



Cisco Unified Attendant Console Advanced Administration and Installation Guide

Version 11.0.1
December 15, 2016

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.

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 Administration and Installation Guide

© 2016 Cisco Systems, Inc. All rights reserved.



Preface ix

CHAPTER 1

Product Overview 1-1

Features 1-1

New Features in Version 11.0.1 1-2

Core Languages 1-2

Server Resilience 1-2

Resilience Provided 1-4

Cisco Unified Attendant Console Advanced Ports 1-5

Integrating Cisco Unified Attendant Console Advanced with Cisco Unified Communications Manager 1-7

AXL Connectivity 1-7

AXL Usage During Installation 1-7

AXL Usage After Installation 1-8

Non-resilient Installation Scenarios 1-8

Resilient Installation Scenarios 1-8

AXL API 1-9

Cisco Unified Communications Manager System Devices 1-10

Centralized Installations and Transcoding 1-10

TAPI Resilience 1-11

Music on Hold 1-11

Cisco Unified Presence Server Integration 1-11

CHAPTER 2

Deployment Checklist 2-1

CHAPTER 3

Hardware and Software Requirements 3-1

Server Requirements 3-1

Physical Server Hardware Requirements 3-1

Physical Server Software Requirements 3-2

VMware Server Requirements 3-5

VMware Guest Machine Requirements 3-5

VMware Software Requirements 3-6

Additional Server Considerations 3-6

SQL Server Express Limitations 3-6

SQL and Cisco Unified Attendant Console Advanced Server Resilience 3-7

- Windows Updates and Service Packs 3-7
- Data Backup 3-7
- Server Redundancy 3-7
- Antivirus Software 3-7
- Network Requirements 3-9
- Citrix Support 3-9
- Jabber Support 3-10
- Cisco Unified Attendant Console Advanced Client Requirements 3-10
 - PC Hardware Requirements 3-10
 - PC Software Requirements 3-10
 - Windows Updates and Service Packs 3-11
 - Operator Phone Requirements 3-11

CHAPTER 4

Preparing Cisco Unified Communications Manager and Cisco Unified Presence 4-1

- Creating an Access Control Group 4-1
- Assigning Roles to an Access Control Group 4-2
- Creating and Assigning an Application User 4-2
- Configuring Access to Cisco Unified Presence Server 4-3

CHAPTER 5

Installing Cisco Unified Attendant Console Advanced Software 5-1

- Preparing SQL 5-2
 - Installing SQL Server 2008 5-2
 - Installing SQL Server 2012 5-3
 - Installing SQL Server 2014 5-5
 - Licensing SQL Server 5-6
- Obtaining Cisco Unified Attendant Console Advanced Software 5-7
 - Evaluating Cisco Unified Attendant Console Advanced Software 5-7
 - Creating a Cisco Unified Attendant Console Advanced Downloads and Licensing Website User Account 5-7
 - Downloading the Software 5-8
- Installing Cisco Unified Attendant Console Advanced Server 5-9
 - Resilient Installation Prerequisites 5-9
 - Cisco Unified Attendant Console Advanced Server Installation Procedure 5-10
 - Disabling Remote Access Connection Manager Service 5-13
 - Disabling CUPS to Harden the System 5-13
- Installing Cisco Unified Attendant Console Advanced Client 5-13
 - Installing JAWS Scripts for Visually Impaired Operation 5-15

Configuring and Licensing Cisco Unified Attendant Console Advanced Server 6-1

Administrator Login	6-1
Home Page	6-2
Menu Options	6-2
Toolbar	6-3
Data Entry Fields	6-4
Accessibility for Users with Disabilities	6-4
Licensing Cisco Unified Attendant Console Advanced Software	6-4
Licensing Evaluation Software	6-5
Licensing Purchased Software	6-6
Relicensing Software	6-7
Engineering Menu	6-7
Administrator Management	6-7
Server Management	6-8
Database Management	6-8
Database Purge	6-10
Service Management	6-10
Cisco Unified Attendant Server Status	6-12
Cisco Unified Attendant LDAP Plug-in Status	6-12
Cisco Unified Attendant CUPS Plug-in Status	6-13
Cisco Unified Attendant BLF Plug-in Status	6-13
CUCM Connectivity	6-13
CUPS Connectivity	6-15
Logging Management	6-16
Cisco Unified Attendant Console Advanced Server Logging	6-16
Cisco Unified Attendant LDAP Plug-in Logging	6-17
Cisco Unified Attendant CUPS Plug-in Logging	6-17
Cisco Unified Attendant BLF Plug-in Logging	6-17
Log Collection	6-18
System Configuration Menu	6-19
Queue Device Groups	6-19
Creating Queue Device Groups	6-20
Deleting Queue Device Groups	6-20
System Device Management	6-21
Synchronize with CUCM	6-23
Directory Source Management	6-27
Mapping Cisco Unified Attendant Console Advanced Fields to an LDAP Directory Source	6-28
Connecting to a Directory Source	6-29
Directory Synchronization	6-30

- Directory Field Mapping 6-31
- Directory Rules 6-32
- Contact Management 6-33
 - Adding Contacts 6-33
 - Modifying Contact Information 6-34
 - Deleting Contacts 6-34
- Directory BLF Rules 6-35
 - Creating Directory BLF Rules 6-35
 - Editing Directory BLF Rules 6-36
 - Deleting Directory BLF Rules 6-36
 - Applying BLF Directory Rules 6-36
- User Configuration Menu 6-37
 - General Properties 6-37
 - Queue Management 6-39
 - Creating Queues 6-39
 - Configuring Queues 6-40
 - Operator Management 6-43
 - Creating Operator Profiles 6-43
 - Configuring Operator Profiles 6-43
 - Configuring Out of Hours Routing 6-44
 - Creating Out of Hours Routing Templates From Scratch 6-45
 - Creating Out of Hours Routing Templates by Copying 6-46
 - Deleting Out of Hours Routing Templates 6-47
 - Editing Out of Hours Routing Templates 6-47
- Bulk Administration Menu 6-48
 - Uploading New CSV Files 6-48
 - Managing Uploaded CSV Files 6-49
 - Inserting and Updating Contacts 6-49
 - Inserting Contacts 6-49
 - Updating Contacts 6-50
 - Scheduling Contact Insertion and Updating 6-50
 - Exporting Contacts to CSV Files 6-51
- Cisco Unified Replication 6-52
 - SQL Server Replication 6-54
 - Configuring Server Replication 6-54
 - Installing Replication 6-56
 - Uninstalling Replication 6-58
 - Re-initializing Replication 6-59
 - Monitoring Replication 6-59

Validating Replication	6-59
Replication Report	6-60

APPENDIX A

Uninstalling Cisco Unified Attendant Console Advanced Server A-1

Uninstalling Microsoft SQL Server	A-2
Uninstalling the .NET Framework	A-2
Uninstalling Cisco TSP	A-3

APPENDIX B

Cisco Unified Reporting B-1

Toolbar	B-2
Setting Report Parameters	B-2
Date Range	B-2
Time Range	B-2
Queue Type	B-3
Attendant Operators	B-3
Incoming Calls by Date and Time System Report	B-3
Operator Calls by Time System Report	B-4
Operator Calls by Queue System Report	B-5
Operator Availability Report	B-5
Overflowed Calls By Date System Report	B-6

APPENDIX C

Example Cisco Unified Attendant Console Advanced Configuration C-1

APPENDIX D

Upgrading Cisco Unified Attendant Console Advanced D-1

Upgrading Cisco Unified Attendant Console Advanced Server	D-3
---	-----

APPENDIX E

Backing-up and Restoring Cisco Unified Attendant Console Advanced E-1

Backing-up Databases	E-1
Manually Backing-up Databases	E-2
Automatically Backing-up Databases	E-2
Restoring Databases	E-4
Preparing the Server	E-4
Restoring the Databases	E-5
Reconnecting a Subscriber Server to a Restored Publisher Server	E-6
Backing-up and Restoring the CUPS Configuration	E-6
Restoring a Subscriber Server	E-7
Licensing Your New Server	E-8

APPENDIX F

Updating the Cisco Unified Attendant Console Advanced Server Host Name F-1

- Updating the Server Registry with the New Host Name F-1
- Changing SQL Server Host Name, Login and Password F-2
 - Obtaining the Batch Files F-2
 - Preparing the Batch Files For Standalone Installation F-3
 - Before Running the Batch Files F-3
 - Running the Batch Files F-4
 - Running SqlCfgChange.bat F-4
 - Running ServerChange.bat F-5
 - After Changing the Servers F-5
 - If the Conversion Fails F-6
- Updating the XML Configuration Files with the New Host Name F-6
 - Updating the CTI Server Configuration File F-6
 - Updating the CUP Server Configuration File F-6
 - Updating the Database Configuration File F-6

INDEX



Preface

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
Chapter 1, “Product Overview”	An overview of Cisco Unified Attendant Console Advanced, including its compatibility with Cisco Unified Communications Manager.
Chapter 2, “Deployment Checklist”	The steps to take when installing Cisco Unified Attendant Console Advanced, cross-referenced to the relevant procedures in this guide.

Section	Contains
Chapter 3, “Hardware and Software Requirements”	The Cisco Unified Attendant Console Advanced server and Cisco Unified Attendant Console Advanced client hardware and software requirements.
Chapter 4, “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.
Chapter 5, “Installing Cisco Unified Attendant Console Advanced Software”	How to download, install and license Cisco Unified Attendant Console Advanced software.
Chapter 6, “Configuring and Licensing Cisco Unified Attendant Console Advanced Server”	How to configure Cisco Unified Attendant Console Advanced using Cisco Unified Attendant Console Advanced Administration.
Appendix A, “Uninstalling Cisco Unified Attendant Console Advanced Server”	How to uninstall Cisco Unified Attendant Console Advanced server.
Appendix B, “Cisco Unified Reporting”	How to create Cisco Unified Attendant Console Advanced Administration reports.
Appendix C, “Example Cisco Unified Attendant Console Advanced Configuration”	An example of a resilient Cisco Unified Attendant Console Advanced configuration.
Appendix D, “Upgrading Cisco Unified Attendant Console Advanced”	How to upgrade a Cisco Unified Attendant Console Advanced system.
Appendix E, “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.
Appendix F, “Updating the Cisco Unified Attendant Console Advanced Server Host Name”	How to update the Cisco Unified Attendant Console Advanced server host name during server migration, upgrade, or rebuild.

Document Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in bold font .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .



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.

Obtaining Documentation and Submitting a Service Request

For information on:

- 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* at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to *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, page 1-7](#). 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, user directory and call record logs are all stored in SQL databases on the Cisco Unified Attendant Console Advanced server.

Features

Cisco Unified Attendant Console Advanced has the following basic features:

- Call queuing engine, with 100 Console queues supported
- The maximum number of system devices (including CT Gateway devices, Service devices, and Park devices) supported by a Cisco Unified Attendant Console Advanced Server is 1000. This total does not include Queue DDIs, which are CTI Route Points. The system devices can be distributed among up to 100 Queue Device Groups. You cannot save more than 100 devices per transaction.
- Up to 50 concurrent operator client logins
- Busy Lamp Field (BLF)
- Blind and consultative transfers
- Optional server resilience
- Cisco Unified Communications Manager versions supported— 9.0(1) to 11.5(1). See the important note in [Integrating Cisco Unified Attendant Console Advanced with Cisco Unified Communications Manager, page 1-7](#).

- Directory search integrated with the Cisco Unified Communications Manager directory
- Directory size supported—100K
- Optional use of these directory sources:
 - Active Directory 2008 R1/R2 or Active Directory 2012
 - iPlanet Netscape 5.0
 - iPlanet Netscape 5.1
- View more information in Parked Calls pane
- Set calls to automatically connect to the Console without needing to answer them
- Turn off Busy Lamp Field Presence notifications
- Display statistics for each queue
- Display calls with an icon colored to match the queue they arrived from
- Operators can enter Unavailable mode when idle for longer than a defined period
- Click a special directory tab to create a Personal Directory Group
- Rearrange directory tabs by dragging
- Console configuration preferences saved in the server for use next session
- Option to enter the fields in an AND search in any order

For a more detailed features list see the product data sheets at http://www.cisco.com/en/US/products/ps7282/products_data_sheets_list.html.

