Cisco Unified Attendant Console Advanced – Administration and Installation Guide

Version 14.0.2.30
November 24, 2025

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

Text Part Number: OL-29382-01

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.

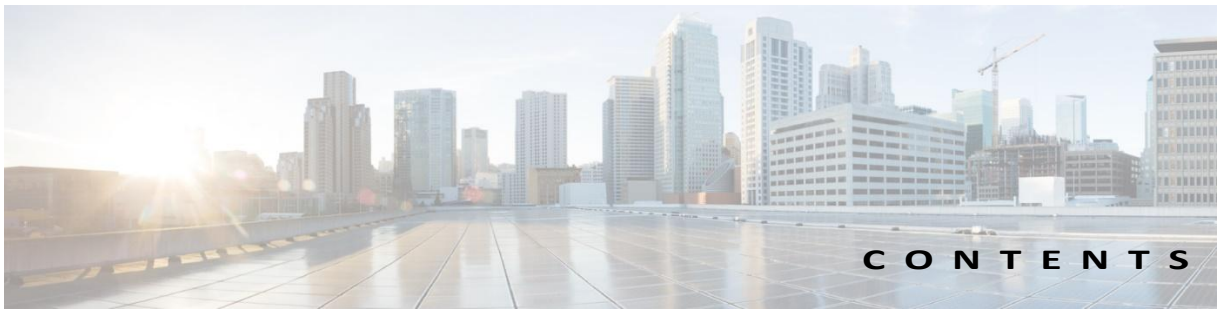
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco Ironport, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0907R)

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

Cisco Unified Attendant Console Advanced User Guide
© 2025 Cisco Systems, Inc. All rights reserved.



About This Guide ix

Who Should Read This Guide ix

How This Guide is Organized x

Document Conventions xi

Obtaining Documentation and Submitting Service Requests xii

Product Overview 1

Server High Availability 1

Resilience Provided 3

Single Sign On 3

Syslog and Alert Server 4

Cisco Unified Attendant Console Advanced Ports 4

Integrating Cisco Unified Attendant Console Advanced with Cisco Unified Communications Manager 6

AXL Connectivity 6

AXL API 8

Cisco Unified Communications Manager System Devices 9

Centralized Installations and Transcoding 9

TAPI Resilience 10

Music on Hold 10

Presence Service Integration 10

Deployment Checklist 11

Hardware and Software Requirements 13

Server Requirements 13

Physical Server Hardware Requirements 13

VMware Guest Machine Requirements 14

Server Software Requirements 14

Additional Server Considerations 17
Citrix Support 20
Jabber Support 21
Cisco Unified Attendant Console Advanced Client Requirements 21
PC Hardware Requirements 21
PC Software Requirements 21
Operator Phone Requirements 22
Supported Windows, SQL Server, Active Directory, Presence Server, Application User and CUAC Password Characters 22

Preparing Cisco Unified Communications Manager and Cisco Unified Presence 24
Cisco Unified Communications Manager (Required) 24
Creating a Unique Reference CTI Port Device 24
Creating an Access Control Group 26
Assigning Roles to an Access Control Group 26
Creating and Assigning an Application User 27
Cisco Unified Presence (Optional) 28
Creating an End User for the Presence Server 28
Presence states chart 29

Installing Cisco Unified Attendant Console Advanced Software 31
Obtaining Cisco Unified Attendant Console Advanced Software 32
Creating a Cisco Unified Attendant Console Advanced Downloads and Licensing Website User Account 32
Downloading the Software 32
Adding Internet Information Service (IIS) 33
Installing and/or configuring SQL 34
Installing SQL Server 34
Installing SQL Server Management Studio 36
Licensing SQL Server 36
High Availability (Resilient Installations) 37
Export Crypto Key File 38
Cisco Unified Attendant Console Advanced Server In-place Upgrade Procedure 39
Cisco Unified Attendant Console Advanced Server Installation Procedure 39
Disabling Plug-ins that are not in use 43
Installing Cisco Unified Attendant Console Advanced Client 43
Installing JAWS Scripts for Visually Impaired Operation 44

Silent Installing Cisco Unified Attendant Console Advanced 45

Cisco Unified Attendant Console Administration 48

Administrator Login 48

Logging On 48

Logging Out 49

Home Page 49

Menu Options 50

Toolbar 50

Data Entry Fields 51

Accessibility for Users with Disabilities 51

Help 52

Contents/This Page 52

Licensing 52

Export Crypto Key File 52

Last Login Info 52

About 53

Cisco Unified Attendant Console Administration - Engineering 54

Engineering Menu 54

Server Management 54

Database Management 55

Test the Database 55

Repair the Database 55

Database Purge 56

Automatic Purge 57

Service Management 57

Cisco Unified Attendant Server Status 59

Cisco Unified Attendant LDAP Plug-in Status 59

Cisco Unified Attendant Presence Plug-in Status 59

Cisco Unified Attendant BLF Plug-in Status 60

Presence Management 60

Configuration 60

CUCM Connectivity 61

Syslog Connectivity 63

Logging Management 64

Cisco Unified Attendant Console Server Logging 64
Cisco Unified Attendant LDAP Plug-in Logging 66
Cisco Unified Attendant Presence Plug-in Logging 66
Cisco Unified Attendant BLF Plug-in Logging 67
Log Collection 67
Setting Up Log Collection 67
Starting Log Collection 67
Canceling Log Collection 68
Downloading the Log Archive 68
Checking Log Collection Progress 68
Marking Text Management 68
Customized Logon Message 68

Cisco Unified Attendant Console Administration – System Configuration 70
System Configuration Menu 70
Queue Device Groups 70
Creating Queue Device Groups 71
Deleting Queue Device Groups 72
System Device Management 72
Synchronize with CUCM 75
Directory Source Management 79
Connecting to a Directory Source 80
Directory Synchronization 82
Directory Field Mapping 83
Directory Rules 85
Contact Management 86
Adding Contacts 86
Modifying Contact Information 88
Deleting Contacts 88
Directory BLF Rules 89
Creating Directory BLF Rules 89
Editing Directory BLF Rules 90
Deleting Directory BLF Rules 90
Applying BLF Directory Rules 91

Cisco Unified Attendant Console Administration – User Configuration 92

User Configuration Menu 92
General Properties 92
Queue Management 95
Creating Queues 96
Deleting Queues 97
Configuring Queues 97
Operator Management 100
Creating Operator Profiles 101
Importing Operators 101
Configuring Operator Profiles 102
Deleting Operator Profiles 103
Realm Management 103
System Accounts Management 104
Adding New System Accounts 104
Account Roles 104
Permissions by Account Role 105
Modify Passphrase 110
Credential Policy Management 111
Templates 112
Configuring Out of Hours Routing 112

Cisco Unified Attendant Console Administration – Bulk Administration 117
Upload/Download Files 117
Managing Uploaded CSV Files 118
Insert, Update and Export Contacts 118
Inserting and Updating Contacts 118
Exporting Contacts to CSV Files 119
Job Scheduler 120

Cisco Unified Attendant Console High Availability 122
SQL Server Replication 124
Accessing High Availability Administration Menus 124
Installing Replication 125
Uninstalling Replication 128
Re-initializing Replication 130
Monitoring Replication 130

Validating Replication 131
Replication Report 132

Licensing Cisco Unified Attendant Console Advanced 133
Licensing the Cisco Unified Attendant Console Advanced Software 133
Locate Server Registration Code 134
Activating Evaluation Software 134
Activate the Software 134
Activating Purchased Software 135
Term-Based License Expiry 136
Relicensing Software 136

Uninstalling Cisco Unified Attendant Console Advanced 137
Uninstalling Microsoft SQL Server 138
Uninstalling the .NET Framework 138
Uninstalling Cisco TSP 139

Cisco Unified Attendant Console Advanced Migration and/or Upgrade 140
Application User Validation 140
Build New Cisco Unified Attendant Console Advanced Server(s) 140
Back Up Existing Databases 141
Back Up Existing Crypto Key and Registry 141
Restore Databases 142
Restore Cryptographic Keys and Registries 142
Install Cisco Unified Attendant Console Advanced Server Application 142
Troubleshooting Post-Migration System Device Registration Issues 143

Cisco Unified Reporting 144
Toolbar 145
Setting Report Parameters 145
Date Range 145
Time Range 145
Abandoned Calls 146
Queue Type 146
Attendant Operators 146
Incoming Calls by Date and Time System Report 146
Operator Calls by Time System Report 147

Operator Calls by Queue System Report 148
Operator Availability Report 149
Overflowed Calls By Date System Report 150

Example Cisco Unified Attendant Console Advanced Configuration 151

Publisher 151
Subscriber 151
Device Groups 153
Attendant Operators 154
Attendant Queues 154

Backing up and restoring Cisco Unified Attendant Console Advanced 155

Backing-up Databases 155
Manually Backing-up Databases 155
Automatically Backing-up Databases 156
Restoring Databases 158
Preparing the Servers 158
Restoring the Databases 159
Reconnecting a Subscriber Server to a Restored Publisher Server 160
Backing-up Cryptographic Keys and Registries 161
Backing-up Using Attendant Administrator 161
Restoring a Subscriber Server 161
Licensing Your New Server 162

Updating the Cisco Unified Attendant Console Advanced Server Host Name, SQL Server Login Name and Password 163

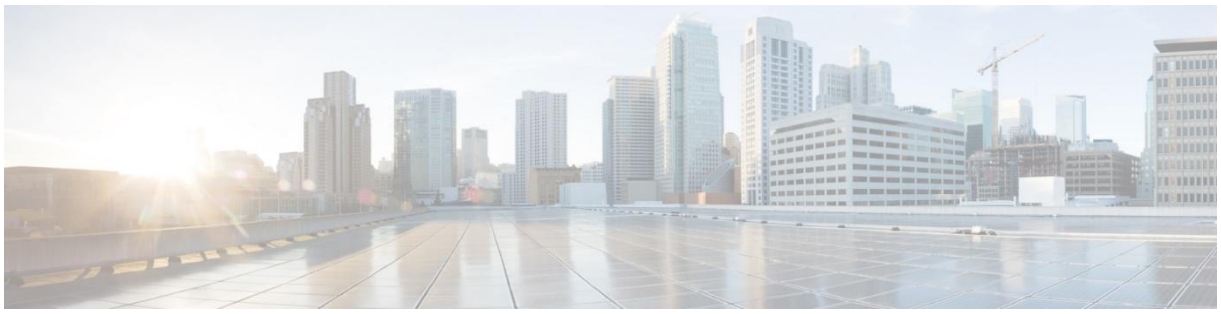
Console Client Instruction 163
Server Instruction 163
Standalone Installs Only: Prepare the Batch Files 165
High Availability Installs Only: Uninstall Replication from Both Servers 165
Set Cisco Unified Attendant Console Advanced Services and Active MQ Service Startup Type to Manual 166
Modify Cisco Unified Attendant Console Advanced server host name and/or SQL Server login name and password 166
Execute the Appropriate Batch Files 166
If the Conversion Fails 168
Hostname change 168

Set Cisco Unified Attendant Console Advanced and SQL Server services startup type to Automatic . 169
Reinstall High Availability (If Required) 170
Restart Cisco Unified Attendant Console Advanced Server(s) 170

Performing CUCM Upgrades and Re-installing Cisco TSP 171

Modifying Cisco Unified Attendant Console Advanced Server IP Address 172

Setting Up Non-standard SQL Server Ports 173
Configuring SQL to Use a Non-standard Port 173
Cisco Unified Attendant Console Advanced Server Alias Configuration 173
Creating an Alias on Client 174



About This Guide

This document describes how to install and configure Cisco Unified Attendant Console Advanced – its databases, connections to Cisco Unified Communications Manager, and its system and user settings – using the Cisco Unified Attendant Console Advanced Administration web application.

Who Should Read This Guide

The document is intended for:

- Deployment Engineers, who are responsible for:
  - System design
  - Preparing Cisco Unified Communications Manager
  - Installing the Cisco Unified Attendant Console Advanced server and Cisco Unified Attendant Console Advanced client
  - Configuring the Cisco Unified Attendant Console Advanced server
- System Administrators

This document assumes that you have knowledge of:

- Cisco Unified Communications Manager
- Windows operating systems
- TCP/IP

How This Guide is Organized

This guide contains the following sections.

Section	Contains
Product Overview	An overview of Cisco Unified Attendant Console Advanced, including its compatibility with Cisco Unified Communications Manager.
Deployment Checklist	The steps to take when installing Cisco Unified Attendant Console Advanced, cross-referenced to the relevant procedures in this guide.
Hardware and Software Requirements	The Cisco Unified Attendant Console Advanced server and Cisco Unified Attendant Console Advanced client hardware and software requirements.
Preparing Cisco Unified Communications Manager and Cisco Unified Presence	How to configure Cisco Unified Communications Manager so that Cisco Unified Attendant Console Advanced can work with it.
Installing Cisco Unified Attendant Console Advanced Software	How to download, install and license Cisco Unified Attendant Console Advanced software.
Cisco Unified Attendant Console Administration	How to use the Cisco Unified Attendant Console Administration to configure the Cisco Unified Attendant Console Advanced server.
Cisco Unified Attendant Console Administration - Engineering	How to configure the Engineering menu options in Cisco Unified Attendant Console Advanced.
Cisco Unified Attendant Console Administration – System Configuration	How to configure the System Configuration menu options in Cisco Unified Attendant Console Advanced.
Cisco Unified Attendant Console Administration – User Configuration	How to configure the User Configuration menu options in Cisco Unified Attendant Console Advanced.
Cisco Unified Attendant Console Administration – Bulk Administration	How to configure the Bulk Administration menu options in Cisco Unified Attendant Console Advanced.
Cisco Unified Attendant Console High Availability	How to provide server high availability using server replication.
Licensing Cisco Unified Attendant Console Advanced	How to license your Cisco Unified Attendant Console Advanced software.
Uninstalling Cisco Unified Attendant Console Advanced	How to uninstall Cisco Unified Attendant Console Advanced server.
Cisco Unified Attendant Console Advanced Migration and/or Upgrade	How to migrate or upgrade Cisco Unified Attendant Console Advanced server.
Cisco Unified Reporting	How to create Cisco Unified Attendant Console Advanced Administration reports.

Section	Contains
Example Cisco Unified Attendant Console Advanced Configuration	An example of a resilient Cisco Unified Attendant Console Advanced configuration.
Backing up and restoring Cisco Unified Attendant Console Advanced	How to back up Cisco Unified Attendant Console Advanced server, and how to restore it following failures requiring a full system rebuild.
Updating the Cisco Unified Attendant Console Advanced Server Host Name, SQL Server Login Name and Password	How to update the Cisco Unified Attendant Console Advanced server host name during server migration, upgrade, or rebuild.
Performing CUCM Upgrades and Re-installing Cisco TSP	How to perform a CUCM upgrade and re-install Cisco TSP.
Modifying Cisco Unified Attendant Console Advanced Server IP Address	How to successfully modify the Cisco Unified Attendant Console Advanced server IP address.
Setting Up Non-standard SQL Server Ports	How to successfully set up non-standard SQL server ports.

Document Conventions

The following textual and typographic conventions are used in this document:

Convention	Usage
bold font	Commands, keywords, and user-entered text appear in **bold** type.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are enclosed in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are enclosed in square brackets and separated by vertical bars.
string	A non-quoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in courier font.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem.*

Caution	Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.
Timesaver	Means *the described action saves time*. You can save time by doing what is described in the paragraph.
Warning	**Means *reader be warned*. In this situation, you might do something that could result in bodily injury.**

Obtaining Documentation and Submitting Service Requests

For information on obtaining additional documentation and submitting service requests,

- Obtaining documentation
- Obtaining support
- Submitting service requests
- Providing documentation feedback
- Security guidelines
- Recommended aliases
- Gathering additional information
- A list of all new and revised Cisco technical documentation

see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Product Overview

Cisco Unified Attendant Console Advanced is a Windows-based operator attendant console application for use exclusively with Cisco Unified Communications Manager.

For more information about which versions of Cisco Unified Attendant Console Advanced and Cisco Unified Communications Manager work together, see Integrating Cisco Unified Attendant Console Advanced with Cisco Unified Communications Manager.

Cisco Unified Attendant Console Advanced emulates the functions of a manual telephone switchboard, and so enables attendant console operators to quickly accept incoming calls and efficiently dispatch them to recipients within an organization.

The Cisco Unified Attendant Console Advanced server monitors extensions within Cisco Unified Communications Manager and routes the calls to the Cisco Unified Attendant Console Advanced clients. Calls from Cisco Unified Communications Manager enter Cisco Unified Attendant Console Advanced server through Cisco Unified Communications Manager Computer Telephony Integration (CTI) Route Point devices, which can route calls, but cannot terminate them. Cisco Unified Communications Manager CTI Ports receive the calls and deliver them to the operators.

You use Cisco Unified Attendant Console Advanced Administration to create the required system devices on the Cisco Unified Communications Manager, and to configure the system parameters on the Cisco Unified Attendant Console Advanced server. Cisco Unified Attendant Console Advanced system parameters, the user directory and call record logs are all stored in SQL databases on the Cisco Unified Attendant Console Advanced server.

Server High Availability

Cisco Unified Attendant Console Advanced supports server high availability in an active/passive (hot standby) deployment, based on SQL Server replication and the synchronization of database objects across publisher and subscriber servers. For more information on how replication is implemented in Cisco Unified Attendant Console Advanced, see Cisco Unified Attendant Console High Availability.

A resilient Cisco Unified Attendant Console Advanced installation runs on two servers:

- Publisher—responsible for normal activity. You configure the system by logging in to Cisco Unified Attendant Console Advanced Administration on the Publisher. By default, all operators using the Attendant Console client are logged onto the Publisher for configuration and call routing. The Publisher includes the LDAP server.

- Subscriber—the passive, secondary (backup) server. The information from the publisher server is replicated onto this server. The Subscriber runs the all the same services as the Publisher except that it does not use an LDAP service to populate the directory, instead this is replicated entirely from the Publisher. If the Publisher fails, the Subscriber takes over, communicating with the Attendant Console clients. You cannot change the configuration through the Subscriber server. On the Subscriber you can:
  - set logging levels
  - monitor replication and run reports.

The following are installed on both server machines:

- BLF server. Responsible for all BLF information and call activity
- Cisco Unified Presence server. Responsible for presence information. For more information, see Presence Service Integration.

The two servers are linked using Apache Active MQ, an open-source message broker. When you update system and user configuration on the Publisher, all the changes are sent to the Subscriber in real-time. If the Publisher fails, the Attendant Console client applications automatically log out and offer their users the option to continue connected to the Subscriber.

Apache Active MQ is also used for real-time synchronization of operator and queue availability. It also enables the Publisher and Subscriber to detect whether the other has failed.

The Publisher and Subscriber servers can be part of a Microsoft Domain, so long as they can access each other by hostname. Call Forwarding is used to transfer calls received on the Publisher Queue DDI numbers to the Subscriber Queue DDI numbers of the same queue.

Note

If the inter-server communication link is down, all online updates will fail. This is also true of the non-resilient version of Cisco Unified Attendant Console Advanced.

To check the status of the inter-server communication link:

1. Log in to Cisco Unified Attendant Console Advanced Administration and choose **Engineering** > **Service Management**.
2. View the activity and status of the Cisco Unified Attendant Server.

If the Inter Server Communication Status is **Suspended**, the ActiveMQ service may not be running. To check and restart the ActiveMQ service:

1. In Control Panel, click **Accessories**, and then click **Services**.
2. If the Status of the ActiveMQ service is blank (meaning that it is stopped), select the service and click **Start**.
3. Use Cisco Unified Attendant Console Advanced Administration to confirm that the Inter Server Communication Status is **Normal**.

You can install Cisco Unified Attendant Console Advanced as a single-server (Publisher-only) system, with no high availability. If you install Cisco Unified Attendant Console Advanced as a non-resilient system, you can convert it to the resilient version by purchasing and installing a high availability license.

For a resilient installation you must first install the Publisher server and then the Subscriber server (the Subscriber installation communicates with the Publisher). When you have installed a Publisher or Subscriber server you cannot convert it into the other server type.

Resilience Provided

The system is resilient to the following failures:

- Cisco Unified Call Manager node failure (partial failover). During normal operation, the primary Cisco Unified Attendant Console Advanced server on the Publisher server and the secondary Cisco Unified Attendant Console Advanced server on the Subscriber server connect to different CTI Managers within the same Cisco Unified Communications Manager cluster. For more information about CTI Manager, see AXL Usage During Installation. If the Cisco Unified Communications Manager node used by the primary Cisco Unified Attendant Console Advanced server fails, another Cisco Unified Communications Manager takes over and the primary Cisco Unified Attendant Console Advanced server continues to run.
- Primary CTI Manager on Publisher fails (partial failover).
- BLF Server fails (partial failover).
- If you remove all Queue DDI or CT Gateway devices using Cisco Unified Attendant Console Advanced Administration (partial failover). For example, if Queue DDIs are manually removed from the TSP User Profile, the server remains active, but calls follow the call forward set on Cisco Unified Communications Manager to the Subscriber. You can still update the system configuration using the Cisco Unified Attendant Console Advanced Administration on the Publisher.
- TSP failure.
- Database failure.
- Cisco Unified Attendant Console Advanced server failure (or server shut down, or failure of the communication channel between the Publisher and Subscriber servers).

During a partial failover some or all of the primary Cisco Unified Communications Manager system devices go out of service. However the primary Cisco Unified Attendant Console Advanced server on the Publisher server continues running because the TAPI-based CT Link continues working.

Single Sign On

Single Sign On is a feature that can be configured if Cisco Unified Communications Manager is configured to run under Single Sign On. It enables Attendant Operator users to sign in to multiple unified communication applications at the same time. Once a user has signed in to one of the unified communication applications, they do not need to sign in to others. This depends on how the Identity Provider (IdP), which authenticates users, is configured.

For more information about SSO, including how to configure the Cisco Unified Communications Manager to use it, see the relevant Cisco documentation.

The Cisco SSO Home Realm identifies which authentication system operators must access to use SSO. Cisco Unified Attendant Console Advanced can work only with a maximum of one SSO Home Realm per server (the Publisher and Subscriber can use the same or different Home Realms). The Home Realm is created by the Database Installation wizard when you install or update the software.

Cisco Unified Attendant Console Advanced can be accessed by both SSO and non-SSO users (contacts cannot be both SSO and non-SSO at the same time). Users are linked to the SSO Home Realm: each SSO user is associated with an LDAP-synchronized contact in Cisco Unified Attendant Console Advanced, while non-SSO (local) users are not. You cannot use Cisco Unified Attendant Console Advanced to add SSO Home Realms, but you can specify which domains are used by the realms. If your Home Realm has no domains defined for it, all SSO users have access to the realm. You can restrict which SSO Users have access to the realm by specifying their domains; how to do this is described in Realm Management.

Non-SSO users can be converted to SSO users by linking them to End Users on the SSO-enabled Cisco Unified Communications Manager. How to do this is described in Configuring Operator Profiles.

Syslog and Alert Server

The Cisco Unified Attendant Console Advanced Server can push its syslog to a remote syslog server that conforms to RFC3164 or RFC5424. The audit logs lend visibility to application and user activities (for example: web administration log in and log out, changing server configuration, accessing server configuration, stopping and starting of Cisco Unified Attendant Server services).

Syslogs are written for the following components:

- Cisco Unified Attendant Server Service
- LDAP Plug-in
- BLF Plug-in
- Presence Plug-in
- SQL Server Syslogs

For how to connect Cisco Unified Attendant Console Advanced to the syslog and alert server, see Syslog Connectivity.

Cisco Unified Attendant Console Advanced Ports

Cisco Unified Attendant Console Advanced applications use TCP/IP and UDP Ports to communicate with each other. In large networks, which often involve a WAN, you may need to prioritize the following ports across the network switches:

Port Number	Port Type	Relationship*	Function
135	TCP	Pub←→Sub	WMI calls use port 135 before choosing a random port. During the Resilience installation, the CUAC process uses WMI to connect to an alternate server. This port is only required during the installation/uninstallation and replication configuration.
389	TCP	Pub/Sub Internal or Pub/Sub←→Directory source	Used to communicate with Microsoft Active Directory or iPlanet Netscape Directory when not using Secure Sockets Layer (SSL).
443	TCP	CUCM←→Pub/Sub	Used by the AXL API to communicate with the Cisco Unified Communications Manager, with or without Secure Sockets Layer (SSL).
443	TCP	Internal/external web browser ←→Pub/Sub	Used by the Cisco Unified Attendant Console Advanced Administration application, which is hosted on the Internet Information Services (IIS) that runs on the Cisco Unified Attendant Console Advanced server.
636	TCP	Pub/Sub Internal or Pub/Sub←→Directory source	Used to communicate with Microsoft Active Directory or iPlanet Netscape Directory when using Secure Sockets Layer (SSL).
1433 and 1434	TCP	Pub←→Sub and Opr←→Pub/Sub	Used for SQL communication between servers and between servers and clients.
1859	TCP	Opr←→Pub/Sub	Used by the Cisco Unified Attendant Console Advanced

Port Number	Port Type	Relationship*	Function
			server and the Cisco Unified Attendant Console Advanced client to communicate across a LAN.
1862	TCP	Pub/Sub Internal	Used by the Cisco Unified Attendant Console Advanced LDAP Server.
1863	TCP	Opr←→Pub/Sub	Used for communication between the Cisco Unified Attendant Presence server and the Cisco Unified Attendant Console Advanced client.
1864	TCP	Opr←→Pub/Sub	Used for communication between Cisco Unified Attendant Console Advanced clients and the Cisco Unified Attendant Console Advanced BLF plug-in that provides phone line status.
2748	TCP	CUCM←→Pub/Sub	Used by the Cisco TSP to communicate between the Cisco Unified Attendant Console Advanced server and the Cisco Unified Communications Manager.
5222	TCP	Presence Server ←→IM&P source Presence Server ←→WebEx source	XMPP connection between Presence Server and IM&P and WebEx presence sources.
11859	TCP	Pub/Sub Internal	Used by the Cisco Unified Attendant Console Advanced service to communicate with the Cisco Unified Attendant Console Advanced server.
49152 to 65535	TCP	Opr←→Pub/Sub CUCM←→Pub/Sub Pub/Sub Internal	Dynamic ports used to communicate between the Cisco Unified Attendant Console Server, Cisco Unified Communications Manager, and the Operator PCs.
50000 to 54000	UDP	CUCM←→Pub/Sub	Cisco TSP Media Driver channels used for communications between Cisco Unified Attendant Console Server and Cisco Unified Communications Manager.
61616	TCP	Pub←→Sub	Used to enable messages to be passed between Publisher and Subscriber servers in resilient installations.
61618	TCP	Pub←→Sub	

*** Relationship Key**

CUCM = Cisco Unified Communications Manager

IM&P = Instant Messaging and Presence Server

Opr = Attendant Console Client

Pub = Publisher Server

Sub = Subscriber Server

LDAP uses the following TCP/IP ports to communicate with Cisco Unified Communications Manager:

TCP/IP Port	Use
389	LDAP server does not use SSL and is not configured as the Global Catalog.
636	LDAP server uses SSL and is not configured as the Global Catalog.
3268	LDAP server does not use SSL and is configured as the Global Catalog.
3269	LDAP server uses SSL and is configured as the Global Catalog.

Integrating Cisco Unified Attendant Console Advanced with Cisco Unified Communications Manager

For more information, see the compatibility matrix in the *Cisco Unified Attendant Console Advanced Release Notes*.

AXL Connectivity

The AVVID XML Layer (AXL) is used both during and after Cisco Unified Attendant Console Advanced installation.

AXL Usage During Installation

During Cisco Unified Attendant Console Advanced server installation, you must specify the following nodes:

- The Cisco Unified Communications Manager that will use it (see Step 14, in the Cisco Unified Attendant Console Advanced Server Installation Procedure). In resilient installations the Publisher and Subscriber servers both need this information.
- The Primary and Backup CTI Manager that will use it (see Step 16, in the Cisco Unified Attendant Console Advanced Server Installation Procedure).

  CTI Manager is a feature service that runs on one or more Cisco Unified Communications Manager subscribers operating in primary/secondary mode to authenticate and authorize Cisco Unified Attendant Console Advanced. A CTI Manager node is a Cisco Unified Communications Manager subscriber that runs only the CTI Manager service.

The Cisco Unified Attendant Console Advanced server installer uses AXL to verify that the specified CTI manager(s) and Cisco Unified Communications Manager versions match, which is essential for successful implementation. After Cisco Unified Attendant Console Advanced is installed, the CTI Manager nodes no longer require the AXL service; so, you can disable it. However, if the main Cisco Unified Communications Manager node and the CTI Manager nodes are hosted on the same servers, you need to retain the AXL service on them.

AXL Usage After Installation

Part of the Cisco Unified Attendant Console Advanced BLF Plug-in service known as Device Resolution Manager (DRM) uses AXL to communicate with Cisco Unified Communications Manager.

The AXL communications enable DRM to resolve the BLFs of operator and system devices, and to synchronize system devices within the Cisco Unified Communications Manager database. System device synchronization is described further in AXL API.

Non-resilient Installation Scenarios

This section illustrates two different AXL use cases based on individualized requirements.

Scenario 1

This scenario uses the following node IP addresses:

- Cisco Unified Communications Manager = 172.29.252.111
- Primary CTI Manager = 172.29.252.111
- Backup CTI Manager = 172.29.252.112

DRM uses only the Cisco Unified Communications Manager at 172.29.252.111. Consequently, the AXL service can be disabled on 172.29.252.112 after installing Cisco Unified Attendant Console Advanced.

Scenario 2

This scenario uses the following node IP addresses:

- Cisco Unified Communications Manager = 172.29.252.111
- Primary CTI Manager = 172.29.252.112
- Backup CTI Manager = 172.29.252.113

DRM uses only the Cisco Unified Communications Manager at 172.29.252.111. Consequently, the AXL service can be disabled on 172.29.252.112 and 172.29.252.113 after installing Cisco Unified Attendant Console Advanced.

Resilient Installation Scenarios

This section describes AXL usage in example resilient Cisco Unified Attendant Console Advanced server installations.

Scenario 3

This scenario uses the following node IP addresses:

- Publisher Cisco Unified Communications Manager = 17.29.252.111
- Publisher Primary CTI Manager = 172.29.252.111
- Publisher Backup CTI Manager = 172.29.252.112
- Subscriber Cisco Unified Communications Manager = 17.29.252.111
- Subscriber Primary CTI Manager = 172.29.252.111
- Subscriber Backup CTI Manager = 172.29.252.112

DRM uses the Cisco Unified Communications Manager pointed to by both Publisher and Subscriber Cisco Unified Attendant Console Advanced servers (both 17.29.252.111). Consequently, the AXL service can be disabled on 172.29.252.112 after installing Cisco Unified Attendant Console Advanced.

Scenario 4

This scenario uses the following node IP addresses:

- Publisher Cisco Unified Communications Manager = 17.29.252.111
- Publisher Primary CTI Manager = 172.29.252.111
- Publisher Backup CTI Manager = 172.29.252.112
- Subscriber Cisco Unified Communications Manager = 17.29.252.112
- Subscriber Primary CTI Manager = 172.29.252.111
- Subscriber Backup CTI Manager = 172.29.252.112

DRM uses the Cisco Unified Communications Manager pointed to by both Publisher and Subscriber Cisco Unified Attendant Console Advanced servers (172.29.252.111 and 172.29.252.112).

Consequently, we need AXL connectivity to both IP addresses, and cannot disable AXL service on either.

Scenario 5

This scenario uses the following node IP addresses:

- Publisher Cisco Unified Communications Manager = 17.29.252.111
- Publisher Primary CTI Manager = 172.29.252.111
- Publisher Backup CTI Manager = 172.29.252.113
- Subscriber Cisco Unified Communications Manager = 17.29.252.112
- Subscriber Primary CTI Manager = 172.29.252.111
- Subscriber Backup CTI Manager = 172.29.252.113

DRM uses the Cisco Unified Communications Manager pointed to by both Publisher and Subscriber Cisco Unified Attendant Console Advanced servers (172.29.252.111 and 172.29.252.112).

Consequently, the AXL service can be disabled on Cisco Unified Communications Manager IP 172.29.252.113 after installing Cisco Unified Attendant Console Advanced.

AXL API

Cisco Unified Attendant Console Advanced Administration and Cisco Unified Communications Manager communicate via the AXL API, using Secure Sockets Layer (SSL), to synchronize the following system devices within the Cisco Unified Communications Manager database:

- Computer Telephony Integration (CTI) Ports—virtual phones that can terminate calls. They can be used for queuing calls and can play music on hold to the caller.
- CTI Route Points—virtual devices that can receive multiple, simultaneous calls for application-controlled redirection. They cannot terminate (answer) calls.

The AXL API enables data to be inserted, retrieved, updated, removed, and retrieved as eXtensible Markup Language (XML) from the database using Simple Object Access Protocol (SOAP). For AXL communication to work, Cisco Unified Communications Manager must contain a User Profile that allows it.

Note AXL communication between the Cisco Unified Attendant Console Server and Cisco Unified Communications Manager supports both SSLv3 and TLSv1.2. Depending on how CUCM is configured, AXL will automatically use the appropriate SSL version.

Cisco Unified Communications Manager System Devices

Cisco Unified Attendant Console uses the following system devices:

- Queue DDI (Direct Dial In)—the number dialed to route calls into a queue. Each DDI is configured on Cisco Unified Communications Manager as a CTI Route Point, and any call intended for this queue must be directed to this port, either directly or through a translation pattern.
- CT Gateway devices—CTI Ports (virtual devices that enable you to create virtual lines) that are created by Cisco Unified Attendant Console Advanced Administration when synchronized with Cisco Unified Communications Manager; they queue calls awaiting distribution to Cisco Unified Attendant Console Advanced.
- Service Queues—CTI Ports that are used to manage calls after they leave the operator's handset, for example when transferring or holding calls.
- Park devices—CTI Ports that are used when an attendant parks a call. The attendant can either select the preferred Park port or allow the system to select the port for them. A parked call can then be picked up by anyone on the system by dialing the park port number.

  The Cisco Unified Attendant Console Advanced Call Park functionality is additional to the standard Cisco Unified Communications Manager call park and directed call park functions. Operators can see what Park devices are available and choose whether to use a specific device or allow the system to select a park device for them. As these park devices are exclusive to Console attendants, they are situated on the Cisco Unified Attendant Console Advanced server and require an additional range of DNs.
- Cisco Unified Attendant Console Advanced Server supports:
  - 1000 CTI Ports per server (collective total of CT gateway devices, service queues and park devices.
  - 100 CTI Route Points (Queue DDIs)

For information on configuring CTI Ports, see System Configuration Menu.

Centralized Installations and Transcoding

To support G729 natively with the New Media Driver you need to do the following:

- On the Cisco Unified Attendant Console Advanced server, change the registry key HKEY_USERS/S-1-5-20/Software/Cisco Systems, Inc./RTPLib/G729PassThrough to 1 in either Hex or Dec, and then reboot the server.
- Ensure that the Device Pool and the region in which the CTI Port(s) are assigned is not restricted to G729. If it is, calls will not be processed correctly, and will be unable to be redirected to the CTI Port.

For more information on transcoding refer to the *Cisco Solution Reference Network Design*.

Note

If you start using a different Cisco Unified Communications Manager Release, access the CUCM Connectivity option and use it to validate and, if necessary, change the media driver, as described in CUCM Connectivity.

TAPI Resilience

Cisco Unified Communications Manager enables a Telephony/TAPI Service Provider (TSP) client to communicate with a primary and backup CTI Manager to receive CTI information. This allows the Cisco Unified Attendant Console Advanced server and clients to carry on functioning if a Cisco Unified Communications Manager failover occurs. The backup CTI Manager should be the Cisco Unified Communications Manager to which the phones fail over.

Music on Hold

Cisco Unified Attendant Console Advanced supports Music on Hold (MoH) from Cisco Unified Communications Manager. It is recommended you use unicast MoH. MoH is used in the following situations:

- When an operator holds a call
- During a blind transfer
- During a re-established transfer
- When Call Arrival Mode is selected to hold queued calls, as described in General Properties.

