert Type</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>ContextServiceClientConfigReloadFailed</td>
<td>Reloading the Context Service Client Config Failed.</td>
<td></td>
</tr>
<tr>
<td>ContextServiceInitParamsFailed</td>
<td>Error occurred while reading the Context Service/System Params Config values.</td>
<td></td>
</tr>
<tr>
<td>ContextServiceFMCNotificationRetry</td>
<td>Retrying the Fusion Management Connector Context Service notification.</td>
<td></td>
</tr>
<tr>
<td>ContextServiceSMNotificationRetry</td>
<td>Retrying Social Miner Context Service notification.</td>
<td></td>
</tr>
<tr>
<td>ContextServiceIntegrationFilterError</td>
<td>Context Service FilterStatus from SM is FILTER_EXECUTION_ERROR.</td>
<td></td>
</tr>
<tr>
<td>ContextServiceStepsExecutionIssue</td>
<td>Issue in Context Service Steps Execution.</td>
<td></td>
</tr>
<tr>
<td>OutboundScheduledContactImportFailed</td>
<td>Scheduled import of outbound contacts failed.</td>
<td></td>
</tr>
<tr>
<td>OutboundContactImportSchedulingFailed</td>
<td>Scheduling of outbound import contact failed.</td>
<td></td>
</tr>
<tr>
<td>UserPasswordMismatchAcrossNodes</td>
<td>One or more user passwords are not same across both the nodes.</td>
<td></td>
</tr>
</tbody>
</table>
Reason Codes Sync from Finesse failed and reached to Maximum number of retries. Ensure that Finesse service and Unified CCX database are active.

<table>
<thead>
<tr>
<th>Reason Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>REASONCODE_SYNC_RETRY_ERROR</td>
<td>Reason Codes Sync from Finesse failed and reached to Maximum number of retries. Ensure that Finesse service and Unified CCX database are active.</td>
</tr>
</tbody>
</table>

SocialMinerSSL.Error | SS_PARTIAL_SERVICE_SOCIALMINER_SSL_ERROR |

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 20:**

<table>
<thead>
<tr>
<th>Alert Name</th>
<th>Syslog Alarm Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IdSInitializationFailure</td>
<td>IDS_INIT_ERROR</td>
<td>This alert occurs when an error is encountered during IdS initialization.</td>
</tr>
<tr>
<td>IDPMetaDataLoadError</td>
<td>IDP_META_DATA_LOAD_ERROR</td>
<td>This alert occurs when the trust could not be established between IdS and IdP during initialization.</td>
</tr>
<tr>
<td>SPMetaDataLoadError</td>
<td>SP_META_DATA_LOAD_ERROR</td>
<td>This alert occurs when SAML SP metadata Initialization fails.</td>
</tr>
<tr>
<td>IDPMetaDataUpdateError</td>
<td>IDP_META_DATA_UPDATE_ERROR</td>
<td>This alert occurs when there is an error updating IdP metadata and propagating across the cluster.</td>
</tr>
<tr>
<td>SPMetaDataUpdateError</td>
<td>SP_META_DATA_UPDATE_ERROR</td>
<td>This alert occurs when SAML SP certificate regeneration fails.</td>
</tr>
<tr>
<td>TokenMetaDataUpdateError</td>
<td>TOKEN_META_DATA_UPDATE_ERROR</td>
<td>This alert occurs when TOKEN Keystore regeneration or update fails.</td>
</tr>
<tr>
<td>IdSSecurityConfigNotPresent</td>
<td>IDS_SECURITY_CONFIG_NOT_PRESENT</td>
<td>This alert occurs when some IdS security configuration files are not present on the secondary node.</td>
</tr>
</tbody>
</table>
This alert occurs when the security config could not be pulled from the primary IdS node.

SAML CertificateLoadFailed 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.

To view or edit values for any alert, right-click the alert and select Set Alert/Properties.

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:


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 21: Triggers Page Options*

<table>
<thead>
<tr>
<th>Counters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TriggerDN</td>
<td>This field displays the directory number that is associated with the trigger.</td>
</tr>
<tr>
<td>Trigger State</td>
<td>This field displays the state of the trigger, which can be In Service, Out of Service, or Unknown.</td>
</tr>
<tr>
<td>Application Name</td>
<td>This field displays the name of Unified CCX application that is associated with the trigger.</td>
</tr>
<tr>
<td>Ready for Call</td>
<td>This field indicates whether the trigger is ready to accept the call.</td>
</tr>
<tr>
<td>CallControlGroup ID</td>
<td>This field displays the ID of the call control group that is associated with the trigger.</td>
</tr>
<tr>
<td>Media Group ID</td>
<td>This field displays the ID of the media group that is associated with the trigger.</td>
</tr>
<tr>
<td>Last State Change Time</td>
<td>This field displays the time of last state change for the trigger.</td>
</tr>
<tr>
<td>Recommended Action</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 22: Call Control Groups Page Options*