New Features in Version 11.0.1

Cisco Unified Attendant Console Advanced version 11.0.1 contains the following new features:

- The archiving of event logs for use by Customer Support staff. For more information, see [Log Collection, page 6-18](#).

Core Languages

Cisco Unified Attendant Console Advanced supports English only.

Server Resilience

Cisco Unified Attendant Console Advanced supports server resilience 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 Replication, page 6-52](#).

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 these are replicated entirely from the Publisher only. 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 only set:
 - the arrival mode for each queue
 - logging levels

You can also 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 [Cisco Unified Presence Server Integration, page 1-11](#).

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 resilience. 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 resilience license. When you install Cisco Unified Attendant Console Advanced as a Publisher-only system, if no SQL Server is detected then SQL Server Express Edition is automatically installed on the server; you will also need to upgrade SQL Server to the Standard or Enterprise edition if you want to convert to a resilient system.

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. The Publisher requires at least SQL Server Standard to be installed, while the Subscriber can use SQL Server Express (which is installed automatically when you install Cisco Unified Attendant Console Advanced, if no version of SQL Server is already installed).

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, page 1-7](#). 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.

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
80	TCP	Pub/Sub Internal and Opr<->Pub/Sub	Used by the Cisco Unified Attendant Console Advanced XML Status Management service, which is hosted on the Internet Information Services (IIS) that runs on the Cisco Unified Attendant Console Advanced server. This service listens for HTTP requests from IP Phones and Web Browsers, and sends requests to IP Phones.
389	TCP	Pub/Sub Internal or Pub/Sub<->Directory source	Used to communicate with Microsoft Active Directory or iPlanet Netscape Directory when <i>not using</i> 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).
636	TCP	Pub/Sub Internal or Pub/Sub<->Directory source	Used to communicate with Microsoft Active Directory or iPlanet Netscape Directory when <i>using</i> 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 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 Console Advanced CUP 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.
5060	UDP	CUPS<->Pub/Sub	Used for communication between the Cisco Unified Attendant Console Advanced and the Cisco CUP servers. This is the default when not using Transport Layer Security.
5061 or 5062	TCP	CUPS<->Pub/Sub	Used for communication between the Cisco Unified Attendant Console Advanced and the Cisco CUP servers. This is the default when using Transport Layer Security.

Port Number	Port Type	Relationship *	Function
11859	TCP	Pub/Sub Internal	Used by the Cisco Unified Attendant Console Advanced service to communicate with the Cisco Unified Attendant Console Advanced server.
61616	TCP	Pub<->Sub	Used to enable messages to be passed between Publisher and Subscriber servers in resilient installations.
61618	TCP	Pub<->Sub	
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 (running Windows Server 2008 and later, or Windows Vista and later). If you are using Operator PCs running Windows XP, ports 1025 to 5000 must also be open to accommodate the default dynamic port range of that operating system. For further information, visit http://support.microsoft.com/kb/832017 .
1025 to 5000	TCP	Opr<->Pub/Sub	Dynamic ports used to communicate between the Cisco Unified Attendant Console Server and Operator PCs running Windows XP. If your site does not have any Operator PCs running Windows XP, you can disregard this range. For further information, visit http://support.microsoft.com/kb/832017 .

* Relationship Key

CUCM = Cisco Unified Communications Manager

CUPS = Cisco Unified 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 <i>does not use</i> SSL and <i>is not</i> configured as the Global Catalog.
636	LDAP server <i>uses</i> SSL and <i>is not</i> configured as the Global Catalog.
3268	LDAP server <i>does not use</i> SSL and <i>is</i> configured as the Global Catalog.
3269	LDAP server <i>uses</i> SSL and <i>is</i> configured as the Global Catalog.

Integrating Cisco Unified Attendant Console Advanced with Cisco Unified Communications Manager

Cisco Unified Attendant Console Advanced V11.0.1 is compatible with Cisco Unified Communications Manager versions 9.0(1) to 11.5(1)*.



Note

The following points:

- The 32-bit version of TSP is required when running Cisco Unified Attendant Console under a 32-bit operating system. The 64-bit version of TSP is required when running Cisco Unified Attendant Console under a 64-bit operating system. Consequently, 64-bit installations are supported only in conjunction with Cisco Unified Communications Manager versions 8.5(1) to 11.5(1).
- If you upgrade your Cisco Unified Communications Manager, you must upgrade the TSP installed on your Cisco Unified Attendant Console Advanced servers to the corresponding version. Failure to do this could result in devices not-registering and a lack of call control. For instructions on how to upgrade your installation, see [Appendix D, “Upgrading Cisco Unified Attendant Console Advanced”](#).
- * There is a known defect – CSCva12833, described at <https://tools.cisco.com/bugsearch/bug/CSCva12833> – that is associated with Cisco TSP 11.5(1). A workaround is available within the bug search tool and the packaged Cisco Unified Attendant Console Advanced installer available at <http://cisco.com/go/ac>.

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 have to specify the following nodes:

- The Cisco Unified Communications Manager that will use it (see [Step 12](#), 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 14](#), 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, page 1-9](#).

Non-resilient Installation Scenarios

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

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 172.29.252.111). 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.

Cisco Unified Communications Manager System Devices

Cisco Unified Communications Manager 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 DNSs.



Note

Cisco Unified Attendant Console Advanced Server is restricted to 1000 system devices. The total number of CTI Port system devices across all Queue Device Groups cannot exceed 1000 per Cisco Unified Attendant Console Advanced Server. For information on configuring CTI Ports, see [System Configuration Menu, page 6-19](#).

Centralized Installations and Transcoding

All Cisco Unified Communications Manager releases support the Cisco TAPI Wave Driver. Cisco Unified Communications Manager Release 8.0 and later also supports the New Cisco Media driver, which is the recommended means of enabling CTI ports to be activated because it allows greater scalability and enables G729 to be used as a codec (compression type) without needing transcoding (the conversion of the output stream of one codec into another codec).

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, page 6-13](#).

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. Music on hold 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, page 6-37](#).

Cisco Unified Presence Server Integration

Cisco Unified Presence collects real-time information from multiple sources to determine a user's availability and their capacity and willingness to communicate.

The Cisco Unified Attendant Console Advanced client can display information extracted from the Cisco Unified Presence Server from Cisco Unified Communications Manager. Cisco Unified Attendant Console Advanced version 11.0.1 is compatible with Cisco Unified Presence Server (CUPS) versions 9.0(1) to 11.5(1). The integration is managed via the Cisco Unified Attendant CUP Plug-in directly to the Cisco Unified Attendant Console Advanced Administration. Cisco Unified Attendant Console Advanced Administration uses SIP SIMPLE to communicate with the Cisco Unified Presence server. Changes to the CUP Plug-in service are managed in real-time: you do not have to stop and restart the CUP Plug-in service for the changes to take effect.

You need to manually configure the Subscriber CUP server connection, which can point to a different CUP node from the one used by Publisher.

For details of how to configure the Cisco Unified Attendant Console Advanced client to use other presence servers, such as OCS, see [Installing Cisco Unified Attendant Console Advanced Client, page 5-13](#).



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.



Note

If you are upgrading an existing Cisco Unified Attendant Console Advanced installation, see [Appendix D, “Upgrading Cisco Unified Attendant Console Advanced”](#).

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

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, page 1-7](#).
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, page 3-1](#)
 - [VMware Server Requirements, page 3-5](#)
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:
 - [Physical Server Software Requirements, page 3-2](#)
 - [Additional Server Considerations, page 3-6](#)
 - [PC Software Requirements, page 3-10](#)
4. Configure Cisco Unified Communications Manager so that it is ready for Cisco Unified Attendant Console Advanced deployment. For more information, see: [Chapter 4, “Preparing Cisco Unified Communications Manager and Cisco Unified Presence”](#)
5. Download, install and license the Cisco Unified Attendant Console Advanced software. For more information, see [Chapter 5, “Installing Cisco Unified Attendant Console Advanced Software”](#).
6. Use Cisco Unified Attendant Console Advanced Administration to configure the Cisco Unified Attendant Console Advanced server. For more information, see [Chapter 6, “Configuring and Licensing Cisco Unified Attendant Console Advanced Server”](#).
7. Install the Cisco Unified Attendant Console Advanced client. For more information, see [Installing Cisco Unified Attendant Console Advanced Client, page 5-13](#).



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 Server Requirements, page 3-5](#).

Physical Server Hardware Requirements

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

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



Note

The following points:

- NIC teaming is not supported.
- Cisco Unified Attendant Console Advanced server is not supported in a production environment if running on a desktop PC.
- If you plan to implement Cisco Unified Attendant Console Advanced server resilience, 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.

- 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 the *Cisco Unified Attendant Console Administration and Installation Guide* have been satisfied.

Physical Server Software Requirements

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

- One of the following activated operating systems, with Windows regional settings set to English:
 - Windows Server 2008 R1 (32-bit)
 - Windows Server 2008 R2 (64-bit)
 - Windows Server 2012 (64-bit)
 - Windows Server 2012 R2 (64-bit)



Note

The following points:

- Cisco Unified Attendant Console Advanced server must be installed and operated exclusively on a supported platform.
- Cisco Unified Attendant Console Advanced server does not run under any version of Windows Server 2003.
- For how to upgrade to Windows Server 2008 visit [http://technet.microsoft.com/en-us/library/cc755199\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc755199(v=ws.10).aspx).
- For how to upgrade to Windows Server 2012 visit <http://social.technet.microsoft.com/Forums/windowsserver/en-US/0905b322-8a4d-4dff-aed7-fa7b642e9f91/upgrading-to-windows-server-2012-and-sql-server-2012>
- 64-bit installations are supported only in conjunction with Cisco Unified Communications Manager versions 8.5(1) or later.
- Windows 2012 is only supported on Cisco Unified Communications Manager 10.0(1) or later.
- Windows 2012 R2 is only supported on Cisco Unified Communications Manager 10.5(1) or later.
- 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.



Note

To install IIS on a system with Windows Server already installed, see either:

- [Adding IIS to Windows Server 2008, page 3-4.](#)
- [Adding IIS to Windows Server 2012, page 3-4.](#)

- ASP.NET 2.0.50727 or later
- .Net Framework 3.5 SP1
- One of the following databases:
 - Microsoft SQL Server 2008 Express, Standard or Enterprise (32-bit or 64-bit)
 - Microsoft SQL Server 2008 R2 Express, Standard or Enterprise (32-bit or 64-bit)
 - Microsoft SQL Server 2008 SP3 Express, Standard or Enterprise (32-bit or 64-bit)
 - Microsoft SQL Server 2012 Express, Standard or Enterprise (32-bit or 64-bit)
 - Microsoft SQL Server 2014 Express, Standard or Enterprise (32-bit or 64-bit)

**Note**

The following points:

- 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.
- No versions of Microsoft SQL Server 2005 are supported.
 - For how to upgrade to SQL Server 2008 visit [http://msdn.microsoft.com/en-us/library/bb677622\(v=sql.100\).aspx](http://msdn.microsoft.com/en-us/library/bb677622(v=sql.100).aspx).
 - For how to upgrade to SQL Server 2012 visit <http://social.technet.microsoft.com/Forums/windowsserver/en-US/0905b322-8a4d-4dff-aed7-fa7b642e9f91/upgrading-to-windows-server-2012-and-sql-server-2012>
 - For the Microsoft SQL Server 2008 Upgrade Advisor visit <http://www.microsoft.com/en-us/download/details.aspx?id=11455>.
 - For the Microsoft SQL Server 2012 Upgrade Assistant visit <http://social.technet.microsoft.com/wiki/contents/articles/2558.upgrade-assistant-tool-for-sql-server-2012.aspx>
 - For considerations when upgrading the database engine to 2008 visit [http://msdn.microsoft.com/en-us/library/bb933942\(v=SQL.100\).aspx](http://msdn.microsoft.com/en-us/library/bb933942(v=SQL.100).aspx).
 - For considerations when upgrading the database engine to 2012 visit <http://msdn.microsoft.com/en-us/library/bb933942.aspx>.
- No 64-bit version of Microsoft SQL Server is supported under Windows Server 2008 R1 (32-bit).
- Cisco Unified Attendant Console Advanced server does not support the Cisco Media Convergence Server (MCS) version of Windows Server.
- If the Cisco Unified Attendant Console Advanced server installer does not detect a supported version of Microsoft SQL Server, it will automatically install Microsoft SQL Server 2008 Express.
- 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.
- **IMPORTANT:** If you plan to implement Cisco Unified Attendant Console Advanced server resilience, you **must** use Microsoft SQL Server Standard or Enterprise (not Express) on the Publisher server. You can use Microsoft SQL Server Express, Standard or Enterprise on the Subscriber server. Furthermore, the Publisher and Subscriber servers must use the *same* version of Microsoft SQL Server: both must use 2008. For guidance on which SQL edition to use, see [Additional Server Considerations, page 3-6](#).