Presence Service Integration

Presence status indicates the ability and willingness of a directory contact to communicate; it can be supplied to Cisco Unified Attendant Console Advanced by the following presence services:

- Cisco Unified Communications Manager (IM&P)
- Cisco WebEx Messenger
- Skype For Business 2015 and 2016

For more information, see the compatibility matrix in the *Cisco Unified Attendant Console Advanced Release Notes*.

The Cisco Unified Attendant Console Advanced Server collects IM&P from dedicated servers and passes it to the Cisco Unified Attendant Console Advanced client for use by the Console attendant. This integration is managed via the Cisco Unified Attendant Presence Plug-in. By contrast, Skype For Business presence is collected directly by the Cisco Unified Attendant Console Advanced client from the Skype For Business application running locally on the attendant's machine.

For details of how to configure the Cisco Unified Attendant Console Advanced to use presence servers, see High Availability (Resilient Installations) and Presence Management.

Deployment Checklist

This section lists the things you must do to install Cisco Unified Attendant Console Advanced server and Cisco Unified Attendant Console Advanced client for the first time. You may find it useful to print this page and annotate it to keep track of your progress.

To install Cisco Unified Attendant Console Advanced for the first time, perform the following steps:

Step 1 Check that your Cisco Unified Communications Manager version is compatible with the version of Cisco Unified Attendant Console Advanced you are installing. For more information, see Integrating Cisco Unified Attendant Console Advanced with Cisco Unified Communications Manager.

Step 2 Decide whether the Cisco Unified Attendant Console Advanced server is going to run on a physical server or in VMware and confirm that your server meets or exceeds the minimum specifications required by Cisco Unified Attendant Console Advanced. For more information, see:

- Physical Server Hardware Requirements
- VMware Guest Machine Requirements_bookmark50

Note To ensure password composition is supported, see Supported Windows, SQL Server, Active Directory, Presence Server, Application User and CUAC Password Characters.

Step 3 Ensure that you have the correct versions of operating system and SQL database required by the Cisco Unified Attendant Console Advanced server and client. For more information, see:

- VMware Guest Machine Requirements
- Server Software Requirements
- PC Software Requirements

Step 4 Configure Cisco Unified Communications Manager so that it is ready for Cisco Unified Attendant Console Advanced deployment. For more information, see Preparing Cisco Unified Communications Manager and Cisco Unified Presence.

Step 5 Download, install and license the Cisco Unified Attendant Console Advanced software. For more information, see Installing Cisco Unified Attendant Console Advanced Software.

Step 6 Use Cisco Unified Attendant Console Advanced Administration to configure the Cisco Unified Attendant Console Advanced server. For more information, see the **Cisco Unified Attendant Console Advanced Administration** chapters.

Step 7 Install the Cisco Unified Attendant Console Advanced client. For more Information, see Installing Cisco Unified Attendant Console Advanced Client.

Hardware and Software Requirements

This section describes the hardware and software requirements for Cisco Unified Attendant Console Advanced server and Cisco Unified Attendant Console Advanced client.

Server Requirements

In a production environment, Cisco Unified Attendant Console Advanced server runs in either a:

- Physical server, with the requirements shown below.
- VMware environment compliant with Cisco's Specification-Based Hardware Support program. For details of the requirements, see VMware Guest Machine Requirements.

Physical Server Hardware Requirements

Cisco Unified Attendant Console Advanced server has the following minimum physical server hardware requirements:

- 2 x 2.2 GHz Pentium 4 processor
- 6 GB RAM
- 120 GB of available hard disk space
- Network card, connected to the network using TCP/IP

Note

- NIC teaming is not supported.
- Cisco Unified Attendant Console Advanced server is not supported in a production environment if running on a desktop PC.

VMware Guest Machine Requirements

In a production environment, Cisco Unified Attendant Console Advanced server is supported on VMware ESXi (Vmotion included) running on a host machine that is compliant with Cisco's UC Virtualization Supported Hardware. For more information, see Virtualization for Cisco Unified Attendant Consoles.

Cisco Unified Attendant Console Advanced server has the following minimum VMware instance (guest machine) requirements:

- 2x vCPU unrestricted
- 6 GB RAM
- 120 GB of available hard disk space

Note

- Cisco Unified Attendant Console Advanced server is not supported in HyperV or any other virtualization products other than VMware.
- Cisco Unified Attendant Console Advanced does not run on a copy (clone) of a virtual machine.
- For more information about VMware requirements, feature support and services, visit Virtualization Software Requirements.
- Due to security restrictions and the resource demands of a domain controller, Microsoft advises against installing SQL server on a domain controller. For more information, see Installing SQL Server on a domain controller. Consequently, Cisco Unified Attendant Console Advanced is not supported if installed on a domain controller.
- OVA template for VMware ESXi version 7.x and prior, with the above specifications, available for download from the following location: https://cisco.com/go/ac. VMware ESXi version 8.x and later require manual creation of virtual machine.

Server Software Requirements

Cisco Unified Attendant Console Advanced server has the following requirements:

- Server host name length must be 15 characters or less
- One of the following activated operating systems, with Windows regional settings set to English:
  - Windows Server 2012 R2 (64-bit)

    Update KB2919355 needs to be applied prior to installing the Cisco Unified Attendant Console Advanced server.
  - Windows Server 2016 (64-bit)
  - Windows Server 2019 (64-bit)
  - Windows Server 2022 (64-bit)
- Microsoft Visual C++ 2019 Redistributable 32-bit*
- Microsoft Visual C++ 2019 Redistributable 64-bit*
- Microsoft URL Rewrite Module 2.0 for IIS (x64)
- Internet Information Service (IIS) 8.0 or later, with the Static Content role service added.
  - To install IIS on a system with Windows Server already installed, see Obtaining Cisco Unified Attendant Console Advanced Software.

- ASP.NET 2.0.50727 or later*

Note * Cisco Unified Attendant Server installs these requirements if no existing installation is detected.

- .NET Framework 4.7
- OpenJDK build 17.0.16+8 (earlier/later builds are not supported)
- One of the following databases: Microsoft SQL Server 2012, 2014, 2016, 2017 and 2019 Standard, Enterprise or Express. SQL Server Express 2016 is installed by the Cisco Unified Attendant Server installer if an existing installation of SQL Server is not detected.

Note SQL Server 2016 and older versions won't be supported on Windows Server 2022 OS. For more information, see SQL Server in Windows operating system.

- SQL Server Requirements
- One of the following browsers: Microsoft Edge, Google Chrome, Firefox.

Note Legacy browsers IE11 and Edge Legacy may work but are not officially supported.

- If you plan to implement Cisco Unified Attendant Console Advanced server high availability, you must ensure that the date time and time zone on your Publisher and Subscriber servers are synchronized. Both servers must be in the same time zone to ensure that any daylight-saving time changes occur simultaneously. If they are not in the same time zone, the operator console will be unable to automatically reconnect to the Publisher when it recovers from failure.

Note

- Cisco Unified Attendant Console Advanced server must be installed and operated exclusively on a supported platform.
- To ensure system security, your operating system must be configured according to your company's operating system hardening guidelines. Take care to ensure that all CUACA-specific configuration requirements are still met after hardening.

SQL Server Requirements

Cisco Unified Attendant Console Advanced server does not support multiple SQL database instances or named instances and requires exclusive use of and access to a local installation of SQL Server.

If you are installing Microsoft SQL yourself, you must install it locally on the Cisco Unified Attendant Console Advanced server. Cisco Unified Attendant Console Advanced does not support the use of external SQL Servers.

Due to security restrictions and the resource demands of a domain controller, Microsoft advises against installing SQL server on a domain controller. For more information, see Installing SQL Server on a domain controller. Consequently, Cisco Unified Attendant Console Advanced is not supported if installed on a domain controller.

To ensure system security, your SQL installation must be configured according to your company's SQL system hardening guidelines. Take care to ensure that all CUACA-specific configuration requirements are still met after hardening.

If you plan to implement Cisco Unified Attendant Console Advanced server high availability, you must ensure that the date time and time zone on your Publisher and Subscriber servers are synchronized. Both servers must be in the same time zone to ensure that any daylight-saving time changes occur simultaneously. If they are not in the same time zone, the operator console will be unable to automatically reconnect to the Publisher when it recovers from failure.

High availability deployments require that the Publisher and Subscriber servers use the same version of SQL Server.

High availability deployments where thresholds defined under SQL Server Express Limitations are not exceeded can leverage SQL Server Express on the Subscriber server.

SQL Server User Account Requirements

The user account you specify for Cisco Unified Attendant Console Advanced to access the system database must meet the following requirements:

- The account must have the 'sysadmin' role associated to it.
- The user ID and passphrase used for the application must be the same for the Publisher and Subscriber servers.
- The SQL Server login password cannot exceed 30 characters.
- The SQL Server login password must be sufficiently complex to meet the requirements described in Microsoft's Password Policy.

SQL Server Express Limitations

Microsoft SQL Server Express has the following limitations:

- Can access only a single CPU
- Uses only 1 GB of RAM
- Cannot be used on publisher server in a high availability deployment.

You should consider using Microsoft SQL Server Standard or Enterprise if you expect your Cisco Unified Attendant Console Advanced deployment to support any of the following:

- More than 10 operators
- More than 500 calls per operator per day
- A directory containing more than 10,000 contacts

If a Cisco Unified Attendant Console Advanced system outgrows Microsoft SQL Server Express, you can upgrade the database to Microsoft SQL Server Standard or Enterprise. Multiple SQL databases are not supported.

Wireshark

In the event that Wireshark needs to be installed on a Cisco Unified Attendant Console Advanced server, install it using the default settings but deselect the Npcap component. If Npcap is installed, it may present issues with Cisco Unified Attendant Console Advanced licensing and the LDAP plug-in.

Additional Server Considerations

This section contains important information you should know about your server hardware and software.

Microsoft Windows and SQL Server Updates and Service Packs

Cisco Unified Attendant Console Advanced server supports and recommends the application of all Microsoft Windows and SQL Server Updates and Service Packs.

Best Practices

- Set Windows Update to **Never check for updates**. Update and Service Pack installations should be executed outside of production to minimize the risk of service impact.
- If using Group Policy to push updates to Cisco Unified Attendant Console Advanced servers, ensure that the push is executed outside of production to minimize the risk of service impact.
- Following the installation of Updates and/or Service Packs, restart the Cisco Unified Attendant Console Advanced server operating system

Java Updates

OpenJDK updates (manual and automatic) are not supported as they may render the system unusable.

OpenJDK updates will be delivered with future Cisco Unified Attendant Console Advanced minor and major releases as required.

Note

Oracle announced changes for its distribution of Java SE 8. For more information, see Oracle Java SE 8 Release Updates.

As a result of these changes, Cisco Unified Attendant Console now leverages OpenJDK. New installations and upgrades will remove any pre-existing releases of Java from the server and install OpenJDK.

Oracle Java SE (any version) cannot be installed on the Cisco Unified Attendant Console Server.

Data Backup

You should provide backup facilities to ensure application and data integrity in the event of unforeseen circumstances. If possible, choose a solution that offers one-step disaster recovery, such as the ability to restore the complete contents of a hard drive from a bootable floppy disk and the backup media.

Instructions for setting up automatic or manual Cisco Unified Attendant Console Advanced server database backups are available in Backing up and restoring Cisco Unified Attendant Console Advanced.

Server Redundancy

We strongly recommended that you configure your Cisco Unified Attendant Console Advanced server as a redundant system with the following redundancy features:

- Multiple hot-swap power supplies
- Hot-swap Hard Drive arrays
- UPS / power conditioners
- RAID

Antivirus Software

Anti-virus applications provide fine control of what data is scanned and how the data is scanned on a server.

The Cisco Unified Attendant Console Advanced software constantly accesses files in certain folders; consequently, your anti-virus software will constantly try to scan them for viruses, which will slow down the server. Therefore, your chosen antivirus product must support exclusions, which you use to specify the following files and folders that are not to be scanned by the antivirus software.

Default Folder	Contains
\\DBData	System configuration databases
\\Apache	Active MQ folder
\\%ALLUSERSPROFILE%\Cisco\CUACA	Cisco profile
Program Files (x86)\Cisco	Cisco Unified Attendant Console Advanced Program Files
\\ProgramData\Cisco\CUACA\	Cisco Unified Attendant Console Advanced Logging Repository, Crypto Key export, Console client default configuration file
\\Temp\CUACA\	Cisco Unified Attendant Console Advanced Installation and database install/upgrade logging repository
\\Temp\CiscoTSP001Log\	Cisco TAPI Plugin, application logging

Note The System Administrator may have set up your Cisco Unified Attendant Console Advanced server to use different folders for these files.

With any anti-virus product, configuration is a balance of scanning versus the performance of the server. The more you choose to scan, the greater the potential performance overhead. Your system administrator should determine the optimal configuration of your anti-virus application within your particular environment. Refer to your anti-virus product documentation for more detailed configuration information.

General best practices are listed below:

- Update AV software scanning engines and definition files on a regular basis, following your organization's current policies.
- Upgrade to the latest supported version of the third-party anti-virus application. Newer versions improve scanning speed over previous versions, resulting in lower overhead on servers.
- Avoid scanning of any files accessed from remote drives (such as network mappings or UNC connections). Where possible, ensure that each of these remote machines has its own anti-virus software installed, thus keeping all scanning local. With a multi-tiered antivirus strategy, scanning across the network and adding to the network load should not be required.
- Schedule full scans of systems by AV software only during scheduled maintenance windows, and when the AV scan will not interrupt other Unified Console ServerICM maintenance activities.
- Do not set AV software to run in an automatic or background mode for which all incoming data or modified files are scanned in real time.
- Due to the higher scanning overhead of heuristics scanning over traditional anti-virus scanning, use this advanced scanning option only at key points of data entry from untrusted networks (such as email and Internet gateways).

- Real-time or on-access scanning can be enabled, but only on incoming files (when writing to disk). This is the default setting for most anti-virus applications. Implementing on-access scanning on file reads will yield a higher impact on system resources than necessary in a high-performance application environment.
- While on-demand and real-time scanning of all files gives optimum protection, this configuration does have the overhead of scanning those files that cannot support malicious code (for example, ASCII text files). Cisco recommends excluding files or directories of files, in all scanning modes, that are known to present no risk to the system.
- Schedule regular disk scans only during low-usage times and at times when application activity is lowest.
- Disable the email scanner if the server does not use email.
- Additionally, set the AV software to block port 25 to block any outgoing email.
- Block IRC ports. IRC uses TCP protocol to communicate on default port 6667. It can also to connect to other TCP ports if TCP port 6667 is blocked.
- If your AV software has spy-ware detection and removal, then enable this feature. Clean infected files, or delete them (if these files cannot be cleaned).
- Enable logging in your AV application. Limit the log size to 2 MB.
- Set your AV software to scan compressed files.
- Set your AV software to not use more than 20% CPU utilization at any time.
- When a virus is found, the first action is to clean the file, the second to delete or quarantine the file.
- If it is available in your AV software, enable buffer overflow protection.
- Set your AV software to start on system startup.

TLS 1.2 Supportability

Cisco Unified Attendant Console Advanced extends TLS 1.2 compliance.

TLS 1.2 compliance:

- HTTPS TLS 1.2 support for Attendant Administrator
- AXL communication with Unified Communications Manager on TLS 1.2
  - Cisco Unified Attendant Console Advanced acts as a TLS client
- XMPP communication with IM&P on TLS 1.2
  - Cisco Unified Attendant Console Advanced acts as a TLS client
- TAPI communication with Unified Communication Manager CTI Manager supported via Cisco TAPI
  - Cisco Unified Attendant Console Advanced installs/leverages the plugin as part of its deployment
- LDAP communication with Active Directory
- SQL Server Authentication

Note

For TLS 1.2 supportability for the SQL Server 64-bit installations, please refer to Microsoft SQL Server documentation.

Network Requirements

For Cisco Unified Attendant Console Advanced to run across a network:

- The network must support TCP/IP.
- Cisco Unified Attendant Console Advanced Administration web application must run under an Administrator profile (Local Administrator is acceptable).
- On Microsoft Windows networks that use DHCP, you must allocate Cisco Unified Attendant Console Advanced server with a static IP address.
- If a DNS Server is not present on the network or the Cisco Unified Attendant Console server machine name (Publisher server machine name in the case of a resilient installation) cannot be resolved, you must amend the Hosts file (WINDOWS\system32\drivers\etc\) to reflect the server IP address and server machine name. Please ensure that the installation prerequisites in this guide have been satisfied.

Note Cisco Unified Attendant Console Advanced supports IPsec should you need to encrypt its network traffic. Cisco Unified Attendant Console Advanced also supports Secure TSP; see the Cisco TAPI documentation for configuration instructions.

Telephony and QWave Server Services

The Cisco TSP client, local to each Cisco Unified Attendant Console Advanced server, is tightly coupled with the Microsoft Telephony and QWave Services. For more information, see the Cisco Unified TAPI Developers Guide for CUCM.

Do not disable or stop the referenced services, as doing so makes the solution unstable and/or stops the solution from working all together.

Note The QWave service is not installed by default as part of the software installation and is not required for successful operation unless it is present on the server. If the service is present in the *services.msc* menu, it must remain enabled.

Citrix Support

Cisco Unified Attendant Console Advanced Server cannot be installed in a Citrix environment. Cisco Unified Attendant Console Advanced Operator Client can be installed in a Citrix environment:

- XenApp 7 2206 (Fundamentals, Advanced, Enterprise, Platinum)
- XenDesktop 7 2206 (VDI, Enterprise, Platinum)

Citrix environments support the following modes:

- Windows Apps delivery
- Windows Desktops delivery
- Windows Hosted Shared (Server) Desktops delivery

The following platforms are not supported:

- Cisco VXI Solution
- VMWare Horizon

Note Update KB4034661 needs to be applied prior to launching seamless applications from a Server VDA running Windows Server 2016. For more information, see Citrix Binary Fix and Known Issues.

Jabber Support

Both standard Jabber installations (locally installed on the operator computer) and VXME installations (installed in a VXME environment) are supported as operator devices and end points.

Cisco Unified Attendant Console Advanced Client Requirements

This section describes the hardware and software requirements of the PC and operator phones running the Cisco Unified Attendant Console Advanced client.

PC Hardware Requirements

The PC running the Cisco Unified Attendant Console Advanced client has the following hardware requirements:

- 2.0 GHz Pentium 4 processor
- 4 GB RAM
- 1 GB of available hard disk space
- Network card, connected to the network using TCP/IP
- SVGA (1024x768) display card
- 17-inch or larger monitor highly recommended
- SoundBlaster-compatible sound card and speakers highly recommended
- Keyboard with 10-key number pad

PC Software Requirements

The PC running the Cisco Unified Attendant Console Advanced client must be running one of the following activated operating systems:

- Microsoft Windows 10 (Desktop Mode)
- Microsoft Windows 11 (Desktop Mode)

The following third party applications are required. If they are not installed on the PC prior to executing the Cisco Unified Attendant Console Advanced client installer, they will be automatically installed:

- Microsoft Visual C++ 2019 Redistributable

Operator Phone Requirements

For more information about operator phone requirements and supported handsets, refer to *Supported Handsets* in the *Cisco Unified Attendant Console Advanced Design Guide*. In addition to a detailed list of supported handsets (console user devices and contact directory - busy lamp field devices) you will see supportability statements for Jabber soft phones, shared lines, and extension mobility.

Supported Windows, SQL Server, Active Directory, Presence Server, Application User and CUAC Password Characters

Below is the list of characters that can be leveraged in passphrases for the following:

- Cisco Unified Communications Manager Application User - Specified in the Cisco TSP connection details and in the Cisco Unified Attendant Console Connection Details
- Cisco Unified Presence Server Connection Details

Name of Character	Character(s)
Lower case alphabet	a - z
Upper case alphabet	A - Z
Numbers	0 - 9

Below is the list of characters that can be leveraged in passwords for the following accounts:

- Windows User Account - leveraged for installation, upgrade and uninstallation of Cisco Unified Attendant Console, and for installing and uninstalling replication.
- SQL Server Account - used for Cisco Unified Attendant Console Database Connection
- Active Directory User Account Details
- Cisco Unified Attendant Console User Account Passwords - Administration accounts and user accounts

Name of Character	Character(s)
Lower case alphabet	a - z
Upper case alphabet	A - Z
Numbers	0 - 9
at sign	@
percent sign	%
plus	+
backslash	\

Name of Character	Character(s)
slash	/
single quotation mark	'
exclamation point	!
number sign	#
dollar sign	$
caret	^
question mark	?
colon	:
comma	,
left parenthesis	(
right parenthesis	)
left brace	{
right brace	}
left bracket	[
right bracket	]
tilde	~
hyphen	-
underscore	_
period	.
asterisk	*
ampersand	&

Preparing Cisco Unified Communications Manager and Cisco Unified Presence

This chapter walks you through the perquisites for successfully deploying Cisco Unified Attendant Console Advanced server in your Cisco Unified Communications Manager environment. The chapter is split into two sections, each having different steps: the steps under Cisco Unified Communications Manager (Required) are required for all deployments; the steps outlined under Cisco Unified Presence (Optional) are only required if you intend to present Cisco IM and Presence or WebEx Messenger presence status within the Cisco Unified Attendant Console client directory.

Cisco Unified Communications Manager (Required)

Creating a Unique Reference CTI Port Device

Cisco Unified Attendant Console BLF Plug-in requires a unique CTI Port reference device meeting the following criteria.

Considerations

- The **CTI Port Reference Device Number** cannot be used in Cisco Unified Attendant Server system devices or queue locations.
- Though the services operate without the creation of the reference device, depending on the number range leveraged for **Cisco Unified Attendant Console Queue Locations**, there is a risk that high availability functionality will be hindered.
- The **CTI Port Referenced Device** is not used for call routing.

CTI Port Reference Device Requirements

- In High Availability deployments, a unique device and directory number is required for each Application User.
- Reference device(s) must be assigned to only one Application User.
- The Directory Number specified must be the lowest device number value of all system devices and queue locations associated with your Cisco Unified Attendant Server. For example:
  - CT Gateway Device Number Range: 1000-1010
  - Service Device Number Range: 1011-1020
  - Park Device Number Range: 1021-1030
  - Queue Locations: 1031, 1034, 2034
  - When creating the CTI Port Reference Device with the above device number ranges, the directory number must be equal to or less than 0999.

Create CTI Port Reference Device

Step 1 Use your Internet browser to access **Cisco Unified CM Administration**, and then log in.

Step 2 Go to **Device** > **Phone** and click **Add New**.

Step 3 Select **Phone Type**, **CTI Port**, and then click **Next**.

Step 4 Populate the following fields:

- **Device Name**: it is recommended using a name illustrating tie to Cisco Unified Attendant Server Publisher or Subscriber.
- **Device Description**: it is recommended using a name illustrating tie to Cisco Unified Attendant Server Publisher or Subscriber.

Step 5 Click **Save**.

Step 6 Under the **Associate** navigation pane, click **Line [1] - Add a New Line**.

Step 7 Enter the required **Directory Number** following the instructions under CTI Port Reference Device Requirements.

Step 8 Click **Save**, and then click **Save** again. You should now see your new **CTI Port Reference Device** name in the **Associated Devices** list.

Step 9 If using High Availability, repeat the process to create a reference device for use by the Subscriber Server.

Creating an Access Control Group

Cisco Unified Attendant Console Advanced communicates with Cisco Unified Communications Manager through an Access Control Group, which you must create in the latter.

To create an Access Control Group with the roles necessary for the Application User to allow the Cisco Unified Attendant Console Advanced server to function, do the following:

Step 1 Use your Internet browser to access **Cisco Unified CM Administration**, and then log in.

Step 2 Choose **User Management > User Settings > Access Control Group**.

Step 3 Click **Add New** to create a new Access Control Group.

Step 4 Type a **Name** for the new Access Control Group.

Step 5 Click **Save** to save the Access Control Group.

Step 6 Assign roles to the Access Control Group, as described below.

Assigning Roles to an Access Control Group

To add the roles to an Access Control Group required to enable the Cisco Unified Attendant Console Advanced server to function, do the following:

Step 1 With the group displayed, in **Related Links** (in upper-right corner) select **Assign Role to User/Access Control Group**, and then click **Go**.

Step 2 Click **Assign Role to Group**.

Step 3 Find **Role** where **Name** is not empty. This lists the roles.

Step 4 Select the following roles:

- **Standard AXL API Access**
- **Standard CCM Admin Users**
- **Standard CTI Allow Calling Number Modification**
- **Standard CTI Allow Control of All Devices**
- **Standard CTI Allow Control of Phones supporting Connected Xfer and conf***
- **Standard CTI Allow Control of Phones supporting Rollover Mode***
- **Standard CTI Allow Reception of SRTP Key Material**
- **Standard CTI Enabled**
- **Standard SERVICEABILITY**

Step 5 Click **Add Selected** to assign the roles.

Step 6 Click **Save**.

Creating and Assigning an Application User

An Application User connects the Cisco Unified Attendant Console Advanced server to Cisco Unified Communications Manager using Cisco TSP and AXL.

Note If you are installing a resilient system, each Cisco Unified Attendant Console Advanced server (Publisher and Subscriber) needs to have a unique Application User.

This section describes how to create an Application User and then assign it to the Access Control Group.

To create and assign an Application User:

Step 1 Log into Cisco Unified Communications Manager Administration.

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

Step 3 Click **Add New**.

Step 4 Enter information in the following fields:

- **User ID** (a name of your choice)
- **Password**
- **Confirm Password** (this must match the Password)

Note Passwords must be comprised using ONLY the following characters: A-Z, a-z, 0-9.

Step 5 Scroll down to the **Permissions Information** section and click **Add to Access Control Group**.

Step 6 Find the Access Control Group you created in the previous section and select it.

Step 7 Click **Save** to save the Application User.

Step 8 Under **Device Information > Available Devices**, click the **Device Association** button.

Step 9 Search for and select the **CTI Port Referenced Device**. For more information about creating a CTI Port Referenced Device, see Creating a Unique Reference CTI Port Device.

Step 10 Click **Save Selected / Changes**.

Cisco Unified Presence (Optional)

Creating an End User for the Presence Server

The Cisco Unified Attendant Console Advanced Presence Server requires a Cisco Unified Communications Manager End User to be able to connect with and interrogate the relevant Presence Service provider (IM&P or WebEx Messenger).

Note The Cisco Unified Presence plug-in does not support Single Sign On (SSO) authentication.

To create an End User:

Step 1 Log into Cisco Unified Communications Manager Administration.

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

Step 3 Click **Add New**.

Step 4 Enter information in the following fields:

- **User ID** (a name of your choice)
- **Password**
- **Confirm Password** (this must match the Password)

Note To ensure password composition is supported, see Supported Windows, SQL Server, Active Directory, Presence Server, Application User and CUAC Password Characters.

- **Last name**
- **First Name** (optional)
- **Directory URI** (depends on the configuration)
- **Mail ID**

Step 5 Define the Service Settings:

- Select **Home Cluster** checkbox.
- Select **Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)** checkbox.

Step 6 Click **Save** to save the End User.

Presence states chart

Note

- In case of multiple device scenarios, the statuses on Cisco Unified Attendant Console could be different to what is explained in the tables.
- Cisco Unified Attendant Console Advanced shows presence in the following ways:
  - **Status**: base presence information for a user. For example, *Available, Away, Busy, Do Not Disturb*.
  - **Info**: supplemental information to a user's availability. For example, *On the phone, In a meeting, Presenting, any custom notes*.

Current State → / Event ↓	Available	Away (idle)	On the phone	In a meeting	Available (Manual)	Away (Manual)	Do not disturb	Offline
Available	Available	Available	On the phone	In a meeting	Available	Away (Manual)	Do not disturb	Available
Device Idle	Away (idle)	Away (idle)	On the phone	In a meeting	Away (idle)	Away (Manual)	Do not disturb	Offline
Make Call	On the phone	On the phone	On the phone	In a meeting	On the phone	Away (Manual)	Do not disturb	Offline, On the phone
Join Meeting	In a meeting	In a meeting	In a meeting	In a meeting	In a meeting	Away (Manual)	Do not disturb	Offline, In a meeting
Set Manual Available	Available	Available	Available	Available	Available	Available	Available	Available
Set Manual Away	Away (Manual)	Away (Manual)	Away (Manual)	Away (Manual)	Away (Manual)	Away (Manual)	Away (Manual)	Away (Manual)
Set Manual DND	Do not disturb	Do not disturb	Do not disturb	Do not disturb	Do not disturb	Do not disturb	Do not disturb	Do not disturb
Offline	Offline	Offline	Offline, On the phone	Offline, In a meeting	Offline	Offline	Offline	Offline

Figure 1 IM&P Presence States chart

Current State → / Event ↓	Available	Away (idle)	In WebEx Meeting	In a meeting (local outlook)	Available (Manual)	Away (Manual)	Do not disturb	Presenting	Offline
Available	Available	Available	In WebEx Meeting	In a meeting	Available	N/A	N/A	N/A	Available
Device Idle	Away (idle)	Away (idle)	In WebEx Meeting	In a meeting	Away (idle)	Away (Manual)	Do not disturb	Presenting	Offline
Join Meeting	In a meeting	In a meeting	In WebEx Meeting	In a meeting	In a meeting	In a meeting	Do not disturb	Presenting	Offline
Set Manual Available	Available	Available	Available	Available	Available	Available	Available	Available	Available
Set Manual Away	Away (Manual)	Away (Manual)	Away (Manual)	Away (Manual)	Away (Manual)	Away (Manual)	Away (Manual)	Away (Manual)	Away (Manual)
Set Manual DND	Do not disturb	Do not disturb	Do not disturb	Do not disturb	Do not disturb	Do not disturb	Do not disturb	Do not disturb	Do not disturb
Presenting	Presenting	Presenting	Presenting	Presenting	Presenting	Presenting	Presenting	Presenting	Presenting
Offline	Offline	Offline	Offline	Offline, In a meeting	Offline	Offline	Offline	Offline	Offline

Figure 2 WebEx Presence States chart

Installing Cisco Unified Attendant Console Advanced Software

This chapter describes how to install Cisco Unified Attendant Console Advanced software:

Step 1 Download the Cisco Unified Attendant Console Advanced server software, as described in Obtaining Cisco Unified Attendant Console Advanced Software.

Step 2 Add IIS to the Windows Server, as described in Adding Internet Information Service (IIS).

Step 3 Prepare SQL, as described in Installing and/or configuring SQL.

Step 4 Install the Cisco Unified Attendant Console Advanced server software, as described in High Availability (Resilient Installations).

Step 5 Install the Cisco Unified Attendant Console Advanced client software, as described in Installing Cisco Unified Attendant Console Advanced Client.

- Alternatively, execute a silent installation, as described in Silent Installing Cisco Unified Attendant Console Advanced.

Note

- If you have a Microsoft Windows network that uses DHCP, you must allocate a static IP address to the Cisco Unified Attendant Console Advanced server machine.
- Under Windows Server, the software must be installed in the following order:
  i. Microsoft .NET framework
  ii. SQL Server Standard or Enterprise
  iii. Cisco Unified Attendant Console Advanced

If, however, the server does not have an active internet connection, the .NET framework cannot be installed, and you must install it using the Microsoft Windows Deployment Image Servicing and Management (DISM) tool before starting the Cisco Unified Attendant Console Advanced installation.

Obtaining Cisco Unified Attendant Console Advanced Software

This section describes how to obtain Cisco Unified Attendant Console Advanced software.

Creating a Cisco Unified Attendant Console Advanced Downloads and Licensing Website User Account

To be able to download or license Cisco Unified Attendant Console Advanced software you require a valid account on the Cisco Unified Attendant Console Advanced Downloads and Licensing website.

To create an account on the Cisco Unified Attendant Console Advanced Downloads and Licensing website:

Step 1 Use your internet browser to go to http://www.cisco.com/go/ac.

Step 2 Under **New Users**, click **Register your details**.

The **Register** page is displayed.

Step 3 Complete the form and click **Register**.

Step 4 Either confirm your Reseller, or—if you are not listed—Add New Reseller.

Step 5 Click **Submit** to register your account.

A confirmation screen is displayed, and you are sent an e-mail containing your password to the website.

Downloading the Software

To download software from the Cisco Unified Attendant Console Advanced Downloads and Licensing website:

Step 1 Use your Internet browser to go to http://www.cisco.com/go/ac.

Step 2 Enter your **User Name** and **Password** and then click **Log In**.

Step 3 In the navigation bar, click **DOWNLOADS**.

Information about downloading, evaluating and activating software, and a list of software available for downloading is displayed.

Step 4 In the list, select the required software.

The versions of the selected software are displayed.

Step 5 Click **Download** for the software you want.

Step 6 When prompted for what to do with the file, click either **Open** or **Save**. Saving the file to a local area is recommended.

Adding Internet Information Service (IIS)

To add IIS to Windows Server 2019, do the following:

Step 1 Run Server Manager.

Step 2 Under the Dashboard, click **Add roles and features**.

The **Add Roles and Features Wizard** appears.

Step 3 In the **Before you begin** page, click **Next**.

Step 4 In the **Installation Type** page, select **Role-based or feature-based installation**, and then click **Next**.

Step 5 In the **Server Selection** page, select **Select a server from the server pool**, then select the server from the pool, and then click **Next**.

Step 6 In the **Server Roles** page, select the check box for the **Web Server (IIS)** role.

The **Add Roles and Features Wizard** dialog box appears.

Step 7 Select **Include management tools (if applicable)**, and then click **Add Features**.

Step 8 In the **Server Roles** page, click **Next**.

Step 9 In the **Features** page, if they are not already installed, under **.NET Framework 4.7 Features**, select:

- .NET Framework 4.7
- ASP.NET 4.7

and then click **Next**.

Note If adding IIS to Windows Server 2016, select **.NET Framework 4.6 Features**: .NET Framework 4.6 and ASP.NET 4.6.

Step 10 In the **Web Server Role (IIS)** page, click **Next**.

Step 11 In the **Role Services** page, select:

- Common HTTP Features
  - HTTP Errors
  - Static Contents
- Health and Diagnostics
  - HTTP Logging
- Performance
  - Static Content Compression
- Security
  - Request Filtering
- Management Tools
  - IIS Management Console

and then click **Next**.

Step 12 In the **Confirm installation selections** page, click **Install**.

Step 13 When installation is complete, click **Close**.

Installing and/or configuring SQL

Before you install Cisco Unified Attendant Console Advanced server, you must manually install Microsoft SQL Server onto the Publisher machine and - if you are installing a resilient system - the Subscriber server. For more information, see Server High Availability.

Note The instructions in this section refer to installing SQL Server Standard Edition. If you are using a different version or edition, or even different installation media, the steps may be slightly different. Perform the equivalent steps as described in your SQL Server user documentation.

Caution You must install SQL locally on the Cisco Unified Attendant Console Advanced server. Cisco Unified Attendant Console Advanced does not support external SQL Servers.

Installing SQL Server

To install SQL Server 2019:

Step 1 Log into the Cisco Unified Attendant Console Advanced server using a login with local administrator rights.

Step 2 Run the SQL Server Standard or Enterprise Edition Setup application.

Step 3 From the SQL Server Installation Center **Installation** page, click **New SQL Server stand-alone installation or add features to an existing installation**.

Step 4 Enter the product key, and then click **Next**.

Step 5 Accept the license terms, and then click **Next**.

Step 6 If all the rules pass the check, select **Use Microsoft Update to check for updates**, and then click **Next**.

The Setup Support files are installed.

Step 7 On the **Install Rules** page, the global setup support rules are checked. If all the rules have passed, click **Next**.

Note You can ignore any Windows Firewall warning at this stage.

Step 8 In the **Setup Role** page, select **SQL Server Feature Installation**, and then click **Next**.

Step 9 In the **Feature Selection** page, accept the default settings and select the following:

- Instance Features
  - **Database Engine Services > SQL Server Replication**
- Shared Features
  - **Client Tools Connectivity**
  - **Client Tools Backward Compatibility**

and then click **Next**.

Step 10 In the **Feature Rules** page, if the rules pass, the **Instance Configuration** page appears.