<table>
<thead>
<tr>
<th>Counters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CallControlGroup ID</td>
<td>This field displays the ID that is associated with the call control group.</td>
</tr>
<tr>
<td>Group State</td>
<td>This field displays the state of the call control group, which can be In Service, Partial Service, or Out of Service.</td>
</tr>
</tbody>
</table>
**CTI Ports Page**

The CTI Ports page provides the following information about the current CTI ports that are configured for Unified CCX:

*Table 23: CTI Ports Page Options*

<table>
<thead>
<tr>
<th>Counters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTI Port DN</td>
<td>This field displays the directory number of the CTI port.</td>
</tr>
<tr>
<td>CallControlGroup ID</td>
<td>This field displays the ID of call control group to which the CTI port belongs.</td>
</tr>
<tr>
<td>Port State</td>
<td>This field displays the state of CTI port, which can be In Service or Out of Service.</td>
</tr>
<tr>
<td>CallID</td>
<td>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. <strong>Note</strong> This field is populated only if the port state is Out of Service.</td>
</tr>
<tr>
<td>Last State Change Time</td>
<td>This field displays the last time when the CTI port state changed.</td>
</tr>
</tbody>
</table>

**Summary Page**

The Summary page provides the following information:

*Table 24: Summary Page Options*

<table>
<thead>
<tr>
<th>Counters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Telephony Subsystem State</td>
<td>This field displays the state of the Unified CCX telephony subsystem, which can be In Service, Partial Service, or Out of Service.</td>
</tr>
<tr>
<td>Call Control Groups In Service</td>
<td>This field displays the number of call control groups that are in service.</td>
</tr>
<tr>
<td>Counters</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Call Control Groups Out Of Service</td>
<td>This field displays the number of call control groups that are out of service.</td>
</tr>
<tr>
<td>Call Control Groups In Partial Service</td>
<td>This field displays the number of call control groups that are in partial service.</td>
</tr>
<tr>
<td>Enabled Triggers</td>
<td>This field displays the number of triggers that are associated with valid call control group IDs.</td>
</tr>
<tr>
<td>Disabled Triggers</td>
<td>This field displays the number of triggers that are associated with invalid call control group IDs.</td>
</tr>
<tr>
<td>Triggers With Config Errors</td>
<td>This field displays the number of triggers with configuration errors.</td>
</tr>
</tbody>
</table>

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:

Backup and Restore

Cisco Disaster Recovery System (Cisco DRS), which you can access from Cisco Unified Contact Center Express Administration, provides complete data backup-and-restore capabilities for all servers in a Cisco Unified Contact Center Express (Unified CCX) cluster. Cisco DRS allows you to perform regularly scheduled automatic or user-invoked data backups and to restore data in the case of a system failure.

To access Cisco DRS, choose Disaster Recovery System from the navigation drop-down list box in the upper-right corner of the Cisco Unified CCX Administration window. Log in to the Disaster Recovery System using platform administrator credentials.

Cisco DRS will back up and restore the following components:

- Cluster configurations and applications profile in the data repository
- Workflow scripts that are already uploaded in the data repository
- Platform
- Databases (such as db_cra, db_cra_repository, and FCRasSvr database)
- Configuration data (such as open LDAP and flat files)
- Recording files
- JTAPI configuration (jtapi.ini)
- Trace Collection Tool (TCT)
- User prompts, grammars, and documents
- CUIC_CONFIG configuration (such as configuration property files, security configuration, and Unified Intelligence Center Tomcat server.xml)
- Finesse components
- Socket.IO Server Configuration Files

In the case of high availability (HA), Cisco DRS performs a cluster-level backup, which means that it collects backups for all servers in a Unified CCX cluster to a central location and archives the backup data to a remote SFTP server.

DRS will back up and restore its own settings, that is, backup device settings (saved in file drfDevice.xml) and schedule settings (saved in file drfSchedule.xml) as part of the platform component. Once a server is restored with these files, you do not need to reconfigure DRS backup device and schedule settings.
Cisco DRS uses 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 makes use of the IPSec certificates for its Public/Private Key encryption. Be aware that if you delete the IPSec truststore (hostname.pem) file from the Certificate Management pages, then Cisco DRS will not work as expected. If you delete the IPSec-trust file manually, then you must ensure that you upload the IPSec certificate to the IPSec-trust. For more details, see the certificate management help pages in the Cisco Unified Communications Manager Security Guide available here:


**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.

- 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.

**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:


For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to the following URL:

http://www.globalscape.com/gsftps/cisco.aspx

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.

---

Master Agent Duties

The Master Agent (MA) performs the following duties:
• Stores system-wide component registration information.

• Maintains a complete set of scheduled tasks in an XML file. The MA updates this file when it receives updates of schedules from the user interface. The MA sends executable tasks to the applicable Local Agents, as scheduled. Local Agents execute 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 executed schedules, 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.
**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**

**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:

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.

⚠️ 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 will prompt 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 need to 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.

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.

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 entire Unified 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.


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.
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.

- 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.

- 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 (Standard, Enhanced, Premium, IP IVR) as the license contained within the backup that was restored.