- 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 <http://support.microsoft.com/kb/2032911>). 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.

Adding IIS to Windows Server 2008

To add IIS to an installed Windows Server 2008 operating system, do the following:

-
- Step 1 Run Server Manager, click **Roles**, and then click **Add Roles** to use the Wizard to install Web Server (IIS).
 - Step 2 In the **Before You Begin** page, click **Next**.
 - Step 3 In the **Server Roles** page, select **Web Server (IIS)**.
 - Step 4 Add the **Required Features**.
 - Step 5 Select and add the following **Role Services**:
 - ASP.Net
 - .NET Extensibility
 - ISAPI Extensions
 - ISAPI Filters
 - Server Side Includes
 - Static Content
 - Step 6 Click **Install**.
-

Adding IIS to Windows Server 2012

To add IIS to an installed Windows Server 2012 operating system (including R2), 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 features that are required for Web Server (IIS)** dialog box appears.
 - Step 7 Select **Add management tools (if applicable)**, and then click **Add Features**.

- Step 8 In the **Select server Roles** page, click **Next**.
- Step 9 In the **Features** page, if they are not already installed, select **.NET Framework 3.5 Features**, and then click **Next**.
- Step 10 In the **Web Server Role (IIS)** page, click **Next**.
- Step 11 In the **Role Services** page, select and add the following **Role Services**:
- ASP.Net
 - .NET Extensibility
 - ISAPI Extensions
 - ISAPI Filters
 - Server Side Includes
 - Static Content
- and then click **Next**.
- Step 12 In the **Confirmation** page, click **Install**.
- Step 13 When installation is complete, click **Close**.
-

VMware Server Requirements

In a production environment, Cisco Unified Attendant Console Advanced server is supported on VMware ESXi 4.x, 5.0, 5.1 or 6.0 (Vmotion included) running on a host machine that is compliant with Cisco's UC Virtualization Supported Hardware (described at http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware).



Note

The following points:

- 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: http://docwiki.cisco.com/wiki/Unified_Communications_VMware_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 <http://support.microsoft.com/kb/2032911>). Consequently, Cisco Unified Attendant Console Advanced is not supported if installed on a domain controller.
-

VMware Guest Machine Requirements

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

- 1x vCPU unrestricted
- 4 GB RAM

- 80 GB of available hard disk space



Note

You can download an OVA template configured with the above specifications from the following location:

[http://software.cisco.com/download/release.html?i=!y&mdfid=284373299&softwareid=283910832&release=10.5.2&os=.](http://software.cisco.com/download/release.html?i=!y&mdfid=284373299&softwareid=283910832&release=10.5.2&os=)

VMware Software Requirements

Cisco Unified Attendant Console Advanced server running on a virtual machine requires one of the following activated operating systems, with Windows regional settings set to English:

- Microsoft Windows Server 2008 R1 (32-bit)
- Microsoft Windows Server 2008 R2 (64-bit)
- Microsoft Windows Server 2012 (64-bit)
- Microsoft Windows Server 2012 R2 (64-bit)
- Windows 2012 R2 is only supported on Cisco Unified Communications Manager 10.5(1) or later.



Note

The following:

- 64-bit installations are supported only in conjunction with Cisco Unified Communications Manager versions 8.5(1) to 11.5(1).
- Windows 2012 is only supported on Cisco Unified Communications Manager 10.0(1) or later.

Additional Server Considerations

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

SQL Server Express Limitations

Microsoft SQL Server Express has the following limitations:

- Can access only a single CPU
- Uses only 1 GB of RAM
- SQL Server Express 2008 a maximum database size of 4 GB
- SQL Server Express 2012 and 2014 have a maximum database size of 10 GB
- Cannot support server resilience
- Server host name cannot be more than 15 characters long

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

- Cisco Unified Attendant Console Advanced server resilience

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.

SQL and Cisco Unified Attendant Console Advanced Server Resilience

Cisco Unified Attendant Console Advanced server resilience uses SQL replication, which is not available in Microsoft SQL Server Express. Therefore, if you plan to implement server resilience, you must use Microsoft SQL Server Standard or Enterprise on the Publisher server. The Subscriber server can use Microsoft SQL Server Express, Standard or Enterprise, depending on the size of your Cisco Unified Attendant Console Advanced deployment. The Publisher and Subscriber servers can be part of a Microsoft Domain, so long as they can access each other by hostname.



Note

The Publisher and Subscriber servers *must* use the same version of Microsoft SQL Server.

Windows Updates and Service Packs

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

Java auto-updates are not supported because they sometimes fail, rendering the system unusable.

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.

Server Redundancy

We strongly recommend 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
\\Program Files\Cisco\	Software and application trace files
\\Apache	Active MQ folder
\\Temp\Cisco\Trace	Cisco TSP trace files
\\%ALLUSERSPROFILE%\Cisco\CUAC A	Cisco profile

**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 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.

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.



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.

Citrix Support

Cisco Unified Attendant Console Advanced Server cannot be installed in a Citrix environment.

Cisco Unified Attendant Console Advanced Operator Client (version 10.0 and earlier) cannot be installed in a Citrix environment.

Cisco Unified Attendant Console Advanced Operator Client (version 10.5 and later) can be installed in a Citrix environment:

- Xen App 6.5 and 7.6
- Xen Desktop 6.5 and 7.6

The following platforms are not supported:

- Cisco VXi Solution
- VMWare Horizon

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 Vista Professional 32-bit
- Microsoft Windows Vista Professional 64-bit (using WoW64 emulation)
- Microsoft Windows 7 32-bit
- Microsoft Windows 7 64-bit (using WoW64 emulation)
- Microsoft Windows 8
- Microsoft Windows 8 Pro
- Microsoft Windows 8 Enterprise
- Microsoft Windows 8.1
- Microsoft Windows 10

Windows Updates and Service Packs

Cisco Unified Attendant Console Advanced client supports the application of all Microsoft Windows Updates and Service Packs.

Java auto-updates are not supported because they sometimes fail, rendering the system unusable.

Operator Phone Requirements

If the operator is using a Cisco 7931 IP phone, maximum calls on the Cisco Unified Communications Manager must be set to at least two.

If the operator is using a Cisco 89xx or 99xx IP phone, the rollover feature on Cisco Unified Communications Manager must be disabled.



Note

The following points:

- Cisco Unified Attendant Console Advanced does not support logging on any device that has a duplicate DN, or that uses Extension Mobility.
 - Attendant console handsets are not supported on shared lines.
-



Preparing Cisco Unified Communications Manager and Cisco Unified Presence

The Cisco Unified Attendant Console Advanced server must be able to communicate with Cisco Unified Communications Manager to enable attendant console directory synchronization (if you are using the Cisco Unified Communications Manager directory), busy lamp field (BLF, the endpoint line state) and call control. This chapter describes how to set up Cisco Unified Communications Manager.



Note

If the E.164 telephone number configured for the user in Cisco Unified Attendant Console Advanced does not exactly match the device number in the Cisco Unified Communications Manager database, BLF will not work correctly, as the information cannot be transferred using AXL.

If you use Cisco Unified Presence in your organization and want to integrate presence status in the attendant console directory, you must configure the Cisco Unified Presence server to work with the Cisco Unified Attendant Console Advanced server.

This chapter describes the following:

- [Creating an Access Control Group, page 4-1](#)
- [Assigning Roles to an Access Control Group, page 4-2](#)
- [Creating and Assigning an Application User, page 4-2](#)
- [Configuring Access to Cisco Unified Presence Server, page 4-3](#)

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 in [Assigning Roles to an Access Control Group](#).

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 Call Park Monitoring**
- **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**



Note

* These are relevant only if you are using phone models 69xx, 7931, 7965, 88xx, 89xx and 99xx.

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 different Application User with a different number plan for the CTI ports.

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)
 - 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.
-

Configuring Access to Cisco Unified Presence Server

Cisco Unified Attendant Console Advanced is capable of integrating with Cisco Unified Presence server to display real-time presence status within the Cisco Unified Attendant Console Advanced directory.

To configure this integration, you must add the address of the Cisco Unified Attendant Console Advanced server to the firewall information on the Cisco Unified Presence server. To add the address, do the following:

-
- Step 1 Use your internet browser to access Cisco Unified Presence Administration, and then choose **System > Security > Incoming ACL**.
The **Find and List Allowed Incoming Hosts** page is displayed.
 - Step 2 Click **Add New**.
 - Step 3 Under **Incoming ACL Information**, type a **Description** of the address, and an **IP Address Pattern**.
 - Step 4 Click **Save**.
-



Installing Cisco Unified Attendant Console Advanced Software

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

1. Prepare SQL, as described in [Preparing SQL, page 5-2](#).
2. Download the Cisco Unified Attendant Console Advanced server software, as described in [Obtaining Cisco Unified Attendant Console Advanced Software, page 5-7](#).
3. Install the Cisco Unified Attendant Console Advanced server software, as described in [Installing Cisco Unified Attendant Console Advanced Server, page 5-9](#).
4. Install the Cisco Unified Attendant Console Advanced client software, as described in [Installing Cisco Unified Attendant Console Advanced Client, page 5-13](#).

For how to license and configure the software, see [Licensing Cisco Unified Attendant Console Advanced Software, page 6-4](#).

For how to uninstall the Cisco Unified Attendant Console Advanced server and its associated applications, see [Appendix A, “Uninstalling Cisco Unified Attendant Console Advanced Server”](#).

For how to upgrade your Cisco Unified Attendant Console Advanced server and client, see [Appendix D, “Upgrading Cisco Unified Attendant Console Advanced”](#).



Note

The following points:

- The instructions in this chapter refer to systems installed on Microsoft Windows Server 2008 and 2012. If you are not using these, please perform the equivalent steps for your operating system.
- IIS must be installed and activated before installing Cisco Unified Attendant Console Advanced. For more information, see [Physical Server Software Requirements, page 3-2](#).
- 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.
- Access to the Cisco Unified Attendant Console Advanced server is not supported at any time via Remote Desktop (RDP), Terminal Services (TS) or any other session-based application. These applications can cause TAPI/TSP and Wave Driver instability. Only local or VNC connection is supported. For more information, see <http://support.microsoft.com/kb/308405>.
- Under Windows Server 2012 64-bit, the software must be installed in the following order:
 - a. Microsoft .NET framework 3.5
 - b. SQL 2012 Standard or Enterprise
 - c. 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.

Preparing SQL

When you install Cisco Unified Attendant Console Advanced server, if Microsoft SQL Server is not already installed on the local machine, SQL Server Express gets installed automatically.

However, if you are installing a resilient Cisco Unified Attendant Console Advanced system (for more information, see [Server Resilience, page 1-2](#)), the Publisher server requires either SQL Server Standard or Enterprise Edition to be installed: SQL Server Express is inadequate. Furthermore, if you have more than ten operators, you should also install SQL Server Standard or Enterprise Edition on the Subscriber server.



Note

The instructions in this section refer to [Installing SQL Server 2008 Standard Edition](#), [Installing SQL Server 2012 Standard Edition](#), and [Installing SQL Server 2014 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 2008

To install SQL Server 2008:

- 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, click **New SQL Server stand-alone installation or add features to an existing installation**.
The standard setup support rules are listed.
- Step 4 Click **Next**.
- Step 5 Enter the product key, then click **Next**.
- Step 6 Accept the license terms, then click **Next**.
- Step 7 **Install** the Setup Support Files.
- Step 8 In the **Setup Support Rules** page, select **All Features With Defaults**, and then click **Next**.
- Step 9 In the **Feature Selection** page, accept the default settings and also select the following:

- Database Engine Services
 - SQL Server Replication
- Shared Features
 - Client Tools Connectivity
 - Client Tools Backward Compatibility
 - Management Tools Basics – Management Tools—Complete

Then click **Next**.