Step 11 Select the **Default instance**, and then click **Next**.

Step 12 Depending on the version of SQL Server you are installing, the **Disk Space Requirements** page may appear. If it does, click **Next**.

Step 13 In the **Server Configuration** page, do the following:

- Set the **SQL Server Agent** to run under the **NT AUTHORITY\SYSTEM** account (browse and enter the **SYSTEM** object name), and then set the **Startup Type to Automatic**.
- Set the **SQL Server Database Engine** to run under the **NT AUTHORITY\NETWORK SERVICE** account (browse and enter the **NETWORK SERVICE** object name), and then set the **Startup Type** to **Automatic**.
- Set the **SQL Server Browser Startup Type** to **Disabled** (the default).

And then click **Next**.

Step 14 In the **Database Engine Configuration** page:

- Set the **Authentication Mode** to **Mixed Mode** (the Cisco Unified Attendant Console Advanced server does not support Windows Authentication).
- Enter and confirm the default password, **Z1ppyf0rever**, for the SQL Server system administrator (sa) account.

  If you require a different user ID and/or passphrase, see SQL Server User Account Requirements before continuing.

Note To ensure password composition is supported, see Supported Windows, SQL Server, Active Directory, Presence Server, Application User and CUAC Password Characters.

- Click **Add Current User** to add your login to the SQL Server administrators list.

And then click **Next**.

Step 15 If the **Feature Configuration Rules** pass, the **Ready to Install** page appears.

Step 16 In the **Ready to Install** page, click **Install**.

Installation may take tens of minutes to complete.

Step 17 When the installation process is complete, click **Close**.

Installing SQL Server Management Studio

Step 1 Run the SQL Server Standard or Enterprise Edition Setup application from the same package used to install the SQL Server.

Step 2 From the **Installation** page in the **SQL Server Installation Center**, click **Install SQL Server Management Tools**. This loads a Microsoft download web page.

Alternatively, the download can be obtained by searching microsoft.com for **Download SQL Server Management Studio (SSMS)**.

Step 3 Click the **Download SQL Server Management Studio** link and save the file.

Step 4 **Run** the downloaded installer.

Step 5 Click **Install**. This loads the package installation and installs the required packages.

Step 6 Once the installation is complete, it prompts for a restart.

Licensing SQL Server

There are two methods of licensing SQL Server:

- Per processor license
- SQL Server and CALS license

It is at the Partners discretion which SQL license option is used. The SQL Server licensing requirements are described at SQL Server licensing requirements.

The Cisco Unified Attendant Console Advanced Server uses two SQL CALS, and each Cisco Unified Attendant Console Advanced client uses one SQL CAL.

Please consult your Microsoft representative if you want to license managed or hosted solutions.

High Availability (Resilient Installations)

Tip You may find it useful to print the following list and annotate it to keep track of your progress.

To install a resilient system, do the following:

Step 1 Ensure that the Console Client, Publisher and Subscriber machines are accessible using their hostname or NetBIOS name, and that these can be resolved to the correct IP Address.

Step 2 Log into the Publisher machine.

Step 3 Ensure that the machine date, time and time zone are correct.

Step 4 If you have a firewall on the Publisher server, configure Firewall Exceptions for:

- Windows Management Instrumentation (WMI)
- Port 135 (TCP) used by WMI

Note WMI calls use port 135 before choosing a random port. During the Resilience installation, the CUAC process uses WMI to connect to an alternate server. This port is only required during the installation/ uninstallation and replication configuration.

- Distributed Transaction Coordinator (MSDTC)
- Port 1433 (used by the SQL Server) – inbound and outbound
- Port 1859 (used for communication between the Cisco Unified Attendant Console Advanced
- client and server) – inbound and outbound
- Port 1864 (used by the BLF Plug-in) – inbound and outbound
- Ports 61616 and 61618, to enable messages to pass between the servers – inbound and outbound

Note When you configure an exception, you should also configure its scope settings; these define which computers are allowed to send traffic for an exception. Choose the scope appropriate to your network setting.

Step 5 Install the Cisco Unified Attendant Console Advanced server on the Publisher, as described in Cisco Unified Attendant Console Advanced Server Installation Procedure.

Step 6 Log into the Subscriber machine.

Step 7 Ensure that the machine date, time, and time zone are correct, and that they match those on the Publisher machine. Both servers must be in the same time zone to ensure that any daylight-saving time changes occur simultaneously. If they are not in the same time zone, the operator console will be unable to automatically reconnect to the Publisher when it recovers from failure.

Step 8 If you have a firewall on the Subscriber server, configure Firewall Exceptions for the same applications and ports as described for the Publisher server in Step 4.

Note When you configure an exception, you should also configure its scope settings; these define which computers are allowed to send traffic for an exception. Choose the scope appropriate to your network setting.

Step 9 Install the Cisco Unified Attendant Console Advanced server on the Subscriber, as described in Cisco Unified Attendant Console Advanced Server Installation Procedure.

Note

- Database replication is uninstalled automatically during Cisco Unified Attendant Console Advanced server installation or uninstallation. If the replication uninstall does not succeed at the first attempt, you are prompted to retry it or abort it.
- When installing or uninstalling resilient server software, both the Publisher and Subscriber server machines must be running. If either machine is turned off or inaccessible, the install or uninstall may fail.
- If the Publisher server software gets uninstalled, the Subscriber server's software link with the Publisher server gets broken. When you reinstall the Publisher server software you must then reinstall the Subscriber server software to restore the link.

Export Crypto Key File

You can use Cisco Unified Attendant Administration to back-up the Publisher's cryptographic keys and registries. This UI only appears on Publisher, but the backup-up key archive should be copied to Subscriber.

To export the cryptographic key file to your computer:

Step 1 Log into Cisco Unified Attendant Administration.

Step 2 Go to **Help** > **Export Crypto Key File**.

Step 3 Type your passphrase and click **Export**.

Step 4 Choose a location on your computer to **Save** the file in a .zip format.

You will import the crypto key file during installation onto the Subscriber server, as described under Cisco Unified Attendant Console Advanced Server Installation Procedure in Step 17.

Note Always keep a backup of the exported crypto key file in case you have to migrate the server to another machine. Without this file, encrypted passwords cannot be recovered.

Cisco Unified Attendant Console Advanced Server In-place Upgrade Procedure

This section applies to in-place upgrades of Cisco Unified Attendant Console Advanced executed on the server hosting the pre-existing installation of Cisco Unified Attendant Console Advanced. For instruction regarding migrating to a new server (same or later version), see Cisco Unified Attendant Console Advanced Migration and/or Upgrade.

Step 1 Confirm that all pre-requisites are satisfied on the server.

Step 2 Backup the publisher server ATTCFG and ATTLOG databases; see Manually Backing-up Databases.

Step 3 Backup the Crypto key export from the server; see Export Crypto Key File.

Step 4 To install the upgraded Cisco Unified Attendant Console software; see the installation procedure below.

Cisco Unified Attendant Console Advanced Server Installation Procedure

Note If you are installing a high availability (resilient) system, you must perform this installation procedure on both the Publisher and Subscriber servers, starting with the Publisher. See High Availability (Resilient Installations) for requirements specific to high availability (resilient) deployments.

To install a Cisco Unified Attendant Console Advanced server:

Step 1 Log in to the machine hosting the server, using a login with local administrator rights.

Step 2 Browse to the folder where the downloaded installation files are saved.

Step 3 Double-click the setup program.

Note If they are not already installed, all required third-party applications are now automatically installed, including the latest Microsoft .NET Framework. If, however, the server does not have an active Internet connection, the Microsoft .NET Framework cannot be installed, and you must install it using the Microsoft Windows Deployment Image Servicing and Management (DISM) tool before continuing with the Cisco Unified Attendant Console Advanced installation. These installations may take several minutes. You are prompted to restart your computer afterwards.

Step 4 If a page listing required software appears, click **Install**.

The software is installed; this may take several minutes. If you are then prompted to restart your computer, click **Yes**.

Step 5 When your computer restarts there may be more items to install. Repeat Step 4 and Step 5 until all the require software is installed.

The Wizard is prepared, and you are presented with the Welcome page.

Step 6 In the Wizard welcome page, click **Next**.

Step 7 In the **Registration Information** page, type or accept the license holder **Name** and **Company Name**, and then click **Next**.

Step 8 In the **SQL Server Login Information** page, type the SQL Server Username (default is **sa**) and Password (default is **Z1ppyf0rever**), then click **Next**.

If you require a different user ID and/or passphrase, see SQL Server User Account Requirements before continuing.

Step 9 In the **Resilient Server Mode** page, click either:

- **Publisher Server**, to install the Publisher server, then continue from Step 12. This is the default selection. If you are installing a non-resilient system, this is the only server you need to install.
- **Subscriber Server**, to install the Subscriber server in a resilient installation.

Note

If you select **Publisher Server**, the following checks and actions are performed:

- If there is no SQL Server on the Publisher server, SQL Server Standard is installed, and a message is displayed telling you that you need to upgrade your SQL Server if you intend to have a resilient installation.
- If SQL Server Express is already installed on the Publisher server, a message is displayed telling you that you need to upgrade your SQL Server if you intend to have a resilient installation. You can either abort installation at this point, to upgrade SQL Server before installing Cisco Unified Attendant Console Advanced, or you can continue with the Cisco Unified Attendant Console Advanced installation, and then upgrade SQL Server later.

If you select **Subscriber Server**, and if SQL Server Express is installed on the Publisher server, the Subscriber server installation is blocked, and you are prompted to upgrade the SQL Server installation on the Publisher server.

Step 10 *This step applies only when you are installing onto the Subscriber server*.

In the **Server Resilience Trial** page, note the information about purchasing a server resilience license, and then click **Next**.

Step 11 *This step applies only when you are installing onto the Subscriber server*.

In the **Publisher SQL Server Information** page, enter the following information about the SQL Server installed on the Publisher machine that you want to communicate with the Subscriber server you are installing:

- **Server Name** — the machine hosting the Publisher
- **Username** — the SQL Server user name (default is sa)
- **Password** — the SQL Server password

and then click **Next**.

If the servers are unable to communicate, verify that the Windows firewall is either off or configured as described in Step 4.

Step 12 In the **Server Information** page, type the Cisco Unified Attendant Console Advanced Server Machine **Name** onto which you are installing the software, and then click **Next**.

Step 13 To install a Publisher server, continue from Step 14.

To install a Subscriber server:

a. When prompted to allow the Wizard to stop the services on the Publisher, click **Yes**.

b. When prompted for the credentials of the Publisher server to communicate with, enter the **Windows Username** (computer name \ user name) and **Password** of your Publisher administrator login, and then click **Next**.

Note To ensure password composition is supported, see Supported Windows, SQL Server, Active Directory, Presence Server, Application User and CUAC Password Characters.

Note If leveraging a Windows account other than the default hostname/administrator or domain administrator account, a registry modification is required on the publisher and subscriber Cisco Unified Attendant Console Advanced servers. The change immediately goes into effect.

1. Open RegEdit.
2. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.
3. Look for an existing key called LocalAccountTokenFilterPolicy. If it does not already exist, do the following:
    a. Right-click and select New > DWORD (32-bit) Value.
    b. Input Name: LocalAccountTokenFilterPolicy.
4. Double-click the line item and select Hexadecimal.
5. Input Value: 1, and then click OK.
6. Close RegEdit and proceed as required.

Step 14 In the **Cisco Unified Communications Manager (CUCM)** connection details page, type the Cisco Unified Communications Manager machine **IP Address**, your **CUCM Application User ID** and **Password**.

If you would like to skip TSP, check **Skip TSP Download and Installation** and then click **Next**. A pop-up shows up to confirm you want to skip TSP. If you have entered incorrect details on purpose (for example, the details of an upcoming CUCM upgrade), you can still proceed. If you have entered incorrect details accidentally, click **Cancel** to fix them, and then click **Next** until the end.

Note The Application User account specified by the User ID must already exist on the Cisco Unified Communications Manager. Creating a Cisco Unified Communications Manager User ID is described in Creating and Assigning an Application User.

If you are installing a Subscriber server, you must enter a different CUCM Application User ID than the one used for the Publisher server. To find out more about resilience and about how to achieve CUCM resilience in conjunction with Cisco Unified Attendant Console Advanced resilience, refer to the *Cisco Unified Attendant Console Advanced Design Guide*.

Step 15 In both security alert messages, click **Yes**.

Step 16 *This step applies only if you have downloaded and installed TSP*.

In the Cisco TSP Information page, select and enter either the **IP Address** or **Host Name** of the **Primary CTI Manager**. If you have one, enter the details for the **Backup CTI Manager**, and then click **Next**.

Note If it is not already installed, the installation process automatically installs the appropriate Cisco TSP version.

Step 17 *This step applies only when you are installing onto the Subscriber server*.

Use the crypto key file exported from the Publisher as described in Export Crypto Key File to import it onto the Subscriber. Enter the **Passphrase,** if necessary, **Browse** for the crypto key file, select it from your computer, and then click Next.

Step 18 In the **Call Logging** page, select either:

- **Enable Call Logging** (the default)
- **Disable Call Logging**

and then click **Next**.

Step 19 In the **Choose Destination Location** page, either accept the default destination folder or **Browse** to where you want to install the files, and then click Next. This destination is for software files only. The database is configured under the *C:\DBData* folder.

Step 20 In the **Start Copying Files** page, click **Next**.

The Cisco Unified Attendant Console Advanced server is installed. The database wizard then runs.

Step 21 In the **Database Wizard**, click **Next**.

Note During database creation, the server driver media setting is set according to the CUCM version detected by the server installer.

If you are upgrading the software, your system already contains a configuration database and a logging database, and you are prompted to overwrite each in turn:

- Click **Yes** to create a new, empty database. This will delete all your server settings, including queues and CTI port numbers.
- Click **No** to upgrade the existing database, retaining all your server settings.

Step 22 When the wizard has installed the Configuration and Logging databases, and updating the registry, click **Finish**.

Cisco Unified Communications Manager TSP is configured.

Step 23 If any third-party applications that might interfere with the TSP configuration are running, you are prompted to close and automatically restart them. Accept this option and click **OK**.

If you receive a message saying that setup was unable to close the applications, click **OK**.

Step 24 In the Wizard Complete page, select *Yes, I want to restart my computer now*, and then click **Finish**.

Your computer restarts, with the Cisco Unified Communications Manager server installed.

Disabling Plug-ins that are not in use

If you are not using the Cisco Unified Attendant Presence Plug-in or the Cisco Unified Attendant LDAP Plug-in you can harden the Cisco Unified Attendant Console Advanced system by stopping them, as described in Service Management.

Disable Cisco Unified Attendant Console Server plug-ins that are not in use to eliminate unnecessary server resource consumption and to harden the system.

This applies to:

- Cisco Unified Attendant LDAP Plug-in: used to sync contacts from external sources.
- Presence Plug-in: used to retrieve contact presence from Cisco IM & Presence and WebEx Messenger.

To disable plug-ins:

Step 1 Click **Start**, type *services.msc*, and then press **Enter**.

Step 2 Right-click the related service, and then select **Properties**.

Step 3 From the Startup type drop-down menu select **Manual**, and then click **Apply**.

Step 4 Click **Stop**, then click **OK**.

Installing Cisco Unified Attendant Console Advanced Client

Note

- If you are upgrading your software, any configured user preferences are maintained.
- If you upgrade from any older version to Cisco Unified Attendant Console Advanced 14.0.1.x, you must enter all existing administrator account and operator profile passphrases in CAPS. For Cisco Unified Attendant Console Advanced version 14.0.2 and above, administrator account is not case-sensitive; however, passphrases remain case-sensitive.

Note

Before installing Cisco Unified Attendant Console Advanced you must satisfy the following prerequisites:

- Ensure that the Console Client, Publisher and Subscriber machines are accessible using their hostname or NetBIOS name, and that these names are resolvable to the correct IP Address.
- If you have a firewall on the client PC, configure firewall exceptions for:
  - Port 1433 (used by the SQL Server)
  - Port 1859 (used by the Cisco Unified Attendant Console Advanced server)
  - Port 1863 (used by the IM&P server)
  - Port 1864 (used by the BLF Plug-in)

When you configure an exception, you should also configure its scope settings; these define which computers are allowed to send traffic for an exception. Choose the scope appropriate to your network setting.

To install Cisco Unified Attendant Console Advanced client:

Step 1 Login as a user with administration rights.

Step 2 Browse to the folder containing the installation files downloaded in High Availability (Resilient Installations).

Step 3 Double-click the setup program.

The Wizard is prepared, and you are then presented with the Welcome page.

Step 4 In the Welcome page, click **Next**.

Step 5 In the **Choose Destination Location** page, accept the default destination: C:*Program Files (x86)\Cisco*\.

To install the application to a different location, click **Browse** and select a different location. Click **Next** to proceed.

Step 6 In the **Server Information** page, enter the host name of the machine running the Cisco Unified Attendant Console Advanced server (the Publisher server), and then click Next. If your previous installation used the IP address of the server, you are prompted to enter the corresponding host name. This information is required so that Cisco Unified Attendant Console Advanced client can talk to the server properly.

Step 7 In the **Language Information** page, select the language to use for the application, and then click **Next**.

Step 8 In the **Icon Information** page, if you want to be able to start the Console from the desktop, select **Add Icon to Desktop** to place the Cisco Unified Attendant Console Advanced icon on your desktop, and then click **Next**. The **Start Copying Files** page lets you review the information you have entered.

Step 9 If you are happy with the settings, click **Next** to copy the files and install the software.

Step 10 In the installation completed page, click **Finish**.

Installing JAWS Scripts for Visually Impaired Operation

Note

- Console Operators must be assigned the VIOC role to use JAWS. For more information, see Operator Management.
- Operating the Cisco Unified Attendant Console Advanced with JAWS via a Remote Desktop connection is not supported due to the user experience being significantly degraded.

The Cisco Unified Attendant Console Advanced client can be used with JAWS screen reader version 2022 on Windows 10 and Windows 11; previous versions of JAWS (18, 2018, 2020, 2021) are supported on Windows 10 only.

For JAWS to work correctly, do the following after installing the Cisco Unified Attendant Console Advanced client:

Step 1 Copy the files from the following folders:

C:\Program Files (x86)\Cisco\Attendant Console\Accessibility Scripts\<language>

where the <language> folder is either English or Spanish.

Note If you did not install Cisco Unified Attendant Console Advanced in the default location, look for the equivalent folders.

Step 2 Navigate to *\Users\<userid>\AppData\Roaming\Freedom Scientific\JAWS\<Version of JAWS being used>\Settings\<language (enu = English)>*. For example, *\Users\JohnDoe\AppData\Roaming\Freedom Scientific\JAWS\2022\Settings\enu*.

Note If the Cisco Unified Attendant Console scripts are pasted in any additional Freedom Scientific\JAWS repositories, JAWS will fail to utilize the custom scripts.

Step 3 Paste the files copied in Step 1 to the repository in Step 2.

Step 4 If running, close Cisco Unified Attendant Console and JAWS.

Step 5 Launch the JAWS application, and then launch Cisco Unified Attendant Console.

Silent Installing Cisco Unified Attendant Console Advanced

If necessary, you can also perform a silent installation. To obtain the Cisco Unified Attendant Console Advanced installer and the Silent Install package, do the following:

Step 1 Navigate to cisco.com/go/ac.

Step 2 Create an account or log in.

Step 3 Select **Downloads** from the left navigation pane.

Step 4 Select **Cisco Unified Attendant Console Advanced**.

Step 5 Download the required version.

Step 6 Download the silent install package *CUACA_Client_Silent_Install*.

To perform a silent installation, do the following:

Step 1 Unzip and prepare the silent install repository. This is the package that you use to create the silent install answer file, as well as to subsequently deploy the package.

a. Unzip the *CUACA_Client_Silent_Install* package and move the enclosed *CUACA_Client_Silent_Install* repository to the parent drive (default C:\) on the workstation used to create the answer file.

b. Unzip the Cisco Unified Attendant Console Advanced package and move the *...\Attendant Console\<<version>>\CUACA_Setup.exe* file to the enclosed folder at *C:\CUACA_Client_Silent_Install* (default).

Step 2 Create the answer file to be used to execute the silent installs. The answer file records all inputs from an install effort, which are then used as a roadmap for the silent install process.

Note If you are using a repository other than the default C:\CUACA_Client_Silent_Install, you must edit the repositories in the *createISS.bat* file before moving forward. To do so, right-click *createISS.bat*, click **Edit** and then modify the location as required. Further instructions will refer to the default location of C:\CUACA_Client_Silent_Install for simplicity purposes.

a. Using full administrative rights, open **Command Prompt/Powershell**.

b. Navigate to the *C:\CUACA_Client_Silent_Install* folder.

c. Type the command *createISS.bat* in the command window and press Enter to execute the batch file. This launches the installer.

d. Provide the inputs required for the subsequent silent installs.

Once the process completes, two new files are added to the *C:\CUACA_Client_Silent_Install* repository, *CUACA_Opr_New.iss* and *createISS.log*.

Step 3 Perform a readiness review. At this point, the *C:\CUACA_Client_Silent_Install* folder should contain the following files. This complete package is used to execute silent installations.

- createISS.bat
- CUACA_Opr_New.iss
- CUACA_Setup.exe
- runSilent.bat

Note The previously generated .log files are not necessary for installation.

To modify the answer file for the purpose of installing with a different localized language, right-click the *CUACA_Opr_New.iss* file, and then click **Edit**. Replace the existing language key with any one of the following, as required:

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Danish
- Dutch
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese
- Russian
- Spanish
- Swedish.

Step 4 Prepare to execute the silent installation by copying the packaged *CUACA_Client_Silent_Install* repository to the parent drive of the target machine, default :C\.

To leverage an alternate repository, right-click *RunSilent.bat* file and click **Edit**. Modify repositories to reflect the alternate location.

Step 5 Finally, execute the *RunSilent.bat* batch file using full administrative rights:

- Group Policy
- Command Prompt/Powershell

a. Using a windows login with local administrative permissions, navigate to your *CUACA_Client_Silent_Install* repository.

b. While holding the Shift key, right-click any of the open white space within the repository, and then select **Open Command Window Here**.

c. Type *runSilent.bat*, and then press the **Enter** key to execute the batch file.

Cisco Unified Attendant Console Administration

Cisco Unified Attendant Console Administration is a web-based tool that administrators use to configure Cisco Unified Attendant Console Advanced server, which, in turn, determines how Cisco Unified Attendant Console Advanced operates. The configuration is stored in a Microsoft SQL Server database.

Administrator Login

Cisco Unified Attendant Console Advanced Administration is accessible only to administrators. The default user name is ADMIN and the default passphrase is CISCO (the passphrase is case-sensitive).

Note If you are using Cisco Unified Attendant Console Advanced up to and including version 14.0.1.x, you must enter all existing administrator account and operator profile passphrases in CAPS. For Cisco Unified Attendant Console Advanced version 14.0.2 and above, administrator account is not case-sensitive; however, passphrases remain case-sensitive.

Logging On

To log on to Cisco Unified Attendant Console Advanced Administration:

Step 1 In an Internet browser, enter the URL specified by your network administrator to access Cisco Unified Attendant Console Advanced Administration. This has the format: *https://<<ip address of Cisco Unified Attendant Console Advanced server>>/WebAdmin/login.aspx*.

For example, *https://209.165.200.224/WebAdmin/login.aspx*.

If you are logged in to the Cisco Unified Attendant Console Advanced server, use localhost instead of the IP address. For example, *https://localhost/WebAdmin/login.aspx*.

Note A certificate warning will appear when accessing Cisco Unified Attendant Console Administration using an IP address, or from a machine other than the Cisco Unified Attendant Console Advanced server. This is due to a self-signed certificate being deployed during installation. You can replace this with your own certificate to avoid the warning. For more details, see Database Management.

The **Login** page opens.

Note Internet Explorer compatibility mode is not supported by Cisco Unified Attendant Console Administration.

Step 2 Enter your **Username** (not case-sensitive). The default is ADMIN.

Step 3 Enter your **Passphrase** (case-sensitive). The default is CISCO.

Note
- To clear the contents of the **Username** and **Passphrase** fields, click **Reset**.
- If you change the **Username** on the Publisher server, you have to relogin on the Subscriber server for the changes to take effect.

Step 4 Click **Login**.

The home page is displayed.

Note If a **Customized Logon Message** is configured, you are required to accept the terms before and/or after you click **Login**. For more information, see Last Login Info.

Logging Out

To log out from Cisco Unified Attendant Console Advanced Administration and end your session immediately, click **Logout** at the right-hand end of the application banner.

If you simply close the browser - by clicking the window Close button - rather than by logging out, the session does not expire for 5 minutes, which is the session timeout limit. Consequently, if the maximum number of sessions are in progress and a user closes the browser rather than logging out, anyone who attempts to log in during the next 5 minutes receives a *Session limit exceed* message and cannot log in. Only when the session times out can a new user log in.

Home Page

The Cisco Unified Attendant Console Advanced Administration home page contains the main menus for configuring the application, and the software version numbers and the registration status.

You can use the **Navigation** controls at the top right of the page to access the following functions:

- Cisco Unified Replication—For more information, see Cisco Unified Attendant Console High Availability.
- Cisco Unified Reporting— For more information, see Cisco Unified Reporting.

Note The minimum supported screen resolution specifies 1024x768. Devices with lower screen resolutions may not display the applications correctly.

Menu Options

The Cisco Unified Attendant Console Advanced Administration menus are:

- **Engineering**—control and configure connectivity and support management. For more information, see Cisco Unified Attendant Console Administration - Engineering.
- **System Configuration**—manage synchronization of devices and queues with Cisco Unified Communications Manager. For more information, see Cisco Unified Attendant Console Administration – System Configuration.
- **User Configuration**—manage Cisco Unified Attendant Console Advanced configuration. For more information, see Cisco Unified Attendant Console Administration – User Configuration.
- **Bulk Administration**—use this menu to upload files, as well as insert, update and delete contacts. For more information, see Cisco Unified Attendant Console Administration – Bulk Administration.
- **Help**—view help on Cisco Unified Attendant Console Advanced Administration and licensing the applications. For more information about the Help menu, see Help. For more information about licensing the software, see Licensing Cisco Unified Attendant Console Advanced.

Toolbar

When you select a menu option a new page is displayed where you configure that aspect of the Cisco Unified Attendant Console Advanced server. Each of these pages includes a toolbar, which contains one of more of the following icons:

Icon	Function
	Add or install an item.
	Remove or uninstall an item.
	Save.
	Reset Passphrase.
	Test Connection or Validate Replication.
	Monitor Replication.
	Repair Database or Repair and Purge Database.
	Directory Field Mappings.
	Directory Rules.
	Database Repair Report or Replication Report.
	Select All (on page) or Select All In Search (including any other pages of results).
	Clear All (on page) or Clear All In Search (including any other pages of results).

Icon	Function
	Delete Selected (Queue/Operator Management).
	Calendar (select a date).
	Start Server.
	Stop Server.
	View information for a service.
	Refresh service display.
	Synchronize directory with Cisco Unified Communications Manager or Re-initialize Replication.
	Set out of hours routing for a queue.

Data Entry Fields

Most pages contain data entry fields with the following properties:

- The valid range or types of characters for each parameter are displayed to the right of the field in red
- Invalid input in any field is denoted by a red asterisk.

Note

Pressing **Backspace** when the cursor is anywhere other than a data entry field displays the previous page.

Accessibility for Users with Disabilities

Cisco Unified Attendant Console Advanced Administration includes features that make it easier for blind and visually impaired users.

- All controls are labeled and have a tool tip. The controls are described in Toolbar.
- Context-sensitive help for every page.
- Attendants can use Cisco Unified Attendant Console Advanced with a screen reader plug-in called JAWS. The screen reader provides the attendant with information on the Cisco Unified Attendant Console Advanced status and the text in the windows. For how to set up JAWS, see Installing JAWS Scripts for Visually Impaired Operation.
  - Console Operators must be assigned the VIOC role to use JAWS. For more information, see Operator Management.

For more information on the Cisco Accessibility Program visit Accessibility at Cisco.

Help

Contents/This Page

Click **Contents** to open the complete help file or click **This Page** from any page in the Administration to open its specific help file page.

Licensing

Go to **Help > Licensing** to see the Licensing Management page. This page lists your active **Licenses** and **Product Details**. Use this page to upload your **Registration File** in RGF format. For more information on licensing, see Licensing Cisco Unified Attendant Console Advanced.

Export Crypto Key File

You can use Cisco Unified Attendant Administration to back-up the Publisher's cryptographic keys and registries. This UI only appears on Publisher, but the backup-up key archive should be copied to Subscriber.

To export the cryptographic key file to your computer:

Step 1 Log into Cisco Unified Attendant Administration.

Step 2 Go to **Help > Export Crypto Key File**.

Step 3 Type your passphrase and click **Export**.

Step 4 Choose a location on your computer to **Save** the file in a .zip format.

You will import the crypto key file during installation onto the Subscriber server, as described in Step 17.

Note Always keep a backup of the exported crypto key file in case you have to migrate the server to another machine. Without this file, encrypted passwords cannot be recovered.

Last Login Info

You can view the date and time of the last successful and unsuccessful log in attempts, and the IP address of the machines from which they were made.

To view the last login information, choose **Help > Last Login Info**.

The **Last Login Information** page contains the following **Last Successful Login Info** and **Last Unsuccessful Login Info**:

- **Machine IP** (address)
- **Last Login Date/Time** (UTC)

You can also view an individual operator's last login date and time by choosing **User Configuration > Operator Management**, and then selecting the operator.

Note

In both cases of **Last Login Date/Time** (UTC), the time displayed is that of the UTC time zone, and not the time zone of the web browser machine.

About

Click **Help > About** to see some basic information about the Cisco Unified Attendant Console Advanced Administration, like the license, system version and administration version.

Cisco Unified Attendant Console Administration - Engineering

The following chapter describes how to configure the Engineering menu options in Cisco Unified Attendant Console Administration.

Engineering Menu

The Engineering menu provides connectivity and support management facilities

Server Management

Note This Engineering menu is not available if you have a non-resilient installation.

The databases in the Publisher and Subscriber server machines contain a Server Details table.

If you have a high availability license, you can change some of these details using the Server Management option.

To change server details:

Step 1 Choose **Engineering > Server Management**. The **Server Management** page is displayed.

Step 2 Under **Server Details**, select the server to manage.

Step 3 Enter the following values:

- **Reconnection Delay (msecs)**—reconnection delay in milliseconds. Default Value 90000. You must enter a value.
- **Buffer Duration (secs)**—buffer duration in seconds. Default Value 259200. You must enter a value.

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

Database Management

The configuration database is created when you install the Cisco Unified Attendant Console Advanced server. The Database Management option enables you to connect to the configuration database, to test the connection and to repair the database.

If you have a resilient Cisco Unified Attendant Console Advanced installation, you cannot connect to a different database. On a non-resilient installation, you can connect to and use a different database, and the page contains a **Save** button, which enables you to save the changed configuration.

To connect to the database:

Step 1 Go to **Engineering > Database Management**.

Step 2 On a resilient system, you can test or repair the databases on either the Publisher or Subscriber server; under **Server Details**, click the server as appropriate.

Step 3 In **Server**, type the name or IP address of the machine where the Microsoft SQL Server is installed. For example, 209.165.202.128.

Step 4 Type your SQL Server **Username**. If Microsoft SQL Server was installed using the Cisco Unified Attendant Console Advanced server Installation Wizard, the user name is **sa**.

Step 5 Type your **Password**. If Microsoft SQL Server was installed using the Cisco Unified Attendant Console Advanced server Installation Wizard, the password is **Z1ppyf0rever**.

Step 6 If you have a non-resilient system, click **Save**, to save your new database selection.

There is no **Save** button in a resilient Cisco Unified Attendant Console Advanced Administration installation.

Step 7 You are prompted that Cisco Unified Attendant Console Advanced server must be restarted for the changes to take effect. Select the option to restart the server immediately.

Test the Database

To test the specified database, click **Test Connection**.

Repair the Database

To repair the specified database, click **Repair Database**.

Before repairing the database, Cisco Unified Attendant Console Advanced Administration must stop the server. After the database is repaired you must manually restart the server service. If you have repaired the database, you can view a repair report by clicking **Database Repair Report**. This opens a window that displays the following information:

- Database Name
- SQL Server

- Activity Start Date
- Activity End Date
- Status
- Error Code
- Error Description

Database Purge

The Database Purge option enables you to purge old call logging and operator session information from the database. If the logging database becomes full, some features and services may fail.

To determine the size of your SQL database, run SQL Management Studio, right-click ATTLOG, and then choose **Reports > Standard Reports > Disk Usage**.

Note

- We recommend that before purging the database you stop all Cisco Unified Attendant Console Services and restart the MSSQLSERVER and MSSQLSERVER Agent (HA deployments only) services from the *services.msc* menu; this will free server resources for the purge process and lessen the impact on the live production environment.
- For best results, purge data in groups of 1-3 months, depending on the amount of data to be purged.
- Only one single account at a time can perform a database purge.

To purge the database:

Step 1 Go to **Engineering > Database Purge**.

Step 2 Enter **Start date** either by entering the format yyyy-mm-dd (year-month-date) or click the calendar and select it from there.

Step 3 Enter **End date** either by entering the format yyyy-mm-dd (year-month-date) or click the calendar and select it from there.

Step 4 Click **Purge Database**.

Step 5 If you have purged the database, you can run a report by clicking **Database Purge Report**. This opens a window containing the following information:

- SQL Server name
- Executed by
- Activity Date (date of purge)
- Purge Start Date (date of oldest record to purge)
- Purge End Date (date of youngest record to purge)
- Table Name
- Rows Effected (the number of records removed)
- Status (usually Completed)
- Error Code (if the purge didn’t complete)
- Error Description (if the purge didn’t complete)

Automatic Purge

If auto-purge is enabled on Publisher, the user will not be able to run a manual purge. An error message will be displayed.

Auto-purge will be disabled on Subscriber; however, users will be able to run manual purges as before and no warning message will be displayed.

If auto-purge is not enabled on the Publisher, the user will be able to run a manual purge. Auto-purge will be disabled on Subscriber; however, users will be able to run manual purges as before and no warning message will be displayed.

Replication is bidirectional on Log Database, so regardless of whether you run a purge from Publisher or Subscriber, data will be replicated across, and should work as before.

Caution **If auto-purge is enabled, do not schedule directory synchronization to execute at midnight, because auto-purge runs at midnight every day.**

If auto-purge is disabled, directory synchronization can be run at midnight.

Service Management

The Service Management option enables you to start, stop, and check the status of the following server services:

- Cisco Unified Attendant Server
- Cisco Unified Attendant BLF Plug-in
- Cisco Unified Attendant LDAP Plug-in
- Cisco Unified Attendant Presence Plug-in.

Note If you are not using LDAP or Presence, you can harden the Cisco Unified Attendant Console Advanced system by disabling the plug-ins using the Service Control Manager (SCM).

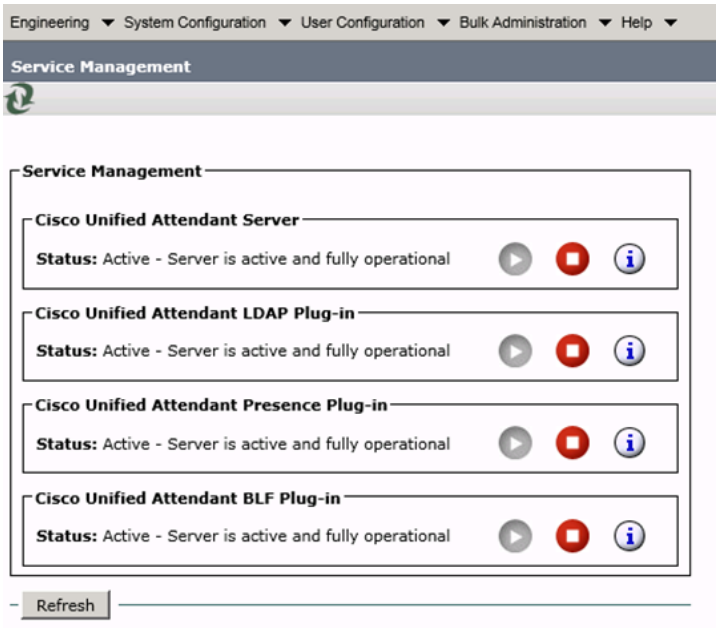
To use the LDAP or Presence Plug-ins, set the startup type of the required service to **Automatically**. If the services are disabled and you try to start them from Web Admin, you will see an error.