---

## 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.

### 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 > Licensing > Display License.

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 (Standard, Enhanced, Premium, IP IVR) as the license contained within the backup that was restored.


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.
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.


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/prodInstallationGuidesList.html.

Step 2 Restore only the first node by following the procedure in Restore Only First Node in HA Setup (with Rebuild), on page 470.
Note: To view the current license package, go to System > Licensing > Display License.

Step 3
Restart the first node.


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 (Standard, 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 CenterExpress available here: https://www.cisco.com/en/US/products/sw/custosw/ps1846/prod_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 471.

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/drLA0 *
• For the user interface, find the trace file at platform/drf/trace/drConfLib0 *
• For the JSch, find the trace file at platforms/drf/trace/drJSch *

You can view trace files by using the command line interface. For more information, see Command Line Interface, on page 473.

Command Line Interface
Cisco DRS also provides command-line access to few backup and restore tasks, as listed in the following table:
Table 25: Disaster Recovery System Command Line Interface Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>utils disaster_recovery backup</td>
<td>Starts a manual backup by using the feature that is configured in the Cisco DRS interface</td>
</tr>
<tr>
<td>utils disaster_recovery restore</td>
<td>Starts a restore and requires parameters for backup location, filename, feature, and nodes to restore</td>
</tr>
<tr>
<td>utils disaster_recovery status</td>
<td>Displays the status of ongoing backup or restore job</td>
</tr>
<tr>
<td>utils disaster_recovery history</td>
<td>Displays the history of previous backup and restore operations</td>
</tr>
<tr>
<td>utils disaster_recovery show_backupfiles</td>
<td>Displays existing backup files</td>
</tr>
<tr>
<td>utils disaster_recovery cancel_backup</td>
<td>Cancels an ongoing backup job</td>
</tr>
<tr>
<td>utils disaster_recovery show_registration</td>
<td>Displays the currently configured registration</td>
</tr>
<tr>
<td>utils disaster_recovery show_tapeid</td>
<td>Displays the tape identification information</td>
</tr>
<tr>
<td>utils disaster_recovery device add</td>
<td>Adds the network or tape device</td>
</tr>
<tr>
<td>utils disaster_recovery device delete</td>
<td>Deletes the device</td>
</tr>
<tr>
<td>utils disaster_recovery device list</td>
<td>Lists all the devices</td>
</tr>
<tr>
<td>utils disaster_recovery schedule add</td>
<td>Adds a schedule</td>
</tr>
<tr>
<td>utils disaster_recovery schedule delete</td>
<td>Deletes a schedule</td>
</tr>
<tr>
<td>utils disaster_recovery schedule disable</td>
<td>Disables a schedule</td>
</tr>
<tr>
<td>utils disaster_recovery schedule enable</td>
<td>Enables a schedule</td>
</tr>
<tr>
<td>utils disaster_recovery schedule list</td>
<td>Lists all the schedules</td>
</tr>
</tbody>
</table>

Alarms

Command Line Interface

Unified CCX provides a command line interface as an alternative to the web administration page to configure and troubleshoot the system.

- Command Line Interface Basics, on page 475
- Show commands, on page 478
- Set Commands, on page 497
- run Commands, on page 505
- Utils Commands, on page 508
- File Commands, on page 525
- High Availability Commands, on page 530
- Cisco Finesse Commands, on page 538
- Cisco Unified Intelligence Center Commands, on page 541

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

---

APPENDIX A

Command Line Interface

Unified CCX provides a command line interface as an alternative to the web administration page to configure and troubleshoot the system.

- Command Line Interface Basics, on page 475
- Show commands, on page 478
- Set Commands, on page 497
- run Commands, on page 505
- Utils Commands, on page 508
- File Commands, on page 525
- High Availability Commands, on page 530
- Cisco Finesse Commands, on page 538
- Cisco Unified Intelligence Center Commands, on page 541

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

---
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
```

```
```

**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 execute 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 executed as a part of Unified Communications Operating System. For detailed information about all the CLI commands available for the Cisco Unified Communications Operating System, see the Command Line Interface Reference Guide for Cisco Unified Communications Solutions available here:


The following Unified Communications Operating System commands are not applicable to Unified CCX:

- delete dscp
- file delete license
- file get license
- file list license
When the `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

#### 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**
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 and Operations Guide*.

Command syntax