Step 10 In the **Instance Configuration** page, select the **Default instance**, then click **Next**.



Note 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.

Step 11 In the **Disk Space Requirements** page, click **Next**.

Step 12 In the **Server Configuration** page, set the following services:

- **SQL Server Agent** runs under the NT AUTHORITY\SYSTEM account. Set the **Startup Type** to **Automatic**.
- **SQL Server Database Engine** runs under the NT AUTHORITY\NETWORK SERVICE account. Set the **Startup Type** to **Automatic**.

Disable the **SQL Server Browser** by clicking under **Startup Type** and selecting **Disabled** (the default); then click **Next**.

Step 13 In **Database Engine Configuration** page:

- Set the **Authentication Mode** to **Mixed Mode** (the Cisco Unified Attendant Console Advanced server does not support Windows Authentication).
- Enter the default password, **Z1ppyf0rever**, for the Built-in SQL Server administration (sa) account.
- Click **Add Current User** to add your login to the SQL Server administrators list.

Then click **Next**.

Step 14 In the **Error and Usage Reporting** page, click **Next**.

Step 15 In the **Installation Rules** page, click **Next**.

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

Step 17 When the setup process is complete, click **Next**.

Installing SQL Server 2012

To install SQL Server 2012:

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**.

The standard setup support rules are checked.

Step 4 If all the rules pass the check, click **OK**.

Step 5 Enter the product key, and then click **Next**.

Step 6 Accept the license terms, and then click **Next**.

Step 7 Include any SQL Server product updates, and then click **Next**.

Step 8 Download and **Install** the Setup Support Files.

Step 9 In the **Setup Support Rules** page, if all the rules have passed, click **Next**.



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

Step 10 In the **Setup Role** page, select **SQL Server Feature Installation**, and then click **Next**.

Step 11 In the **Feature Selection** page, accept the default settings and also select the following:

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

And then click **Next**.

Step 12 In the **Installation Rules** page, if the rules pass, click **Next**.

Step 13 In the **Instance Configuration** page, select the **Default instance**, and then click **Next**.

Step 14 Depending on the version of SQL Server you are installing, the **Disk Space Requirements** page may appear. If it does, click **Next**.

Step 15 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 16 In **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.
- Click **Add Current User** to add your login to the SQL Server administrators list.

And then click **Next**.

- Step 17 In the **Error Reporting** page, click **Next**.
- Step 18 In the **Installation Configuration Rules** page, if the rules all pass, click **Next**.
- Step 19 In the **Ready to Install** page, click **Install**.
- Step 20 When the installation process is complete, click **Close**.
-

Installing SQL Server 2014

To install SQL Server 2014:

-
- 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**.
The global setup support rules are checked.
- 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 In the **Install Rules** page, 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 also select the following:
- Instance Features
 - **Database Engine Services > SQL Server Replication**
 - Shared Features
 - **Client Tools Connectivity**
 - **Client Tools Backward Compatibility**
 - **Management Tools - Basics > Management Tools - Complete**
- 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.
- 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**.

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 <http://www.microsoft.com/sql/howtobuy/default.mspx>.

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.

Obtaining Cisco Unified Attendant Console Advanced Software

This section describes how to obtain Cisco Unified Attendant Console Advanced software. It contains the following main topics:

- [Evaluating Cisco Unified Attendant Console Advanced Software](#)
- [Creating a Cisco Unified Attendant Console Advanced Downloads and Licensing Website User Account](#)
- [Downloading the Software](#)

Evaluating Cisco Unified Attendant Console Advanced Software

You can try out the Cisco Unified Attendant Console Advanced software free of charge. First you must register with Cisco; then you can download and install the trial software. You can use the software for 5 days without having to take any further action.

If you want to trial the software for more than 5 days, you must license it within 5 days of installing it. The application of an evaluation license allows you to use the software free of charge for another 60 days. If you do not license the trial software, you will be unable to use it after the fifth day. You cannot extend the 60 day evaluation license.

You can purchase the software at any time in the evaluation periods, giving you unlimited use. If you do not purchase the software within either evaluation period, the software will stop working at the end of them. When you purchase the software Cisco provides you with a 27-digit license activation code. After licensing the software, you cannot revert to the trial version.

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.
 - Step 7 When the software is downloaded, continue with the installation process described in the next section.
-

Installing Cisco Unified Attendant Console Advanced Server

Before you can install the Cisco Unified Attendant Console Advanced software, you must download it as described in [Obtaining Cisco Unified Attendant Console Advanced Software, page 5-7](#).

Resilient Installation Prerequisites



Tip

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

Before installing a resilient system, do the following:

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. You can add the servers to a Windows domain if you want.
2. Log into the Publisher machine.
3. Ensure that the machine date, time and time zone are correct.
4. If you have a firewall on the Publisher server, configure Firewall Exceptions for:
 - Windows Management Instrumentation (WMI)
 - 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.

5. Install the Cisco Unified Attendant Console Advanced server on the Publisher, as described in [Cisco Unified Attendant Console Advanced Server Installation Procedure, page 5-10](#).
6. Log into the Subscriber machine.
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.
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.

9. Install the Cisco Unified Attendant Console Advanced server on the Subscriber, as described in [Cisco Unified Attendant Console Advanced Server Installation Procedure, page 5-10](#).



Note

The following points:

- Database replication is uninstalled automatically during Cisco Unified Attendant Console Advanced server installation, upgrade or uninstallation. If the replication uninstalls 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.

Cisco Unified Attendant Console Advanced Server Installation Procedure



Note

If you are installing a resilient system, you must perform this installation procedure on both the Publisher and Subscriber servers. You must have installed SQL Server Standard or Enterprise on the Publisher.

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.

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



Note

If they are not already installed, all required third-party applications are now automatically installed, including the Microsoft .NET Framework 3.5, and Microsoft SQL Server Express (if you have no SQL Server installed). These installations may take several minutes. You are prompted to restart your computer afterwards.

Step 4 In the Wizard welcome page, click **Next**.

Step 5 In the **Registration Information** page, type or accept the license holder **Name** and **Company Name**, and then click **Next**.

Step 6 In the **SQL Server Login Information** page, type the SQL Server Username (default is **sa**) and Password (default is **Z1ppyf0rever**), then click **Next**.



Note

The SQL Server login password must be sufficiently complex to meet the Windows policy requirements described at <http://support.microsoft.com/kb/965823>.

Step 7 In the **Resilient Server Mode** page, click either:

- **Publisher Server**, to install the Publisher server, then continue from [Step 10](#). 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 Express 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 8** *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 9** *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](#) on [page 5-9](#).
- Step 10** 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 11** To install a Publisher server, continue from [Step 12](#).
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**.
- Step 12** 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**, and then click **Next**.

**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, page 4-2](#).

If you are installing a Subscriber server, you must enter a different CUCM Application User ID than the one used for the Publisher server.

- Step 13** In both security alert messages, click **Yes**.
- Step 14** 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**

The installation process automatically installs the appropriate Cisco TSP version.

- Step 15** In the **Call Logging** page, select either:
- **Enable Call Logging** (the default)
 - **Disable Call Logging**
- and then click **Next**.
- Step 16** 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**.
- Step 17** In the **Start Copying Files** page, click **Next**.
- The Cisco Unified Attendant Console Advanced server is installed. The database wizard then runs.
- Step 18** 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 of your server settings, including queues and CTI port numbers.
- Click **No** to upgrade the existing database, retaining all of your server settings.

- Step 19** When the wizard has installed the Configuration and Logging databases, and updating the registry, click **Finish**.
- Cisco Unified Communications Manager TSP is configured.
- Step 20** 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 21** 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.

You need to license your system before the 5-day evaluation period expires. For more information, see [Licensing Purchased Software, page 6-6](#).

If you have installed a resilient system, set up replication on your Publisher and Subscriber servers as described in [Cisco Unified Replication, page 6-52](#).

Disabling Remote Access Connection Manager Service

The Microsoft Windows Remote Access Connection Manager service can cause problems with the Cisco Unified Attendant Console Advanced server and Cisco TSP; so you must disable it.

-
- Step 1** In Control Panel, open **Administrative Tools**, and then double-click **Services**.
- Step 2** Right-click the **Remote Access Connection Manager** service, and then click **Properties**.
- Step 3** In the dialog box **General** tab set **Startup type** to **Disabled**, and then click **OK**.
- Step 4** Restart your machine for the change to take effect.
-

Disabling CUPS to Harden the System

If you are not using the Cisco Unified Attendant CUP server (CUPS) you can harden the Cisco Unified Attendant Console Advanced system by stopping the Plug-in, as described in [Service Management, page 6-10](#).

Installing Cisco Unified Attendant Console Advanced Client



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 CUP server)
 - Port 1864 (used by the BLF Plug-in)
 - Port 5060 as an incoming and outgoing UDP port (used by the CUP server)

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.



Note If you are upgrading your software, any configured user preferences are maintained.

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 [Obtaining Cisco Unified Attendant Console Advanced Software, page 5-7](#).
- 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**.



Note Click **Back** on any Wizard page to go back to the previous one.

- 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.



Note For a resilient installation you must enter the host name of *Cisco Unified Attendant Console Advanced Publisher server* (and not any other server), otherwise Cisco Unified Attendant Console Advanced will not work properly.

Where a DNS Server is not present on the network or the Server Machine Name 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 have been satisfied.

- Step 7** In the **Presence Information** page, select the type of presence required:
- Microsoft Presence Status – OCS 2007 R2, Lync 2010 or Lync 2013
 - Cisco Presence Status
 - None
- and then click **Next**.



Note After installation, you can change the presence setting in Cisco Unified Attendant Console Advanced by choosing **Options > Preferences > Presence**.

- Step 8** In the **Language Information** page, select the language to use for the application, and then click **Next**.

- Step 9** 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 10** If you are happy with the settings, click **Next** to copy the files and install the software.
- Step 11** In the installation completed page, click **Finish**.
-

Installing JAWS Scripts for Visually Impaired Operation

The Cisco Unified Attendant Console Advanced client can be used with JAWS screen reading software versions 15 and 16.

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\<<version>*
- where the *<version>* folder is *JAWS15* and *JAWS16*.



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

- Step 2** Paste the copied files into the JAWS installation folder, which is:
- C:\Users\All Users\Freedom Scientific\JAWS\<<version>\Settings\<<language>*
- where *<version>* and *<language>* are folders appropriate to your installation. For more information on these folders, see your JAWS documentation.
- For example:
- C:\Users\All Users\Freedom Scientific\JAWS\16.0\Settings\enu*
-



Configuring and Licensing Cisco Unified Attendant Console Advanced Server

Cisco Unified Attendant Console Advanced 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.

Cisco Unified Attendant Console Advanced server and Cisco Unified Communications Manager communicate through the AXL API, using SSL, to synchronize the system devices used for queuing, servicing and parking calls. These devices are created as CTI Ports and CTI Route Point devices within the Cisco Unified Communications Manager database.

This chapter describes how to license the Cisco Unified Attendant Console Advanced server, and how to configure it using Cisco Unified Attendant Console Advanced Administration. Most configuration changes take place in real-time, but for some you have to restart the Cisco Unified Attendant Console Advanced server. This chapter covers the following main topics:

- [Administrator Login, page 6-1](#)
- [Home Page, page 6-2](#)
- [Licensing Cisco Unified Attendant Console Advanced Software, page 6-4](#)
- [Engineering Menu, page 6-7](#)
- [System Configuration Menu, page 6-19](#)
- [User Configuration Menu, page 6-37](#)
- [Bulk Administration Menu, page 6-48](#)
- [Cisco Unified Replication, page 6-52](#)

Example Configuration

For examples of the parameters you use to set up a resilient Cisco Unified Attendant Console Advanced installation, see [Appendix C, “Example Cisco Unified Attendant Console Advanced Configuration”](#).

Administrator Login

Cisco Unified Attendant Console Advanced Administration is accessible only to administrators. The default user name is ADMIN and the default password is CISCO (the user name and password are not case sensitive).