To manage a service:

Step 1 Go to **Engineering** > **Service Management**.

Note If you have a resilient installation and are logged into the Subscriber server, the LDAP Plug-in is not displayed.

Figure 3 Service Management Page



Step 2 Use the following controls as appropriate.

Control	Icon	Description
Start Server		Start the server.
Stop Server		Stop the server.
Information		View the server activity and status.
Refresh		Update the page.

The following information about the server and its connections is displayed.

Status	Description
Connected	The server and databases are connected.
Not Connected	The server and databases are not connected.
Standby	Logging Database only. The connection between the service and the Logging Database is not in use.

The data displayed depends on which server you choose.

Cisco Unified Attendant Server Status

The following are displayed for the Cisco Unified Attendant (Console) server:

- The Server Activity of Active Calls and Logged-in Operators.
- The status of the following servers:
  - BLF-Plug-in — status of connection between Attendant Server and Attendant BLF plug-in
  - Configuration Database
  - Logging Database
  - Network — event network
- The Resilience Status (only with resilient installations):
  - The Inter Server Communication Status shows the status of the link between the Publisher and Subscriber servers.
  - The Publisher Failover Status shows the status of the Publisher server.
  - The Subscriber Failover Status shows the status of the Subscriber server.

Cisco Unified Attendant LDAP Plug-in Status

Note If you have a resilient installation and are logged into the Subscriber server, you do not have access to the LDAP Plug-in status.

The following are displayed for the Cisco Unified Attendant LDAP Plug-in:

- The Server Activity of Active Sources and Active Synchs
- The status of the following servers:
  - Primary Server
  - Configuration Database

Cisco Unified Attendant Presence Plug-in Status

The following are displayed for the Cisco Unified Attendant Presence Plug-in:

- The **Server Activity**, consisting of active presence **Subscriptions** and **Connected Users** (Console clients and Web Admin itself).
- The status of the **Unified CM** server and the **WebEx** server.
- **Comms** — the Presence server port status
- **Database** — the configuration database connectivity status
- If your Cisco Unified Attendant Console Advanced is running in resilient mode, the **Inter Server Communication Status** is also shown (the status of the link between the Publisher and Subscriber servers).

Cisco Unified Attendant BLF Plug-in Status

The following are displayed for the Cisco Unified Attendant BLF Plug-in:

- The Server Activity of Subscriptions and Connected Users
- The status of the following servers is displayed:
  - CT Link
  - DRM
  - Comms
  - Database — the configuration database connectivity status
- If your Cisco Unified Attendant Console Advanced is running in resilient mode, the Inter Server Communication Status is also shown (the status of the link between the Publisher and Subscriber servers).

Presence Management

Use the Presence Management page to select the driver for your default presence source (the source of the presence information displayed by default in the Console clients), and to configure the link to any source.

Configuration

To configure a presence source:

Step 1 Go to **Engineering** > **Presence Management**.

The **Presence Management** page is displayed, listing all the presence drivers that satisfy the Find filter.

Step 2 If required, **Find** the presence source to configure.

These drivers are available:

- **Unified CM (IM and Presence)**
- **WebEx (IM and Presence)**
- **Skype Local**

An ID in the **Presence User ID** column shows that the driver has been configured and is connected to the presence server.

A **Yes** in the **Default Driver** column shows which (if any) of the drivers is providing all the clients with their default presence data.

Note

- If you are using Cisco Unified CM (IM&P) the Cisco Unified Attendant Presence Plug-in has to be added to the firewall information on the Communications Manager.
- If you are not using Presence data, you can make your Cisco Unified Attendant Console Advanced system more secure by disabling the associated plug-in using Service Management, as described under Service Management.

Step 3 Click **Select** alongside the presence driver and source to select or configure.

The connection details are displayed.

Step 4 If you have a resilient installation, select the **Server Details** of the Publisher or Subscriber to configure that server.

Step 5 Under **General**, select the **Presence User ID** - the Console directory field containing the user ID for this presence source - and, if required, type the **Domain** necessary for your configuration, which is appended to the ID from the directory field. To make this source the one displayed by default in the Console client, select **Default driver**.

Note The **General** section is the only section available when you configure Skype Local.

Step 6 Under Connectivity, type the following:

- The **Host name** or **IP** address of the presence source. To disable a source, simply blank out this field.
- The **Host port**, in the range 0 to 65535. The default is 5222.
- The **End user**, in the format user@domain.
- The end user **Password**.

Step 7 To use TLS encryption on the connection, select **TLS**.

Step 8 To test the connection without saving the settings, click **Test Connection**. A message appears telling you the result of the test. If the test fails, check that you have entered the correct parameter values.

Note **Test Connection** is not available when you configure Skype Local.

Step 9 Click **Save**. The settings are tested and, if the test is successful, the settings are saved.

When you have configured the driver, use **Service Management** to stop and then restart the Cisco Unified Attendant Presence Plug-in so that it uses the new settings.

CUCM Connectivity

The Cisco Unified Communications Manager connection is essential to enable system devices to be configured automatically on Cisco Unified Communications Manager.

If the media driver configuration does not match the Cisco Unified Communications Manager version, the Cisco Unified Attendant Console Advanced Server will not start and the BLF Plug-in will not be able to establish a CTI channel. Cisco Unified Attendant Console Advanced Administration can detect any differences and correct them for you.

The **CUCM Connectivity** option enables you to set up and test the Cisco Unified Communications Manager connection. It also detects what Cisco Unified Communications Manager you are connected to and automatically changes the media driver configuration so that the correct one is used.

Note If you have a resilient installation, you can make changes only when logged into the Publisher machine. If you are logged into the Subscriber machine, the data is read-only, and you cannot change anything.

The Publisher and Subscriber servers must have different Cisco Unified Communications Manager

users.

To set up and test the Cisco Unified Communications Manager connection:

Step 1 Go to **Engineering > CUCM Connectivity**.

The Cisco Unified Attendant Console Advanced Server validates its internal driver settings against the Cisco Unified Communications Manager Release.

Step 2 If the media driver is correct, continue at Step 3.

If the media driver is incorrect, a message is displayed:

- If you have either a non-resilient installation, or a resilient Cisco Unified Attendant Console Advanced installation and are logged in to the Publisher, the message says:

  Attendant Admin detected that the media driver configuration for the selected Cisco UAC Advanced server did not match your CUCM version and has changed the media driver configuration to match your CUCM version. Please restart Attendant Console services of selected Cisco UAC Advanced server for this change to take effect.

  Follow the instructions in the message.

- If you have a resilient Cisco Unified Attendant Console Advanced installation and are logged in to the Subscriber, the message says:

  Attendant Admin has detected that the media driver configuration for the selected Cisco UAC Advanced server does not match your CUCM version. Please use Publisher Attendant Admin to correct the media driver configuration for the selected Cisco UAC Advanced server. You also need to click on other Cisco UAC Advanced servers to make sure that the media driver configuration for other servers is correct.

  Follow the instructions in the message.

Step 3 On a resilient Cisco Unified Attendant Console Advanced Administration installation, you can manage the Cisco Unified Communications Manager connectivity on the Publisher and Subscriber servers; simply click the server under **Server Details**. You must be logged into the Publisher machine to be able to do this.

Step 4 Enter **CUCM name or IP**. The name or IP address of the machine where Cisco Unified Communications Manager is installed. For example, 209.165.201.0.

Step 5 Enter **CUCM Port number**. The Cisco Unified Communications Manager port to connect to. Accept the default, 443.

Step 6 Enter **User name**, the Cisco Unified Communications Manager application user ID. For more information about application users, see Creating and Assigning an Application User.

Step 7 Enter the Cisco Unified Communications Manager application user **Password**.

Note

- The Username and Password are case-sensitive. Make sure you enter the information in these fields in the correct case.
- Passwords must be comprised using ONLY the following characters: A-Z, a-z, 0-9.
- The Username and Password you enter must belong to an application user, for example CCMAdministrator.

Step 8 If you have a resilient Cisco Unified Attendant Console Advanced Administration installation with details of a secondary Cisco Unified Communications Manager stored on the other server, you can add these details to the secondary DRM. If the Publisher AXL service fails, this information can then be used by the BLF Plug-in to resolve devices using the secondary Cisco Unified Communications Manager connection. To store this information in the BLF plug-in you are connected to, check **Add secondary CUCM information from other server**.

Step 9 To save the connection details, click **Save**.

Cisco Unified Attendant Console Advanced Administration validates the media driver used to communicate with the specified Cisco Unified Communications Manager.

- If the media driver setting of the selected server is correct and Attendant Server is not running, the following message appears:

  Update Complete. Please restart Attendant Console services of selected Cisco UAC Advanced server for this change to take effect.

- If the media driver setting is incorrect, the media driver setting of the selected server is corrected and the following message appears:

  Attendant Admin detected that the media driver configuration for the selected Cisco UAC Advanced server did not match your CUCM version and has changed the media driver configuration to match your CUCM version. Please restart Attendant Console services of selected Cisco UAC Advanced server for this change to take effect.

Step 10 Restart the Attendant Console services of the selected Cisco Unified Attendant Console Advanced Server.

Step 11 To test the connection, click **Test Connection**.

Syslog Connectivity

For a description of the role of the syslog server, see Syslog and Alert Server.

To connect Cisco Unified Attendant Console Advanced to a syslog server:

Step 1 Go to **Engineering > Syslog Connectivity > Syslog Server Connectivity**. The information on this page is read-only when logged into the Subscriber server.

Step 2 Type the **Syslog Server IP or FQDN**, or leave the field empty to disable the Syslog Server.

Step 3 Type the **Syslog Server port**. (See note below.)

Step 4 Click **Save** to save the settings and restart the syslog services.

Step 5 To test the connection to the Syslog Server, click **Test Syslog Connection**.

To connect Cisco Unified Attendant Console Advanced to an alert server:

Step 1 Go to **Engineering > Syslog Connectivity > Alert Server Connectivity**. The information on this page is read-only when logged into the Subscriber server.

Step 2 Type the **Alert Server IP or FQDN**, or leave the field empty to disable the Alert Server.

Step 3 Type the **Alert Server port**. (See note below.)

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

Step 5 To test the connection to the Alert Server, click **Test Alert Connection**.

Note Cisco Unified Attendant Console Advanced uses TCP connection with the syslog server. Please read the syslog documentation on port requirements for TCP connections and make sure to update your firewall policy accordingly.

Logging Management

When you install Cisco Unified Attendant Console Advanced, logging is set up with a default configuration that suits most requirements. However, you can use the Logging Management option to enable/disable real-time logging of:

- Cisco Unified Attendant Server
- Cisco Unified Attendant LDAP Plug-in (If you have a resilient system and are logged into the subscriber, the LDAP Plug-in is not available.)
- Cisco Unified Attendant Presence Plug-in
- Cisco Unified Attendant BLF Plug-in

You can also configure and control log collection, which involves compressing the logs and other information into a ZIP file that you can use to check and troubleshoot the server.

To manage logging:

Step 1 Go to **Engineering > Logging Management**. The **Logging Management** page appears.

Step 2 As required, do the following:

- Manage Cisco Unified Attendant Console Server Logging.
- Manage Cisco Unified Attendant LDAP Plug-in Logging_bookmark219.
- Manage Cisco Unified Attendant Presence Plug-in Logging.
- Manage Cisco Unified Attendant BLF Plug-in Logging.
- Set up and run Log Collection.

Cisco Unified Attendant Console Server Logging

Cisco Unified Attendant Console Advanced server logs every event that it generates. The following processes are logged:

- Main process
- Router process
- CTI process
- Database process
- Communication process

By default, all except the Communication process are selected for logging. To keep the log file to a manageable size, log the fewest processes possible.

You should only need to amend these settings if requested as part of a support case investigation.

To manage Cisco Unified Attendant Console Advanced server logging:

Step 1 Select the process(es) to log.

Step 2 View the **Logging path & file name**. This field is read-only.

Step 3 Specify the **Number of files** that can be created in the logging folder. The default is 50.

Step 4 Specify the **Lines per file**. The number of lines of data each log file can contain. The default is 30000.

Step 5 View the **Service logging path** and **file name** of the Cisco Unified Attendant Console Advanced server service log. This field is read-only.

Step 6 Click **Save** to save the changes.

Cisco Unified Attendant LDAP Plug-in Logging

Note If you have a resilient system and are logged into the subscriber, the LDAP Plug-in is not available.

Cisco Unified Attendant Console Advanced Administration can log all the LDAP Plug-in events and processes, so that you can check LDAP Plug-in performance and activity, and functionality and configuration problems.

To manage Cisco Unified Attendant LDAP Plug-in logging:

Step 1 Select the **Logging Level**. One of: **Detailed** (default), **Advanced**, **Minimum**, **Full**.

Step 2 View the **Logging path & file name**. This field is read-only.

Step 3 Specify the **Number of files** that can be created in the logging folder. The default is 10.

Step 4 Specify the **Lines per file**. The number of lines each log file can contain. The default is 200000.

Step 5 Click **Save** to save the changes.

Cisco Unified Attendant Presence Plug-in Logging

Cisco Unified Attendant Console Advanced Administration can log all Cisco Unified Attendant Presence Plug-in events and processes, so that you can check its performance and activity.

To manage Cisco Unified Attendant Presence Plug-in logging:

Step 1 Select the **Logging Level**. One of: **Detailed** (default), **Advanced**, **Minimum**, **Full**.

Step 2 View the **Logging path & file name**. This field is read-only.

Step 3 Specify the **Number of files** that can be created in the logging folder. The default is 10.

Step 4 Specify the **Lines per file**. The number of lines each log file can contain. The default is 10000.

Step 5 Click **Save** to save the changes.

Cisco Unified Attendant BLF Plug-in Logging

Cisco Unified Attendant Console Advanced Administration can log all BLF Plug-in's events and process, so that you can check BLF Plug-in performance and activity, and functionality and configuration problems.

To manage Cisco Unified Attendant BLF Plug-in logging:

Step 1 Select the **Logging Level**. One of: **Detailed** (default), **Advanced**, **Minimum**, **Full**.

Step 2 View the **Logging path & file name**. This field is read-only.

Step 3 Specify the **Number of files** that can be created in the logging folder. The default is 100.

Step 4 Specify the **Lines per file**. The number of lines each log file can contain. The default is 100000.

Step 5 Click **Save** to save the changes.

Log Collection

The Cisco Unified Attendant Console Advanced server can create a ZIP archive of the log files, which administrators can either view or download to check and troubleshoot the system. Also included in the archive are the Cisco TSP logs and the ActiveMQ logs.

When you collect your logs into an archive, any existing archive file is first deleted and then the new one is built, but not saved until complete. If you cancel the collection process, there will be no archive stored, and you will not be able to view or download it until you run a collection to completion. Depending on the size of your log files, log collection can take a considerable length of time to complete; however, you do not need to remain on the logging page or even logged into your web browser during this period. At any time you can manually check on the progress of collection or whether it has completed successfully.

Setting Up Log Collection

To set up log collection:

Step 1 The **Archive file name** is the name of the logging archive ZIP file. This field is read-only. The log file name has the format *WAD_<server_machine_name>_<YYYYMMDD>.zip*.

Step 2 Select the **From** date - the date of the oldest logs to archive.

Step 3 The **To** date is set to today's date and is read-only.

Step 4 If you want to password protect the archive ZIP file and the files it contains:

- **a.** Select **Password protected**.
- **b.** Type the **Password** required to view the files in the archive.
- **c.** Confirm the passphrase.

Starting Log Collection

To start collecting the logs into an archive file, click **Start Log Collection**. The previous archive file is deleted and a new one created.

Canceling Log Collection

To cancel a log collection that is in progress, click **Cancel Log Collection**. If you cancel log collection, there will be no archive on the server because the previous one is deleted before the new one is saved.

Downloading the Log Archive

To view the log archive or download it to your computer, click **Download Logs**. If an archive file exists on the server, you are prompted to open it or save it to default download folder configured for your browser.

Checking Log Collection Progress

To check how log collection is proceeding, click **Log Collection Report**. The Log Collection Report page shows you the status of the current or most recent log collection, and any errors encountered.

During archive file creation the percentage complete is displayed and this is updated regularly; you can manually update the report page by clicking **Refresh**.

Marking Text Management

Use the **Marking Text Management** feature to define a message about confidentiality that appears on selected Cisco Unified Attendant Console Administration interface pages, and in the Cisco Unified Reporting and Cisco Unified Replication interfaces.

To manage marking text:

Step 1 Go to **Engineering > Marking Text Management**. The **Marking Text Management** page appears.

Step 2 Under **General**, type the **Marking Text** to appear on the interface pages.

Step 3 Under **Page Selection**, in **Available Pages**, select the pages on which the text will appear, and then click the down-arrow beneath the list to move the pages to the **Selected Pages** list. The up-arrow moves pages selected in the **Selected Pages** list back to the **Available Pages** list.

Step 4 Click **Save**.

Customized Logon Message

To create a customized message for users to accept before being able to use Cisco Unified Attendant Console Advanced:

Step 1 In Cisco Unified Attendant Console Administration, go to **Engineering > Customized Logon Message**.

Step 2 Click **Add New**.

Step 3 In **General > Language**, select the language you are using in the Client. The available languages are Arabic, Chinese (PRC), Chinese (Taiwan), Danish, Dutch, English, French, German, Italian, Japanese, Korean, Portuguese, Russian, Spanish, Swedish.

Note The language of the customized logon message must be the language of your Client, otherwise this function will not work.

Step 4 Enter the **Before login message**.

Step 5 Enter the **After login message**.

Note You do not have to use both fields - you can create a message for either before or after login, or both.

Step 6 Click **Save**.

To edit a customized message:

Step 1 Go to **Engineering > Customized Logon Message**.

Step 2 Click **Find**.

Step 3 Click **Select** for the message you want to edit.

Step 4 Edit the message and click **Save**.

To delete a customized message:

Step 1 Go to **Engineering > Customized Logon Message**.

Step 2 Click **Find**.

Step 3 Select the checkbox of the message(s) you want to delete.

Step 4 Click **Delete Selected**.

Cisco Unified Attendant Console Administration – System Configuration

The following chapter describes how to configure the **System Configuration** menu options in Cisco Unified Attendant Console Administration.

System Configuration Menu

The System Configuration menu enables you to manage the synchronization of devices and directories with Cisco Unified Communications Manager. It includes the following options:

- **Queue Device Groups**. This option enables you to create and configure Queue Device Groups (resource groups), and to add and manage system devices.
- **Synchronize with CUCM**, which includes the CUCM Sync Report.
- **Directory Source Management**
- **Contact Management**
- **Directory BLF Rules**

Queue Device Groups

Note Only the master account and solution administrator accounts can amend DDI and queue device groups and synchronize with CUCM. Moderator, supervisor, and reporting accounts can only view the **CUCM Sync Report**. For more information, see System Accounts Management.

The **Queue Device Groups** option enables you to create and configure up to 100 Queue Device Groups—each queue has its own resource group with its own audio source for music on hold; calls to the queue DDI number use the devices in a resource group pool. The option also provides access to the **System Device Management** page, which you use to configure the pooled devices as described in System Device Management.

A default Queue Device Group, called **Default Queue Device Group**, is created when you install Cisco Unified Attendant Console Advanced.

Note

- Empty queue device groups (including the **Default Queue Device Group** if unused) should be deleted before putting the server in to production. Failure to do so may result in device registration and call control inconsistencies.
- If you have a resilient system and you are logged into the Subscriber server, you cannot change any of the Queue Device Groups.

Creating Queue Device Groups

To create a queue device group:

Step 1 Choose **System Configuration > Queue Device Groups**.

The **Queue Device Groups** page is displayed, listing all the queue device groups that satisfy the Find filter.

Step 2 Either

Click **Add New**, enter a name and then click **Save** to create a new Queue Device Group.

or

Find a Queue Device Group to configure:

a. Specify a filter: a string to search for and where to search for it:

- Accept **Queue Device Group** to search the queue device group names.
- Select a condition of the Queue Device Group name, such as **is not empty**, or how to compare the name with a string, such as **begins with**.
- Type a string to compare to the Queue Device Group name in the specified way (used only with **begins with**, **ends with**, **contains** and **is exactly**).

You can also add another filter using the plus (+) and minus (-) controls to narrow the search.

b. Click **Find**.

A list of the queue device groups matching the Find filter is displayed.

Step 3 Under **Select queue device group profile**, click **Select** alongside the Queue Device Group to configure.

Another **Queue Device Groups** page is displayed.

Step 4 Use this page to change the name of the selected group or to manage the system devices in the group:

- To change the name of the queue device group, under **General** edit the text in the field, and then click **Save**.
- To access the System Device Management page so that you can manage the system devices in the group, under **System Devices** select the appropriate server. For the full procedure, see System Device Management.

Note

If you have a resilient system and you are logged into the Subscriber server, you cannot change any of the device settings, or the Queue Device Group.

Deleting Queue Device Groups

You cannot delete a Queue Device Group until all devices in it have been removed. To delete a Queue Device Group, do the following:

Step 1 Choose **System Configuration** > **Queue Device Groups**.

The **Queue Device Groups** page is displayed.

Step 2 Find the Queue Device Group to delete.

Step 3 Click **Select** alongside the Queue Device Group to delete.

Step 4 Under **System Devices**, select the server on which the Queue Device Group is configured.

The **System Device Management** page is displayed.

Step 5 Delete all CT Gateway, Service, and Park Device ranges, and then click **Save**.

Step 6 Click **Synchronize with CUCM**, and then allow the synchronization to complete.

Step 7 Return to the **Queue Device Groups** page.

Step 8 Select the check box to the left of the Queue Device Group to delete, and then click **Delete Selected**.

System Device Management

The maximum number of system devices (CT Gateway devices, Service devices, and Park devices) supported by a Cisco Unified Attendant Console Advanced Server is 1000; they can be distributed among up to 100 Queue Device Groups. You cannot save more than 100 devices per transaction.

Note If you have a resilient installation:

- You must create the same numbers of each type of system device on both the Publisher and Subscriber.
- You cannot configure system devices when logged into the Subscriber server.

To configure system devices and synchronize device ranges with Cisco Unified Communications server:

Step 1 Choose **System Configuration** > **Queue Device Groups**.

The **Queue Device Groups** page is displayed, listing all the queue device groups that satisfy the Find filter.

Step 2 Under **Select queue device group profile**, click **Select** alongside the Queue Device Group to configure.

Another **Queue Device Groups** page is displayed.

Step 3 Under **System Devices**, click the appropriate server (Publisher or Subscriber on a resilient installation).

The **System Device Management** page appears, containing the following fields and controls:

Field or Control	Description
Queue Device Group	The name of the queue device group for this server.
Template Device	
Copy all device properties from this device	You can create a template CTI device with custom settings in Cisco Unified Communications Manager and use it as a quick way of assigning these settings to your Cisco Unified Attendant Console Advanced devices. If you do not have a template, default values are assigned to your devices. All the properties of the Template Device, such as device pool, partition, and Calling Search Space (CSS), are mapped onto any new devices you create. Click **Find Template Device** to search for a template. **Notes**: • The Music On Hold (MOH) source configured against Cisco Unified Attendant Console Advanced CTI ports must be set to unicast, otherwise call control issues may arise. *CTI devices do not support the multicast MOH feature.* • Template Device must have the **Device Information > Allow Control of Device from CTI** setting enabled. Additionally, the template device line(s) must have the **Directory Number Information > Allow Control of Device from CTI** setting enabled. These options are not visible in the Cisco Unified Communications Management Administration if the device type is a CTI Port because the options are enabled by default for CTI Ports. • The template device should be based on an end point (a phone) or a CTI Port. *Do not use a CTI Route Point as a template device.* • If under **Protocol Specific Information a Subscribe Calling Search Space** is configured, then under **Device Information an Owner User ID** must also be configured, otherwise an error occurs when you to synchronize the CTI ports with Cisco Unified Communications Manager. • If a template device is specified for a Queue DDI it must outline the Calling Search Space (CSS) for the following: – Forward on CTI Failure – Forward Unregistered Internal – Forward Unregistered External Set these within Cisco Unified Communications Manager, under **Directory Number Configuration > Call Forward and Call Pickup Settings**.
Queue Devices	
CT Gateway Devices **Service Devices** **Park Devices**	Click a link to display a page for managing that type of device. For descriptions of these devices, see Cisco Unified Communications Manager System Devices. **Note**: The Music On Hold (MOH) source configured against Cisco Unified Attendant Console Advanced CTI ports must be set to unicast, otherwise call control issues may arise. *CTI devices do not support the multicast MOH feature.*

Step 4 Click **Find Template Device** to list and search for template devices to use.

Define the search filter:

- The device property to check—such as **Device Name, Description**, or **Directory Number**.
- A condition of the device property, such as **is not empty**, or how to compare the property with a string, such as **begins with**.
- A string to compare to the device property in the specified way (used only with **begins with, ends with, contains** and **is exactly**).

You can also add search filters (up to a maximum of 10) using the plus (+) and minus (-) controls; thereby narrowing the search.

Step 5 In the **Device Search** page, select a template device, and then click **Save**.

Tip When you select a Template Device, the template must have a unique, unused DN on Cisco Unified Communications Manager. If the same DN is used for multiple devices calls may route incorrectly.

Step 6 *Repeat this step for each type of device you want to configure*.

Under **Queue Devices**, click the device type:

- **CT Gateway Devices**
- **Service Devices**
- **Park Devices**

A page appears, listing the devices of that type on the selected server that satisfy the Find filter. Use this page to find and add new devices of that type, and to delete existing selections.

- To delete devices, click the check box to the left of the device, and then click **Delete Selected**. You can delete all the devices in one go by clicking **Select All**, and then clicking **Delete Selected**.
- To add devices, click **Add New**.

  The **Add <device type>** page appears.

  a. Under **General**, enter a range (**From** and **To**) for the devices.

Note You can add system devices in E.164 format as long as *, + or # is used only at the start or end of the DN. For example, **+16000#** is allowed but **16*00#** is not.

By default, the maximum internal device digit length is set to 4 digits. To change this setting, choose **User Configuration > General Properties** and **Maximum internal device digit length**.

You can only add ranges of up to 100 devices.

  b. Click **Save**.

  c. Go back to the **System Device Management** page.

Step 7 Click **Save**.

Note Each time you change devices you must synchronize Cisco Unified Attendant Console Advanced with Cisco Unified Communications Manager.

Step 8 Click **Synchronize with CUCM** to display the **Synchronize with CUCM** page, as described below.

Synchronize with CUCM

Note Only the master account and solution administrator accounts can amend DDI and queue device groups and synchronize with CUCM. Moderator, supervisor, and reporting accounts can only view the **CUCM Sync Report**. For more information, see System Accounts Management.

All devices from all servers are synchronized with Cisco Unified Communications Manager. Devices are associated with their own TSP profile.

The **Synchronize with CUCM** function enables you to synchronize device configurations with Cisco Unified Communications Manager via the AXL API. It creates the devices that have been configured if they don't already exist and assigns them to the Application User profile.

This option synchronizes the following devices:

- Queue Locations
- CT Gateway Devices
- Service Devices
- Park Devices

To synchronize devices with Cisco Unified Communication Manager:

Step 1 Choose **System Configuration > Synchronize with CUCM**.

The Queue Device Groups that satisfy the Find filter are listed, with the following displayed for each:

Field	Description
Check box	Click to select/clear that Queue Device Group.
Queue Device Group	The Queue Device Group name.
Publisher Devices (<server_name>)	The number of devices in that group that are on the Publisher server.
Subscriber Devices (<server_name>)	*Displayed only if you have a resilient installation. The devices on both servers are synchronized.* The number of devices in that group that are on the Subscriber server.

Step 2 Click the appropriate check boxes to select the Queue Device Groups to synchronize. To speed the synchronization process, select only new or amended groups. You can use the buttons below the list (for example, **Select All**) to simplify the selection.

Step 3 **Ignore Call Forwarding Option** - (Visible for fully licensed standalone installations. If an Evaluation or High Availability license is applied to the server, this option will not be visible.)

- **Unchecked** - Pre-existing Queue DDI call forwarding configuration will be overwritten with either template device values or the default CUCM values during the synchronization with CUCM.

- **Checked** - Pre-existing Queue DDI call forwarding configuration is retained during the synchronization with CUCM.

Step 4 Click **Synchronize with CUCM**.

A message appears showing and estimate of how long synchronization will take.

Step 5 If you are satisfied with the time required to synchronize, click **Yes**.

Cisco Unified Attendant Console Advanced Administration synchronizes the devices with Cisco Unified Communications Manager. You do not have to login to Cisco Unified Communications Manager administration.

Once synchronization is underway, you can click **CUCM Sync Report** to see how it is progressing.

The report contains the following fields:

Field or Control	Description
Sync Status	
Status	Synchronization status; one of: • Associating • Completed • Creating • Deleting • Validating
Ignore call forward settings	Whether **Ignore call forward** is set.
Started At	The date and time when Cisco Unified Communications Manager synchronization started. For example, 2015-04-12 16:08:52.
Ended At	The date and time when Cisco Unified Communications Manager synchronization ended. For example, 2015-04-12 16:10:52.
CUCM Connection Validation	
User Name	The Cisco Unified Communications Manager Application User profile ID.
Server Name	The name of the server hosting Cisco Unified Communications Manager.
Status	The status of the connection validation; one of: • Completed • Error • Validating
Error Code	The code of the error that has been encountered. For example, 9400. The error codes are described in Table 1 Error Codes.
Error Description	This field gives a brief description of the error that has been encountered. For example, HTTP/1.1 503 Service Unavailable.

Field or Control	Description
Template Device Validation	
Queue Device Group	A Queue Device Group.
Template Device Pkid	The unique ID of the Queue Device Group from Cisco Unified Communications Manager.
Status	The status of the template device validation; one of: • Completed • Error • Validating
Error Code	The code of any error encountered while validating a device. For example, 9300. The error codes are described in Table 1 Error Codes.
Error Description	The description of the error. For example, Template device not found.
Device Sync	
Server Name	The server for which the Queue Device Group is configured.
Queue Device Group	The Queue Device Group containing the device.
Device DN	The number of the device being synchronized. For example, 6101.
Device Type	The type of device being synchronized. for example, CT Gateway Device.
Executed By	Populated with account names that executed a sync.
Status	The status of the device synchronization; one of: • Completed • Error • Inprogress
Error Code	The code of any error encountered while synchronizing a device. For example, 9550. The error codes are described in the table below.
Error Description	The description of the error. For example, HTTP/1.1 403 Access to the requested resource has been denied.

The following errors may occur during CUCM synchronization.

Table 1 Error Codes

Error Code	Error Description
Cisco Errors	
Less than 5000	These errors correspond to DBL exception error codes.
5000	Unknown Error—an unknown error occurred while processing the request. This can be due to a problem on the server or errors in the request.

Error Code	Error Description
5002	Unknown Request Error—the user agent saves a request that is unknown to the API.
5003	Invalid Value Exception—an invalid value is detected in the XML request.
5007	Item Not Valid Error—the system identified the specified item does not exist or was specified incorrectly at input.
599	Schema Not Supported—there has been an AXL request error because the schema is not supported.
Internal Errors	
9000	Exception in AXL component—an unknown error occurred while processing the AXL component.
9100	Function parameter error—the parameter value is empty or null.
9200	Device already created—the device being synchronized already exists in Cisco Unified Communications Manager and is synchronized with the client.
9300	Template device not found—the template device that you have selected does not exist.
9400	HTTP/1.1 503 Service Unavailable—the AXL service is unavailable.
9500	HTTP/1.1 401 Unauthorized—the user authentication credentials are invalid.
9550	HTTP/1.1 403 Access to the requested resource has been denied—access denied error from AXL response.
9555	HTTP/1.1 404—there is an invalid header location in the SOAP Request.
9600	Call Manager OS not recognized—the operating system returned by Cisco Unified Communications Manager is neither Linux nor Windows.
9650	Call Manager Version not detected—the AXL Response from Cisco Unified Communications Manager did not provide the version.
9700	Socket error—there are network problems.
9750	Connection refused—the server did not respond or the request has been posted to an invalid URL.
9755	Read Timeout—the server did not respond.
9800	Normal Exit—normal exit on completion.
10000	Connection timeout—connection timeout from the server.

Directory Source Management

Cisco Unified Attendant Console Advanced Administration can synchronize to one external source directory of the following kinds:

- Cisco Unified Communications Manager (using CCM)
- Microsoft Active Directory 2008 R1/R2 or Active Directory 2012 (using LDAP)
- iPlanet Netscape Directory 5.0 or 5.1 (using LDAP)
- Active Directory Lightweight Directory Services (using LDAP)

You can connect to only one instance of each of these types and use only one directory at a time. When you select a directory source you can configure the directory and connection, and access these additional configuration functions:

- **Directory Synchronization**
- **Directory Field Mappings**
- **Directory Rules**

In addition to populating your contacts database (also known as the full directory) from an external source directory, you can also:

- Manually add contacts to your contacts database.
- Import contacts from CSV files and export contacts to CSV files.

Each contact within any configured directory source must have a static and unique identifier. Cisco Unified Attendant Console leverages this field to marry the locally stored contact with its source. If for any reason the unique identifier value changes, it results in the contact being removed from the Cisco Unified Attendant Console directory, and subsequently being repopulated as a new contact, thus removing any contact notes, absent messages, alternate/assistant contact ties, and manually populated fields.

Cisco Unified Attendant Console Advanced references the following non-configurable native fields:

- Microsoft Active Directory - Object GUID (objectGUID)
- Microsoft Active Directory Lightweight Directory Services / ADAM - Object GUID (objectGUID).
- Cisco Unified Communications Manager - Primary Key Identifier (PKID)
- iPlanet - Distinguished Name (DN)

Note

Because you can synchronize to more than one source directory it is possible for you to add duplicate contacts (which are in more than one of the directories) into your contacts database, or to exceed the maximum number of contacts allowed by your license (or even Cisco Unified Attendant Console Advanced's 100K limit). Because of this, a warning message is displayed when you have more than one directory source enabled.

However, if you synchronize to a source directory and then disable that source, the synchronized contacts are not automatically deleted from the contacts database. If you now enable another source directory, you will not see the warning message—because only one source is enabled—but you may still end up with duplicate contacts or more contacts than your license permits. To prevent this, before synchronizing to the second source directory you must remove from the database all contacts from the disabled directory. You do this by setting up import rules that don't match any contact in either the database or the disabled source directory.

Caution **Do not perform directory synchronization when the Subscriber server is not running. If you do, the server must go through all the pending online requests when it comes back online, which may delay the server becoming available**.

Connecting to a Directory Source

To connect to a directory source, do the following:

Step 1 Choose **System Configuration > Directory Source Management**.

The **Directory Source Management** page is displayed, listing the directory sources available to you.

Step 2 **Select** the directory source to manage.

The page changes to show information about the directory source and your connection to it.

Step 3 Set the following parameters:

- **General**
  - **Source Name**—The name of the source directory
  - **Directory platform**—The name of the selected external directory (read only)
  - **Enable synchronization**—Select to enable synchronization
- **Connection**
  - **Host name or IP**—The host name or IP address of the source directory server
  - **Host port**—The port number, which depends on the type of source directory you select and whether you use secure sockets layer (SSL):

Directory Source	SSL	Host Port
Microsoft Active Directory	Selected	636
Microsoft Active Directory	Not Selected	389
iPlanet Netscape Directory	Selected	636
iPlanet Netscape Directory	Not Selected	389
Cisco Unified Communications Manager	Selected	443
Cisco Unified Communications Manager	Not Selected	443
Active Directory Lightweight Directory Services	Selected	636
Active Directory Lightweight Directory Services	Not Selected	389

- **Authentication**
  - **Username**—A valid username in the selected source directory server
  - **Password**—The password of the specified directory user

Note To ensure password composition is supported, see Supported Windows, SQL Server, Active Directory, Presence Server, Application User and CUAC Password Characters.