```
show uccx license
```

Requirements

Level privilege: 0
Command privilege level: 0
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
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
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 command 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 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—Refersto 1.0 (TLS Version 1.0), 1.1 (TLS Version 1.1), and 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—Refersto 1.0 (TLS Version 1.0), 1.1 (TLS Version 1.1), and 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
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

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.
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 dbschema db_cra
Output is in file: uccx/cli/schema_db_cra_080212-110543.txt

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

<table>
<thead>
<tr>
<th>SNO.</th>
<th>DATABASE NAME</th>
<th>TOTAL SIZE (MB)</th>
<th>USED SIZE (MB)</th>
<th>FREE SIZE (MB)</th>
<th>PERCENT FREE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>rootdbs</td>
<td>358.4</td>
<td>66.3</td>
<td>292.1</td>
<td>81%</td>
</tr>
<tr>
<td>2</td>
<td>log_dbs</td>
<td>317.4</td>
<td>307.3</td>
<td>10.1</td>
<td>3%</td>
</tr>
<tr>
<td>3</td>
<td>db_cra</td>
<td>512.0</td>
<td>8.8</td>
<td>503.2</td>
<td>98%</td>
</tr>
<tr>
<td>4</td>
<td>db_hist</td>
<td>13000.0</td>
<td>3651.4</td>
<td>9348.6</td>
<td>71%</td>
</tr>
<tr>
<td>5</td>
<td>db_cra_repository</td>
<td>10.2</td>
<td>2.9</td>
<td>7.3</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>db_frascal</td>
<td>512.0</td>
<td>2.8</td>
<td>509.2</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>temp_uccx</td>
<td>1572.9</td>
<td>0.1</td>
<td>1572.7</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>uccx_sbspace</td>
<td>3145.7</td>
<td>2988.1</td>
<td>157.6</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>uccx_er</td>
<td>204.8</td>
<td>0.1</td>
<td>204.7</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>uccx_ersb</td>
<td>1572.9</td>
<td>1494.1</td>
<td>78.8</td>
<td></td>
</tr>
</tbody>
</table>

CHUNK NO. OFFSET TOTAL SIZE (MB) FREE SIZE (MB) FILENAME

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>358.4</td>
<td>292.1</td>
<td>/var/opt/cisco/uccx/db/root_uccx_dbs</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>317.4</td>
<td>10.1</td>
<td>/var/opt/cisco/uccx/db/log_dbs</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>512.0</td>
<td>503.2</td>
<td>/var/opt/cisco/uccx/db/db_cra_dbs</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>13000.0</td>
<td>9348.6</td>
<td>/common/var-uccx/dbc/db_hist_dbs</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>10.2</td>
<td>7.3</td>
<td></td>
</tr>
</tbody>
</table>
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 id user tty pid hostname threads memory memory explain
id used dynamic
27 cudbeven - 6750 crslnx 1 151552 75400 off

Memory pools count 2

name class addr totalsize freesize #allocfrag #freefrag
27 V 5309a020 147456 73704 148 50
27*00 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
```
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

<table>
<thead>
<tr>
<th>session</th>
<th>effective</th>
<th>#RSAM</th>
<th>total</th>
<th>used</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>id</td>
<td>user</td>
<td></td>
<td>user</td>
<td>tty</td>
</tr>
<tr>
<td>explain</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>uccxuser</td>
<td>-</td>
<td>-1</td>
<td>sakkumar</td>
</tr>
<tr>
<td>off</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Memory pools

<table>
<thead>
<tr>
<th>name</th>
<th>class</th>
<th>addr</th>
<th>totalsize</th>
<th>freesize</th>
<th>allocfrag</th>
<th>freefrag</th>
</tr>
</thead>
<tbody>
<tr>
<td>58</td>
<td>V</td>
<td>4caa9028</td>
<td>122880</td>
<td>17064</td>
<td>332</td>
<td>18</td>
</tr>
<tr>
<td>58*00</td>
<td>V</td>
<td>4c9d0028</td>
<td>4096</td>
<td>2416</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
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 USERNAMEN SESSION PROCESS ID
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

+--------------+------------+--------+-------------+
<table>
<thead>
<tr>
<th>DATABASE</th>
<th>USERNAME</th>
<th>SESSION</th>
<th>PROCESS ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysadmin</td>
<td>informix</td>
<td>15</td>
<td>0</td>
</tr>
<tr>
<td>sysadmin</td>
<td>informix</td>
<td>16</td>
<td>0</td>
</tr>
<tr>
<td>sysmaster</td>
<td>uccxuser</td>
<td>18</td>
<td>-1</td>
</tr>
<tr>
<td>db_cra</td>
<td>uccxuser</td>
<td>24</td>
<td>-1</td>
</tr>
<tr>
<td>db_cra</td>
<td>uccxuser</td>
<td>25</td>
<td>-1</td>
</tr>
<tr>
<td>fcrassvr</td>
<td>uccxuser</td>
<td>26</td>
<td>-1</td>
</tr>
<tr>
<td>sysmaster</td>
<td>uccxuser</td>
<td>44</td>
<td>-1</td>
</tr>
<tr>
<td>db_cra</td>
<td>uccxuser</td>
<td>45</td>
<td>-1</td>
</tr>
<tr>
<td>sysmaster</td>
<td>uccxuser</td>
<td>46</td>
<td>-1</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
```

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

<table>
<thead>
<tr>
<th>USERNAME</th>
<th>SESSION ID</th>
<th>LATCH</th>
<th>LOCK</th>
<th>BUFFER</th>
<th>CHECKPOINT</th>
<th>TRANSACTION</th>
<th>INCritical</th>
</tr>
</thead>
<tbody>
<tr>
<td>informix</td>
<td>16</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>informix</td>
<td>17</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>informix</td>
<td>15</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>uccxcliuser</td>
<td>33927</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>uccxcliuser</td>
<td>32784</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>uccxcliuser</td>
<td>32737</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>uccxcliuser</td>
<td>32631</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>uccxcliuser</td>
<td>34424</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>uccxcliuser</td>
<td>32522</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>uccxcliuser</td>
<td>34364</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>uccxcliuser</td>
<td>32508</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>uccxcliuser</td>
<td>32480</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>uccxcliuser</td>
<td>31616</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>uccxcliuser</td>
<td>31601</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>uccxcliuser</td>
<td>34327</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>uccxcliuser</td>
<td>34071</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>uccxcliuser</td>
<td>33981</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>uccxcliuser</td>
<td>33939</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>uccxhruser</td>
<td>31224</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>uccxuser</td>
<td>30278</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>uccxuser</td>
<td>60</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

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.

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**