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: `http://<ip address of Cisco Unified Attendant Console Advanced server>/WebAdmin/login.aspx`.

For example, `http://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, `http://localhost/WebAdmin/login.aspx`.

The **Login** page opens.

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

Step 3 Enter your **Password** (not case-sensitive). The default is CISCO.



Note

To clear the contents of the **User name** and **Password** fields, click **Reset**.

Step 4 Click **Login**.

The home page is displayed.

Home Page

The Cisco Unified Attendant Console Advanced Administration home page contains the main menus for configuring the application, and also 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 Replication, page 6-52](#).
- Cisco Unified Reporting— For more information, see [Appendix B, “Cisco Unified Reporting”](#).





















Menu Options

The Cisco Unified Attendant Console Advanced Administration menus are:

- **Engineering**—control and configure connectivity and support management. For more information, see [Engineering Menu, page 6-7](#).
- **System Configuration**—manage synchronization of devices and queues with Cisco Unified Communications Manager. For more information, see [System Configuration Menu, page 6-19](#).
- **User Configuration**—manage Cisco Unified Attendant Console Advanced configuration. For more information, see [User Configuration Menu, page 6-37](#).
- **Help**—view help on Cisco Unified Attendant Console Advanced Administration and licensing the applications. For more information about licensing the software, see [Licensing Cisco Unified Attendant Console Advanced Software, page 6-4](#).

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 or more of the following icons:

Icon	Function
	Add or install an item
	Remove or uninstall an item
	Save
	Reset Password
	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)
	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 [Chapter 6, “Configuring and Licensing Cisco Unified Attendant Console Advanced Server.”](#)
- 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, page 5-15.](#)

For more information on the Cisco Accessibility Program visit

<http://www.cisco.com/web/about/responsibility/accessibility/contact.html>

Licensing 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. Resilience 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. It contains the following main topics:

- [Licensing Evaluation Software](#)
- [Licensing Purchased Software](#)
- [Relicensing Software](#)



Note

Once a system is fully licensed you cannot apply temporary licenses for additional seats. You must wait for the order process to be fulfilled by Cisco before you can add additional seats to an already licensed server.

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.

Licensing 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.

To license the evaluation software for a server, do the following:

- 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 **ACTIVATE EVALUATION SOFTWARE**.
- Step 4 Select your **Reseller**, then select your **Customer**, and then select your **Customer Site**.



Note

If your reseller, customer or site are not available, click the control to add them.

- Step 5 Select the **Version** and the **Product** that you have installed, and then click **Next**.
- Step 6 Enter your Cisco Unified Attendant Console Advanced **Registration Code**.



Note

To find your Registration Code, log into Cisco Unified Attendant Console Advanced Administration and choose **Help > Licensing**.

- Step 7 A registration (.RGF) file is e-mailed to you, and a message to this effect is displayed in the web page. 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 Advanced Administration and choose **Help > Licensing**.
- Step 9 In the **License Management** page, select **Registration File**.
- Step 10 Click **Browse** and then open the Registration File.
- Step 11 Click **Submit** to complete license activation.
- Step 12 Stop and then restart the services, as described in “[Service Management](#)” on page 6-10. If you have configured a resilient server, you need to stop then restart the services once the Publisher server services are restored.

Licensing 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.

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.

To activate your purchased software, do the following:

-
- 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 **ACTIVATE PURCHASED SOFTWARE**.
 - Step 4 Select your **Reseller**, then select your **Customer**, and then select your **Customer Site**.



Note If your reseller, customer or site are not available, click the control to add them.

- Step 5 Select the **Version** and the **Product** that you have installed, and then click **Next**.
- Step 6 Enter the **Registration Code** from the server, and then click **Next**.



Note To find your Registration Code, log into Cisco Unified Attendant Console Advanced Administration and choose **Help > Licensing**.

- Step 7 Enter at least one **License Activation Code** and then click **SUBMIT**.
 - Step 8 In the License Request Confirmation page, optionally enter an additional e-mail address and click **Submit**. If you want to change the License Activation Code you entered in [Step 7](#) before proceeding, click **Back**.

If you have a resilient system you only need to license the Publisher—where all the licenses for the system are stored—and configure Resilience. If you do not configure resilience the Subscriber remains under evaluation mode and will cease to work at the end of the evaluation period.

A registration (.RGF) file is e-mailed to you, and license request confirmation information is displayed in the web page.
 - Step 9 Open the email and save the registration file to a location that can be browsed by the Cisco Unified Attendant Console Advanced server.
 - Step 10 Log into Cisco Unified Attendant Console Advanced Administration and choose **Help > Licensing**.
 - Step 11 In the **License Management** page, select **Registration File**.
 - Step 12 Click **Browse** and then open the Registration File.
 - Step 13 Click **Submit** to complete the registration.
 - Step 14 Stop and then restart the services, as described in [“Service Management” on page 6-10](#). If you have configured a resilient server, you need to stop then restart the services once the Publisher server services are restored.
-

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 on the same hardware
- Add or remove certain hardware (such as an NIC card)
- Install the software on different hardware
- Install a different operating system
- Perform a major upgrade of the Cisco Unified Attendant Console Advanced software

And within a VM Environment:

- Copy the VM image
- 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 Admin.

To re-license a server, contact Cisco TAC and request a re-host. You will need to provide them with either the original license activation codes or the SO number of your purchase.

Engineering Menu

The *Engineering* menu provides connectivity and support management facilities. It includes the following options:

- **Administrator Management** (not available when logged in to Subscriber server). This is described in [Administrator Management, page 6-7](#).
- **Server Management**. This is described in [Server Management, page 6-8](#).
- **Database Management** (cannot be changed if you have a resilient installation). This is described in [Database Management, page 6-8](#).
- **Database Purge**. This is described in [Database Purge, page 6-10](#).
- **Service Management**. This is described in [Service Management, page 6-10](#).
- **CUCM Connectivity**. This is described in [CUCM Connectivity, page 6-13](#).
- **CUPS Connectivity**. This is described in [CUPS Connectivity, page 6-15](#).
- **Logging Management**. This is described in [Logging Management, page 6-16](#).

Administrator Management

The *Administrator Management* option enables you to change or reset the administrator password used when logging into Cisco Unified Attendant Console Advanced Administration. This option is not available on a resilient system if you are logged into the Subscriber server.



Note

The password is not case sensitive.

To change the password:

Step 1 Choose **Engineering > Administrator Management**.

Step 2 Enter **Old Password**. The current password.

Step 3 Enter **New Password**.

It is good practice to have a strong password 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 %, \$, £, &.

Step 4 Re-enter the new password in the **Confirm New Password** field.

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

To set the password back to its default value, CISCO, click **Reset Password**.

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 resilience license, you can change some of these details using the *Server Management* option.

To change server details:

Step 1 Choose **Engineering > Server Management**.

Step 2 The **Server Management** page is displayed.

Step 3 Under **Server Details**, select the server to manage.

Step 4 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 5 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.

**Note**

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** Choose **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**.

**Note**

The SQL Server login password must be sufficiently complex to meet the Windows policy requirements described at <http://support.microsoft.com/kb/965823>.

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

**Note**

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 affect. 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. Customers using SQL Server Express may need to do this because their database size is limited to 4 GB. 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 the database, and then choose **Reports > Standard Reports > Disk Usage**.

To purge the database:

-
- Step 1 Choose **Engineering > Database Purge**.
 - Step 2 Enter **Start Date** either by entering the format yyyy-mm-dd (year-month-date) or click and select it from the calendar.
 - Step 3 Enter **End Date** either by entering the format yyyy-mm-dd (year-month-date) or click and select it from the calendar.
 - Step 4 Click **Purge the Database**.
Cisco Unified Attendant Console Advanced Administration stops the server and purges the database. You must manually restart the server service.
 - 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:
 - Database Name
 - SQL Server
 - Activity Date
 - Purge Start Date
 - Purge End Date
 - Table Name
 - Number of Records effected
 - Status
 - Error Code
 - Error Description
-

Service Management

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

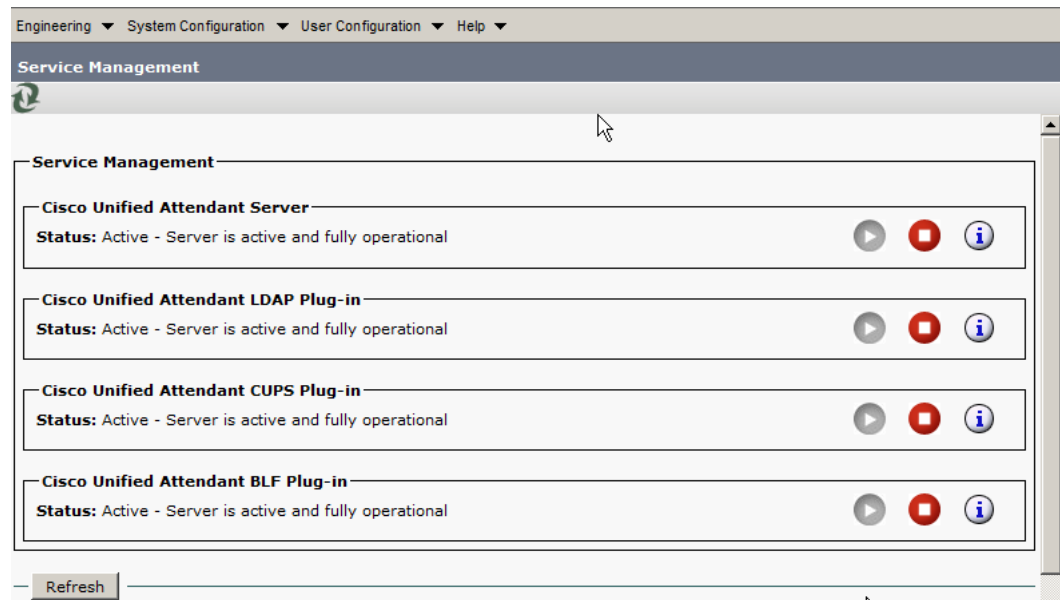
- Cisco Unified Attendant Server
- Cisco Unified Attendant LDAP Plug-in

- Cisco Unified Attendant CUPS Plug-in. *If you are not using CUPS you can harden the Cisco Unified Attendant Console Advanced system by disabling the plug-in using the Service Control Manager (SCM).*
- Cisco Unified Attendant BLF Plug-in

To manage a server:

Step 1 Choose **Engineering** > **Service Management**.

Figure 6-1 Service Management Page



Note

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

Step 2 Use the following controls as appropriate:

Table 6-1

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

Information Displayed

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
 - If your Cisco Unified Attendant Console Advanced is running in resilient mode, the Inter Server Communication Status is also shown.
- 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 CUPS Plug-in Status

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

- The Server Activity of User Activity and Active Subscriptions
- The status of the Primary Server

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 for the Cisco Unified Attendant Plug-in:
 - 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 Inter Server Communication Status shows the status of the link between the Publisher and Subscriber servers.

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 Choose **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, page 4-2](#).
- 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 correct case.

The Username and Password you enter must belong to an application user, for example CCMAAdministrator.

- 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**.

CUPS Connectivity

The CUPS Connectivity page is used to configure the Cisco Unified Attendant CUPS Plug-in with the Cisco Unified Presence server component of Cisco Unified Communications Manager. Cisco Unified Attendant Console Advanced Administration uses SIP SIMPLE to communicate with the Cisco Unified Presence server.

To manage connectivity details:

Step 1 Choose **Engineering > CUPS Connectivity**.

Step 2 Type the **CUPS IP or FQDN**. The IP Address or Fully Qualified Domain Name of the Cisco Unified Presence Server. For example, 209.165.201.0. Leave this empty to disable Cisco Unified Presence server.

Step 3 Type the **CUPS Port** to connect to. This is set to 5060 by default.

Step 4 Type the **Proxy domain**, which is used to authenticate the SIP SIMPLE communication. Set this to the Cisco UP SIP Proxy Domain setting. If you leave this blank, the IP address of the Cisco Unified Presence server is used.

Step 5 To save, click **Save**.

Step 6 To test, click **Test Connection**.