- **Container** (displayed only with Microsoft Active Directory, iPlanet and ADLDS sources)
  - **Base DN**—The top level of the LDAP directory tree
  - **Object class**—The object class of the base DN (the default for Microsoft Active Directory is **contact**; the default for iPlanet Netscape Directory is **inetOrgPerson**, the default for ADLDS is **person**).
  - **Scope**—Select either **One Level** or **Sub Tree Level** (default). With **One Level** the data is searched to one level below the specified Object class and Base DN. With **Sub Tree Level** the data is searched in all levels below the specified Object class and Base DN.
- **Notifications**
  - **Monitor Change Notifications**—If enabled, changes made to the directory source are immediately reflected in the Cisco Unified Attendant Console Advanced contact directory. Otherwise, the directory is updated as defined in the **Directory Synchronization** menu described below.

    For more information about important design considerations before continuing, see the **Monitor Change Notifications** section in the *Cisco Unified Attendant Console Advanced Design Guide*.

Note If **Monitor Change Notifications** is enabled, implement the following synchronization settings to achieve optimal server performance:

- Enable Directory Synchronization > Auto Synchronization > On start-up and On reconnect
- Under Directory Synchronization > Auto Synchronization > Schedule Settings, select None from the Type dropdown.

Step 4 Click **Save** to save your changes.

You can use the controls at the bottom of the page to:

- Test the connection to the directory. Click **Test Connection**; the system tells you whether the connection to the directory works.
- Access the Directory Synchronization functionality.
- Access the Directory Field Mapping functionality.
- Access the Directory Rules functionality.

Directory Synchronization

Use Directory Synchronization to configure the synchronizing of the contacts database with your chosen directory source.

Caution

- **Do not perform directory synchronization when the Subscriber server is not running. If you do, the server must go through all the pending online requests when it comes back online, which may delay the server becoming available.**
- **If auto-purge is enabled, do not schedule directory synchronization to execute at midnight, because auto-purge runs at midnight every day. If auto-purge is disabled, directory synchronization can be run at midnight.**

To configure directory synchronization, do the following:

Step 1 In the **Directory Source Management** page, click **Directory Synchronization**.

The **Directory Synchronization** page is displayed. The page contains the following **Directory Synchronization** parameters:

- **Directory Source**—The name of directory chosen as the source.
- **Auto Synchronization**—Set the automatic synchronization preferences:
  - **On start-up**—Select this to start the synchronization when Cisco Unified Attendant Console Advanced server starts.
  - **On reconnect**—Select this to start the synchronization when Cisco Unified Attendant Console Advanced server reconnects with the LDAP plug-in after a connection failure.
- **Route Partition**—(Only displayed when the Cisco Unified Communications Manager directory is used). This prioritizes which DN to import when there are identical DNs in different partitions. Either **Select a route partition** or one of the following:
- **<None>**—disregard the route partition field when synchronizing the directory.
- **CUCM <None> partition**—picks up only those devices in the Cisco Unified Communications Manager specified as (None).
- **Schedule Settings**—The synchronization schedule. Enter the following:
  - **Type**—The frequency of synchronization. Select one of:
    - **None**
    - **Hourly**
    - **Daily**
    - **Weekly**
    - **Monthly**
  - **Every [(Number)(Type)]**—The data type changes according to the **Type** just chosen. For example, Every 2 Week(s) or Every 1 Day(s).
  - **Start date**—The date on which to start synchronizing.
  - **Start time**—The time on which to start synchronizing.

Step 2 Set the Directory Synchronization parameters.

Step 3 Click **Save** to save the changes.

Directory Field Mapping

Use Directory Field Mapping to map information from your chosen directory to the contacts database.

Note Internal contacts cannot have **Extensions** associated with Cisco Unified Communications Manager CTI Route Points. To designate a CTI Route Point number for a contact, the contact must be deleted and recreated as an external contact. You must exclude the contact from the directory sync using a Directory Rule.

To map a field:

Step 1 In the **Directory Source Management** page, click **Directory Field Mapping**. The mappings are listed.

Step 2 Click **Add New**. The **Field Mapping Information** is displayed.

Step 3 Select a **Source field** in the AXL component of Cisco Unified Communications Manager database, or from the LDAP server of other directory types

Step 4 Select a **Destination field** in the contacts database.

Note If you are mapping CUCM fields and select Extension as your Destination field, you will not be able to delete the mapping.

Step 5 If you are mapping:

- Microsoft Active Directory
- iPlanet Netscape Directory
- Active Directory Lightweight Directory Services
- CUCM and your Destination field is anything other than Extension

type a Default value, which is written to the Destination field if the Source field is empty.

If you are mapping CUCM fields and your Destination field is Extension, you cannot type a Default value.

Step 6 Click **Save** to add the mapping.

Mapping Cisco Unified Attendant Console Advanced Fields to an LDAP Directory Source

The following Cisco Unified Attendant Console Advanced fields can be mapped to an LDAP data source:

Cisco Unified Attendant Console Advanced Field	Number of Characters
Absent Message	4000
Alternate Department	100
Alternate First Name	40
Alternate Last Name	50

Cisco Unified Attendant Console Advanced Field	Number of Characters
Business 1	40
Business 2	40
Company Name	100
Cost Center	100
Department	100
Email	100
Email 2	100
Email 3	100
Extension	40
Fax	40
First Name	40
Full Job Title	255
Full Name	100
Home	40
Home Address Line 1	50
Home Address Line 2	50
Home Address Line 3	50
Home Address Line 4	50
Home Post Code	50
Initials	40
Job Title	3
Keyword	100
Last Name	50
Location	100
MAC Address	255
Middle Name	40
Mobile	40
Pager	40

Cisco Unified Attendant Console Advanced Field	Number of Characters
Notes	4000
Room Name	50
Section	50
Title	4
User Field 1	100
User Field 2	100
User Field 3	100
User Profile	255

Directory Rules

Use Directory Rules to manage the filters to use when importing information from your selected directory to the Cisco Unified Attendant Console Advanced server. The filters are built into rules. You can have multiple filters in a rule and apply multiple rules.

Note If contacts in the LDAP source contain directory numbers associated with Cisco Unified Communications Manager CTI Route Points, you must exclude them from directory synchronization using Directory Rules, and then manually add them to the directory as External contacts, as described in Contact Management.

Tip Multiple filters within a rule are combined with a logical AND. So, if a rule contains lastname = T* and Department = Product, all people in the Product team who have a last name starting with T are imported.

If you have multiple rules, each containing a single filter, the rules/filers are combined with a logical OR. For example, if Rule 1 contains lastname = T* and Rule 2 contains Department = Product, all the people with a lastname beginning with T are imported, as are all the people in the Product team.

To add a Directory Rule:

Step 1 In the **Directory Source Management** page, click **Directory Rules**.

Note If you are using Microsoft Active Directory, iPlanet or ADLDS, you will not be offered a default rule when you first access this page. You must create your own rule.

Step 2 To create a new rule, click **Add New**. To add a filter to an existing rule, **Select** the rule and continue from Step 4.

Step 3 Enter a **Rule Name**, and then click **Save**.

Step 4 To add a filter to the rule, click **Add New**.

Step 5 Select a **Source field**, against which the filter Value is matched.

Step 6 Select an Operator, which determines how the **Value** is matched in the Source field. Choose one of: **Equal to, Approx. Equal to, Less and Equal to (<=), Greater** and **Equal to (>=)**.

Step 7 Enter the **Value** to match against the **Source field** using the **Operator**.

Step 8 Click **Save** to save the filter in the rule.

Contact Management

The **Contact Management** menu allows you to add, modify*, delete** and view*** contacts in the full directory. Contacts belonging to the full directory will be visible to all console users.

*Mapped LDAP source contact fields cannot be modified by Cisco Unified Attendant Console Advanced users or administrators. Sync fields will appear unavailable in the **Contact Details** window within the console and in the **Contact Management** menu of the Web Administration. Field modifications must be made at a source level.

LDAP source contacts cannot be deleted via the Contact Management menu. To remove synchronized contacts, you must exclude them from directory synchronization using **Directory Rules, see Directory Rules.

***Private Personal Directory Group contacts created by end users will not be visible in the Contact Management menu.

Note

Internal contacts cannot have **Extensions** associated with Cisco Unified Communications Manager CTI Route Points. To designate a CTI Route Point number for a contact, the contact must be deleted and recreated as an external contact. If the contact belongs to a sync source, then it must be excluded using a **Directory Rule**.

Adding Contacts

To manually add a contact to the full directory:

Step 1 Choose **System Configuration > Contact Management**.

The **Contact Management** page is displayed.

Step 2 Click **Add New**.

Step 3 For **Contact type**, select either **Internal** (the default) or **External**.

Step 4 Depending on the Contact type you choose, enter at least the following information for the contact:

- For Internal contacts:
  - **Main extension**

    If the main extension has a device name (or if it has extension mobility, a Profile Name), you can find it by clicking **Find Device Name**. If one is found, click **Save** to insert it in the **Device name** field.

    On the **Contact Management** page, this number is displayed in the **Number** column.

- For External contacts, either:
  - **Contact Numbers**

    Enter at least one number. On the **Contact Management** page, this number is displayed in the **Number** column. Which number is shown depends on its priority. The numbers from highest to lowest priority are:
  - **Business 1**
  - **Business 2**
  - **Mobile**
  - **Home**
  - **Pager**
  - **Fax**

Step 5 Add any other contact information, including numbers, company details, keywords, and notes.

- **Limit BLF to Device Name** defines how Cisco Unified Attendant Console Advanced obtains the BLF for the new contact. If the contact has only a single phone, we recommend that you select **Limit BLF to Device Name**. If you know the contact's CUCM device name, type it in **Device Name**, and the system will attempt to get the BLF using it. If you don't know the CUCM device name, leave **Device Name** blank; if it has permission to update the record, the Console will insert the **Device Name** once the user appears in its directory with a BLF status, after it has determined the best device from which to obtain it. If the contact is using Extension Mobility, or uses their extension number across multiple devices, we recommend that you clear **Limit BLF to Device Name** to let the system find the best device from which to obtain BLF using the device selection algorithm described in the *Cisco Unified Attendant Console Advanced Design Guide*.

  Device Name is case-sensitive and is inactive if **Limit BLF to Device Name** is not selected. Specify the default **Limit BLF to Device Name** setting in **General Properties**. For more information, see General Properties.
- **Notes**: leave at **Default** or select another color from the drop-down list and enter **Contact information** and/or a **Contact absent message**. If you enter a color code manually and it corresponds to the color you selected from the drop-down list, the code is removed upon saving. However, if the color code does not match the color you selected from the drop-down list, it appears as part of the entered text, but the color used for the note is the one selected from the drop-down list. The following color codes are in use:

Color	Color code	Color	Color code
BLUE	{B}	OLIVE	{O}
CYAN	{C}	PINK	{P}
GREEN	{G}	RED	{R}
LIME	{L}	TEAL	{T}
MAROON	{M}	VIOLET	{V}
NAVY	{N}		

Note Notes can be disabled for contacts synced from CUCM by editing the Directory Field Mapping information. Under **Field Mapping Information**, select a **Source field** (for example, firstname or lastname). Then, under **Destination fields** select **Absent Message** to disable only the **Contact absent message**, or **Notes** to disable the whole **Notes** area. Click **Save**.

When in use, colored notes are visible on the console in the First Name column, for example: *Contact unavailable until tomorrow*.

Step 6 Click **Save**.

Modifying Contact Information

You can modify the information stored with each contact in the full directory.

Note For contacts you have added, you can change any field: for contacts synchronized from an external source, you can only change non-mapped fields.

To modify a contact in the full directory:

Step 1 Choose **System Configuration > Contact Management**. The **Contact Management** page is displayed.

Step 2 Create a filter to **Find** the contact to modify. A table of matching contacts is displayed.

Step 3 In the table row containing the contact to modify, click **Select**.

Step 4 In the Contact Management page, modify the data fields as required, and then click **Save**.

Deleting Contacts

You can delete contacts that have been manually added to the full directory.

Note You cannot delete contacts synchronized from an external directory.

To delete a contact:

Step 1 Choose **System Configuration > Contact Management**. The **Contact Management** page is displayed.

Step 2 Create a filter to **Find** the contacts to delete. A table of matching contacts is displayed.

Step 3 Click the checkbox in the table row of every contact you want to delete.

Step 4 Click **Delete Selected**.

Directory BLF Rules

Contact extension numbers are displayed in a user-friendly format - including E.164 - but this number cannot always be used to retrieve BLF phone state information. Consequently, certain user-friendly numbers must be converted to BLF Subscription Numbers, which are DNs within Cisco Unified Communications Manager that accurately reflect the BLF phone state. This conversion is done by the application of Directory BLF Rules when creating or amending contacts manually using Cisco Unified Attendant Console Advanced Administration and Console client, or via LDAP import.

This section tells you how to create these rules and then manually apply them to the contacts.

Creating Directory BLF Rules

To create a Directory BLF Rule:

Step 1 Choose **System Configuration** > **Directory BLF Rules**.

The **Directory BLF Rules** page is displayed, with the rules listed that satisfy the Find filter, which consists of:

- The rule property. You can select either **Name** or **Sample Number**.
- A condition of the rule property, such as begins with. *This part of the filter is displayed only if you select the **Name** property.*
- A string to compare to the rule property under that condition. If you select the **Name** property, type a string; all the rules with matching names are listed.

If you select the **Sample Number** property, type a sample phone number; all the rules with **Select Directory Numbers** regular expressions that match the format of this number are listed.

You can add filters (up to a maximum of 10) using the plus (+) control; thereby narrowing the search.

Step 2 Click **Add New**.

The page changes to show the input fields for the new rule, and at the bottom of the page a list of the existing rules, labeled **Directory BLF Rules Priority**. The order of the rules in this list is the order in which they are applied—the output of the first rule being input to the second rule, and so on.

Step 3 Under **General**, type the **Name** of the new rule.

Step 4 Optionally, under **Select Directory Numbers**, specify the directory numbers to convert by selecting either:

- **Number Begins with**, and then typing a pattern to match the start of the numbers.
- **Regular Expression**. and then typing the expression to use.

Step 5 If you want to remove certain non-numeric characters from the telephone number, select **Remove Non-numeric Characters** – which will remove all the non-numeric characters – and then specify the Exceptions that you want to keep.

Step 6 Optionally, under **Remove/Replace Digits**, define how to convert the start of the number string by selecting either:

- **Total Digits to be Removed**, and then typing the number of digits to remove from the start of the string. If you want to replace the digits with some others, type these into the corresponding **Replace with** field.
- **Regular Expression**, and then typing the expression to use. If you want to replace the digits with some others, type these into the corresponding **Replace with** field.

Step 7 Optionally, under **Add to String**, specify a **Prefix** and **Suffix** to add to the number string.

Step 8 To test your new rule, under **Test Directory BLF Rule**, type a **Sample Directory Number** to convert, and then click **Test Rule**. If the number that appears in the **Result** is not what you expect, modify the rules, and try again. Otherwise, click **Save** to save the rule in the database. The new rule appears in the **Directory BLF Rules Priority** list.

Step 9 To change the position of a rule in the list, and hence the processing order, click the **Up** or **Down** arrows as required, and then click **Save**.

Editing Directory BLF Rules

To edit a Directory BLF Rule:

Step 1 Choose **System Configuration > Directory BLF Rules**.

The **Directory BLF Rules** page is displayed, with the rules listed that satisfy the Find filter, which consists of:

- The rule property. You can select either **Name** or **Sample Number**.
- A condition of the rule property, such as begins with. *This part of the filter is displayed only if you select the **Name** property.*
- A string to compare to the rule property under that condition. If you select the **Name** property, type a string; all the rules with matching names are listed.

If you select the **Sample Number** property, type a sample phone number; all the rules with **Select Directory Numbers** regular expressions that match the format of this number are listed.

You can add filters (up to a maximum of 10) using the plus (+) control; thereby narrowing the search.

Step 2 If necessary, **Find** the rule.

Step 3 Click **Select** to display that rule's parameters.

Step 4 Edit the rule's parameters, and then click **Save**.

Deleting Directory BLF Rules

To delete a Directory BLF Rule:

Step 1 Choose **System Configuration > Directory BLF Rules**.

The **Directory BLF Rules** page is displayed, with the rules that satisfy the **Find** filter listed.

Step 2 If necessary, **Find** the rule.

Step 3 Select the check box at the start of each rule to delete. Click **Select All** to select all the rules for deletion.

Step 4 Click **Delete Selected**.

Applying BLF Directory Rules

BLF Directory Rules are applied when you create or amend contacts using the Cisco Unified Attendant Console Advanced client, Cisco Unified Attendant Console Advanced Administration, or via LDAP import. You can also manually apply the rules to update contacts as follows:

Step 1 Choose **Bulk Administration** > **Job Scheduler**.

The **Job Scheduler** page appears.

Step 2 **Find** the **BLF Subscription Number conversion** job, and then **Select** it.

The **General** section is read-only.

Step 3 Under **Scheduled Date/Time**, enter or select a **Date**, then enter or select a **Time**. If you do not set the date and time, the job will run immediately.

Step 4 Activate the job, ready for processing, by clicking **Activate Job**. You can deactivate an activated job by clicking **De-activate Job**.

Step 5 Click **Save** to save your changes and run the job at the specified time.

The contact BLF subscription numbers are updated; you can view them in the **Contact Numbers** section of the **Contact Management** page.

For more information about scheduling updates, see Job Scheduler.

Cisco Unified Attendant Console Administration – User Configuration

The following chapter describes how to configure the User Configuration menu options in Cisco Unified Attendant Console Administration.

User Configuration Menu

The User Configuration menu enables administrators to configure Cisco Unified Attendant Console Advanced.

General Properties

The **General Properties** option enables you to manage the Cisco Unified Attendant Console Advanced global configuration.

Note If you have a resilient system and you are logged into the Subscriber server, you can only change certain General Properties, such as **Hold queued calls**.

To configure Cisco Unified Attendant Console Advanced:

Step 1 Choose **User Configuration** > **General Properties**.

Step 2 Enter the **General Properties**:

- **Internal/External Access**

  To learn how the solution processes overflow and outbound calls by default and in conjunction with the following settings, see Dial Plans in the *Cisco Unified Attendant Console Advanced Design Guide*.

  – **Minimum/Maximum Number of Characters for Internal Numbers**

    The minimum and maximum number of characters for internal numbers defines the character length range for internal numbers.

The default minimum is 1, and the default maximum is 4, with a supported maximum of 24. The defined range impacts the application in the following ways:

- Outbound calls require a character length *equal to* or *greater than* the defined **Minimum Number of Characters for Internal Numbers**.
- Console client call tags flag calls as Internal or External based on the number length either falling *within* the specified minimum and maximum range (**Internal**) or *in excess of* the maximum number of characters (**External**).
- Triggering the External access number or External international access number requires the number length to be *in excess of* the defined maximum number of characters for internal numbers.

- **External access number**—the prefix that enables you to call external numbers
- **External international access number**—the prefix that enables you to call international external numbers. (See note for requirements.)
- **Exclude local country code**—the Country Code of the Cisco Unified Communications Manager location. When processing international numbers that contain this country code, the country code is excluded, and the number is dialed as a domestic call. (See note for requirements.)

Note

International Dialing Requirements

- Use of the **External International Access Number** requires that contact numbers be in E.164 format (for example, +1 555 555 5555).
- **Exclude local country code** must be formatted as +<country code>. The <bold>+<bold> prefixed **Exclude local country code** is required for the External International Access Number to go into effect. Otherwise, outbound calls will default to the **External Access Number**.

- **Default FAC and CMC Settings**—**Forced Authorization Codes (FAC) and Client Matter Codes (CMC)** are configured in Cisco Unified Communications Manager, and they must be added in Cisco Unified Attendant Console Administrator if the system performs the following actions on calls:
  - Overflows
  - Night Service destination
  - Attendant Operators perform a Blind Transfer

  If the destination number is an **External Number** (external to your organization or CUCM), the system may require you to provide FAC and CMC information to perform the above actions. If the information is configured in Cisco Unified Attendant Console Administrator under General Properties, the system will automatically append this information when requested by CTI during its call operation.

  If this information is not configured in Cisco Unified Attendant Console Administrator but is required to make an external call, then any calls initiated by the user (Attendant Operator) will be prompted with a FAC and CMC dialog box. However, system transfers like overflows, night service and emergency overflows will fail.

To configure FAC and CMC, refer to the *Cisco Unified Communications Manager Feature Configuration Guide*.

Note

- Client Matter Code (CMC) is used to provide extra call logging facilities within the Cisco Unified Communications Manager. The user has to enter their CMC Code before their external consult transfer can proceed. The CMC code is written into the call detail records, which can then be used to charge calls to different cost centers.
- Forced Authorization Code (FAC) is used to provide security in the Cisco Unified Communications Manager for dialing "Route Patterns". In some call centers, some callers are only allowed to make external consult transfers if they first enter a FAC. If they fail to enter a FAC or enter an incorrect FAC the transfer fails

- **Recall Timers**—these properties are used to set the duration of each type of recall:
  - **Hold recall**—the maximum time a call put on hold by an operator remains on hold before an audible alert is played
  - **Transfer recall**—the maximum time before an unanswered operator-transferred call is returned to that operator
  - **Park recall**—the maximum time before an unanswered parked call is returned to the operator. The call can still be picked up by the intended recipient once the Parked timeout has happened.
  - **Camp On recall**—the maximum time an unanswered call remains camped-on before it is returned to the operator.
- **Default Queue Device Group**—select the system default queue device group: the group of devices to use to route the call if the system is otherwise unable to attach a device group to it.
- **Call Arrival Mode**—Select to enable **Hold queued calls** mode, which is used to trigger Music on Hold (MoH) within the Cisco Unified Communications Manager.

Note

Cisco Unified Communications Manager enables you to configure a queue to hold queued calls when they arrive on the CTI Port and play Music on Hold to the caller while they wait for an operator to answer. *If you use this mode the call is charged from the time that it is answered and put on hold on the CT Gateway*.

- **Contact Directory Setting**—The Cisco Unified Communications Manager device name is used to retrieve a contact's BLF information. This device name is either:
  - Part of the contact's details entered manually when the contact is created in the **Contact Management** page**.**
  - Automatically found by Cisco Unified Attendant Console Advanced using the device selection algorithm described in the *Cisco Unified Attendant Console Advanced Design Guide.*

The **Limit BLF to Device Name** setting determines which of these is used by default when you create new contacts in the **Contact Management** page. If most of your directory contacts have a single phone, select **Limit BLF to Device Name**, otherwise clear it.

- **Call Logging Setting**—Select **Call Logging** to enable call logging, clear it to disable call logging.

Note

After disabling call logging, you can remove old logging data using **Engineering > Database Purge**. For more information, see Database Purge.

- **Login Rate Settings**—Select this to protect the system against denial of service (DOS) attacks.

  The login rate is checked at these levels:

  - **User Level**—This applies only to non-SSO users, and only when a correct login name is used with an incorrect password. If the login name is incorrect, the Session Level setting applies.
  - **Session Level**—This setting applies to both SSO and non-SSO users and concerns the use of incorrect login names that are not in the system cash and cannot then be found in the system's list of authorized users.

  In both cases, the user has 60 seconds from first attempt in which to log in successfully. During this time, if the user login attempt fails because of either an invalid login name or invalid password on three consecutive occasions, on the fourth attempt (irrespective of whether correct credentials are provided) the server makes the user wait for 60 seconds before they can try again. After this time, the server is reset, counts and timers are zeroed, and the check repeated, and so on until the user either logs in or gives up.

  Once the Login Rate has struck, the console GUI will be greyed out and not usable until the application is restarted. In the case of Web Admin, when Login Rate has struck, it will display Online Login Failure Message.

  Successfully logging in resets the timers and counts to zero.

  On a resilient system the Publisher and Subscriber do not share a cache - each has its own - meaning that more bogus logins than configured could be attempted during system failover.

- **Session Idle Setting**—Select this to dictate how long a user can be idle before being logged off. Enter value between 1 and 60 minutes to enable the feature and set duration, or 0 to disable the function.
- **Session Management**—type the number of concurrent Web Administration log in sessions in the range 1 to 5 (default), or unlimited (0).

Step 3 Click **Save** to save the changes.

Queue Management

Depending on the number of incoming calls and staffing levels, operator queues may receive more calls than they can handle. For this reason, you must define what to do with these calls when the following overflow conditions exist for your queues:

- Maximum number of calls waiting to be answered exceeded
- Maximum call wait time exceeded
- No operator

If you want, overflowed calls can be simply discarded, but it is better to route them to an overflow destination. You must define a destination for each overflow condition, which can be different for each. In a similar way, when a queue is in emergency mode you can route calls made to it to another destination. In both cases, this destination is either an overflow number (DDI) or an overflow queue.

The overflow number cannot be the same as that of the overflow queue, and you cannot overflow a queue to itself.

The **Queue Management** option enables you to create and configure operator queues, including the overflow destinations.

Note

- For how to best set up queue overflow see **Queue Overflow - Best Practice** in the *Cisco Unified Attendant Console Advanced Design Guide*.
- If you have a resilient system and you are logged into the Subscriber server, you cannot change any of the Queue Management parameters.

Creating Queues

To create a queue:

Step 1 Choose **User Configuration** > **Queue Management**.

The **Queue Management** page is displayed.

Step 2 Click **Add New**.

Step 3 Under **General**, set the following:

- **Name**—type the name of the queue.
- **Priority**—specify the priority of the selected queue's calls in relation to calls belonging to other queues (1 highest - 99 lowest):
  - Calls in queue are prioritized from top (highest priority) to bottom (lowest priority) based on delivery queue, followed by wait time within that queue.
  - If all queues have the same priority (such as the default value - 99), then calls are arranged and/or delivered based on wait time and delivery method as opposed to delivery queue.
  - Forced delivery calls always take priority over broadcast delivery calls, irrespective of the priority specification.
- **Salutation**—optionally type a greeting to be displayed in a pop-up for the operator to use. This is the same for all servers.
- **Queue device group**—select the queue device group to use.

Step 4 Specify the **Call Delivery Method**:

- **Broadcast**—select this so that all logged-in operators can see the call in their Queued Incoming Calls (F8) pane, and any can pick up the call. This is the default queue type. If this option is selected, **Circular** and **Longest waiting** options are unavailable.
- **Forced Delivery**—select to make the queue a forced delivery queue. Selecting this option enables **Circular** (default) and **Longest waiting** options.
  - **Circular** - if **Forced Delivery** is selected, the **Circular** option is selected by default. This makes an enquiry call from the CTI Port to the next attendant handset in a circular, round-robin pattern. Attendants receive calls in a specific order, and after the last receives a call, the first receives the next one. Attendants are skipped if they are still busy on a previous call.

  - **Longest waiting** - select to change the pattern of delivering calls so that the next call is always delivered to the longest waiting attendant.

- **Forced delivery answer time (secs)**—the length of time that a forced delivery call rings at an attendant extension before it gets routed to the next available attendant, whether it is the next attendant in line or the next longest waiting attendant.

Note

The **Call Delivery Method** can be partially modified after the queue is created. If you selected **Forced Delivery** during queue creation, you can modify the queue by toggling the **Circular** and **Longest Waiting** options. However, you can't switch to **Broadcast**. Similarly, if you selected Broadcast during queue creation, you can't switch to **Forced Delivery**. In that case, you must delete the queue and then recreate it with the new method.

Step 5 Click **Save**.

You can now set the queue DDI and configure the Full CTI Failure, Emergency, Overflow and Out of House routing properties, as described in Configuring Queues.

Deleting Queues

To delete a queue:

Step 1 Choose **User Configuration > Queue Management**. The **Queue Management** page is displayed.

Step 2 Click **Find** to see the list of available queues.

Step 3 Select the checkbox of the queue(s) you want to delete.

Step 4 Click **Delete Selected**.

Configuring Queues

To configure a queue (if you are viewing the **Queue Management** page, start at Step 5):

Step 1 Choose **User Configuration > Queue Management**.

Step 2 Find the queue to configure. Specify a filter:

- Select the queue identifier to search: **Queue Name**, **Queue Type** or the **Queue DDI number**.
- A condition of the queue identifier, such as **is not empty**, or how to compare the identifier with a string, such as **begins with**.
- A string to compare to the queue identifier in the specified way (used only with **begins with, ends with, contains** and **is exactly**).

You can also add another filter using the plus (+) and minus (-) controls to narrow the search.

Step 3 Click **Find**.

Step 4 In the list of queues, click **Select** to configure that one. The **Queue Management** page is displayed. You can use this to change most of the parameters you set when creating the queue, and the emergency, overflow, and out of hours routing properties.

Step 5 Each queue requires a DDI—the number dialed internally to reach the queue session (external calls must be routed to this to reach the queue). To set or change the queue DDI, under **Association Information**, click the server you want to change.

Note In resilient installations, each queue on the Publisher and Subscriber requires a unique DDI.

The **General** page is displayed. This page is a copy of the **General** section of the main **Queue Management** page, but with a queue **DDI** field that you can edit.

Note You can set out of hours routing from this page. The process is described in Step 9.

Step 6 Enter a queue **DDI**, click **Save**, and then, in **Related Link**, select **Back to Queue**, and then click **Go**.

Step 7 In the **Queue Management** page, if required, modify the **General** properties; see Creating Queues.

Step 8 Set the following properties:

- **Full CTI Failure device**—(only in resilient installations). Type the name of the device to use if there is a full CTI failure. Calls get forwarded to this device when both servers are down and are unable to take any calls.

  If, in Cisco Unified Communications Manager, you have specified destinations for the following Call Forward and Call Pickup Settings:

  – Forward on CTI Failure

  – Forward Unregistered Internal

  and you have:

  – Configured a resilient Cisco Unified Attendant Console Advanced Administration installation

  – Assigned Publisher and Subscriber DDIs

  – Created a Queue and configured a Full CTI Failure device on the queue

  – Used Cisco Unified Attendant Console Advanced Administration to synchronize the device

  Then an AXL SOAP request synchronizes the devices on Cisco Unified Communications Manager. This sets the queue's Subscriber DDI as the forwarding destination of the queue's Publisher DDI, and the Full CTI failure device is made the forwarding destination of the queue's Subscriber DDI.

Note If you change the Full CTI Failure device or Queue DDI you must re-**Synchronize with CUCM** to update the Cisco Unified Communications Manager device configuration. For instructions on how to do this, see Synchronize with CUCM.

- **Emergency**—the destination calls must be forwarded to when the queue is in emergency mode.

  – **Destination type**—select:

  – **Device** (then type a DDI number in the **Emergency destination**),

- **Queue** (then find and select a Queue as the **Emergency destination**) or
- **None**, to disable the forwarding of Emergency calls.

If you select **Queue**, the **Find Queue** button is displayed next to the destination field; click this to display the **Queue Selection** page.

Use the **Find** controls to list particular queues (find by **Name**, **DDI** or **Queue Type**), click a radio button to select the required queue, and then click **Save**.

- **Emergency destination**—the destination DDI (if Destination type is Device), or Queue Name (if the **Destination type** is **Queue**) to which to send calls when the queue is in emergency mode.

- **Overflow**—This controls the routing (overflow) of calls from a queue when certain parameters are exceeded. It contains these properties:
  - **Maximum calls**—The maximum number of calls that can wait in the queue. Additional calls are routed to the **Maximum calls destination**.
  - **Destination type**—select:
    - **Device** (then type a DDI number in the **Maximum calls destination**),
    - **Queue** (then find and select a Queue as the **Maximum calls destination**) or
    - **None**, to disable the Maximum calls overflow.

    If you select **Queue**, click **Find Queue** to select a queue from the **Queue Selection** page, as described for the Emergency destination.
  - **Maximum calls destination**—the destination DDI (if **Destination type** is **Device**), or **Queue Name** (if the **Destination type** is **Queue**) to which to route calls when the Maximum calls parameter is exceeded.
  - **Wait Time**—The maximum time a call can wait in the queue before being routed to the **Wait time destination**. This has the format **hours:Minutes:Seconds**, with a maximum of 23:59:59
  - **Destination** type—select:
    - **Device** (then type a DDI number in the **Wait time destination**),
    - **Queue** (then find and select a Queue as the **Wait time destination**) or
    - **None**, to disable the Wait time overflow.

    If you select **Queue**, click **Find Queue** to select a queue from the **Queue Selection** page, as described for the Emergency destination.
  - **Wait time destination**—the destination DDI (if Destination type is Device), or Queue Name (if the Destination type is Queue) to which to route calls when the Wait time parameter is exceeded.
  - **Destination type**—select:
    - **Device** (then type a DDI number in the **No operator destination**),
    - **Queue** (then find and select a Queue as the **No operator destination**) or
    - **None**, to disable the No operator overflow.

    If you select **Queue**, click **Find Queue** to select a queue from the **Queue Selection** page, as described for the Emergency destination.
- **No operator destination**—the destination **DDI** (if **Destination type** is **Device**), or **Queue Name** (if the **Destination type** is **Queue**) to which to route calls when there is no operator logged into this queue.

Step 9 If you want to set out of hours routing for the queue, you must first define the out of hours periods, as described in Operator Management, and then do the following:

a. Click **Out of Hours Routing** .

The **Out of Hours Routing** page is displayed.

b. Under **General**, select the required **Out of Hours Routing template**, and then click **Apply**.

Note If the template uses the current queue as a destination, a message appears saying that you cannot apply it.

c. If you already have an out of hours routing template applied to the queue, you are prompted to do one of the following:

- **Overwrite** the existing out of hours routing settings with the selected template
- **Append** the selected template to the existing out of hours routing settings
- **Cancel** the operation and continue using the existing out of hours routing settings unchanged.

The **Specific Dates** and **Days of the Week** defined in the template are displayed.

d. If you want, you can edit the selected template.

- To add a new time period configuration, click **Add New**, specify the time period, and then click **Save**.
- To edit an existing time period configuration, click **Select alongside**, change the configuration, and then click **Save**.
- To remove time period configurations from your template, select the corresponding check boxes on the left, and then click **Delete Selected**.

For more information on editing out of hours routing templates, see Operator Management.

e. Under **Related Link**, navigate **Back to Queue**.

Step 10 Click **Save** to save the settings.

Step 11 Click **Synchronize with CUCM** to access the Synchronize with CUCM page. For more information, see Synchronize with CUCM.

Operator Management

The Operator Management option enables you to create and configure operator profiles, including associating queues with profiles. You can also import users as operators from the Cisco Unified Communications Manager or other LDAP-compliant directory servers and convert non-SSO users to SSO users.

Creating Operator Profiles

To create an operator profile:

Step 1 Choose **User Configuration** > **Operator Management**. A list of existing operators appears.

Step 2 Click **Add New**.

Step 3 Under **General**, do the following:

a. Enter a **Login name**.

b. Enter a **Passphrase**, and then re-enter it to confirm it.

c. In **Role**, select either:

- **Full**
- **VIOC** – enables attendant operators who are blind or have low vision to use the Console with the help of the JAWS screen reader. For more information, see Accessibility for Users with Disabilities.

d. To force a non-SSO user to change their passphrase when they next log in, select **Account Reset**. This setting is cleared when the user changes their passphrase.

e. To lock the account of a non-SSO user, select **Account Locked**. To unlock a locked account, clear the checkbox. For a list of situations in which an account is locked, see Credential Policy Management.

The **Last Login Date/Time (UTC)** shows the date and time that the operator last successfully logged in.

Step 4 Click **Save**.

You must now configure the operator. If you have just created an operator you can continue from Step 5.

Importing Operators

You can import LDAP contacts as operators with these user characteristics:

- Cisco Single Sign-on (SSO) Users
- Local Users – who do not use SSO and can be logged in without federation authentication. You can convert these users to SSO users by linking them to existing SSO users.

The number of contacts you can import in one go is restricted by the number specified under your Cisco Unified Attendant Console Advanced license, with a maximum of 50.

To import contacts:

Step 1 Choose **User Configuration** > **Operator Management**.