```bash
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 sub-component 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, 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, XDebugging3, XDebugging4 and XDebugging5.

**Requirements**

- Level privilege: 1
- Command privilege level: 1
- Allowed during upgrade: No

**Example 1**

```bash
admin:set uccx trace enable uccxengine SS_VB debugging
Trace for uccxengine:SS_VB:debugging is enabled.
Command successful.
```

**Example 2**

```bash
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**

```bash
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, 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 Cisco VVB. 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:
```

Cisco Unified Contact Center Express Administration and Operations Guide, Release 11.6(1)
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 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**

When you upgrade Unified CCX, you must reinstall the Cisco Unified CCX Editor and Cisco Unified Real-Time Monitoring Tool.

---

**Command syntax**

`set tls server min-version [tls server minVersion]`

**Options**

`tls server minVersion`—Refers to 1.0 (TLS Version 1.0), 1.1 (TLS Version 1.1), and 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.
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.

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.
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
admin: appadmin
```

---
admin:set uccx appadmin administrator username
UCCX appadmin administrator 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-SO mode.

**Requirements**

Level privilege: 4

Command privilege level: 4

Allowed during upgrade: No

**Example**

admin:set authmode non_sso

---

**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.
When the command is executed, 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**

```bash
run uccx hrdataexport all [Start Date] [End Date]
```

Dumps all the historical reporting data.

```bash
run uccx hrdataexport reports report names [Start Date] [End Date]
```

Dumps all the historical reporting data for given reports.

```bash
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**

```bash
admin:run uccx hrdataexport all "2012-01-01 00:00:00" "2012-02-01 00:00:00"
```

```bash
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"
```

```bash
admin:run uccx hrdataexport tables "agentconnectiondetail,agentstatedetail,contactcallldetail" "2012-01-01 00:00:00" "2012-02-01 00:00:00"
```

**run uccx sql database_name sql_query**

Executes 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**

```bash
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 rtlitel
11  agent130
14   sk1
15   sk2
24   User RT Pro
```

```
run uccx sp database_name sp_name
```

Executes 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','')
```

```
<table>
<thead>
<tr>
<th>CONTACT_ID</th>
<th>SEQUENCE_NUMBER</th>
<th>CSQ_NAME</th>
<th>AGENT_NAME</th>
<th>RECEIVED</th>
<th>RETRIEVED</th>
<th>DISCARDED</th>
<th>FROM_ADDRESS</th>
<th>REPLY_TO_ADDRESS</th>
<th>TO_ADDRESS</th>
<th>SUBJECT</th>
<th>CONTACT_TYPE</th>
<th>CONTACT_DISPOSITION</th>
<th>EMAIL_REPLY_TO</th>
<th>EMAIL_REPLY_CC</th>
<th>EMAIL_REPLY_BCC</th>
</tr>
</thead>
<tbody>
<tr>
<td>D82AC141C00015800000EFF0A4E5D8A</td>
<td>0</td>
<td>testemailcsq1</td>
<td>FinesseAgent1</td>
<td>2016-12-07 07:22:49.0</td>
<td>2016-12-07 07:59:45.051</td>
<td>2016-12-07 08:00:47.06</td>
<td>null</td>
<td><a href="mailto:reboottest2@sky13.sm">reboottest2@sky13.sm</a></td>
<td>&quot;RebootTestUser2 Reboot.&quot;</td>
<td><a href="mailto:reboottest2@sky13.sm">reboottest2@sky13.sm</a></td>
<td><a href="mailto:reboot1test2@sky13.sm">reboot1test2@sky13.sm</a></td>
<td>test1</td>
<td>2</td>
<td><a href="mailto:reboot1test2@sky13.sm">reboot1test2@sky13.sm</a>, <a href="mailto:reboot1test1@sky13.sm">reboot1test1@sky13.sm</a></td>
<td></td>
</tr>
</tbody>
</table>
```

Command successful.

**Utils Commands**

### utils uccx notification-service log

This command allows you to enable, disable, and check the status of debug logging for Cisco Unified CCX Notification Service.