Note The following:

- **IMPORTANT**—The Cisco Unified Attendant CUPS Plug-in has to be added to the firewall information on the Communications Manager. See section [Configuring Access to Cisco Unified Presence Server, page 4-3](#).
 - If you are not using CUPS, you can make your Cisco Unified Attendant Console Advanced system more secure by disabling it using the Service Control Manager (SCM), described on [page 6-10](#).
-

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 CUPS 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** Choose **Engineering > Logging Management**.
The **Logging Management** page appears.
- Step 2** As required, do the following:
- Manage [Cisco Unified Attendant Console Advanced Server Logging](#).
 - Manage [Cisco Unified Attendant LDAP Plug-in Logging, page 6-17](#).
 - Manage [Cisco Unified Attendant CUPS Plug-in Logging, page 6-17](#).
 - Manage [Cisco Unified Attendant BLF Plug-in Logging, page 6-17](#).
 - Set up and run [Log Collection, page 6-18](#).
-

Cisco Unified Attendant Console Advanced 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, the Main and Router processes 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** Specify the **Logging path** and **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 Specify the **Service logging path** and **file name** to maintain log of the Cisco Unified Attendant Console Advanced server service. **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 Specify the **Logging path** and **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 CUPS Plug-in Logging

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

To manage Cisco Unified Attendant CUPS Plug-in logging:

- Step 1 Select the **Logging Level**. One of: **Detailed** (default), **Advanced**, **Minimum**, **Full**.
 - Step 2 Specify the **Logging path** and **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 Specify the **Logging path** and **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 password.
-

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**.

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), as described in [Queue Device Groups, page 6-19](#), and to add and manage system devices, as described in [System Device Management, page 6-21](#).
- **Synchronize with CUCM.** This includes the CUCM Sync Report, and is described in [Synchronize with CUCM, page 6-23](#).
- **Directory Source Management.** This is described in [Directory Source Management, page 6-27](#).
- **Contact Management.** This is described in [Contact Management, page 6-33](#).
- **Directory BLF Rules.** This is described in [Directory BLF Rules, page 6-35](#).

Queue Device Groups

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, page 6-21](#).

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



Note

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, page 6-21](#).



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 system and you are logged into the Subscriber server, you cannot configure system devices.

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 these 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	<p>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.</p> <p>Click Find Template Device to search for a template.</p> <p>Notes:</p> <ul style="list-style-type: none"> • The template device should be based on an end point (a phone) or a CTI Port. <i>Do not use a CTI Route Point as a template device.</i> • If under <i>Protocol Specific Information</i> a <i>Subscribe Calling Search Space</i> is configured, then under <i>Device Information</i> an <i>Owner User ID</i> 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: <ul style="list-style-type: none"> – Forward on CTI Failure – Forward Unregistered Internal – Forward Unregistered External <p>Set these within Cisco Unified Communications Manager, under Directory Number Configuration > Call Forward and Call Pickup Settings.</p>
Queue Devices	
CT Gateway 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, page 1-10 .
Service Devices	
Park Devices	

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

Define the search filter:

- The device property—such as **Device Name**, **Description**, or **Directory Number**—to check.
- 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 Select a template device and 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 in [Synchronize with CUCM](#).

Synchronize with CUCM

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/deselect that Queue Device Group.
<i>Queue Device Group</i>	The Queue Device Group name.
<i>Publisher Devices</i> (<i><server_name></i>)	The number of devices in that group that are on the Publisher server.
<i>Subscriber Devices</i> (<i><server_name></i>)	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 Click **Synchronize with CUCM**.

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

Step 4 If you are happy 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	Description
Sync Status	
Status	Synchronization state; one of: <ul style="list-style-type: none"> • Associating • Completed • Creating • Deleting • Validating
Ignore call forward settings	Whether Ignore call forward is set.

Field	Description
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: <ul style="list-style-type: none"> Completed Error Validating
Error Code	The code of the error that has been encountered. For example, 9400. The error codes are described in the table on page 6-26 .
Error Description	This field gives a brief description of the error that has been encountered. For example, HTTP/1.1 503 Service Unavailable.
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: <ul style="list-style-type: none"> Completed Error Validating
Error Code	The code of any error encountered while validating a device. For example 9300. The error codes are described in the table on page 6-26 .
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.
Status	The status of the device synchronization; one of: <ul style="list-style-type: none"> Completed Error Inprogress

Field	Description
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 6-2

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.
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 simultaneously to one external source directory of each of these 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)

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.** This is described in [Directory Synchronization, page 6-30](#).
- **Directory Field Mappings.** This is described in [Directory Field Mapping, page 6-31](#).
- **Directory Rules.** This is described in [Directory Rules, page 6-32](#).

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, as described in [Contact Management, page 6-33](#).
- Import contacts from CSV files and export contacts to CSV files, as described in [Bulk Administration Menu, page 6-48](#).



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.

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
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
Notes	4000

Cisco Unified Attendant Console Advanced Field	Number of Characters
Room Name	50
Section	50
Title	4
User Field 1	100
User Field 2	100
User Field 3	100
User Profile	255

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

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

- **Property Settings**—Used by the LDAP server during synchronization to ensure that the contact is unique (if Microsoft Active Directory and iPlanet Netscape Directory are selected but not correctly configured their property settings are not displayed)
 - **Unique property**—Select the database property used to identify records
 - **Native property**—Select this checkbox to use several predefined native properties, rather than a unique property.
- **Container** (displayed only with Microsoft Active Directory or iPlanet Netscape Directory 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**)
 - **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.

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. For more information, see below.
- Access the [Directory Field Mapping](#) functionality. For more information, see [Directory Field Mapping, page 6-31](#).
- Access the [Directory Rules](#) functionality. For more information, see [Directory Rules, page 6-32](#).

Directory Synchronization

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



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.

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 type 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**. 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.

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 Cisco Unified Communications Manager 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

- Cisco Unified Communications Manager, 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 Cisco Unified Communications Manager fields, and your Destination field is Extension, you cannot type a Default value.

Step 6 Click **Save** to add the mapping.

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, or 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, page 6-33](#).



Tip

Multiple filters in a rule are combined with a logical AND. So, if a rule contains lastname = T* and Department = Product, all people in the Product team with a last name starting with T are imported.

If you have multiple rules, each containing a single filter, the rules/filters 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 or iPlanet, 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 a 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* option enables you to manually add contacts to your contacts database (full directory) that do not already exist in the LDAP source, and to delete these contacts. You can add both internal and external contacts. All operators can see contacts you add to the full directory. You can also use Contact Management to modify any contact in the full directory, but if it is an LDAP contact (synchronized from the directory source) and not added by you, you can only edit its unmapped fields. You cannot delete contacts that were not manually added.



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 (see [page 6-32](#)), and then manually add them to the directory as *External* contacts.

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:
 - **First name**
You can also specify one or more alternative first names. To do so, click **Alternate First Names** to display the **Alternate First Names** page, click **Add New**, type the name, and then click **Save**. You can also use the controls on the Alternate First Names page to modify and delete alternative first names.
 - **Last name**
You can also specify one or more alternative last names. To do so, click **Alternate Last Names** to display the **Alternate Last Names** page, click **Add New**, type the name, and then click **Save**. You can also use the controls on the Alternate Last Names page to modify and delete alternative last names.
 - **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.
 - For External contacts, either:
 - **First name and Last name**
 - or
 - **Company name**
- And* at least one of the following contact numbers:
- **Business 1**

- **Business 2**
- **Home**
- **Mobile**
- **Pager**
- **Fax**

- Step 5 Add any other contact information. The fields you can enter are the same as the Contact Details available in the Cisco Unified Attendant Console Advanced client.
- 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 check-box 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 that satisfy the Find filter listed.
- 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 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.
- 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 **Deactivate 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 [Appendix 6, “Scheduling Contact Insertion and Updating”](#).

User Configuration Menu

The User Configuration menu enables administrators to configure Cisco Unified Attendant Console Advanced. It includes the following options:

- **General Properties.** This is described in [General Properties, page 6-37](#).
- **Queue Management.** This is described in [Queue Management, page 6-39](#).
- **Operator Management.** This is described in [Operator Management, page 6-43](#).
- **Templates.** This is described in [Configuring Out of Hours Routing, page 6-44](#).

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**—These properties enable Cisco Unified Attendant Console Advanced to distinguish between internal and external calls:
 - **Minimum internal device digit length**—the minimum number of digits used by an internal device
 - **Maximum internal device digit length**—the maximum number of digits used by an internal device



Note

The default maximum setting is 4 digits. If your internal extension numbers have more digits than this, enter the number here. Internal numbers can have up to 24 digits.

- **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
- **External area code**—the Country Code of the Cisco Unified Communications Manager location. International numbers that include this country code are dialed as domestic calls.
- **Default FAC and CMC Settings**—If **Forced Authorization Codes (FAC)** and/or **Client Matter Codes (CMC)** are configured in Cisco Unified Communications Manager, these may be needed when the system makes Attendant calls or transfers. For example, a blind transfer where the final outbound call is made from a Service Queue CTI port. If an external call is made from the operator's handset, the operator is presented with a FAC or CMC dialog box in which they manually enter the code from their application.



Note

Client Matter Code (CMC) is used to provide extra call logging facilities within the 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.



Note

Forced Authorization Code (FAC) is used to provide security in the 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 with Call Arrival Mode to **Hold Queued Calls when it arrives on the CTI Port**. This function places calls on hold so that Music on Hold can be played 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.**

- **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, page 6-10](#).

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**

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**—type the priority of the queue when calls are being routed. This is used to manage the order in which calls in different queues are handled. A queue with a high priority has its calls processed before those in queues with a lower priority. This is the same for all servers.
- **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.
- **Forced Delivery**—select this to make the queue a *forced delivery* queue. This causes an enquiry call to be made from the CTI Port to the next attendant handset in a circular, round-robin pattern. Attendants receive calls in the order in which they log in, and after the last attendant receives a call, the first receives the next one. Attendants are skipped if they are still busy on a previous call.
- **Forced delivery answer time (secs)**—the length of time that a forced delivery call rings at an attendant's extension before it gets routed to the next available attendant.

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](#), below.

Configuring Queues

To configure a queue (if you are viewing the **Queue Management** page you can 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 also 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](#) on [page 6-42](#).

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 (these are described in [Creating Queues](#), [page 6-39](#)).

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, page 6-23](#).

- **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 [Configuring Out of Hours Routing, page 6-44](#), and then do the following:

- a. Click **Out of Hours Routing** or .

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 [Configuring Out of Hours Routing, page 6-44](#).

- 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, page 6-23](#).

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 server.

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 **Password**, and then re-enter it to confirm it.
- c. In **Role**, select either:
 - **Standard**
 - **VIOC** – enables visually impaired attendant operators to use the Console with the help of the JAWS screen reader.

Step 4 Click **Save**.

You must now configure the operator. If you have just created an operator you can continue from [Step 5](#) in the operator configuration procedure.

Configuring Operator Profiles

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.

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**, **Password**, and then **Confirm password**.

Step 6 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 7 Select the queue(s) to associate with the profile and deselect any already-associated queues you do not want associated.

Step 8 Click **Save Selected/Changes** to return to the profile information.

Step 9 Click **Save** to save the changes.

You can click **Reset password** to reset the user password to match the login name.

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. See the *Cisco Unified Attendant Console Advanced Design Guide* for instructions on how to configure out of hours routing across time zones.

Out of hours routing is defined using named *templates*, which you apply to your queues, as described in [Configuring Queues, page 6-40](#). 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.

This section describes the following:

- [Creating Out of Hours Routing Templates From Scratch](#)
- [Creating Out of Hours Routing Templates by Copying, page 6-46](#)
- [Deleting Out of Hours Routing Templates, page 6-47](#)
- [Editing Out of Hours Routing Templates, page 6-47](#)

**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**

The following points:

- 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 [Step 6](#):
- 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 [Step 6](#):

- 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 The following points:

- 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 [Step 9](#), type the corresponding **Destination** number, and then continue at [Step 11](#).
- If you selected **Queue** in [Step 9](#), 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, page 6-45](#).
 - Change existing out of hours date and time periods, as described in [Editing Out of Hours Routing Templates, page 6-47](#).
-

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, page 6-45](#).
 - 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**.
-

Bulk Administration Menu



Note

The Bulk Administration menu is accessible only when you are logged in to the Publisher server. It is also inaccessible if you are using Cisco Unified Attendant Console Advanced Administration in off line mode.