The **Operator Management** page listing existing operators appears.

Step 2 Click **Import**.

The Import Contact page appears, listing the contacts you can import from Cisco Unified Communications Manager.

Step 3 For each contact to import, select the check box in the left-hand column. All the contacts you select are imported with the Role that you choose in the next step.

Step 4 In **User Type**, select either **Local** or **SSO**.

Step 5 In **Role**, select either **Full** or **VIOC**.

Step 6 Click **Save Selected/Changes**.

The imported operators are added to the list on the Operator Management page.

Configuring Operator Profiles

You can configure operator profiles, including linking local users with SSO users so that they can use SSO.

To configure an operator profile:

Step 1 Choose **User Configuration** > **Operator Management**.

Step 2 **Find** an operator profile to manage. Specify a filter: a string to search for and where to search for it.

- Select **Login Name**.
- A condition of the login name, such as **is not empty**, or how to compare the login name with a string, such as **begins with**.
- A string to compare to the login name in the specified way (used only with **begins with, ends with, contains** and **is exactly**).

You can add another filter using plus (+) and minus (-) controls to narrow the search.

Step 3 Click **Find**.

Step 4 **Select** the operator profile you want to configure or link.

The profile information is displayed.

If any queues are associated with the operator, they are listed in **Associated Queues**.

Step 5 If required, under **General**, edit the **Login name**, **Passphrase**, and then **Confirm passphrase**.

Step 6 Under the **Role**, select either **Full** or **VIOC** (for blind people and people with low vision).

Step 7 To force the user to change their passphrase when they next log in, select **Account Reset**.

Step 8 To associate the profile with a queue, under **Queue Association**, click **Queue Association**.

You can use **Find** to search for a specific queue if it is not displayed.

Step 9 Select the queue(s) to associate with the profile and clear any already-associated queues you do not want associated.

Step 10 To convert the user profile to use SSO by linking it to an SSO User, click **Link** (if **Link** is not displayed the profile already uses SSO).

The **Link Contact** page appears.

Step 11 Select the control in the left-hand column of the row containing the contact to link to, and then click **Save Selected/Changes**.

The contact User Profile data name now matches that of the linked operator.

Step 12 Click **Save** to save the changes.

You can click **Reset passphrase** to reset the user passphrase to match the login name.

Deleting Operator Profiles

To delete an operator profile:

Step 1 Choose **User Configuration > Operator Management**. The **Operator Management** page is displayed.

Step 2 Click **Find** to see the list of available operator profiles.

Step 3 Select the checkbox of the operator profile(s) you want to delete.

Step 4 Click **Delete Selected**.

Realm Management

The Realm Management option enables you to specify which domains have access to the single sign-on (SSO) Home Realm on a Cisco Unified Attendant Console Advanced server. If no domains are assigned to the Home Realm, all SSO users have access to it. If you specify one or more domains for the realm, only users in those domains have access to the realm and to SSO.

Note You can configure the Home Realm only when logged into the Publisher server.

To configure a Home Realm or assign domains to it:

Step 1 Choose **User Configuration > Realm Management**. The **Realm Management** page appears.

Step 2 If you have a resilient installation, in **Server Details**, select the Publisher or Subscriber server, as appropriate.

Step 3 Under **Realm Management**, click **Select** alongside the Home Realm to manage (**Default SSO Home Realm**).

Step 4 Under **SSO Connectivity**, in **CUCM name or IP**, type the IP address or FQDN of the Cisco Unified Communications Manager providing SSO.

Step 5 If required, change the **CUCM port** (default, 443) and then click **Save**.

To test the SSO connection, click **Test SSO**. The connection is tested and the result displayed. To view, add, edit, or delete the domains assigned to the realm, click **Add Domain**; the **Domain Configuration** page appears. This lists the domains currently assigned to the realm and enables you to add others. You can only add domains that are valid on the selected server.

To add a new domain to the realm:

Step 1 Click **Add New**.

Step 2 Under **General**, type a **Domain Name**, and then click **Save**.

To edit a domain, under **Select Domain**, click Select alongside the domain, change the **Domain Name**, and then click **Save**.

To delete a domain, under **Select Domain**, select the appropriate check box, and then click **Delete Selected**.

System Accounts Management

This page enables you to add new system accounts and manage the personal details of all existing accounts, both master and non-master. You can have up to 50 system accounts, including the master.

Use the search bar to find existing system accounts and click **Select** to configure them. To delete accounts, check their boxes and click **Delete Selected**.

Only the master account can edit its own details. A new master account cannot be created nor can the existing one be deleted - it can, however, be disabled for security reasons. For more information, see Disabling the Master Account.

Adding New System Accounts

Go to **User Configuration > System Accounts Management**, click **Add New** to create a new account and enter the following **General** information:

- **Name**: enter a name for this system account.
- **Login name**: enter a login name. This field is required.
- **Passphrase/Confirm passphrase**: enter and confirm a passphrase.
- **Account Role**: select the appropriate Account Role from the drop-down menu. For a description of the available options, see Account Roles.
- **Account Reset**: select this option to force the newly-created user to change their passphrase when they login for the first time. (Not applicable to master account.)
- **Account Locked**: select to lock the account. (Not applicable to master account.)
- **Last Login Date/Time (UTC)**: if editing an existing account, this parameter displays the last login date and time.

Click **Save**.

Account Roles

System accounts on Cisco Unified Attendant Console Advanced Administration have varying permission levels based on the designated Account Role. The Account Role determines the options available under Administration and designates whether an account has login access to Administration while the Cisco Unified Attendant Server is in online or offline mode.

- Online Mode - the Cisco Unified Attendant Server service status is Active - Server is active and fully operational.
- Offline Mode - the Cisco Unified Attendant Server service status is anything other than Active - Server is active and fully operational.

The following account roles are ranked based on permission level, where 1 represents the highest and 5 the lowest permission level.

- **(1) Master**: referred to as the Admin account in prior releases; superuser account with full access to the system. There is only one master account. Only the master account can edit its own details. A new master account cannot be created nor can the existing one be deleted - it can, however, be disabled for security reasons. For more information, see Disabling the Master Account. This account role is a superuser and has full access in the system. The master account can login in both online and offline mode.

- **(2) Solution Administrator**: superuser account with full access to the system. It can add/amend or delete all accounts except the master. The solution administrator account can login in both online and offline mode.
- **(3) Moderator**: can add/amend or delete supervisor or reporting accounts. A moderator account can login in both online and offline mode.
- **(4) Supervisor**: can add/amend or delete reporting accounts. A supervisor account can only login in online mode.
- **(5) Reporting**: account access is limited to reporting. A reporting account can only login in online mode.

Default System Accounts

Fresh installs and upgrades from an earlier version to 14.x create the following default roles and system accounts in the system:

System account	Passphrase	Role
Admin	If this is a new install, the default passphrase is CISCO but you are required to modify the passphrase at initial login. However: • If you upgraded from a pre-v12.0 release your existing passphrase carries over, but it is converted to all caps. • If you upgraded from 12.x or later, your existing passphrase carries over unmodified.	Master
SolAdmin	CISCO	Solution Administrator
Moderator	CISCO	Moderator
Supervisor	CISCO	Supervisor
Reporting	CISCO	Reporting

Permissions by Account Role

Master

- The master account represents the ADMIN account of previous releases.
- Master account role has unrestricted access to **Administration**.

Disabling the Master Account

The master account can be disabled if required. To disable it, do the following:

Step 1 Go to *C:/Program Files (x86)/Cisco/Utilities/Master Account Control*.

Step 2 Run the *MasterAccountChange.bat* file. The **Database Wizard** opens.

Step 3 Provide the master account authentication details and click **Next**.

Step 4 Under **Account Status**, click **Disabled** and then click **Next**.

Note When you enable the master account again, its authentication details are reset to the default setting: username ADMIN and passphrase CISCO.

Step 5 For the changes to take effect, the CT server must be restarted. Go to **Engineering > Service Management** and stop and then restart the Cisco Unified Attendant Server.

Solution Administrator

The solution administrator account has full access to **Administration**.

Solution Administrator-specific Restrictions

Menu/Web Admin page	Note
User Configuration > System Accounts	Cannot modify the master account.

Moderator

The moderator account has limited access to the system. It has the following permissions and specific restrictions.

Menu/Web Admin page	Read	Add	Amend	Delete	Note
Engineering > Presence Management	Y	N	N	N	Read-only permission. Applicable to main and its sub-pages.
Engineering > Database Purge	Y	N	N	N	Read-only permission. Applicable to main and its sub-pages.
Engineering > Service Management	Y	N	Y	N	Full control on main and its sub-pages. Amending permission allows user to stop/start the services.
Engineering > Logging Management	Y	N	Y	N	Full control on main and its sub-pages.
System Configuration > Directory Source Management	Y	N	N	N	Read-only permission. Applicable to main and its sub pages.
System Configuration > Contact Management	Y	Y	Y	Y	Full control on main and its sub pages.
System Configuration > Directory BLF Rules	Y	N	N	N	Read-only permission. Applicable to main and its sub pages.
User Configuration > General Properties	Y	N	Y	N	Limited access. Can modify settings except those indicated in Moderator-specific Restrictions.
User Configuration > System Accounts	Y	Y	Y	Y	Limited access. Can Add/Amend/Delete system accounts of “Moderator”, “Supervisor” and “Reporting” roles as well as modify its personal details. For more

Menu/Web Admin page	Read	Add	Amend	Delete	Note
					information, see Moderator-specific Restrictions.
User Configuration > Operator Management	Y	Y	Y	Y	Full control on main and its sub pages.
User Configuration > Queue Management	Y	N	Y	N	Limited access. Can perform search and amend queue configuration except those indicated in Moderator-specific Restrictions.
User Configuration > Templates > Out of Hours Routing	Y	Y	Y	Y	Full control on main and its sub pages.
Bulk Administration > Upload/Download Files	Y	Y	N	Y	Full control on main and its sub pages.
Bulk Administration > Insert Contacts	Y	Y	N	N	Full control on main and its sub pages.
Bulk Administration > Update Contacts	Y	Y	N	N	Full control on main and its sub pages.
Bulk Administration > Export Contacts	Y	Y	N	N	Full control on main and its sub pages.
Bulk Administration > Job Scheduler	Y	N	Y	Y	Full control on main and its sub pages.
Help > Contents	Y	N	N	N	Full control on main and its sub pages.
Help > This page	Y	N	N	N	Full control.
Help > Licensing	Y	N	N	N	Read-only permission.
Help > Last Login Info	Y	N	N	N	Read-only permission.
Help > About	Y	N	N	N	Read-only permission.
Cisco Unified Reporting > System Reports	Y	N	N	N	Full access to all system reports.
Replication Management	Y	N	N	N	Read-only permission.
User Configuration > Credential Policy Management	Y	Y	Y	N	

Moderator-specific Restrictions

Menu/Web Admin page	Note
User Configuration > System Accounts	Cannot modify Passphrase and Role of Master Account (ADMIN). Cannot add/amend/delete system accounts having "Solution Administrator" Roles. Rank information stored in role group configuration will help in restricting it.
User Configuration > Queue Management	Cannot amend DDI and Queue Device Group. Cannot Synchronize with CUCM.
User Configuration > General Properties	Cannot modify Internal/External Access, Default FAC and CMC Settings, Default queue device group, Call Arrival Mode, Call Logging Setting, Login Rate Setting, Session Idle Setting.

Supervisor

The supervisor account has limited access to the system. It has the following permissions and specific restrictions.

Menu/Web Admin page	Read	Add	Amend	Delete	Note
System Configuration > Contact Management	Y	Y	Y	Y	Full control on main and its sub-pages.
System Configuration > Synchronize with CUCM	Y	N	N	N	Read-only permission. Applicable to main and its sub-pages.
Engineering > Database Purge	Y	N	N	N	Read-only permission. Applicable to main and its sub-pages.
User Configuration > System Accounts	Y	Y	Y	Y	Limited access. Can Add/Amend/Delete system accounts of "Supervisor" and "Reporting" roles as well as modify its personal details. For more information, see Supervisor-specific Restrictions.
User Configuration > Operator Management	Y	Y	Y	Y	Full control on this page and its sub-pages.
User Configuration > Queue Management	Y	N	Y	N	Limited access. Can perform search and amend queue configuration with several exceptions. For more information, see Supervisor-specific Restrictions.

Menu/Web Admin page	Read	Add	Amend	Delete	Note
User Configuration > Templates > Out of Hours Routing	Y	Y	Y	Y	Full control on main and its sub-pages.
Bulk Administration > Upload/Download Files	Y	Y	N	Y	Full control on main and its sub-pages.
Bulk Administration > Insert Contacts	Y	Y	N	N	Full control on main and its sub-pages.
Bulk Administration > Update Contacts	Y	Y	N	N	Full control on main and its sub-pages.
Bulk Administration > Export Contacts	Y	Y	N	N	Full control on main and its sub-pages.
Bulk Administration > Job Scheduler	Y	N	Y	Y	Full control on main and its sub-pages.
Help > Contents	Y	N	N	N	Full control on main and its sub-pages.
Help > This page	Y	N	N	N	Full control on this page.
Help > Licensing	Y	N	N	N	Read-only permission.
Help > Last Login Info	Y	N	N	N	Read-only permission.
Help > About	Y	N	N	N	Read-only permission.
Cisco Unified Reporting > System Reports	Y	N	N	N	Full access to all system reports.
Replication Management	Y	N	N	N	Read-only permission.
User Configuration > Credential Policy Management	Y	N	N	N	Read-only permission.

Supervisor-specific Restrictions

Menu/Web Admin page	Note
User Configuration > System Accounts	Cannot modify Passphrase and Role of Master Account (ADMIN). Cannot add/amend/delete system accounts having “Solution Administrator” and “Moderator” Roles. Rank information stored in role group configuration will help in restricting it.
User Configuration > Queue Management	Cannot amend DDI and Queue Device Group. Cannot synchronize with CUCM.

Reporting

The reporting account has limited access to the system. It has the following permissions and specific restrictions.

Menu/Web Admin page	Read	Add	Amend	Delete	Note
Cisco Unified Attendant Console Administration > User Configuration > System Accounts	Y	Y	Y	Y	Limited access. Can Add/Amend/Delete system accounts of "Reporting" role as well as modify its personal details. For more information, see Reporting-specific Restrictions.
Cisco Unified Reporting > System Reports	Y	N	N	N	Full access to all system reports.
Help > This page	Y	N	N	N	Full control on this page.
Help > Contents	Y	N	N	N	Full control on main and its sub-pages.
Help > About	Y	N	N	N	Read-only permission.

Reporting-specific Restrictions

Menu/Web Admin page	Note
User Configuration > System Accounts	Cannot modify Passphrase and Web Admin Role of Master Account (ADMIN). Cannot add/amend/delete system accounts having "Solution Administrator", "Moderator" and "Supervisor" roles.

Modify Passphrase

To change the passphrase:

Step 1 Go to User **Configuration > Account Passphrase Change**.

Step 2 Enter the current passphrase in **Old passphrase**.

Step 3 Type the **New passphrase**.

It is good practice to have a strong passphrase that utilizes both numeric and alpha characters. The Cisco Unified Attendant Console Advanced server allows up to a maximum of 20 characters including the use of special characters such as %, $, £, &.

Note The passphrase is case-sensitive.

Step 4 Re-enter the new passphrase in **Confirm new passphrase**.

Step 5 Click **Save** to save the changes.

Credential Policy Management

The Credential Policy Management feature enables you to define the lifetimes of the passphrases used by Console Client users when they log in, and the conditions under which the Cisco Unified Attendant Console Advanced server locks out Console Client users to prevent Denial of Service (DOS) attacks on the system.

Note

- The credential policy affects both Operators and Web Administration accounts.
- The **Master** account on the Web Administration will never be locked. Instead, users can disable this account by following the instructions under Disabling the Master Account.

Passphrases identify authorized users. This feature enables you to define, system-wide:

- How long before a user passphrase must be changed - users are prompted to change their passphrases before they are due to expire.
- How long before a new user passphrase can be changed - this prevents frequent changes of legitimate passphrases, as might be attempted by a bogus user.
- How long before an old user passphrase can be reused - to ensure that users enter new passphrases rather than simply re-use old ones.
- How many of the most recent passphrases cannot be re-used - to ensure that users enter new passphrases rather than simply re-use old ones.
- The composition of passphrases: their minimum length and the minimum numbers of the following character types they must contain:
  - Numeric
  - Special

Note

Certain combinations of special and normal characters are not allowed as they resemble malicious code used in attacks on the Web Administration application. If you choose such a combination, for example, "<" followed by a character, an error message is displayed.

  - Lower case letters
  - Upper case letters

Note

- The minimum number of any of these character types must not be greater than the minimum passphrase length.
- Minimum upper and lower case letter check will not work for the following languages: Arabic, Chinese (simplified), Chinese (traditional), Hebrew, traditional Cantonese, Japanese, Korean.

- Whether passphrases in the passphrase dictionary can be used. The passphrase dictionary is a database containing a list of common passphrases that might be used by dictionary attack software.

Console Client user lockout (when a user is locked out, the server does not respond to login requests) is configured with the following parameters:

- The number of failed login attempts by a user before the account is locked.
- The period after a failed login attempt during which further failed attempts may lock the account.
- How long an account can remain inactive (no logins) before it is locked out.
- How long before their passphrase expires that the server starts sending change warnings to users.
- The number of expiry warnings that can be dismissed by a user before the account is locked.
- How long after their passphrase expires before a user's account is locked.

Note

- If a user account is locked due to passphrase expiry and the administrator unlocks the user account from the Web Admin application without changing the passphrase, the account will be locked again when the user tries to login. To avoid this, the administrator must change the passphrase after unlocking the account.
- The **Master** account on the Web Administration will never be locked. Instead, users can disable this account by following the instructions under Disabling the Master Account.

To configure the login credential policy, do the following:

Step 1 Choose **User Configuration > Credential Policy Management**.

Step 2 Type the **Passphrase Lifetime** and **Passphrase Content** parameters.

Step 3 Type the **Account Lockout** parameters.

Step 4 Click **Save**.

Templates

Configuring Out of Hours Routing

The out of hours routing feature enables you to define destinations (numbers or queues) to which calls to a queue are routed outside office hours or during staff breaks. Each queue can have its own out of hours routing configuration.

Note The out of hours configuration refers to the date and time on the server hosting the queue. It is not defined for other time zones.

Out of hours routing is defined using named templates, which you apply to your queues, as described in Configuring Queues. The template's profile defines the out of hours date and time period(s) and the destination to receive the calls during that period.

Note A queue's out of hours routing configuration is set at the instant a template is applied. If you change a template after it has been applied to a queue, those changes do not affect the queue.

You can create out of hours routing templates either from scratch (you define all properties of the template) or by copying an existing template and then editing its properties.

Note

If you have upgraded a pre-version 10.0 Cisco Unified Attendant Console Advanced installation to version 10 or later, and your old installation had working days configured, during the upgrade the details are automatically incorporated into your out of hours routing configuration for all existing queues. For example, if your previous working days were set to Monday, 9 am to 5 pm, your new out of hours settings will be:

- All day Tuesday to Sunday
- Monday from 12 am to 9 am, and 5 pm to 11.59 pm

Creating Out of Hours Routing Templates From Scratch

To create an out of hours routing template from scratch, do the following:

Step 1 Choose **User Configuration** > **Templates** > **Out of Hours Routing**.

The **Out of Hours Routing Template** page appears.

Step 2 Click **Add New**.

Step 3 Under **General**, type a **Template name** (up to 50 alphanumeric characters and spaces; each name must be unique), and then click **Save**.

Step 4 If you want to change the Template name, enter the new name, and click **Update**.

You now need to define the out of hours date and time periods.

Step 5 Click **Add New**.

The **Time Period Configuration** page is displayed.

Step 6 Under **General**, select the **Configuration type**, either **Day** (of the week) or **Date** (specific calendar date).

Note

- Your template can contain both configuration types, with multiple definitions of each. You define each of these separately by repeating Step 5 to Step 12.
- If you specify a Date which matches a Day configuration, the Date overrides the Day. For example, if you have break hour defined for every Monday, and a break hour for a specific date that happens to be a Monday, the system uses the Date break hour information to forward calls to the destination.

Step 7 Depending on the selected Configuration type, do one of the following:

If you selected **Day** in the previous step:

a. Select the **Day(s) of the week** on which the out of hours period occurs. You must select at least one day.

b. Select the **From** and **To** times marking the start and end of the out of hours period.

These time periods apply to all the days of the week selected, and an editable time period is created for each day.

If you selected **Date** in the previous step:

a. Select or enter (in YYYY-MM-DD format) the **Specific date** on which the out of hours period occurs.

b. Select the **From** and **To** times marking the start and end of the out of hours period. These time periods apply to all the dates selected.

Step 8 Click **Save**.

Note

- You cannot change a saved Configuration type; if you made a mistake, you must delete it and create a new one.
- If you specify a date and time period that is already defined in the template, you are notified that you must change it.

You are now prompted to define the destination—queue or device—to which calls are routed during the specified time period.

Step 9 Select the **Destination type**; either **Queue** or **Device** (the default).

Step 10 Depending on the selected Destination type, do one of the following:

- If you selected **Device** in the previous step, type the corresponding **Destination** number, and then continue at Step 11.
- If you selected **Queue** in the previous step, either:
  - Type the name of the queue and then continue at Step 11.
  - Click **Find Queue**, then select the queue profile and click **Save**, and then click **Back to Time Period Configuration**.

Step 11 Click **Save**.

Step 12 Click **Back to Out of Hours Routing Template** to view the template.

Step 13 Repeat Step 5 to Step 12 for each time period you want in your template.

The **Specific Dates** you add to your template are displayed in date and time order. The Days of Week you add to your template are displayed in day and time order, starting with Monday.

Creating Out of Hours Routing Templates by Copying

To create an out of hours routing template by copying an existing template, do the following:

Step 1 Choose **User Configuration** > **Templates** > **Out of Hours Routing**.

The **Out of Hours Routing Template** page appears.

Step 2 If necessary, **Find** the template(s) to copy.

Step 3 Alongside the template to copy, click **Copy** .

Step 4 Under **General**, type a **Template name** (up to 50 alphanumeric characters, each name must be unique), and then click **Save**.

A new template is created with the name you just typed and the profile of the template you copied.

Step 5 If you want to change the **Template name**, enter the new name, and click **Update**.

Step 6 Do the following, as required:

- Define new out of hours date and time periods, as described in Creating Out of Hours Routing Templates From Scratch.
- Change existing out of hours date and time periods, as described in Editing Out of Hours Routing Templates.

Deleting Out of Hours Routing Templates

To delete an out of hours routing template, do the following:

Step 1 Choose **User Configuration** > **Templates** > **Out of Hours Routing**.

The **Out of Hours Routing Template** page appears.

Step 2 If necessary, **Find** the template(s) to delete.

Step 3 Click the appropriate check boxes on the left or use the **Select All** (on page) or **Select All In Search** (including any other pages of results) to select the template(s) to delete.

Step 4 Click **Delete Selected**.

Editing Out of Hours Routing Templates

To edit an out of hours routing template, do the following:

Step 1 Choose **User Configuration** > **Templates** > **Out of Hours Routing**.

The **Out of Hours Routing Template** page appears.

Step 2 If necessary, **Find** the template(s) to edit.

Step 3 Click **Select** next to the template to edit.

Step 4 If you want to change the name of the template, under **General**, type the new **Template name**, and then click **Update**.

Step 5 Do the following as required:

- To add a new time period configuration (Specific Dates or Days of the Week) follow the instructions in Creating Out of Hours Routing Templates From Scratch.
- To edit an existing time period configuration, click **Select** alongside, change the configuration, and then click **Save**.
- To remove time period configurations from your template, select the corresponding check boxes on the left, and then click **Delete Selected**.

Cisco Unified Attendant Console Administration – Bulk Administration

The following chapter describes how to configure the **Bulk Administration** menu options in Cisco Unified Attendant Console Administration.

Upload/Download Files

To upload a new CSV file to the server, do the following:

Step 1 Choose **Bulk Administration > Upload/Download Files**.

The **Upload/Download Files** page appears.

Step 2 Click **Add New**.

The **File Upload Configuration** page appears.

Step 3 Browse to the **File** to upload.

Step 4 Select whether to **Insert contacts** (the contacts will be added to the database when imported) or **Update contacts** (the contacts will overwrite/update matching contacts in the database when imported). The uploaded file is tagged with the transaction you choose.

Step 5 If you want to overwrite an existing file with the same name when you upload the file, select **Overwrite File if it exists**. If a matching CSV file is being processed, you cannot overwrite it.

Step 6 Click **Save**.

The file is uploaded to the server. During uploading the file format is validated, and any errors are displayed.

Managing Uploaded CSV Files

You can delete or download CSV files that have already been uploaded to the server in the following way:

Step 1 Choose **Bulk Administration > Upload/Download Files**.

The **Upload/Download Files** page appears.

Step 2 Find the file either by **File Name** or **File Type** (where the file type is the transaction type: **Update contacts, Insert contacts**, or **Exported contacts**).

Matching files are listed.

Step 3 Select the relevant file(s) from the list. Either select the check box, or use the **Select All, Clear All, Select All In Search** and **Clear All In Search** controls, as required.

Step 4 You can now delete or download the selected files.

Note You cannot delete a file if it is linked with a scheduled job. To delete such a file you must delete that job as well.

- To delete the files, click **Delete Selected**.
- To download the files to your computer, click **Download Selected**.
  - If you selected just one file, you are prompted to **Open** or **Save** it.
  - If you selected more than one file, they are stored in a ZIP archive, which you are prompted to **Open** or **Save**.

Insert, Update and Export Contacts

Note The following fields are excluded from contact imports, updates, and exports: Alternate First Name, Alternate Last Name, Alternate Department, Linked Alternate Contacts, Linked Assistants.

Inserting and Updating Contacts

Depending on the type of CSV file that you have created from the upload (Update contacts or Insert contacts), you can either update the contacts in the full directory or add to them (insert new contacts); and you can do either immediately or at a more convenient time using the Job Scheduler, as described in Job Scheduler.

Note Files containing non-English/Unicode characters must be in UTF8 format.

Inserting Contacts

To insert contacts from a CSV file, do the following:

Step 1 Choose **Bulk Administration > Insert Contacts**.

The **Insert Contacts Configuration** page appears.

Step 2 Under **Insert Contacts**, select a file. Only files of the correct type are offered. You can use each CSV file in only one job.

If you want, you can view the contents of the file (click **View File**) or the contents of a sample file (click **View Sample File**).

Step 3 If required, edit the **Job Description** to give it a unique identity.

Step 4 Select either **Run immediately**, to run the job when you click **Save** in the next step, or **Run Later**, to run the job using the **Job Scheduler**.

Step 5 Click **Save**.

An insert contacts job is created.

Updating Contacts

To update contacts using a CSV file, do the following:

Step 1 Choose **Bulk Administration > Update Contacts**.

The **Update Contacts Configuration** page appears.

Step 2 Under **Update Contacts**, select a file. Only files of the correct type are offered. You can use each CSV file in only one job.

If you want, you can view the contents of the file (click **View File**) or the contents of a sample file (click **View Sample File**).

Step 3 If required, edit the **Job Description** to give it a unique identity.

Step 4 Select either **Run immediately**, to run the job when you click **Save** in the next step, or **Run Later**, to run the job using the **Job Scheduler**.

Step 5 Click **Save**.

An update contacts job is created.

Exporting Contacts to CSV Files

You can export selected contacts into a CSV file for archiving or sharing. You cannot schedule the exporting of contacts. To export contacts to a CSV file, do the following:

Step 1 Choose **Bulk Administration > Export Contacts**.

The **Export Contacts** page appears.

Step 2 Find contacts to export by matching against one of the following:

- First name

- Last name
- Department
- Extension
- Locations
- Business 1
- Full Job Title
- Mobile
- User field 1

Matching contacts are listed.

Note You can apply multiple filters to select just those contacts you want to export.

Step 3 Click **Next**.

Step 4 Under **General**, enter the name of the CSV file to contain the contacts. The file name can be up to 11 characters long.

Step 5 Click **Save**.

The contacts are exported. You cannot export one set of contacts until the last export has completed.

Step 6 If you are exporting large numbers of contacts, you can check how it is progressing by clicking **Export Contact Report**.

You can list and access the exported file under **Bulk Administration > Upload/Download Files**.

Job Scheduler

You can automatically insert and update contacts in the full directory at a later time or date using the Job Scheduler. First, create the job as described in Inserting and Updating Contacts, and then configure it as follows:

Step 1 Choose **Bulk Administration > Job Scheduler**.

The **Job Scheduler** page appears. Use this page to schedule or activate/deactivate jobs.

Step 2 Find the job either by **Job Description, Scheduled Date Time**, or **Job Status** (described below):

Job Status	Meaning
Inactive	Job not activated and never run.
Pending	Job activated and scheduled to run.
Processing	Job running. You can stop the job by selecting it and then deactivating it using the controls.

Job Status	Meaning
Failed	Job failed because of: • File not found or can't be opened. • Unique reference not found • File has invalid format.
Expired	Job not activated and run before its configured date and time.
Stopped	Job deactivated by user or LDAP server stopped it during shut down.
Suspended	Link to one of the following has failed: Arc Server, Configuration database, CSV driver.
Completed	Job completed successfully.

Matching jobs are listed.

Step 3 Select the relevant job from the list. Either select the check box, or use the **Select All, Clear All, Select All In Search** and **Clear All In Search** controls, as required.

Note You cannot reconfigure or re-schedule completed jobs.

Step 4 Within the job to schedule, click **Select**.

Step 5 Under **Scheduled Date/Time**, enter or select a **Date**, then enter or select a **Time** in the formats indicated. If you do not set the date and time, the job will be configured to run immediately.

Step 6 Click **Save** to save your changes.

Step 7 Saved jobs will not be processed until you activate them. To activate the job, ready for processing, click **Activate Job**. You can deactivate an activated job by clicking **Deactivate Job**. You can use **Activate Selected** and **De-activate Selected** to activate or deactivate all selected jobs. If a job has completed, you cannot activate or deactivate it.

Note When a job has been run, you cannot reconfigure it.

Cisco Unified Attendant Console High Availability

Cisco Unified Attendant Console Advanced server high availability is provided partly by server replication. For more information on high availability, see Server High Availability.

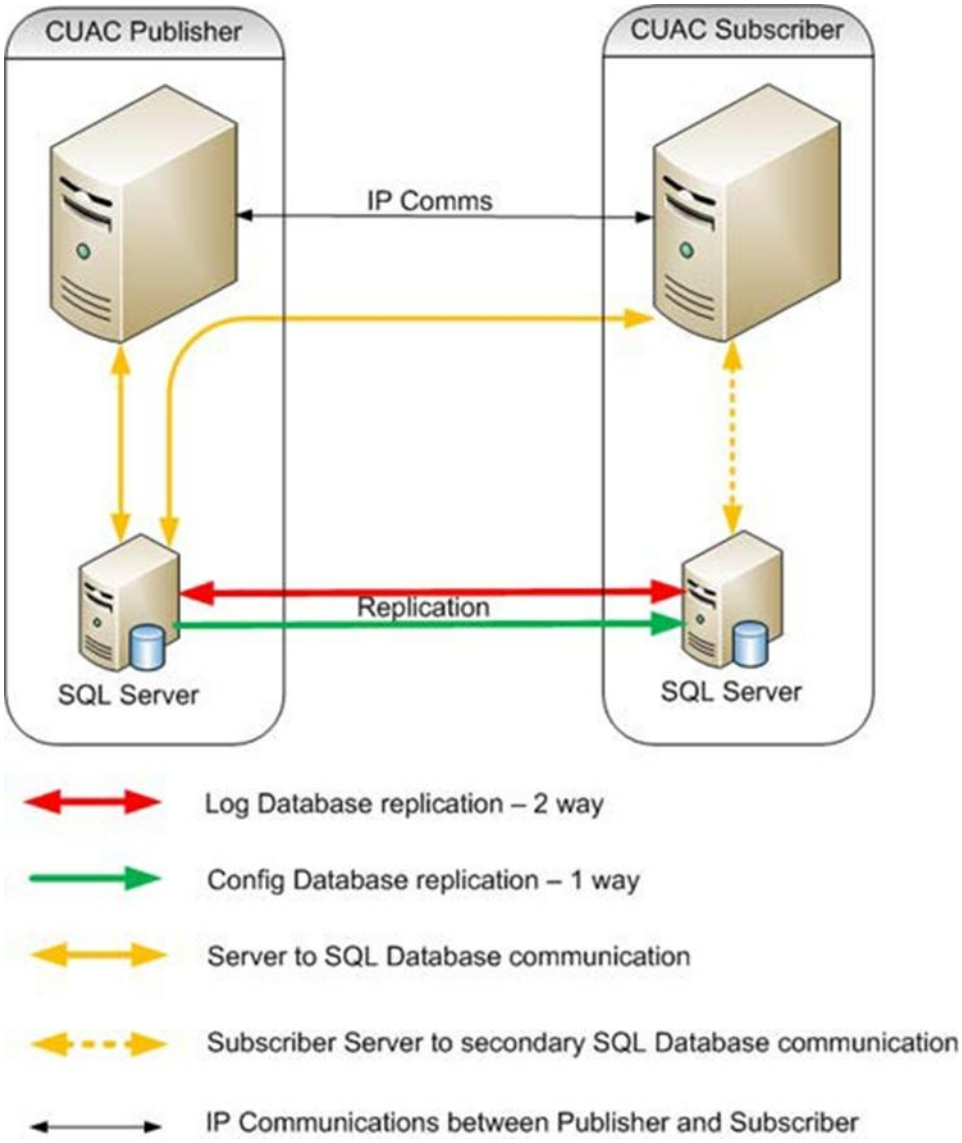
Cisco Unified Attendant Console Advanced contains two databases:

- Configuration database, ATTCFG, which contains all user configurations and the contact directories.
- Logging database, ATTLOG, which is responsible for logging.

The Configuration database is synchronized between the Publisher and Subscriber server using SQL Server replication and the synchronization of database objects across multiple database servers. The configuration database can be updated only on the Publisher server. The copy on the Subscriber server is read-only.

The Logging database is synchronized between Publisher and Subscriber using Microsoft DTC. Log information is replicated both ways between the SQL databases on the servers, with the log on each containing a full record of call transactions on both servers. The copy on the Subscriber server allows limited adding, amending, and deleting of user/call-related real-time activities when the Publisher logging database is unavailable.

The connections between Publisher and Subscriber required for high availability are summarized in this figure:



Note

- Database replication is uninstalled automatically during Cisco Unified Attendant Console Advanced server installation, upgrade, or uninstallation. If the replication uninstall does not succeed at the first attempt, you are prompted to retry it or abort it.
- Do not install Cisco Unified Replication during SQL Server installation, and do not manually configure it using SQL Server Feature Selection. Set up server high availability through Cisco Unified Replication only. If you do install or configure Cisco Unified Replication within SQL Server, you may experience unexpected results and other problems

SQL Server Replication

SQL Server replication involves these types of replication:

- Snapshot replication
- Transactional replication

Snapshot replication makes an exact copy (snapshot) of the Publisher and distributes it to the Subscriber; this includes queue and operator details, and the contact directory. It does not monitor for updates to the data. Snapshot replication is used to provide the initial data set for transactional replication; and it can also be used to completely refresh the data on the subscriber. After the initial snapshot, the Subscriber is kept up to date with the Publisher using transactional replication. Subsequent data transactions (INSERTed, UPDATEd, and DELETEd data) in the Publisher are captured by the transaction log and then stored in the distribution database, which acts as a data queue. The changes are then propagated and applied to the Subscriber in the order in which they occurred.

- SQL Server replication uses standalone programs called agents to track changes and distribute data between databases. The agents are:
- SQL Server Agent—executes scheduled administrative tasks or jobs consisting of one or more job steps. Job information is stored in the SQL Server. The other agents run as directed by this agent; and it is required for the Publisher and Subscriber to be able to talk to each other.
- Distributor Agent—moves the snapshot and transactions from Publisher to Subscriber.
- Q Reader—a SQL Server agent that handles the data queues.
- Snapshot Agent—prepares snapshot files containing schema and data of published tables and database objects, stores the files in the snapshot folder, and records synchronization jobs in the distribution database.
- Log Agent—monitors the transaction log of each database configured for transactional replication, and copies the transactions marked for replication from the transaction log into the distribution database.