By default, debug logging is disabled for Cisco Unified CCX Notification Service. Enable debug logging for Cisco Unified CCX Notification Service when there is an issue in the system related to this service and when you require detailed logs for troubleshooting. After the troubleshooting is complete, disable logging for Cisco Unified CCX Notification Service.

You can retrieve the logs from the log-collection facility provided by Cisco Unified Real-Time Monitoring Tool.

You can execute **utils uccx notification-service log** only if Cisco Unified CCX Notification Service is running. If the service is not running, start the service first and then execute the command.

**Note**

- Logging for Cisco Unified CCX Notification Service affects system performance; therefore, disable logging when it is not required.

- Logging is disabled automatically when you restart Cisco Unified CCX Notification Service.

**Command syntax**

- `utils uccx notification-service log enable`
- `utils uccx notification-service log disable`
- `utils uccx notification-service log status`

**Arguments**
None

**Requirements**

Level privilege: 1
Command privilege level: 1
Allowed during upgrade: No

**Examples**

**Check status of logging**

```
admin:utils uccx notification-service log status
```
Cisco Unified CCX Notification Service logging is currently DISABLED.

**Enable logging**

```
admin:utils uccx notification-service log enable
```
WARNING! Enabling Cisco Unified CCX Notification Service logging can affect system performance and should be disabled when logging is not required.

Do you want to proceed (yes/no)?
Cisco Unified CCX Notification Service logging enabled successfully.

**Disable logging**

```
admin:utils uccx notification-service log disable
```
Cisco Unified CCX Notification Service logging disabled successfully.

---

**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**

```bash
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, OAMP, CUIC Admin property, and CUIC Administrator.

**Command syntax**

```bash
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.

```bash
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
OAMP 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 starting, stopping, and restarting of the following services:

- System SSH
- Service Manager
- A Cisco DB
- Cisco Database Layer Monitor
- Cisco DRF Local
- Cisco DRF Master
- Cisco Tomcat
- Cisco Unified Serviceability RTMT
- Cisco Finesse Tomcat
- Cisco Unified CCX Cluster View Daemon
- Cisco Unified CCX Database
- Cisco Unified CCX Administration
- Cisco Unified CCX Serviceability
- Cisco Unified CCX Engine
- Cisco Unified CCX DB Perfmon Counter Service
- Cisco Unified CCX Notification Service
- Cisco Unified CCX Perfmon Counter Service
• Cisco Unified CCX SNMP Java Adapter
• Cisco Unified CCX WebServices
• Cisco Unified CCX Configuration API
• Cisco Unified CCX Voice Subagent
• Cisco Unified CCX Socket.IO Service
• Cisco Unified Intelligence Center Reporting Service
• Cisco Unified Intelligence Center Serviceability Service
• Cisco Identity Service

Command syntax
utils service [option] [service-name]

Arguments
option — The option to stop, start, or restart a service.
service-name — The service which is to be stopped, started, or restarted.

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 proceeds with the command execution. 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.

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, execute the delete command first, and then restart the Unified CCX node. For the HA system, execute 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**

- **CustomJarName**—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
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 version 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 the execution of 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 this command is executed, a successful execution 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 execution / operation.
- **TotalHours**—Total duration of the execution.

**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
## 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
**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 custom_file * detail
08 Dec,2009 16:56:11 0 text.txt
dir count = 0, file count = 1
```

```
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> UserDialog
16 May,2012 17:50:19 <dir> gen
```
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
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 10 2005-08-03 15:01:41,248 DEBUG
 [main] - cmdMVL size = 0
2005-08-03 15:01:41,248 INFO [main] - adding command in level1 (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
```

---

**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
deleing file : log/cli00002.log
deleing file : log/cli00003.log
deleing file : log/cli00004.log
files: found = 4, deleted = 4
```
High Availability Commands

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 command lists 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
```
show uccx dbreplication servers

This command is only available in the High Availability deployment of Unified CCX. This command lists 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

<table>
<thead>
<tr>
<th>SERVER ID</th>
<th>STATE</th>
<th>STATUS</th>
<th>QUEUE</th>
<th>CONNECTION</th>
<th>CHANGED</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.76.253.106</td>
<td>110</td>
<td>Active</td>
<td>Connected</td>
<td>0 Apr 7 22:01:19</td>
<td>0</td>
</tr>
<tr>
<td>10.76.253.107</td>
<td>100</td>
<td>Active</td>
<td>Local</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

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. Execute 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 executed 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

<table>
<thead>
<tr>
<th>SERVER</th>
<th>ID</th>
<th>STATE</th>
<th>STATUS</th>
<th>QUEUE</th>
<th>CONNECTION</th>
<th>CHANGED</th>
</tr>
</thead>
<tbody>
<tr>
<td>g_alpha</td>
<td>1</td>
<td>Active</td>
<td>Connected</td>
<td>0</td>
<td>Aug 8 18:45:26</td>
<td></td>
</tr>
<tr>
<td>g_alpha</td>
<td>2</td>
<td>Active</td>
<td>Local</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

```
REPLICATE STATE

| ----------------------------------------------- |   |
| db_cra:informix.agentconnectiondetail         | 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

```bash
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

```bash
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 executes 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 Contact Center Express 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
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 activities, 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.