The Bulk Administration menu enables administrators to import contacts from comma-separated value (CSV) files into the full directory, and to export the contacts from the full directory into CSV files. When importing contacts, they can be added to the full directory as new contacts, or they can be used to update existing contact details.



Note

CSV importing does not support Unicode characters.

The import process has these stages:

1. Upload the CSV file to the server, as described in [Uploading New CSV Files, page 6-48](#)
2. Import the contacts from the CSV file into the full directory, as described in [Inserting and Updating Contacts, page 6-49](#). You can do this immediately, or at a later date or time using the job scheduler, as described in [Scheduling Contact Insertion and Updating, page 6-50](#).

The export process is described in [Exporting Contacts to CSV Files, page 6-51](#).

Uploading New CSV 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**.
-

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 [Scheduling Contact Insertion and Updating, page 6-50](#).

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 (Step 5), or **Run Later**, to run the job using the *Job Scheduler*, as described in [Scheduling Contact Insertion and Updating, page 6-50](#).
- 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 (Step 5), or **Run Later**, to run the job using the *Job Scheduler*, as described in [Scheduling Contact Insertion and Updating, page 6-50](#).
- Step 5 Click **Save**.
An update contacts job is created.
-

Scheduling Contact Insertion and Updating

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, page 6-49](#), 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.
Failed	Job failed because of: <ul style="list-style-type: none"> • File not found or can't be opened. • Unique reference not found • File has invalid format.

Job Status	Meaning
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** To schedule the job, within the job, 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.

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 must be less than 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**.

Cisco Unified Replication

Cisco Unified Attendant Console Advanced server resilience is partly provided by server replication. For more information on resilience, see [Server Resilience, page 1-2](#).

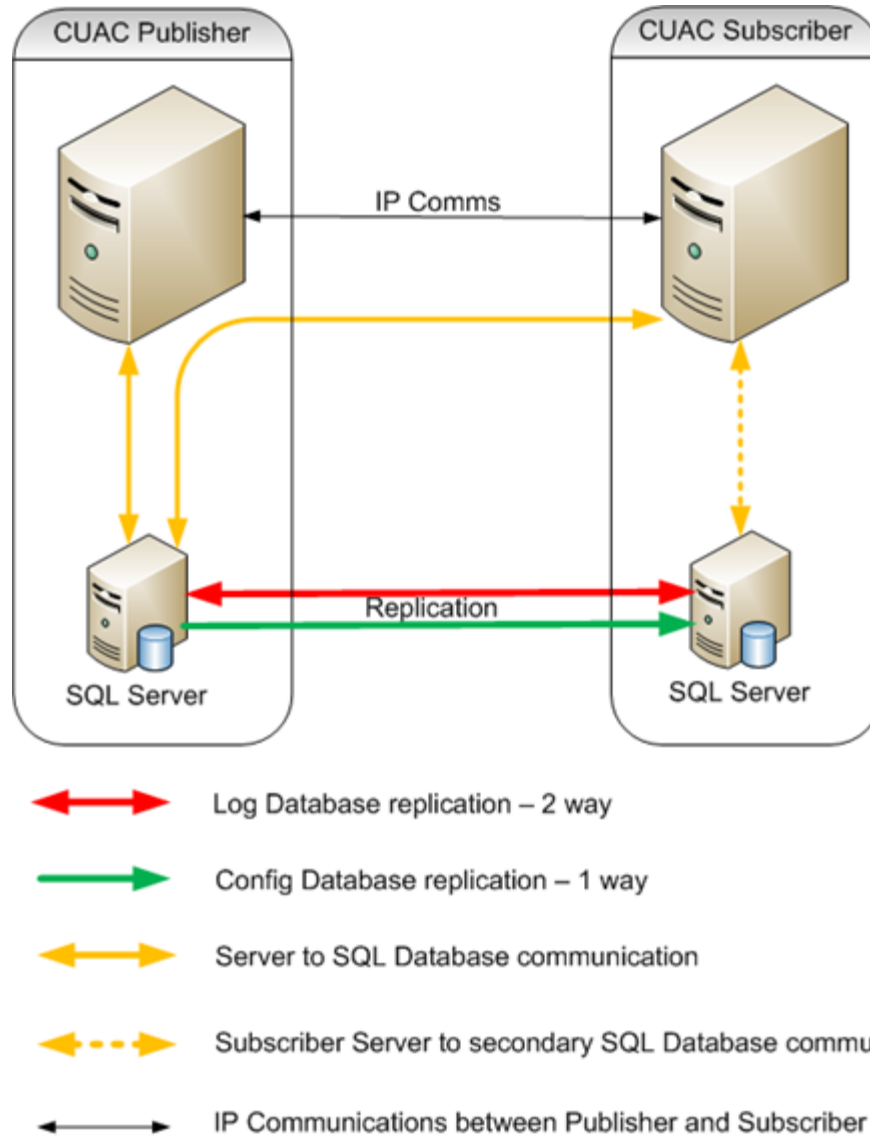
Cisco Unified Attendant Console Advanced contains two databases:

- Configuration database—contains all user configurations and the contacts directory
- Logging database—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 resilience are summarized in this figure:



Note

The following points:

- Cisco Unified Attendant Console Advanced **does not** run on a copy (clone) of a Virtual machine. For more information about VMware requirements, visit: http://docwiki.cisco.com/wiki/Unified_Communications_VMware_Requirements.
- 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 resilience 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, page 6-59](#).

Configuring Server Replication



Note

The instructions in this section refer to using SQL Server 2008 Standard Edition. If you are using a different version or edition the steps may be slightly different. Perform the equivalent steps as described in your SQL Server user documentation.

You configure replication using **Cisco Unified Replication**, with the following restrictions:

- Full replication functionality is available only if a current resilience license and SQL Server Standard or Enterprise edition are installed on the Publisher server.

- If the license has expired, or if there is no resilience license installed, you can only uninstall any existing replication.

**Note**

The following points:

- You must configure replication for *both* the ATTCFG and ATTLOG databases on *both* the Publisher and the Subscriber. Configure the Publisher databases *before* configuring the Subscriber databases. (the Subscriber communicates with the Publisher). When you have installed a Publisher or Subscriber server you cannot convert it into the other type. The Publisher requires at least SQL Server Standard to be installed, while the Subscriber can use SQL Server Express (which is installed when you install Cisco Unified Attendant Console Advanced).
- 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.
- 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, and are started again afterwards.

Before you can configure Cisco Unified Replication, you must 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**. For more information, see [Installing Replication, page 6-56](#).
 - **Uninstall Replication**. For more information, see [Uninstalling Replication, page 6-58](#).
 - **Reinitialize Replication**. For more information, see [Re-initializing Replication, page 6-59](#).
 - **Monitor Replication**. For more information, see [Monitoring Replication, page 6-59](#).
 - **Validate Replication**. For more information, see [Validating Replication, page 6-59](#).
 - **Replication Report**. For more information, see [Replication Report, page 6-60](#).
-

Installing Replication



Note

The information in this section refers to using SQL Server 2008 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.

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 (MSSQLSERVER)**, and then select **Properties**.
The **SQL Server (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)
 - 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.

You must install a replication license before you can install replication.

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 on [page 6-55](#).
- Step 2 Under **Server Credentials (<server_name>)**, type the **Windows username** (domain name\username or server name\username) and **Password** of a user with administrator rights to the Subscriber server.
- 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, page 6-60](#).
- 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.



Note

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, page 6-10](#).

Uninstalling Replication

Before uninstalling replication, perform the checks and procedures at the start of [Installing Replication, page 6-56](#).

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.
- 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, page 6-60](#) and [Monitoring Replication, page 6-59](#).
- Step 8** When replication has been uninstalled for *ATTCFG*, repeat steps 4 to 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 steps 4 to 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, page 6-56](#).

To re-initialize replication for a selected database on a selected server:

- Step 1 In the **Replication Management** page, select the database as described on [page 6-55](#).
- 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 on [page 6-55](#):

- Step 1 In the **Replication Management** page, select the database as described on [page 6-55](#).
- 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 state 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 on [page 6-55](#).
- Step 2 Click **Validate Replication**.

The **Validation Report** is displayed. For example:

Figure 6-2 Example Validation Report

Validation Report

Servers

Publisher:	PAK-KSHAHZAD-7
Subscriber:	WEB-2008-004

Validation Report

1 - 7 of 7 Rows Per Page: 16 ▾

Publication Name	Article Name	Status	Difference	Error Code	Description
PAK-KSHAHZAD-7_ATTCFG	ValidateCTIPorts	Success	0		
PAK-KSHAHZAD-7_ATTCFG	ValidateOverFlow	Success	10		
PAK-KSHAHZAD-7_ATTCFG	ValidateNightService	Success	0		
PAK-KSHAHZAD-7_ATTCFG	ValidateDirEntries	Success	964		
PAK-KSHAHZAD-7_ATTCFG	ValidateResourceGrp	Success	-1		
PAK-KSHAHZAD-7_ATTCFG	ValidateCTIRoute	Success	-1		
PAK-KSHAHZAD-7_ATTCFG	ValidateUserConfig	Success	3		

i Difference Column Description:

- 0 = Publisher and Subscriber contain the same number of records.
- Positive value = Publisher contains this many more records than Subscriber.
- Negative value = Publisher contains this many fewer records than Subscriber.

- 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 on [page 6-55](#).
- Step 2** Click **Replication Report**.

The **Replication Report** is displayed.

Figure 6-3 Example Replication Report

Replication Report						
Replication Report						
1 - 16 of 63						Rows Per Page: 16
Task	Publication Name	Task Date	Status	Error Code	Description	
Install Publication	PAK-ASHAH-7_ATTCFG	2011-11-17 10:26:04.50	Completed			
Verify SQL Server Edition	PAK-ASHAH-7_ATTCFG	2011-11-17 10:26:04.51	Completed		Verified	
Verify Replication Feature	PAK-ASHAH-7_ATTCFG	2011-11-17 10:26:04.53	Completed		Installed	
Set startup type for windows service "SQLServerAgent" at "PAK-ASHAH-7"	PAK-ASHAH-7_ATTCFG	2011-11-17 10:26:04.56	Completed		Already set to automatic	
Set startup type for windows service "MSDTC" at "PAK-ASHAH-7"	PAK-ASHAH-7_ATTCFG	2011-11-17 10:26:05.25	Completed		Already set to automatic	
Start windows service "SQLServerAgent" at "PAK-ASHAH-7"	PAK-ASHAH-7_ATTCFG	2011-11-17 10:26:05.60	Completed		Already started	
Start windows service "MSDTC" at "PAK-ASHAH-7"	PAK-ASHAH-7_ATTCFG	2011-11-17 10:26:05.65	Completed		Already started	
Stop windows service "Cisco Unified Attendant Server" at "PAK-ASHAH-7"	PAK-ASHAH-7_ATTCFG	2011-11-17 10:26:05.94	Completed		Stopped	
Stop windows service "Cisco Unified Attendant LDAP Plug-in" at "PAK-ASHAH-7"	PAK-ASHAH-7_ATTCFG	2011-11-17 10:26:06.28	Completed		Stopped	
Stop windows service "Cisco Unified Attendant Server" at "PAK-2003VM1-WEB"	PAK-ASHAH-7_ATTCFG	2011-11-17 10:26:06.66	Completed		Stopped	
Stop windows service "Cisco Unified Attendant LDAP Plug-in" at "PAK-2003VM1-WEB"	PAK-ASHAH-7_ATTCFG	2011-11-17 10:26:07.08	Completed		Invalid windows service name	
Configure Distribution	PAK-ASHAH-7_ATTCFG	2011-11-17 10:26:07.28	Completed			
Add Publication	PAK-ASHAH-7_ATTCFG	2011-11-17 10:26:07.37	Completed			
Add article for table "Agent_Details"	PAK-ASHAH-7_ATTCFG	2011-11-17 10:26:14.57	Completed			
Add article for table "Agent_Options"	PAK-ASHAH-7_ATTCFG	2011-11-17 10:26:17.17	Completed			
Add article for table "Agent_Skills"	PAK-ASHAH-7_ATTCFG	2011-11-17 10:26:17.35	Completed			

Go 1 of 4

Refresh Close

- 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** next to Related link: Back to Replication Management.