You can check how the agents are running using the Monitor Replication function, described in Monitoring Replication.

Accessing High Availability Administration Menus

Pre-requirements for Installing and Uninstalling Replication

You configure replication using **Cisco Unified Replication**, with the following restrictions:

- Full replication functionality is available only if a current high availability license and SQL Server Standard or Enterprise edition are installed on the Publisher server.
- If the license has expired, or if there is no high availability license installed, you can only uninstall any existing replication.

Note

- When you have installed a Publisher or Subscriber server you cannot convert it into the other type.
- The date, time and time zone on the Publisher and Subscriber machines must be the same, otherwise Console users will not be notified that the Publisher has become available after recovering from a failure and will be unable to switch from the Subscriber back to the Publisher. One way to achieve this is to synchronize the time of both servers with the same time server.

To access the Replication Management menus, do the following:

Step 1 On the Publisher server, in Cisco Unified Attendant Console Advanced Administration, use the **Navigation** control at the right-hand end of the banner to select **Cisco Unified Replication** and click **Go**.

The **Cisco Unified Replication** home page is displayed.

Step 2 Click **Replication Management**.

The **Replication Management** page is displayed. This lists the databases on the selected server:

- ATTCFG—the configuration database
- ATTLOG—the logging database

The **Publication Name** is a unique name used by SQL Server during replication. It has the format <Server_Name>_<Database_Name>. A database with a Publication name (a publication) has replication configured.

Step 3 Under **Server Details**, select the server to check or configure.

Step 4 Under **Replication Management**, click **Select** alongside the database to check or configure.

The **Information** for that database is displayed, below which are the following control buttons:

- **Install Replication**
- **Uninstall Replication**
- **Reinitialize Replication**
- **Monitor Replication**
- **Validate Replication**
- **Replication Report**

Installing Replication

Note

The information in this section refers to using SQL Server 2019 Standard Edition. If you are using a different version or edition the information may be slightly different. The equivalent information is described in your SQL Server user documentation.

The CT and LDAP servers on the Publisher and the CT server on the Subscriber are stopped when you install, uninstall or re-initialize replication.

IMPORTANT: Installing replication shuts down both servers. Consequently, after installing replication you must either restart your computer or restart the services as described in Service Management.

Before installing or uninstalling replication, you must ensure that the SQL Server network uses the correct protocols and settings:

- On both the Publisher and Subscriber, the SQL Server Service (MSSQLSERVER) must be running under the Network Service account.
- On the Publisher, the SQL Agent Service must be running under the Local System account.
- On both Publisher and Subscriber, MSSQLSERVER and the Clients must have TCP/IP, Shared Memory and Named Pipes protocols enabled.

How to do these is explained below.

Ensuring that MSSQLSERVER is running under the Network Service account

On both the Publisher and Subscriber, do the following:

Step 1 Click the **Start** button, and then, in the **Start** menu, choose **Administrative Tools** > **Component Services**.

The **Component Services** window appears.

Step 2 In the navigation pane, select **Services (Local)**.

Step 3 In the list of services, right-click **SQL Server (MSSQLSERVER)**, and then select **Properties**.

The **SQL Server (MSSQLSERVER) Properties** dialog box appears.

Step 4 Click the **Log On** tab.

Step 5 Select **This account**, and then click **Browse**.

Step 6 In **Enter the object name to select**, type **Network Service**, and then click **OK**.

Step 7 In the **SQL Server (MSSQLSERVER) Properties** dialog box, click **OK**.

Ensuring that the SQL Agent Service is running under the Local System account

On the Publisher, do the following:

Step 1 Click the **Start** button, and then, in the **Start** menu, choose **Administrative Tools** > **Component Services**.

The **Component Services** window appears.

Step 2 In the navigation pane, select **Services (Local)**.

Step 3 In the list of services, right-click **SQL Server Agent (MSSQLSERVER)**, and then select **Properties**.

The **SQL Server Agent (MSSQLSERVER) Properties** dialog box appears.

Step 4 Click the **Log On** tab.

Step 5 Select **Local System account**, and then click **OK**.

Ensuring that MSSQLSERVER has TCP/IP, Shared Memory, and Named Pipes protocols enabled

On both the Publisher and Subscriber, do the following:

Step 1 Click the **Start** button, and then, in the **Start** menu, choose **All Programs** > **Microsoft SQL Server <version>** > **Configuration Tools** > **SQL Server Configuration Manager**.

Step 2 In the navigation pane, expand **SQL Server Network Configuration**, and then select **Protocols for MSSQLSERVER**.

Step 3 In the list of protocols, do the following:

- Double-click **TCP/IP** to display its properties; then, under the **Protocol** tab, set **Enabled** to **Yes**, and then click **OK**.
- Double-click **Shared Memory** to display its properties; then, under the **Protocol** tab, set **Enabled** to **Yes**, and then click **OK**.
- Double-click **Named Pipes** to display its properties; then, under the **Protocol** tab, set **Enabled** to **Yes**, and then click **OK**.

Before installing or uninstalling replication you must also:

- Close SQL Management studio and all SQL connections. If you do not, the installation or uninstallation may fail.
- If you have a firewall on the Publisher or Subscriber server, on the affected servers configure Firewall Exceptions for:
  - Windows Management Instrumentation (WMI)
  - Port 135 (TCP) used by WMI

Note WMI calls use port 135 before choosing a random port. During the Resilience installation, the CUAC process uses WMI to connect to an alternate server. This port is only required during the installation/ uninstallation and replication configuration.

  - Distributed Transaction Coordinator (MSDTC)
  - Port 1433 (used by the SQL Server)
  - Port 1864 (used by the BLF plug-in)
  - Ports 61616 and 61618, to enable messages to pass between the servers

Note When you configure an exception, you should also configure its scope settings; these define which computers are allowed to send traffic for an exception. Choose the scope appropriate to your network setting.

Installing Replication on a Specific Database

You must install replication on both the ATTCFG and ATT LOG databases on both the Publisher and the Subscriber. Configure the Publisher databases before configuring the Subscriber databases.

To install replication on a specific database:

Step 1 On the Publisher server, select the database as described in Step 4.

Step 2 Under **Server Credentials (<server_name>)**, type the **Windows username** (domain name\username, fully qualified domain name\username, or server name\username as required by your local and group security policies) and **Password** of a user with local administrator rights to the opposite server.

Note To ensure password composition is supported, see Supported Windows, SQL Server, Active Directory, Presence Server, Application User and CUAC Password Characters.

Note If leveraging a Windows account other than the default hostname/administrator or domain administrator account, a registry modification is required on the publisher and subscriber Cisco Unified Attendant Console Advanced servers. The change immediately goes into effect.

1. Open **RegEdit**.
2. Navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System*.
3. Look for an existing key called **LocalAccountTokenFilterPolicy**. If it does not already exist, do the following:
    a. Right-click and select **New > DWORD (32-bit) Value**.
    b. Input Name: **LocalAccountTokenFilterPolicy**.
4. Double-click the line item and select **Hexadecimal**.
5. Input Value: **1**, and then click **OK**.
6. Close RegEdit and proceed as required.

Step 3 Click **Install Replication**.

Step 4 In the message, click **OK** to confirm that you want to install replication on that database.

Replication is installed. You can check the progress of the installation by clicking **Replication Report**. For more information, see Replication Report.

When replication has been installed for that server and database, click **Go** next to **Related Link: Back to Replication** and repeat this procedure for each remaining databases.

Uninstalling Replication

Before uninstalling replication, perform the checks and procedures at the start of Installing Replication.

To uninstall replication:

Step 1 On the Publisher server, in Cisco Unified Attendant Console Administration, use the **Navigation** control at the right-hand end of the banner to select **Cisco Unified Replication**, and then click **Go**.

The **Cisco Unified Replication** home page is displayed.

Step 2 Click **Replication Management**.

The **Replication Management** page is displayed.

Note Replication must be uninstalled from the Subscriber server first; then from the Publisher server.

Step 3 Under **Server Details**, select the Subscriber server.

Step 4 In the ATTCFG row, click **Select**.

Step 5 Type the user credentials.

Note To ensure password composition is supported, see Supported Windows, SQL Server, Active Directory, Presence Server, Application User and CUAC Password Characters.

Note If leveraging a Windows account other than the default hostname/administrator or domain administrator account, a registry modification is required on the publisher and subscriber Cisco Unified Attendant Console Advanced servers. The change immediately goes into effect.

1. Open **RegEdit**.
2. Navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System*.
3. Look for an existing key called **LocalAccountTokenFilterPolicy**. If it does not already exist, do the following:
    a. Right-click and select **New > DWORD (32-bit) Value**.
    b. Input Name: **LocalAccountTokenFilterPolicy**.
4. Double-click the line item and select **Hexadecimal**.
5. Input Value: **1**, and then click **OK**.
6. Close RegEdit and proceed as required.

Step 6 Select **Uninstall Replication**, and then click **OK** to confirm that you want to uninstall replication.

Replication is uninstalled for the ATTCFG database.

Step 7 Click **Replication Report** or **Monitor Replication** to check progress of the uninstallation.

For details of using these controls, see Replication Report and Monitoring Replication.

Step 8 When replication has been uninstalled for ATTCFG, repeat Step 4 to Step 7 for the ATTLOG database (substitute ATTLOG for ATTCFG in the instructions).

Step 9 When replication has been uninstalled on both databases on the Subscriber server, repeat Step 3, this time selecting the Publisher server, and then repeat Step 4 to Step 8 to uninstall replication on both its databases.

Re-initializing Replication

If replication has been suspended as a result of a Publisher-Server communication failure, you can re-initialize it. Re-initialization restores the Publisher snapshot to the Subscriber and re-starts transactional replication.

Note If replication has been dropped you must install replication again, as described in Installing Replication.

To re-initialize replication for a selected database on a selected server:

Step 1 In the **Replication Management** page, select the database as described in Step 4.

Step 2 Click **Reinitialize Replication**.

Step 3 Click **OK** to confirm that you want to reinitialize replication.

Monitoring Replication

To monitor how replication is proceeding for a server and database selected as described in Step 4, do the following:

Step 1 In the **Replication Management** page, select the database as described in Step 4.

Step 2 Click **Monitor Replication**.

The **Monitor Replication** page is displayed. It contains details of the following:

- the Publisher and Subscriber servers
- the replication latency—the time delay between transaction at the Publisher resulting in a corresponding transaction at the Subscriber
- the throughput—the bandwidth of the replication—the data transfer rate in database rows per second
- the states of the replication agents

Step 3 To update the display, click **Refresh**.

Step 4 To validate that replication is working correctly, click **Validate Replication**. This summarizes the differences between the Publisher and Subscriber copies of each database.

Validating Replication

You can check whether replication is working and is up to date by creating a validation report, which lists the main database tables, along with their status, a comparison of the number of records in the Publisher and Subscriber, and a summary of any errors.

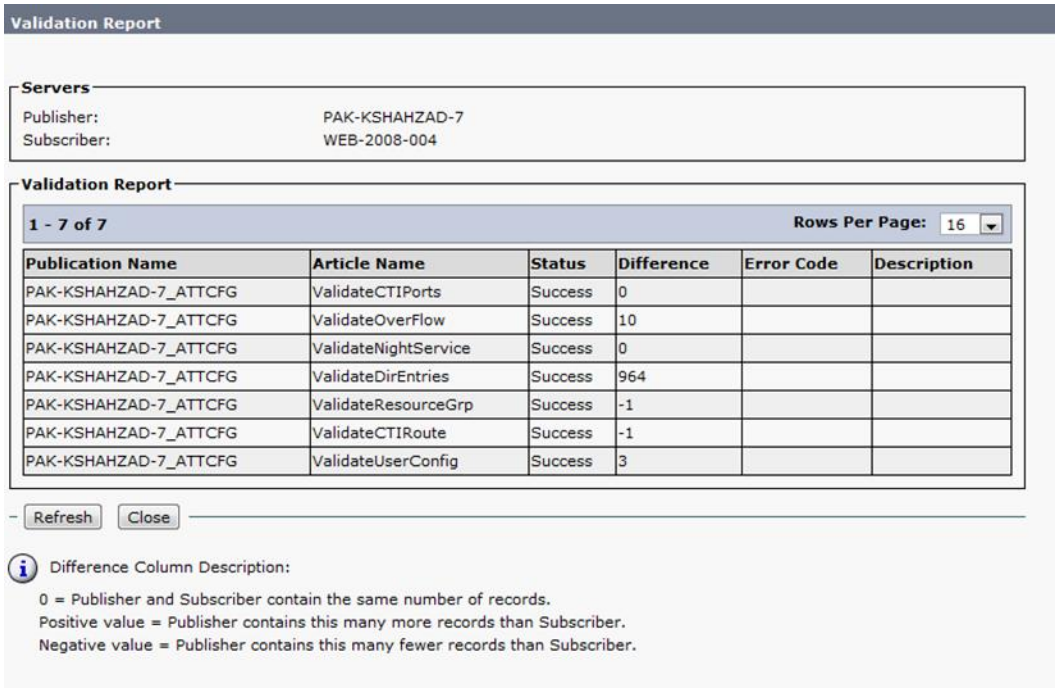
To validate replication for a selected database on a selected server:

Step 1 In the **Replication Management** page, select the database as described in Step 4.

Step 2 Click **Validate Replication**.

The **Validation Report** is displayed. For example:

Figure 4 Example Validation Report



Step 3 Use the **Rows Per Page** control to change the number of lines displayed.

The display refreshes at intervals. You can refresh it manually by clicking **Refresh**.

Replication Report

A cumulative record is kept of all replication transactions. You can view this record as a Replication Report.

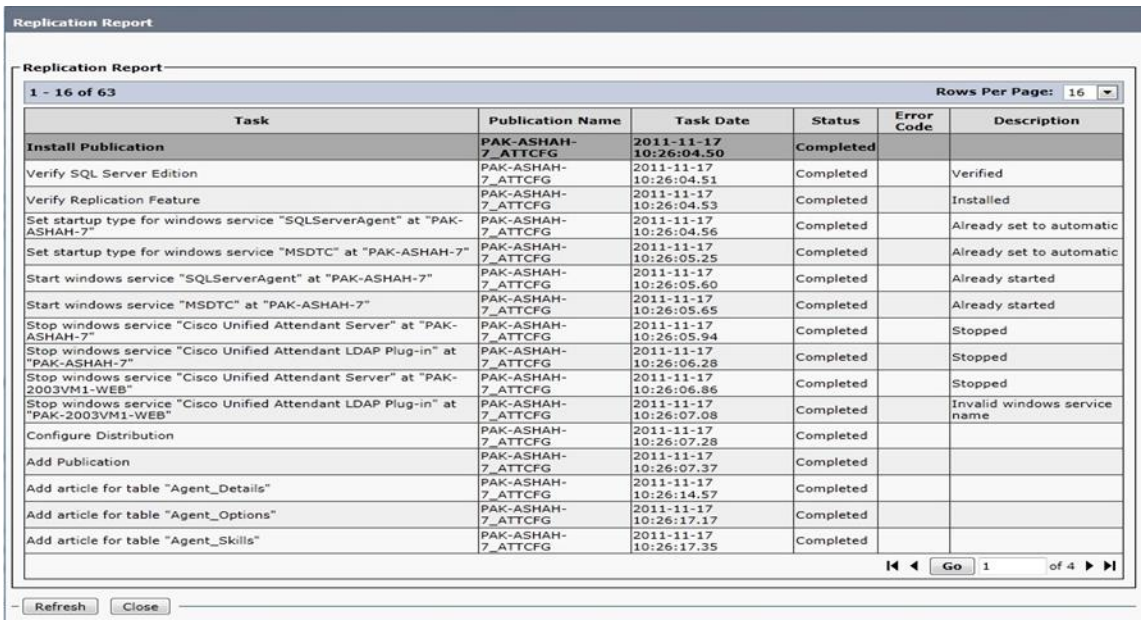
To produce a replication report for a selected database on a selected server:

Step 1 In the **Replication Management** page, select the database as described in Step 4.

Step 2 Click **Replication Report**.

The **Replication Report** is displayed.

Figure 5 Example Replication Report



Step 3 Use the **Rows Per Page** control to change the number of lines displayed, and the controls at the bottom right of the report to display specific pages.

Step 4 To return to the **Replication Management** page, click **Go** at the top right of the screen with **Replication** selected in the **Navigation** field.

Licensing Cisco Unified Attendant Console Advanced

Licensing the Cisco Unified Attendant Console Advanced Software

Note If you want to install a resilient Cisco Unified Attendant Console Advanced system, you need to license it separately from the server and user licenses. High availability functionality is available to use in both the 5-day and 60-day evaluation mode.

This section describes how to license your Cisco Unified Attendant Console Advanced software. The instructions assume that you have logged into the Cisco Unified Attendant Console Downloads and Licensing website.

Note

- Once a system is fully licensed you cannot revert to a temporary license.
- You need a valid license to be able to perform a major upgrade. When you install a major upgrade your existing license information is erased, and the five-day evaluation period is restarted. To continue using the application after this time you must obtain a new license.

When you install or upgrade the Subscriber, the license there is erased, and a 5-day evaluation license is created. Licenses cannot be deployed on the Subscriber.

Locate Server Registration Code

Step 1 From the Web Administration, navigate to the **Help > Licensing** menu.

Step 2 The **Registration Code** is located under the **Product Details** header.

Activating Evaluation Software

You can use downloaded software for 5 days before you must license it. Licensing the software enables you to evaluate it for 60 more days. If you do not license the download, you will be unable to use it after the fifth day.

Note You cannot extend the 60-day evaluation period or apply a second 60-day evaluation license. If you need more evaluation time, you must reinstall your system from the operating system level, and then apply a new 60-day evaluation license.

Activate the Software

Before starting, log into Cisco Unified Attendant Console Administration, choose **Help > Licensing**, and make a note of the **Registration Code**. Then, on the Cisco Unified Attendant Console Downloads and Licensing website, **Activate Evaluation Software** page:

Step 1 Select your **Customer**, and then select your **Customer Site**.

Note If your customer or site are not available, click the options to add them.

Step 2 Select the **Version** and the **Product** that you have installed, and then click **Next**.

Step 3 Enter your **Registration Code** and click **Submit**.

A registration (.RGF) file is e-mailed to you, and a message to this effect is displayed in the web page.

Step 4 Open the email and save the registration file to a location that can be browsed by the Cisco Unified Attendant Console Advanced server.

Step 5 Log into Cisco Unified Attendant Console Administration and choose **Help > Licensing**.

Step 6 In the **License Management** page, select **Registration File**.

Step 7 Click **Browse** and then open the Registration File.

Step 8 Click **Submit** to complete license activation.

Step 9 Stop and then restart the services, as described in Service Management. If you have configured a resilient server, you need to stop then restart the services on the Publisher server, and then once the Publisher is back online, restart the services of the Subscriber server.

Activating Purchased Software

You can purchase the software at any time in the evaluation periods, giving you unlimited use. When you purchase the software Cisco provide you with a 27-digit license activation code (LAC). After activating the software, you cannot revert to the trial version.

Note If you have purchased à la carte upgrade licenses or requested UCSS upgrade licenses through My Cisco Entitlements (MCE), you must ensure that the previous version's 27-digit LACs are activated before activating the upgrade LACs. If you do not do this the upgrade activation will fail.

In resilient installation, all licensing information is held on the Publisher server, and then replicated to the Subscriber. You only need to license the Publisher - the Subscriber inherits this information via replication.

Step 1 On the Cisco Unified Attendant Console Downloads and Licensing website, select **Activate Purchased Software** from the navigation page.

Step 2 Select **Customer**, and then select **Customer Site**.

Note If customer or site are not available, click the control to add them.

Step 3 Select the **Version**:

- **Flex Std** - This option applies to all A-Flex-3 - Named User licenses (PID - A-FLEX-CUAC-A, A-FLEX-CUAC-A-HA, and A-FLEX-CUAC-S).
- **10.x - 14.x** - For all other offerings (including perpetual licenses, upgrade licenses, Enterprise Agreement perpetual licenses, and A-Flex Enterprise Agreement licenses), select the version associated with your license activation codes.

Step 4 Select the **Product** (Cisco Unified Attendant Console Advanced) that you have installed, and then click **Next**.

Step 5 Depending on the **Version** you selected before, proceed as follows:

- If Version is **Flex Std**, input the **Registration Code** from your server, the **License Activation Code(s)**, and the **Term Start Date** (date the license becomes active). Click **Next**.
- If Version is **10.x -14.x**, input the **Registration Code** from your server, and then click **Next**. Input the **License Activation Code(s)**, and then click **Submit**.

Step 6 On the **License Request Confirmation** page, optionally enter an additional e-mail address and click **Submit**.

A registration (.RGF) file is e-mailed to you, and license request confirmation information is displayed in the web page.

Step 7 Open the email and save the registration file to a location that can be browsed by the Cisco Unified Attendant Console Advanced server.

Step 8 Log into Cisco Unified Attendant Console Administration and choose **Help > Licensing**.

Step 9 On the **License Management** page, select **Choose File**.

Step 10 Click **Submit** to complete the registration.

Step 11 Stop and then restart the services, as described in Service Management. If you have configured a resilient server, you need to stop then restart the services on the Publisher server, and then once the Publisher is back online, restart the services of the Subscriber server.

Term-Based License Expiry

Cisco Unified Attendant Console Administration will display license expiry alerts beginning 30 days prior to the date of expiration. Following expiration, users are warned that the license(s) have expired but are given a 30-day grace period to act before experiencing service interruption. Once the grace period elapses, the license(s) will deactivate.

Cisco Unified Attendant Console Administration presents the following licensing status messages:

- Alert messages are presented at login for licenses set to expire within 30 days. License type alerts appear as follows:
  - *User license(s) are approaching expiration, refer to License Management. Take action now to prevent service interruption.*
  - *High Availability license is approaching expiration, refer to License Management. Take action now to prevent service interruption.*
- Warning messages are presented at login and in the License Management menu, on the date of expiration and for the duration of the 30-day grace period that follows. License type warnings appear as follows:
  - At login:
    - *User license(s) are approaching expiration, refer to License Management. Take action now to prevent service interruption.*
    - *High Availability license is approaching expiration, refer to License Management. Take action now to prevent service interruption.*
  - In Help > Licensing > License Management:
    - The license line item(s) are displayed in bold red text.
- Following grace period expiration, in Help > Licensing > License Management menu:
  - The fully expired license line item(s) are displayed in gray with a status of inactive - expired.

Relicensing Software

If you do any of the following to the server environment, you must re-license the software with a new registration code:

- Reinstall the operating system on the same hardware
- Install a different operating system
- Modify network configuration
- Migrate to a new VM host
- Perform a major upgrade of the Cisco Unified Attendant Console Advanced software

All these cause the license to expire, and the System and User Configuration menus to disappear from Cisco Unified Attendant Console Administration. To re-license a server, contact Cisco Global Licensing Operations and request a re-host. You will need to provide them with the Registration Code of the prior install or License Activation Codes that were used with prior activation.

Uninstalling Cisco Unified Attendant Console Advanced

This section describes how to uninstall the Cisco Unified Attendant Console Advanced server and its associated applications.

Note

- Database replication is uninstalled automatically during Cisco Unified Attendant Console Advanced server installation or uninstallation. If the replication uninstall does not succeed at the first attempt, you are prompted to retry it or abort it.
- When installing or uninstalling resilient server software, both the Publisher and Subscriber server machines must be running. If either machine is turned off or inaccessible, the install or uninstall may fail.
- If the Publisher server software gets uninstalled, the Subscriber server's software link with the Publisher server gets broken. When you reinstall the Publisher server software you must then reinstall the Subscriber server software to restore the link.

When you uninstall a resilient system, it doesn't matter whether you start with the Publisher or the Subscriber.

To uninstall Cisco Unified Attendant Console Advanced server (the exact steps depend on the operating system of the host system):

Step 1 Choose **Start > Control Panel**, and then double-click **Add/Remove Programs**.

Step 2 From the list, select **Cisco Unified Attendant Server**, and then click **Remove**.

The Wizard prepares to (un)install the server application.

Step 3 When you are prompted to confirm that you want to remove Cisco Unified Attendant Console Advanced server from your machine, click **Yes**.

Step 4 If you have a resilient installation and both servers are running, you are prompted that the services on the other server (Subscriber or Publisher, as appropriate) need to be stopped. In the message click **Yes** to stop the services. In the Server screen, enter the **Username** and **Passphrase** of the administrative account on the other server.

The server application is uninstalled.

Step 5 When you are asked whether to restart the computer, select **Yes, I want to restart my computer now**, and then click **Finish**.

You must now remove all the third-party components installed with the Cisco Unified Attendant Console Advanced server:

- SQL Server
- .NET Framework
- Cisco TSP

Uninstalling Microsoft SQL Server

To uninstall the Microsoft SQL Server from your Cisco Unified Attendant Console Advanced server:

Step 1 Choose **Start > Control Panel**, and then double-click **Add/Remove Programs**.

Step 2 From the list, select **Microsoft SQL Server**, and then click **Remove**.

The server instances are listed.

Step 3 Select the instance to remove, and then click **Next**.

You are asked to confirm that you want to uninstall the selected instance

Step 4 Click **Finish** to remove the components. Click **Back** to go back and change any of the information.

While the components are being uninstalled the Setup Progress is displayed.

Step 5 When all the components have been removed, click **Finish**.

Step 6 When you have uninstalled Microsoft SQL Server, delete the *C:\DBdata* folder and the databases it contains.

Uninstalling the .NET Framework

Caution If you uninstall the .NET Framework Cisco Unified Attendant Console Advanced will not function.

To uninstall the .NET Framework:

Step 1 Choose **Start > Control Panel**, and then double-click **Add/Remove Programs**.

Step 2 From the list, select whatever .NET you have installed, and then click **Remove**.

You are prompted to either **Repair or Uninstall the .NET Framework**.

Step 3 Select **Uninstall**, and then click **Next**.

You are asked to confirm that you want to remove the .NET Framework.

Step 4 Click **OK**.

While the components are being uninstalled the Setup Progress is displayed.

Step 5 When all the components have been removed, click **Finish**.

Uninstalling Cisco TSP

If you need to uninstall the Cisco TSP follow the instructions in ciscotsp.txt, which was created when the TSP was installed. The file's default location is *C:\Program Files\Cisco*.

Cisco Unified Attendant Console Advanced Migration and/or Upgrade

This section provides instructions required to migrate an existing installation to a new server. The instructions tend to scenarios such as:

- Migrating to a new server, running the same version of Cisco Unified Attendant Console Advanced.
- Migrating to a new server and upgrading to a later release of Cisco Unified Attendant Console Advanced.
- Migrating to a new server, running either the same or later Microsoft Server Operating System.
- Migrating to a new server, running either the same or later Microsoft SQL Server version.
- Disaster recovery using database backups.

Application User Validation

Confirm that the existing Application User(s) for Cisco Unified Attendant Console Advanced meet the role requirements defined in Assigning Roles to an Access Control Group.

Build New Cisco Unified Attendant Console Advanced Server(s)

Step 1 Build the new machines and install/configure Windows Server. For more information, see Hardware and Software Requirements.

Note

High availability requirements:

- Cisco Unified Attendant Console Advanced Publisher and Subscriber must be able to validate one another by host name. If required, modify the host's file on each server to support the requirement.
- Cisco Unified Attendant Console Advanced Publisher and Subscriber Timezone, Date, and Time must match.

Step 2 Install IIS. For more information, see Adding Internet Information Service (IIS).

Step 3 Install SQL Server. For more information, see Installing and/or configuring SQL.

Note

- Do not install SQL Server until the permanent host name is defined.
- Host name cannot exceed 15 characters.

- SQL Server must be installed, as defined in Installing Cisco Unified Attendant Console Advanced Software. Errors tied to deviating from the installation instruction will not be supported by Cisco, requiring a rebuild of the solution to bring it back into compliance.
- SQL Server Version: When migrating or restoring Cisco Unified Attendant Console Advanced database(s), the SQL Server version on the destination server must match or be later than the version of SQL on the originating server. For example:
  - Success: Database backup SQL Server Version: 2008 > Restore using SQL Server 2016
  - Failure: Database backup SQL Server Version: 2016 > Restore using SQL Server 2012 R2
- In instances where SQL Server Express satisfies the deployment requirements (for more information, see SQL Server Express Limitations), SQL Server requires manual installation prior to installing Cisco Unified Attendant Console Advanced. The installation media is available at Microsoft Development Network (MSDN). The installation procedure follows the instruction provided in Installing Cisco Unified Attendant Console Advanced Software. Menus related to replication and/or SQL Server Agent should be either hidden or unavailable. Proceed with the instruction as advised.

Back Up Existing Databases

Caution If the existing solution is configured to support High Availability/Resilience, Replication must be uninstalled prior to backing up the databases. For more information, see Uninstalling Replication.

- Back up the Cisco Unified Attendant Console Advanced Publisher server, ATTCFG and ATTLOG databases. If the existing reporting is not required, do not backup the ATTLOG database. For more information, see Manually Backing-up Databases.
- Database backups are not required for the Cisco Unified Attendant Console Advanced Subscriber server.

Back Up Existing Crypto Key and Registry

If pre-existing version is 12.0.x or later, collect a Crypto Key and Registry backup from the Cisco Unified Attendant Console publisher server.

For more information on how to collect it via the Web Administrator, see Export Crypto Key File.

For more information on how to manually back up the crypto key and registries, see Manually Backing-up and Restoring Cryptographic Keys and Registries.

Restore Databases

If required, restore the ATTCFG and ATTLOG databases on the new Cisco Unified Attendant Console Advanced Publisher server.

Step 1 Launch **SQL Management Studio**.

Step 2 Login with SA account (or an account with equivalent permissions).

Step 3 Expand server name.

Step 4 Right click **Databases** and select **Restore Database**.

Step 5 Select **General** from the left navigation pane.

Step 6 Select **Device** radio button and click button to the right of the field.

Step 7 Select backup media type file.

Step 8 Click **Add** and navigate to database backup. Select the file and click **OK**.

Step 9 Select the backup, then click **OK**.

Step 10 Click **OK**.

Step 11 If required, repeat the above steps to attach the ATTLOG database.

Restore Cryptographic Keys and Registries

If migrating or upgrading from version 12.0.x or later, the cryptographic key and registry backup from the existing server must be migrated to the new Cisco Unified Attendant Console servers (publisher and subscriber), prior to installing Cisco Unified Attendant Console.

For more information on importing registries and cryptographic keys, see Manually Backing-up and Restoring Cryptographic Keys and Registries.

Install Cisco Unified Attendant Console Advanced Server Application

Caution It is imperative that the pre-existing Cisco Unified Attendant Console Advanced servers are permanently taken offline prior to completing the installation on the new servers. Failure to comply will result in device registration errors and other erratic behaviors tied to device control.

Tip If upgrading to version 12.0.x or later from an earlier release, all passphrases will be converted to all uppercase. This includes console user account passphrases and the Web Admin passphrase.

Follow the installation steps presented in Installing Cisco Unified Attendant Console Advanced Software.

During the Database Wizard steps of the installation, when prompted *A database with the name already exists, do you wish to overwrite?*, select **No**.

High Availability/Replication Users

- Install the same version of Cisco Unified Attendant Console Advanced on the Subscriber server.
- Install Replication as described in Cisco Unified Attendant Console High Availability.

Troubleshooting Post-Migration System Device Registration Issues

Once the server restarts, if there is an issue with Cisco Unified Attendant Console Advanced device registration, execute the following steps.

Validate that Cisco TSP has been installed, and that the *CiscoTSP001.tsp* instance is configured:

Step 1 Launch **Cisco TSPx64 Configuration**.

Step 2 Instance name *CiscoTSP001.tsp* should appear. Any additional instances indicate an issue with the TSP install.

Step 3 Select the instance and click **Configure**. Validate that the User and CTI Manager tabs are populated.

Step 4 Select the **Advanced** tab, change the provider open completed value to **300**.

Step 5 Click **OK**, and **OK** again.

Step 6 Then, restart the server.

If the devices still do not register, recreate the Cisco Unified Attendant Console Advanced system devices and route points the following way:

Step 1 Access the **CUCM Web UI**.

Step 2 Delete all the Cisco Unified Attendant Console Advanced System (Gateway, Service, and Park) Devices, CTI Route Points, and their associated directory numbers.

Step 3 Navigate to the application user for each Cisco Unified Attendant Console Advanced server, remove all devices from the list of controlled devices with the exception of any template devices.

Step 4 Access the Cisco Unified Attendant Console Advanced **Webadmin > System Configuration > Sync with CUCM menu**.

Step 5 Select all queue device groups and execute a sync with CUCM to recreate all the Cisco Unified Attendant Console Advanced server devices and route points.

Step 6 Once complete, restart the server.

Cisco Unified Reporting

Cisco Unified Reporting enables you to create reports about the information coming through Cisco Unified Attendant. It will be available only if you enabled it during installation.

This section describes how to configure Cisco Unified Reporting using Cisco Unified Attendant Console Advanced Administration. Only administrators can access Cisco Unified Attendant Console Advanced Administration.

To access Cisco Unified Reporting:

Step 1 Log in to Cisco Unified Attendant Console Advanced Administration, as described in Administrator Login.

The Cisco Unified Attendant Console Advanced Administration home page is described. For more information, see Home Page.

Step 2 In **Navigation** at the top right of the home page, select **Cisco Unified Reporting**, and then click **Go**.

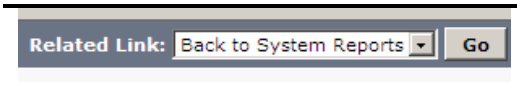
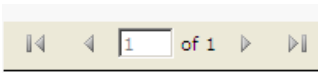
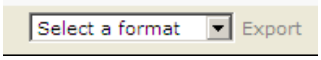
The Cisco Unified Reporting home page is displayed. This contains the **System Reports** menu from which you can run the following reports:

- Incoming Calls by Date and Time
- Operator Calls by Time
- Operator Calls by Queue
- Operator Availability
- Overflowed Calls by Date

Note CUAC reports cache the data for database optimization. With big databases, it can take some time to cache the reporting data before generating the report. In that case, users see a timeout error. To resolve this, you can rerun the same report with the same parameters to see the desired results.

Toolbar

At the top of each system report is a toolbar containing the following for controlling the report:

Control	Function
	Click **Go** to return to the System Reports home page.
	Navigate to a specific page in the report: Start Page, Back One Page, Forward One Page, Last Page. Alternatively, enter a number to go to that page.
	Export a copy of the report. First select the format from Excel (.XLS) or Acrobat (.PDF).
	Refresh the Report screen.
	Print the report to the printer configured on the Server. Use the printer page setup functions specific to your internet browser to configure the format of your printed report.

Setting Report Parameters

To run a System Report you must specify the type of report and the report parameters. These vary according to the report you choose, and may require a:

- Date Range
- Time Range
- Abandoned Calls
- Queue Type
- Attendant Operators

When you have set the report parameters, click **Generate Report**.

Date Range

Most of the reports require you to select a **From** date, and some also require a **To** date so that the report covers the range of specified dates. You can restrict a date range to a single day by specifying the same **From** and **To** dates. The **Operator Calls by Time** report only covers a single date; so a range is not required. You can select the date by clicking the calendar control.

Time Range

Most of the reports require you to select a **From** time and a **To** time. These times have the format *hh:mm:ss*, where hh uses a 24 hour clock. Both times are compared to the start time of the calls on that day. For example, with a **From** time of 09:00:00, calls starting at 08:59:59 or earlier are omitted from the report. With a **To** time of 17:00:00, calls starting at 17:00:01 or later are omitted from the report.

Abandoned Calls

The **Incoming Calls by Date and Time** reports contain the parameter **Abandoned Calls** where you can enter a time in the *hh:mm:ss* format to list only those calls that were abandoned after the specified amount of time had passed.