Note
Password values entered by the user is not echoed on the console.

Cisco Finesse Trace Logging

Use the following commands to toggle trace logs for Cisco Finesse, enable trace logs for Finesse IPPA, and enable debug logs for realm.

Note
Enabling trace logging may cause an overload in the system and must be used for debugging purposes only.

• *utils finesse trace enable*

  This command allows you to:
  • Enable trace logs for Cisco Finesse.
  • Turn on command dispatcher logs.
  • Enable trace logs for Finesse IPPA.
  • Enable debug logs for Realm.

• *utils finesse trace disable*

  This command allows you to:
  • Disable trace logs for Cisco Finesse.
  • Turn off command dispatcher logs.
  • Disable trace logs for Finesse IPPA.
  • Disable debug logs for Realm.

Note
After execution of each command, wait for 60 seconds for the changes to take effect.

• *utils finesse trace status*

  This command allows you to displays status as:
  • Enabled - When all four actions are enabled.
• Disabled - When all four actions are disabled.

If all actions are not enabled or disabled, a warning message is displayed.

**Cisco Finesse 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]**: Enable Cisco Finesse toaster notification.

  ![Note](Note) 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.

  The `closeTimeout` parameter is only available in Windows OS for Chrome browser. In Mac OS, the Chrome browser automatically closes the toaster notification.

- **utils finesse toaster disable**: Disable Cisco Finesse toaster notification.

- **utils finesse toaster status**: Display the status (enable or disable) of the Cisco Finesse toaster notification.

  ![Note] Cisco Finesse toaster notifications do not work with Internet Explorer browser.

**Cisco Finesse IPPA Inactivity Timeout**

Use the following CLI commands to enable or disable the Inactivity Timeout feature in Cisco Finesse IPPA. You must either disable the Cisco 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 does not get logged out of Cisco Finesse IPPA if the agent is on any other screen:

- **utils finesse ippa_inactivity_timeout enable**: To enable Cisco Finesse IPPA Inactivity Timeout feature.

  ![Note] The default time set for Cisco Finesse IPPA Inactivity Timeout is 120 seconds.

- **utils finesse ippa_inactivity_timeout disable**: To disable Cisco Finesse IPPA Inactivity Timeout feature.

  ![Note] When Cisco Finesse IPPA Inactivity Timeout is disabled, you will not be logged out of Cisco Finesse IPPA, if the agent is on any other screen.
• utils finesse ippa_inactivity_timeout enable inactivity_timeout: To enable Cisco 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: To check the status of Cisco Finesse IPPA Inactivity Timeout.

  **Note**  The Finesse IPPA Inactivity Timeout CLIs should be run on both the primary and secondary Finesse servers. Enabling or disabling the Cisco Finesse Inactivity Timeout 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/td/docs/voice_ip_comm/cust_contact/contact_center/crs/express_compatibility/matrix/uccxcompat11_6_1.html#Client_Operating_System

---

## 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
- **SchedulerStatus**—Shows status of the report scheduler

**Requirements**

- Level privilege: 0
- Command privilege level: 0
- Allowed during upgrade: No

**Example**
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
- **http-enabled**—Displays the value on or off depending on the current value that is set for the http-enabled property
- **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

**Requirements**

Level privilege: 0
Command privilege level: 0
Allowed during upgrade: Yes

**Example**

```shell
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 cuireport**

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 trace

This command shows the log level and trace masks of the given subsystem. If the logging level is set to DEBUG, the trace mask is displayed. If the logging level is set to INFO, the trace masks are not displayed.

The command is case sensitive and can only be run on the Controller node.

To set traces on the member nodes, use the Operations Console command Device Management > Log And Trace Settings.

Command syntax

show cuic trace cuicserver [options]

Options

This consists of the subsystems of Unified Intelligence Center. The various subsystems available are:

- CUIC
- Infrastructure
- CUIC_MODEL_OBJECTS
- CUIC_DATA_PROCESSING
- CUIC_SECURITY
- CUIC_DISPLAY
set cuic properties

Use these commands to set values for the 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_address—Enter the IP address of the server for the historical or real-time database

set cuic properties session-timeout

Parameter
#numberofSeconds—This command sets the session timeout for the Unified Intelligence Center Reporting web application. The default is 14,400 seconds (4 hours).

Requirements
Level privilege: 0
Command privilege Level: 0
Allowed during upgrade: Yes

Example
admin:set cuic properties session-timeout 1900
Value has been successfully set

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
```

---

**set cuic trace**

Use these commands to set or change the log levels and trace setting for the subsystems of two server processes (cuicserver and oampserver) to basic or detailed.