Queue Type

In several reports you must also specify which queue's data to analyze, and whether this data is from the **Arrival Queue** or the **Delivery Queue**.

The Arrival Queue is where calls arrive after filtering. The Delivery Queue is the queue from which calls are delivered to the Cisco Unified Attendant Console Advanced. Depending on the configuration, calls may overflow from one queue to another before reaching the Console attendant.

You can select multiple queues by holding **Ctrl** while selecting queue names.

Attendant Operators

In several reports you must also specify which attendant operator's data to analyze. You can select multiple Operators by holding **Ctrl** while selecting Operator names.

Incoming Calls by Date and Time System Report

The Incoming Calls by Date and Time report is a summary of the incoming calls in the queues during a specific period. A single line of information is provided for a particular date/time and queue.

Specify the following parameters before running this report:

- From and To Date
- Start and End Time
- Queue(s)
- Abandoned Call Timer
- Arrival or Delivery Queue

The report contains the following information:

Field	Description
Total Calls	Number of calls reaching the Cisco Unified Attendant Console Advanced.
Answered Calls	Number of calls answered.
Abandoned Calls	Number of calls abandoned.
Overflowed Calls	Number of calls overflowed to a queue, device or external number.
% Answered	Percentage of calls answered.
% Abandoned	Percentage of calls abandoned.
% Overflowed	Percentage of calls overflowed.

Field	Description
Average Answered Wait	Average time calls wait before being answered.
Average Answered Talk Time	Average talk time for answered calls.
Average Abandoned Wait	Average time a caller waits before the call is abandoned.
Answer Time Profile	For 10, 20, 30, 40, this is the cumulative percentage of calls answered in less than the specified number of seconds. 40+ is the percentage of calls answered after 40 or more seconds.
Longest Wait	The longest time a caller had to wait to be answered.
Break Hour	Break hours.

Operator Calls by Time System Report

The Operator Calls by Time report is a summary of incoming and outbound calls involving specific attendant operators by time, on a single date. A line of information is displayed per hour per operator. Totals are displayed for each operator.

Specify the following parameters before running this report:

- Start and End Time
- Start Date
- Operator(s)

The report contains the following information:

Field	Description
Operator	Operator name.
Total Calls	Total number of inbound calls to the attendant operator.
Console	Total number of calls to the queue attended by the attendant operator, including: • Incoming queue calls • Retrieved calls from F5 • Calls retrieved from park by double-clicking the Park DN on the screen
Others	Total number of calls not to the Console attended by the attendant operator. Normally, these are direct calls to the DN the operator uses for answering console calls.
Inbound Total talk time	Total talk time for the inbound queue calls only.
Inbound Average talk time	Average talk time for the inbound queue calls only.
Inbound Longest talk time	Longest talk time for the inbound queue calls.
Total Outbound Calls	Total number of outbound calls made by the operator, including:

Field	Description
	• Normal outbound calls • Consult transfer enquiry calls • Conference enquiry calls • Park calls retrieved by dialing the park DN • Abandoned calls
Outbound Total talk time	Total talk time for outbound answered calls.
Outbound Average talk time	Average talk time for outbound answered calls.
Outbound Longest talk time	Longest talk time for outbound answered calls.

Operator Calls by Queue System Report

The Operator Calls by Queue report is a summary of the queued calls handled by attendant operators during a specific date range. The summary data is grouped by date, with a line of information per operator on that date.

Specify the following parameters before running this report:

- Start and End Date
- Queue(s)
- Operator(s)

The report contains the following information:

Field	Description
Operator	Logged in attendant operator's name.
Queue	The queue assigned to that attendant operator.
No. of calls	Total number of queue calls answered within that queue.
Total Talk	The total talk time by the operator on inbound calls from that queue.
Average Talk	Average talk time on answered calls on that queue.
Longest Talk	Longest talk time for answered calls on that queue.

Operator Availability Report

The Operator Availability report shows the daily availability of one or more operators between the start and end date. Statistics are displayed for each logged in period, with totals for each day.

Specify the following parameters before running this report:

- Start and End Date
- Operator

Note

- Duration of the report cannot exceed one year.
- You can only select one operator at a time.

The report contains the following information:

Field	Description
Operator	Logged in attendant operator's name.
Logged In	Times the specified operator logged in on that day.
Logged Out	Times the specified operator logged out on that day.
Time Logged In	Duration of the logged in period.
Time Available	Amount of time in the logged in period that the operator was available.
Number of Calls	Number of calls handled during the logged in period.
Avg Call Duration	Average length of calls handled during the logged in period.

Note

- Individual calls may be counted multiple times in the following situations:
  - The attendant operator is engaged in a call when the Publisher server experiences a full or partial failover and cuts over to the Subscriber server. The report will not contain a log out time, but a new call will be registered against the log in session.
  - The attendant operator establishes a conference with a third or additional parties.
- When log in sessions span multiple dates, the call data is shown on the log in date page only.
- **Time Available** information may not be available in the following scenarios:
  - CUAC Server crashed unexpectedly
  - CUAC Server machine crashed unexpectedly.

Overflowed Calls By Date System Report

The Overflowed Calls By Date report summarizes the calls that overflow from Arrival Queues – the first, direct destinations for calls. Queues that only ever receive re-routed calls are not included in the report. Specify the following parameters before running this report:

- Start and End Date
- Start and End Time
- Queue(s)

The report contains the following information:

Field	Description
Queue	The Queue(s) for which the report is generated.
Total Queue Calls	The total number of incoming calls at the Queue.
Total Overflow In	The total number of calls overflowed from the Queue.
Overflow In	The number of calls overflowed into the Queue from other Queues during business hours.
Night Service In	The number of calls overflowed into the Queue during break hours.
Overflow out Time Limit	The number of calls that overflowed because the maximum call waiting time was exceeded.
Overflow out No Operators	The number of calls that overflowed because no attendant operator was logged into the queue.
Emergency	The number of calls that overflowed because the queue was in emergency mode.
Overflow out Destination Time Limit	The destination for calls overflowed for exceeding the maximum wait time.
Overflow out Destination No Operators	The destination for calls overflowed when no operator was logged into the queue.
Emergency	The destination for calls overflowed when the queue was in emergency mode.
% In	The percentage of incoming calls that had overflowed from another queue.
% Out	The percentage of incoming calls that overflowed from the queue.

Example Cisco Unified Attendant Console Advanced Configuration

This appendix contains an example resilient Cisco Unified Attendant Console Advanced system configuration.

Publisher

Parameter	Example Value	For more information, see...
TSP application user	CUACAPUB01	Creating and Assigning an Application User
Machine Name	CUACAPUB01	
CT Gateway	1600 - 1609	Device Groups
Service Device	1610 - 1619	
Park Device	1620 - 1629	
Queue DDI	1630 - 1639	

Subscriber

Parameter	Example Value	For more information, see...
TSP application user	CUACASUB01	Creating and Assigning an Application User
Machine Name	CUACASUB01	
CT Gateway	1650 - 1659	Device Groups
Service Device	1660 - 1669	
Park Device	1670 - 1679	
Queue DDI	1680 - 1689	

Device Groups

For a description of how to define device groups and the devices in them, see System Device Management.

For a description of how to create queues and define queue DDIs, see Queue Management.

Name	Devices	
DEFAULT	**Primary (Publisher)**	
	CT Gateway	1600 - 1604
	Service Device	1610 - 1614
	Park Device	1620 - 1624
	Queue DDI	1630 - 1634
	Secondary (Subscriber)	
	CT Gateway	1650 - 1654
	Service Device	1660 - 1664
	Park Device	1670 - 1674
	Queue DDI	1680 - 1684
DEVELOPMENT	**Primary (Publisher)**	
	CT Gateway	1605 - 1609
	Service Device	1615 - 1619
	Park Device	1625 - 1629
	Queue DDI	1635 - 1639
	Secondary (Subscriber)	
	CT Gateway	1655 - 1659
	Service Device	1665 - 1669
	Park Device	1675 - 1679
	Queue DDI	1685 - 1689

Attendant Operators

For a description of how to create and configure attendant operators, see Operator Management.

Name	Passphrase
OPERATOR1	cisco
TESTOP	<BLANK>

Attendant Queues

Name	Type	Primary DDI (Publisher)	Secondary DDI (Subscriber)
BROADCAST	Broadcast	1630	1680
CONSOLE - FORCE	Forced delivery	1631	1681

Backing up and restoring Cisco Unified Attendant Console Advanced

This appendix describes how to back up Cisco Unified Attendant Console Advanced server, and how to restore it to service following any failure that requires a full system (including operating system) rebuild.

Note The instructions in this appendix are for SQL Server 2008 databases. The procedures may vary slightly for other versions.

Backing-up Databases

Cisco Unified Attendant Console Advanced uses the following SQL databases, which are created when you install the software:

- ATTCFG—Stores the server configuration.
- ATTLOG—Stores call history information. Cisco Unified Attendant Administration reports use this data.

By backing-up these databases you will be able to restore your configuration and call history following server failure.

You can back up your databases either:

- Manually
- Automatically

Manually Backing-up Databases

To manually back up the databases, do the following:

Step 1 Start Microsoft SQL Server Management Studio and connect to the server.

Step 2 In the Object Explorer, expand **Databases**.

Step 3 Right-click a ATTCFG and choose **Tasks > Back Up**.

Step 4 In the Back Up Database dialog box, ensure that the following are set or selected:

- The correct Source **Database**
- The Source Backup type is **Full**
- A backup **Destination**

Step 5 Click **OK**.

The database is backed-up. This may take some time, depending on the size of the database.

When the backup is complete, the following messages is displayed: *The backup of database 'ATTCFG' completed successfully*.

Step 6 In the message, click **OK**.

Step 7 Repeat Step 3 to Step 6 for ATTLOG.

Automatically Backing-up Databases

SQL enables you to create a maintenance plan that automatically backs-up specified databases.

The following procedure creates a maintenance plan for an automatic back up that runs according to a specific schedule; it overwrites the backup file created the previous day and shrinks the database transaction logs. You should modify the settings to meet your specific requirements.

To create a maintenance plan, do the following:

Step 1 Start Microsoft SQL Server Management Studio and connect to the server.

Step 2 In the Object Explorer, expand **Management**.

Step 3 Right-click **Maintenance Plans** and select **New Maintenance Plan**.

Step 4 Type a name for the Maintenance Plan and then click **OK**.

The new plan is created and listed in the design view in the right-hand half of the interface. The Maintenance Plan Tasks toolbox is displayed in the lower left-hand corner of the interface.

Step 5 Optionally, type a plan **Description**.

Step 6 Double-click **Subplan_1**.

Step 7 In the Subplan Properties dialog box, enter a meaningful **Name** and **Description**, and click the **Schedule** calendar icon.

Step 8 In the Job Schedule Properties dialog box, select or specify the following:

- A **Schedule type**
- The job **Frequency**
- The **Daily frequency** (times) when the job must run.

Note We strongly recommend that you schedule this task to run out of working hours.

Step 9 Click **OK**.

Step 10 In the **Subplan Properties** dialog box, click **OK**.

Step 11 Drag an **Execute T-SQL Statement Task** from the Maintenance Plan Tasks toolbox and drop it into the lower right-hand corner of the interface. You will use this task to shrink the transaction logs of both databases.

Step 12 Click the task and rename it as required.

Step 13 Right-click the task and choose **Edit**, then enter the following into the **T-SQL statement** field:

Note

For SQL 2014 databases, substitute the following for the lines in **red**:

- ALTER DATABASE ATTCFG SET RECOVERY SIMPLE
- ALTER DATABASE ATTLOG SET RECOVERY SIMPLE

```
Use ATTCFG
EXEC sp_dboption 'ATTCFG','trunc. log on chkpt.', 'true'
CHECKPOINT
DBCC SHRINKFILE (ATTCFG_log, 1,TRUNCATEONLY)

Use ATTLOG
EXEC sp_dboption 'ATTLOG','trunc. log on chkpt.', 'true'
CHECKPOINT
DBCC SHRINKFILE (ATTLOG_log, 1,TRUNCATEONLY)
```

Step 14 Click **OK**.

Step 15 Do the following for the configuration database (ATTCFG) and then repeat for the logging database (ATTLOG):

a. Drag a **Back Up Database Task** from the Maintenance Plan Tasks toolbox and drop it below the Execute T-SQL Statement Task.

b. Click the task and rename it as required.

c. Right-click the task and choose **Edit**.

d. We recommend applying the following settings:

- Set **Backup Type** to **Full**.
- In **Database(s)**, click the down-arrow and select ATTCFG or ATTLOG, as appropriate.
- In **Back up databases across one or more files**, enter a file path and name.

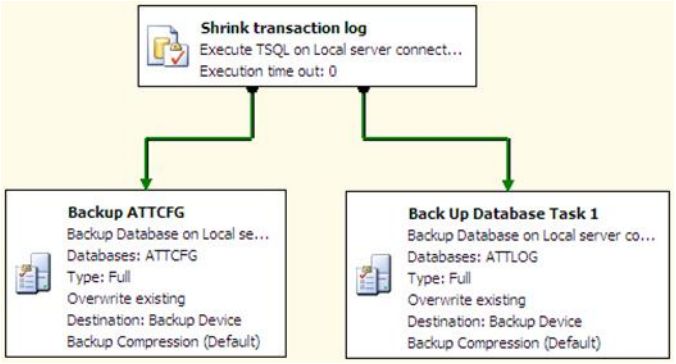
Note

If you save the backup files to your server's local drive, you must copy them to another location to ensure they are still available if the server fails.

- Set **If backup files exist** to **Overwrite**.

e. Click **OK**.

Step 16 Click the shrink transaction log task and drag the component outputs to join it to the backup tasks as shown in the following example:



Step 17 In the Microsoft SQL Server Management Studio main menu, choose **File > Save Selected Items**.

Restoring Databases

This section describes how to restore the server and databases for the following installations of Cisco Unified Attendant Console Advanced:

- Non-resilient installations
- The Publisher server on resilient installations.

  If you have to rebuild and restore your Publisher server, you will then need to reconnect it to your existing Subscriber server, as described in Reconnecting a Subscriber Server to a Restored Publisher Server.

  For instructions on how to restore a failed Subscriber server, see Restoring a Subscriber Server.

Preparing the Servers

Before you can restore the databases, you must prepare the server hardware and software, and install Cisco Unified Attendant Console Advanced.

Step 1 Install the Publisher, as described in Installing Cisco Unified Attendant Console Advanced Software.

Step 2 Back-up the cryptographic keys and registries, as described in Backing-up Cryptographic Keys and Registries.

Step 3 Install the Subscriber, as described in Installing Cisco Unified Attendant Console Advanced Software.

New, blank configuration and call history databases are created when you install the Cisco Unified Attendant Console Advanced software.

Note

- You must install the same version of software you were using before the failure. If you install a different version your database will have an incorrect schema and you will experience unpredictable problems.
- To be able to restore the database onto a new server, you must set its host name to match that of the backed-up server; do this before installing SQL and Cisco Unified Attendant Console Advanced on the new server. For more information on how to update the host name, see Updating the Cisco Unified Attendant Console Advanced Server Host Name, SQL Server Login Name and Password.
- If you are installing a Cisco Unified Attendant Console Advanced Publisher server, ensure that you select Publisher when prompted.

After installing the Cisco Unified Attendant Console Advanced software on your new server, you must license it, as described in Licensing Your New Server.

Restoring the Databases

When you have installed Cisco Unified Attendant Console Advanced you can restore your backed-up databases.

To restore the databases, do the following:

Step 1 In Control Panel, open Administrative Tools, and then double-click **Services**.

Step 2 **Stop** the following services:

- BLF Plug-in
- Cisco Unified Attendant LDAP Plug-in
- Cisco Unified Attendant Server

Step 3 **Restart** the SQL Server (MSSQLSERVER) service. This will also restart the SQL Server Agent service, if it is running.

Step 4 Start Microsoft SQL Server Management Studio and connect to the server.

Step 5 In the Object Explorer, expand **Databases**.

Step 6 Do the following for the configuration database (ATTCFG) and then repeat for the logging database (ATTLOG):

a. Right-click the appropriate database and choose **Tasks** > **Restore** > **Database**.

b. In the Restore Database dialog box, select the **General** page.

c. Under **Source for restore**, select **From device**.

d. Browse to the file at the **Backup location**.

e. Select the **Backup sets to restore**.

f. In the Restore Database dialog box, select the **Options** page.

g. Select **Overwrite the existing database (WITH REPLACE)**.

h. Click **OK**.

The database is restored. When the restore has completed successfully a message is displayed.

i. In the message, click **OK**.

Step 7 Restart the services you stopped in Step 2.

Note

- If you are migrating your databases to a new server, rebuilding the existing server/virtual machine, or changing domain/host names, complete the steps outlined in Updating the Cisco Unified Attendant Console Advanced Server Host Name, SQL Server Login Name and Password.
- If you are using the same System Devices (CT Gateway, Service, and Park Devices) and queue DDIs on the new or re-imaged server as were used with the backed-up server, you must access Cisco Unified Communications Manager and delete the associated Devices, CTI Route Points and Device Names before using the Cisco Unified Attendant Console Advanced Administration **Configuration > Synchronize with CUCM** function.

Reconnecting a Subscriber Server to a Restored Publisher Server

Note This section applies only to resilient Cisco Unified Attendant Console Advanced installations where you have restored a failed Publisher Server. For how to rebuild and restore a failed Subscriber server, see Restoring a Subscriber Server.

To reconnect your existing Subscriber server to your restored Publisher server, do the following:

1. Uninstall the software on the Subscriber server.
2. Re-install the software on the Subscriber server.

Note You must install the same version of software you were using before the failure. If you install a different version your database will have an incorrect schema and will be unable to accept replicated data from the Publisher.

3. Configure replication between the Publisher and Subscriber.

For more information on how to perform any of these steps, see Cisco Unified Attendant Console High Availability.

Backing-up Cryptographic Keys and Registries

Before installing the Subscriber, you must back-up the Publisher's cryptographic keys and registries, and copy them to the Subscriber, otherwise the latter will not function correctly.

Backing-up Using Attendant Administrator

You can use Cisco Unified Attendant Administration to back-up the Publisher's cryptographic keys and registries. This is described in Export Crypto Key File. The backup-up key archive should be copied to Subscriber.

Manually Backing-up and Restoring Cryptographic Keys and Registries

To back-up the keys and registries manually:

Step 1 On the Publisher, use regedit to export the key:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Arc Solutions\Call Connect\Crypto to a disk file.

Step 2 Note the folder name in the *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Arc Solutions\Call Connect\Crypto\Security\KeyFilePath* registry value, and then copy the *aesKey.dat* file from that folder.

To restore the keys and registry to a server:

Step 1 Copy the disk file from Step 1 in the back-up procedure to the new machine, double-click the file, and then respond to all the prompts to merge the exported keys.

Step 2 Copy the *aesKey.dat* file from Step 2 in the back-up procedure to the same repository on the machine. If the repository does not already exist, you need to manually create it, then copy the file to it.

You can now restore the Subscriber.

Restoring a Subscriber Server

Note This section applies only to resilient Cisco Unified Attendant Console Advanced installations where the Subscriber server has failed.

If your Subscriber server fails and you have had to build a new one, do the following:

1. Prepare the Subscriber server hardware and software. For more information, see Hardware and Software Requirements.
2. Install the Cisco Unified Attendant Console Advanced software on the Subscriber server.

During installation, do the following:

a. After entering the Publisher server credentials you are prompted that another Subscriber server has been detected and that the new Subscriber server will replace the existing one. Click **Yes**.

b. When prompted for the Subscriber server credentials, enter details of the connection to the old Subscriber server. If the old server cannot be found, you are prompted to continue. Click **Yes**.

Note

You must install the same version of software you were using before the failure. If you install a different version your database will have an incorrect schema and will be unable to accept replicated data from the Publisher.

For more information, see Installing Cisco Unified Attendant Console Advanced Software.

3. License the software, as described in Licensing Your New Server.
4. Configure replication between the Publisher and Subscriber. For more information, see Accessing High Availability Administration Menus.

   As the Cisco Unified Attendant Console Advanced configuration information is stored in the Publisher database, you do not need to restore the Subscriber database—the information is automatically added to the Subscriber database once you have configured replication.

Licensing Your New Server

Each new Publisher server requires a new license file.

Immediately after installation your new server will run for a 5-day evaluation period without a license. You can extend this period to 60 days.

To obtain a new full (purchased) license file, contact the Cisco Technical Assistance Center (TAC) with either:

- The SO number for the software you purchased
- The license activation code (LAC) for your previous installation

and request a re-host. Cisco TAC will reset the LAC, which will allow you to generate a new permanent license.

For more information about how to obtain and apply evaluation and full software licenses, see Licensing Cisco Unified Attendant Console Advanced.

Updating the Cisco Unified Attendant Console Advanced Server Host Name, SQL Server Login Name and Password

This appendix describes how to update the Cisco Unified Attendant Console Advanced server host name and SQL Server connection details of an existing installation.

Console Client Instruction

Use the following instruction to modify the server hostname for the client connection.

Step 1 Close the Cisco Unified Attendant Console Client application.

Step 2 Navigate to the *C:\ProgramData\Cisco\CUACA* repository, and then open the *OPR.config* file with Notepad.

Step 3 Change the 'servername' value to reflect the desired server hostname. Save the changes and exit the application.

Step 4 Navigate to *C:\Users\<<userid>>\AppData\Roaming\Cisco\CUACA* replacing <<userid>> with the Windows User ID, and then open the *OPR_Startup.config* file with Notepad.

Step 5 Change the 'LastConnectedServer' value to reflect the desired server hostname.

Step 6 Save your changes and exit the application.

Server Instruction

Note Prior to modifying the server host name, take note of the existing server registration code (required only for publisher/primary server). The registration code is noted in the **Web Administrator > Help > Licensing** menu. Modifying the server host name will modify the server registration code, which will remove any existing licensing from the server. After making the required changes, open a case with **Cisco Global Licensing Operations**, requesting that the pre-existing licensing be reset. The team will require the old server registration code and/or license activation codes to assist.

There are two utilities in the Cisco Unified Attendant Console Advanced server program files.

- Modify pre-existing installation, server host name: *ServerChange.bat*
- Modify SQL Server credentials used by Cisco Unified Attendant Console Advanced: *SqlCfgChange.bat*

Complete the following steps in entirety for each server that is modified. You must execute all of the following steps for a publisher, and then subscriber if using high availability. It is imperative that all changes be made in entirety to one server at a time.

Step 1 *Standalone installs* only. Prepare the batch files.

Step 2 *High Availability installs only.* Uninstall replication from both servers.

Step 3 Set Cisco Unified Attendant Console Advanced services and Active MQ service startup type to **Manual**.

Step 4 Modify Cisco Unified Attendant Console Advanced server host name and/or SQL Server login name and password.

Note To ensure password composition is supported, see Supported Windows, SQL Server, Active Directory, Presence Server, Application User and CUAC Password Characters.

Step 5 Execute the appropriate batch file(s).

Step 6 Set Cisco Unified Attendant Console Advanced services and Active MQ service startup type to **Automatic**.

Step 7 *High Availability installs only*. Reinstall High Availability if required.

Step 8 Restart Cisco Unified Attendant Console Advanced server(s).

Standalone Installs Only: Prepare the Batch Files

Edit the configuration files associated with the host name and SQL server credentials change utilities. To edit the configuration files:

Step 1 Navigate to *\Program Files (x86)\Cisco\Utilities\Server and SQL Change Tool*.

Step 2 Use a text editor to open the relevant configuration file(s):

- Modify SQL login name and/or passphrase: *SQLCfgChangeXML*.
- Modify server hostname: *ServerChangeXML*.

Step 3 Change the *AllConnectedServers* key to **No**.

Step 4 Save and then close the file.

High Availability Installs Only: Uninstall Replication from Both Servers

High Availability must be uninstalled before implementing any changes and before executing the database update utilities. See Uninstalling Replication.

Set Cisco Unified Attendant Console Advanced Services and Active MQ Service Startup Type to Manual

1. Navigate to Control Panel, and then select **Administrative Tools**.
2. Select **Services**.
3. Stop the following services:
   - ActiveMQ
   - BLF Plug-in
   - Cisco Unified Attendant LDAP Plug-in (Primary server only)
   - Cisco Unified Attendant Server
   - Cisco Unified Attendant Presence Plug-in
4. Set the start-up type of the services listed above to **Manual**.
   a. Right-click the service name, and then select **Properties**.
   b. In the **Properties** dialog box, click the **General** tab, set the **Startup type** to **Manual**, and then click **OK**.

Modify Cisco Unified Attendant Console Advanced server host name and/or SQL Server login name and password

High Availability installs only: as previously noted, it is imperative that changes are made to one server at a time. Once the steps have been completed for the first server, follow the same steps for the second server. Implementing changes to both servers at the same time will break the solution.

Execute the Appropriate Batch Files

Follow the instruction relevant to the change being made to the Cisco Unified Attendant Console Advanced servers.

The order in which the batch files are executed is not important. If you want to modify the details associated with a publisher and subscriber, the order in which the changes are made is not important.

Modify SQL Login Name and/or Passphrase: SqlCfgChange.bat

To change the SQL Server user name and password, do the following:

Step 1 Double-click *SqlCfgChange.bat*.

The **SQL Server Connection** page appears.

Step 2 In **User Name**, type the new user name.

Step 3 In **Password**, type a new password.

Note

- To ensure password composition is supported, see Supported Windows, SQL Server, Active Directory, Presence Server, Application User and CUAC Password Characters.
- The new user must have the necessary privileges and access rights as mentioned in the Cisco Unified Attendant Console Advanced installation instructions.

Step 4 Confirm that the **Server** name matches the current server name.

Step 5 Click **Test Connection**.

Step 6 If the message **Connected Successfully** appears, click **OK**. Retype the password.

If the message **Connection Failed** appears, retype the user name and password and try again.

Step 7 Click **Next**.

The **Installation Progress** page appears. If a cross appears alongside any progress message it means that stage of the update has failed; you must run the *SqlCfgChange.bat* file again using valid data. Details of any errors are displayed on the **Errors** tab.

Step 8 Click **Finish**.

Modify Server Hostname: ServerChange.bat

To change the server host name, do the following:

Step 1 Double-click *ServerChange.bat*.

The **SQL Server Connection** page appears.

Step 2 Type the new **Server** name, SQL username and password.

Note

To ensure password composition is supported, see Supported Windows, SQL Server, Active Directory, Presence Server, Application User and CUAC Password Characters.

Step 3 Click **Test Connection**.

Step 4 If the message **Connected Successfully** appears, click **OK**. Retype SQL password.

If the message **Connection Failed** appears, retype the user name and password and try again.

Step 5 Click **Next**.

The **Host Machine Name** page appears, containing the **Machine Name configured in the database** and **Host Name of your machine**.

Step 6 Click **Next**.

The **Installation Progress** page appears. If a cross appears alongside any progress message it means that stage of the update has failed; you must run the *ServerChange.bat* file again using valid data. Details of any errors are displayed on the **Errors** tab.

Step 7 Click **Finish**.

Step 8 Launch SQL Server Management Studio and log in with SA account.

a. Click **File** > **Open** > **File**.

b. Navigate to and open *\Program Files (x86)\Cisco\Utilities\Server and SQL Change Tool\SQLServerChange.sql*.

c. Click **Execute**.

d. Exit SQL Management Studio after the script successfully executes.

Step 9 If you have a resilient system and have changed the Publisher host name, log in to the Subscriber server and use a text editor to open the *C:\Apache\ActiveMQ\conf\credentials.properties* file; change the line starting:

othernode=

to specify the new publisher host name. For example:

othernode=PAK-SZA-WIN2009

and then save the file.

If the Conversion Fails

The batch files log everything they do in the folder:

%programdata%\Cisco\CUACA\Server\Logging\DBW.

If the conversion fails, please supply Cisco TAC support with a copy of this folder and the following files:

- The .bat and .xml files from the folder *\<installation_folder>\Utility\Server and SQL Change Tool*
- The Arc Solutions registry
- The databases
- The files *CTI Server.exe.config* and *PresenceServer.exe.config* from the CTI and Presence Server folders.

Hostname change

If the hostname of the Cisco Unified Attendant Console Advanced Server machine is changed, you will need to perform the following steps to manage HTTPS:

Step 1 Create a self-signed certificate.

Step 2 Associate the new self-signed certificate.

Create a Self-Signed Certificate

To create a Self-Signed Certificate, do the following:

Step 1 On your computer, open the **Server Manager** and go to **Tools > Internet Information Services (IIS) Manager**. Internet Information Services (IIS) Manager window opens.

Step 2 Under **Connections**, click your server.

Step 3 Under **IIS**, double-click **Server Certificates**.

Step 4 In **Actions**, click **Create Self-Signed Certificate**.

Step 5 Under **Specify a friendly name for the certificate**, type the name you want to use for your domain.

Step 6 Under **Select a certificate store for the new certificate**, select **Personal**.

Step 7 Click **OK** and the new certificate will appear in the list of **Server Certificates**.

Associate the new Self-Signed Certificate

To associate the new Self-Signed Certificate, do the following:

Step 1 On your computer, open the Server Manager and go to **Tools** > **Internet Information Services (IIS) Manager**. Internet Information Services (IIS) Manager window opens.

Step 2 Under **Connections**, click the arrow next to your server, and then under **Sites** click **Default Web Site**.

Step 3 In **Actions**, under **Edit Site**, click **Bindings**. The **Site Bindings** window opens.

Step 4 If an https binding does not already exist, do the following:

a. Click **Add**. The **Add Site Binding** window opens.

b. Set your binding settings:

- **Type**: https
- **IP address**: All Unassigned
- **Port**: 443
- **Host name**: the FQDN of the machine or localhost

OR

If an https binding already exists, do the following:

a. In **Site Bindings**, click the HTTPS (port 443) binding, and the click Edit. The **Edit Site Binding** window appears.

b. Under **SSL certificate**, from the drop-down menu select the Self-Signed Certificate you created previously as described in Create a Self-Signed Certificate.

c. Click **Select**. The **Select Certificate** window appears.

d. Click the certificate you want to use and click **OK**.

e. In the **Edit Site Binding** window, click **OK** and close all other windows.

Set Cisco Unified Attendant Console Advanced and SQL Server services startup type to Automatic

After updating all affected servers, on each do the following:

1. Navigate to Control Panel, and then select **Administrative Tools**.
2. Select **Services**.
3. Set the start-up type of the following services to **Automatic**:
   - BLF Plug-in
   - ActiveMQ
   - Cisco Unified Attendant Server

- Cisco Unified Presence Server
- Cisco Unified Attendant LDAP Plug-in (Publisher Only)

Reinstall High Availability (If Required)

If leveraging high availability, install replication. See Installing Replication.

Restart Cisco Unified Attendant Console Advanced Server(s)

For changes to take effect, restart Cisco Unified Attendant Console Advanced server(s).

Performing CUCM Upgrades and Re-installing Cisco TSP

Note Whether installing for the first time or reinstalling, the Cisco Media Driver Configuration UDP Port Range should account for a minimum of 1000 Media Channels. When Cisco Unified Attendant Console Advanced silently installs Cisco TSP, the Start Range is set to 50000 and End Range is set to 54000. If opting to use a different range, ensure that the firewall exclusions are modified accordingly.

To perform a CUCM upgrade and re-install Cisco TSP, do the following:

Step 1 Launch Cisco TSP Media Driver Configuration and take note of the **Starting** and **Ending** ports.

Step 2 Launch Cisco TSP Configuration and click **Configure**.

Step 3 Select the **General** tab and take note of the **Auto Update Information** settings.

Step 4 Select the **User** tab and take note of the application user ID and password.

Step 5 Select the CTI Manager tab and take note of the **Primary** and **Backup** CTI Manager locations.

Step 6 Take note of the configurations under the **Security** and **Advanced** tabs.

Step 7 Login to CUCM Administration, select **Application > Plug-ins**. Download the relevant Cisco TAPI client.

Step 8 Stop all CUAC Services.

Step 9 Uninstall Cisco TSP.

Step 10 Restart server.

Step 11 Login as a local administrator, then stop all CUACA Services.

Step 12 Navigate to *Program Files (x86)/Cisco/CTI Server/*. Delete the **Driver Instance** folder.

Step 13 Install Cisco TAPI client using the configuration from steps 1 through 6. If something is missed during the install, you can launch the configuration screens post install to modify.

Step 14 Restart server.

Modifying Cisco Unified Attendant Console Advanced Server IP Address

If you want to modify the IP address(es) of the Cisco Unified Attendant Console Advanced Server(s), be mindful of the following:

- Prior to modifying the server network configuration, take note of the existing server registration code(s). The registration code is noted in the **Web Administrator > Help > Licensing menu**. Modifying the network configuration may change the registration code(s), which will remove any existing licensing from the server. After making the required changes, first confirm whether the existing licensing remained intact. If it did, no further action is needed on this topic. If it did not, open a case with **Cisco Global Licensing Operations**, requesting that the pre-existing licensing be reset. The team will require the old server registration code and/or license activation codes to assist.
- If the Cisco Unified Attendant Console Advanced Server(s) and console clients are unable to resolve one another by host name, the hosts file located on each machine must be updated to reflect the IP address change. The hosts file is located in the *\\Windows\System32\drivers\etc\ repository*.
- After implementing any needed changes, restart the server(s), validating that all services start successfully. Services status can be observed from the **Web Administration > Engineering > Service Management** menu.

Setting Up Non-standard SQL Server Ports

Configuring SQL to Use a Non-standard Port

In order for the application to function as expected with non-standard ports, SQL Aliases need to be created on the Cisco Unified Attendant Console Advanced Server(s) and Client machines.

If replication is in place, each Server requires an Alias for itself and the other Server. Each Cisco Unified Attendant Console Advanced client also requires an alias for each server.

The following instructions were compiled using SQL Server 2014, therefore they may differ slightly for alternative versions.

Cisco Unified Attendant Console Advanced Server Alias Configuration

To configure a server alias, do the following:

Step 1 Launch **SQL Configuration Manager**.

Step 2 Expand the **SQL Native Client X.XX Configuration (32-bit)**, right-click **Aliases**, select a new **Alias** and enter the appropriate details.

Step 3 Repeat the above for **SQL Native Client X.XX Configuration (64-bit)**.

Note In a scenario where Replication is intended to be utilized, a SQL Alias needs to be defined on both Servers, where alias matches the respective server's host name.

Step 4 Then, select **SQL Native Client X.XX Configuration (32-bit) > Client Protocols**.

Step 5 Disable all options except **TCP/IP** by right-clicking the option and clicking **Disable**.

Step 6 Open **TCP/IP** by double-clicking or right-clicking and then clicking **Open**.

Step 7 Change the **Default Port** to the required port number.

Step 8 Click **Apply** and **OK** to store the change.

Step 9 Repeat this for **SQL Native Client X.XX Configuration (64-bit) > Client Protocols**.

Step 10 Then, select the option **SQL Server Network Configuration > Protocols for MSSQLSERVER**.

Step 11 Open **TCP/IP** by double-clicking or right-clicking and then clicking **Open**.

Step 12 Select the **IP Addresses** tab.

Step 13 Scroll to the bottom of the list and change the **IPAll TCP Port** value to your selected port number.

Step 14 Click **Apply** and **OK** to store the change.

Step 15 Repeat the above steps on the Cisco Unified Attendant Console Advanced Subscriber server.

Creating an Alias on Client

Repeat this procedure for each client, remembering to set up the connection to each Cisco Unified Attendant Console Advanced server.

Step 1 Browse to either *%windir%\SysWow64*.

Step 2 Double-click *cliconfg.exe*. The **SQL Server Client Network Utility** window appears.

Step 3 Select the Alias tab, and then click **Add**. The **Add Network Library Configuration** window appears.

Step 4 In Server alias, type the hostname of the server.

Step 5 Under Network libraries, select **TCP/IP**.

Step 6 Under Connection parameters, leave **Dynamically determine port** un-selected.

Step 7 Type the non-standard Port number used by the Cisco Unified Attendant Console Advanced client to communicate with the Cisco Unified Attendant Console Advanced server.

Step 8 Click **OK**.