**Command Syntax**

- `set cuic trace basic  cuicserver [subsystem] none`
- `set cuic trace basic  oampserver [subsystem] none`
- `set cuic trace infrastructure  cuicserver [subsystem] [TRACE_FLAGS | none]`
- `set cuic trace infrastructure  oampserver [subsystem] [TRACE_FLAGS | none]`
- `set cuic trace subsystem  cuicserver [subsystem] [trace_mask1 trace_mask2]`
- `set cuic trace subsystem  oampserver [subsystem] [trace_mask1 trace_mask2]`

For cuicserver, the valid subsystems are:

- `Infrastructure`
• CUIC
• CUIC_MODEL_OBJECTS
• CUIC_DATA_PROCESSING
• CUIC_SECURITY
• CUIC_DISPLAY
• CUIC_MIGRATION
• CUIC_USER_HISTORY
• CUIC_JSP
• CUIC_STATISTICS

For oampserver, the valid subsystems are:

• Infrastructure
• OAMP_BO
• OAMP
• WSM_BO

Detailed log levels are set by enabling trace flags, which allows debug statements to appear in the logs. You can control debug tracing for specific functionalities (specified in the TRACE flag name), within specific subsystem components.

`basic` indicates to set a basic level of tracing. With this setting, messages and warnings are displayed.

`detailed` indicates to set a debug level and allows you to turn on tracing for specific components.

`subsystem` indicates the subsystem you are setting and displays the list of all valid subsystems.

`none` indicates that you do not want to set a flag for tracing.

**Requirements**

Level privilege: 1
Command privilege level: 1
Allowed during upgrade: Yes

**Example**

```
admin:set cuic trace basic cuicserver CUIC_SECURITY
```

Log level updated successfully. Trace masks are cleared

**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 Successfully
```

**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 execute 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 executed in the TCP/IP mode and must be executed when there is an addition or deletion of nodes to the CUIC cluster.
Command Syntax
utils cuic cluster refresh
Cisco Unified Contact Center Express License Packages

This appendix describes the features that are available with each Unified CCX license package.

- Application Availability by License Package, on page 551
- Trigger Availability by License Package, on page 551
- Subsystem Availability by License Package, on page 552
- Unified CCX Services Availability by License Package, on page 552
- Unified CCX Component Availability by License Package, on page 553

Application Availability by License Package

The following table lists the applications available with each license package:

<table>
<thead>
<tr>
<th>Application</th>
<th>Unified IP IVR</th>
<th>Unified CCX Standard</th>
<th>Unified CCX Enhanced</th>
<th>Unified CCX Premium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Script Application</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Busy</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Ring No Answer</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Trigger Availability by License Package

The following table lists the triggers available with each license package:

<table>
<thead>
<tr>
<th>Trigger</th>
<th>Unified IP IVR</th>
<th>Unified CCX Standard</th>
<th>Unified CCX Enhanced</th>
<th>Unified CCX Premium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified CM Telephony</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>HTTP</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Subsystem Availability by License Package

The following table lists the subsystems available with each license package:

<table>
<thead>
<tr>
<th>Subsystem</th>
<th>Unified IP IVR</th>
<th>Unified CCX Standard</th>
<th>Unified CCX Enhanced</th>
<th>Unified CCX Premium</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMT Subsystem</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Core RTR Subsystem</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Database Subsystem</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>eMail Subsystem</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>HTTP Subsystem</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Unified CM Telephony Subsystem</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>MRCP ASR Subsystem</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>MRCP TTS Subsystem</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Outbound Subsystem⁴</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>RmCm Subsystem</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Voice Browser Subsystem</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>RouteAndQueue Subsystem</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

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 Component Availability by License Package

The following table lists the Unified CCX Component available with each license package:

<table>
<thead>
<tr>
<th>Unified CCX Services</th>
<th>None 5</th>
<th>Unified IP IVR</th>
<th>Unified CCX Standard</th>
<th>Unified CCX Enhanced</th>
<th>Unified CCX Premium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified CCX Cluster View Daemon</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Unified CCX Administration</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Unified CCX Engine</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cisco Unified CCX Database</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

5 Available upon installation, before license package is activated.

---

<table>
<thead>
<tr>
<th>Unified CCX Component</th>
<th>None 6</th>
<th>Unified IP IVR</th>
<th>Unified CCX Standard</th>
<th>Unified CCX Enhanced</th>
<th>Unified CCX Premium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified CCX Cluster View Daemon (CVD)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Unified CCX Engine</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Unified CCX Repository Datastore</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Unified CCX Historical Datastore</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Unified CCX Configuration Datastore</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Unified CCX Recording</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Unified CCX Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

6 Available upon installation, before license package is activated.
The Context Service client provides `REQUEST_TIMEOUT` connection property that significantly affect the user experience for your customers and agents. `REQUEST_TIMEOUT` defines how long the client waits for a response from Context Service. Defaults 5000 ms.

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

If Context Service does not respond on that first retry, then the request fails. If there is an issue with your connection, then you are potentially doubling the wait defined in `REQUEST_TIMEOUT`. The default `REQUEST_TIMEOUT` is 5000 ms (5 seconds). This combination results in a 10 second wait (wait time = `REQUEST_TIMEOUT` + 2). In a worst-case scenario, wait time can be significant if there are network issues between your client and Context Service and your timeouts are set too high.

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

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

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

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