Uninstalling Cisco Unified Attendant Console Advanced Server

This section describes how to uninstall the Cisco Unified Attendant Console Advanced server and its associated applications.



Note

The following points:

- 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.
- When installing, upgrading 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, upgrade 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 **Password** 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. For more information, see [Uninstalling Microsoft SQL Server, page A-2](#)
- .Net Framework. For more information, see [Uninstalling the .NET Framework, page A-2](#)
- Cisco TSP. For more information, see [Uninstalling Cisco TSP, page A-3](#)

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 **Microsoft .NET Framework 3.5**, and then click **Remove**.
You are prompted to either Repair or Uninstall the .NET Framework.
- Step 3 Select **Uninstall**, and then click **Next**.
- Step 4 You are asked to confirm that you want to remove the .NET Framework.
- Step 5 Click **OK**.
While the components are being uninstalled the Setup Progress is displayed.

Step 6 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 Reporting

Cisco Unified Reporting enables you to create reports about the information coming through Cisco Unified Attendant.

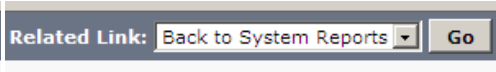
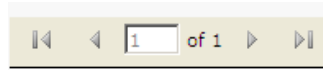
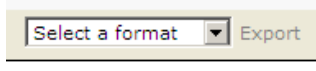


This section describes how to configure Cisco Unified Reporting using Cisco Unified Attendant Console Advanced Administration. Only administrators can access Cisco Unified Attendant Console Advanced Administration.

To access Cisco Unified Reporting:

-
- Step 1** Log in to Cisco Unified Attendant Console Advanced Administration, as described in [Administrator Login, page 6-1](#).
- The Cisco Unified Attendant Console Advanced Administration home page is described. For more information, see [Home Page, page 6-2](#).
- 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. For more information, see [Incoming Calls by Date and Time System Report, page B-3](#).
 - Operator Calls by Time. For more information, see [Operator Calls by Time System Report, page B-4](#).
 - Operator Calls by Queue. For more information, see [Operator Calls by Queue System Report, page B-5](#).
 - Operator Availability. For more information, see [Operator Availability Report, page B-5](#).
 - Overflowed Calls by Date. For more information, see [Overflowed Calls By Date System Report, page B-6](#).
-

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, but all reports require a:

- Date Range
- Time Range

Several reports also require a Queue Type and/or the Attendant Operators to analyze.

When you have set the report parameters, click **Generate Report**.

Date Range

All 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. You can also select the date by clicking the calendar control.

Time Range

All 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.

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.
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.

Field	Description
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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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:

- Operator(s)
- Start and End Date

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**

The following:

- 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.

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.

Field	Description
% 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...
TSP application user	CUACAPUB01	See Creating and Assigning an Application User , page 4-2.
Machine Name	CUACAPUB01	
CT Gateway	1600 - 1609	See Device Groups , page C-2.
Service Device	1610 - 1619	
Park Device	1620 - 1629	
Queue DDI	1630 - 1639	

Subscriber

Parameter	Example Value	Notes
TSP application user	CUACASUB01	See Creating and Assigning an Application User , page 4-2.
Machine Name	CUACASUB01	
CT Gateway	1650 - 1659	See Device Groups , page C-2.
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, page 6-21](#).

For a description of how to create queues and define queue DDIs, see [Queue Management, page 6-39](#).

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, page 6-43](#).

Name	Password
OPERATOR 1	cisco
TESTOP	<BLANK>

Attendant Queues

Name	Type	Primary DDI (Publisher)	Secondary DDI (Subscriber)
BROADCAST	Broadcast	1630	1680
CONSOLE - FORCE	Forced delivery	1631	1681



Upgrading Cisco Unified Attendant Console Advanced

This section describes how to upgrade your Cisco Unified Attendant Console Advanced server and client.



Note

The following:

- Server and Client upgrades are manually instigated, and do not occur automatically.
- You cannot upgrade to version 11.0.1 from any version of Cisco Unified Attendant Console Advanced Department Edition.

Use the following table to determine whether your current Cisco Unified Attendant Console Advanced version and Edition can be upgraded to version 11.0.1,

Your Cisco Unified Attendant Console Advanced version	Edition	Can be directly upgraded to version 11.0.1
Pre-8.6.2	All Editions	No
8.6.2	All Editions	Yes
9.0.1	All Editions	Yes
9.1.1	All Editions	Yes
10.0.1	All Editions	Yes
10.5.1	All Editions	Yes
10.5.2	All Editions	Yes



Note

The following points:

- Cisco Unified Attendant Console Advanced runs under Microsoft Windows Server 2008 and 2012.
 - For how to upgrade to Windows Server 2008 visit [http://technet.microsoft.com/en-us/library/cc755199\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc755199(v=ws.10).aspx)
 - For how to upgrade to Windows Server 2012 visit <http://social.technet.microsoft.com/Forums/windowsserver/en-US/0905b322-8a4d-4dff-aed7-fa7b642e9f91/upgrading-to-windows-server-2012-and-sql-server-2012>

- Cisco Unified Attendant Console Advanced runs under Microsoft SQL Server 2008 and 2012.
 - For how to upgrade to SQL Server 2008, visit [http://msdn.microsoft.com/en-us/library/bb677622\(v=sql.100\).aspx](http://msdn.microsoft.com/en-us/library/bb677622(v=sql.100).aspx).
 - For how to upgrade to SQL Server 2012 visit <http://social.technet.microsoft.com/Forums/windowsserver/en-US/0905b322-8a4d-4dff-aed7-fa7b642e9f91/upgrading-to-windows-server-2012-and-sql-server-2012>
 - For the Microsoft SQL Server 2008 Upgrade Advisor visit <http://www.microsoft.com/en-us/download/details.aspx?id=11455>
 - For the Microsoft SQL Server 2012 Upgrade Assistant visit <http://social.technet.microsoft.com/wiki/contents/articles/2558.upgrade-assistant-tool-for-sql-server-2012.aspx>
 - For considerations when upgrading the database engine to 2008 visit [http://msdn.microsoft.com/en-us/library/bb933942\(v=SQL.100\).aspx](http://msdn.microsoft.com/en-us/library/bb933942(v=SQL.100).aspx)
 - For considerations when upgrading the database engine to 2012 visit <http://msdn.microsoft.com/en-us/library/bb933942.aspx>.
- If you upgrade the Cisco Unified Attendant Console Advanced server you also need to upgrade the Cisco Unified Attendant Console Advanced client. If you do not, differences between the databases may cause inconsistent system performance.
- When upgrading resilient server software, both the Publisher and Subscriber server machines must be running. If either machine is turned off or inaccessible, the upgrade may fail.
- If you upgrade your Cisco Unified Communications Manager, you must upgrade the TSP installed on your Cisco Unified Attendant Console Advanced servers to the corresponding version. Failure to do this could result in devices not-registering and a lack of call control.

To upgrade Cisco Unified Attendant Console Advanced:

1. Ensure that your Cisco Unified Communications Manager version is compatible with the version of Cisco Unified Attendant Console Advanced you are upgrading to. For more information, see [Integrating Cisco Unified Attendant Console Advanced with Cisco Unified Communications Manager, page 1-7](#).
2. Ensure that you have the correct version of operating system and SQL database engine required by the Cisco Unified Attendant Console Advanced version. For more information, see:
 - [Physical Server Software Requirements, page 3-2](#)
 - [VMware Software Requirements, page 3-6](#)
3. Ensure that you are using an Application User account for integration with Cisco Unified Communications Manager.

Cisco Unified Attendant Console Advanced version 8.0.0.5 and earlier used an End User account to communicate with Cisco Unified Communications Manager. Cisco Unified Attendant Console Advanced 8.0.3 and later uses an Application User instead of an End User. For details of how to create an Application User, see [Creating and Assigning an Application User, page 4-2](#).



Note

If you are upgrading from Cisco Unified Attendant Console Advanced version 8.0.0.5 or earlier, you must first delete the End User account from Cisco Unified Communications Manager.

4. Download the Cisco Unified Attendant Console Advanced software. For more information, see [Downloading the Software, page 5-8](#).
5. Sometimes you will need to re-license your Cisco Unified Attendant Console Advanced server. Each release of Cisco Unified Attendant Console Advanced has a three-part build number; for example: 8.0.3, where 8 is the major release number, 0 is the minor release number, and 3 is the maintenance release number.

During major release upgrades—for example, upgrading from version 10.5.2 to version 11.0.1—the permanent licensing gets removed and your server reverts to a 5-day evaluation period. If you have a valid UCSS contract, you can request a new license activation code by visiting <http://www.cisco.com/upgrade> and using the tool there. You will need your service contract number to use this tool and order the upgrade.



Tip

Cisco strongly recommends that you have your new license activation code before performing your upgrade.

If you are upgrading to a new minor or maintenance release, for example from version 9.0.1 to 9.1.1, a new license file is required only if you are:

- Renaming your server
- Using new hardware
- Using a new virtual machine

To re-license your Cisco Unified Attendant Console Advanced server, contact Cisco TAC and request a license re-host. You will need to supply either:

- Original sales order number for the software
- Original license activation code

6. Once your license activation code has been reset or you have received a new license activation code, install the Cisco Unified Attendant Console Advanced server on top of the existing installation.

When upgrading resilient server software, you must upgrade the Publisher server and then the Subscriber server. If you try to upgrade the Subscriber server first it will fail with a version mismatch error. [Upgrading Cisco Unified Attendant Console Advanced Server](#) is described below.

7. License your Cisco Unified Attendant Console Advanced server, as described in [Licensing Cisco Unified Attendant Console Advanced Software, page 6-4](#).
8. Install the Cisco Unified Attendant Console Advanced client over the existing installation. For more information, see [Installing Cisco Unified Attendant Console Advanced Client, page 5-13](#).

Upgrading Cisco Unified Attendant Console Advanced Server

To upgrade 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.
The Wizard is prepared and you are presented with the Welcome screen.
- Step 4 In the Wizard welcome screen, click **Next**.

Step 5 In the **License Confirmation** screen, click **Next**.



Note

You will need to upload and install a new license after installing the software to prevent it from running in 5-day evaluation mode.

Step 6 In the **Registration Information** screen accept or change the license holder **Name** and **Company Name**, and then click **Next**.

Step 7 In the **SQL Server Login Information** screen, accept the SQL Server Username (default is **sa**) and type the Password (If you are using the SQL Server Express that was installed with the Cisco Unified Attendant Console Advanced software, the default password for the sa account is **Z1ppyf0rever**), and then click **Next**. This information is required to connect to the SQL databases.



Note

The SQL Server login password must be sufficiently complex to meet the Windows policy requirements described at <http://support.microsoft.com/kb/965823>.

Step 8 If you have a resilient system and are upgrading the Subscriber server, do the following:

- a. In the **Server Resilience Trial** screen, note the information about purchasing a server resilience license, and then click **Next**.
- b. In the **Publisher SQL Server Information** screen type the Publisher **Server Name**, **SQL User Name** and **Password**, and then click **Next**.

Step 9 In the **Server Information** screen enter the Cisco Unified Attendant Console Advanced **Server Machine** host name, and then click **Next**. If the server machine was previously specified by IP address, you are prompted to enter the host name.

Step 10 Do one of the following:

- If you are upgrading a non-resilient system, the server is treated as the Publisher. If SQL Server Express is installed on the 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 at [Step 11](#), and then upgrade SQL Server later.
- If you have a resilient system and are upgrading the Publisher server, you are prompted to allow the Wizard to stop the services on the Subscriber. Click **Yes** to continue. When prompted for the credentials of the Subscriber server to stop, enter the **Windows Username** and **Password**, and then click **Next**.
- If you have a resilient system and are upgrading the Subscriber server, the following checks and actions are performed:
 - 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.
 - If the SQL Server on the Publisher server is OK, you are prompted to allow the Wizard to stop the services on the Publisher. Click **Yes** to continue. When prompted for the credentials of the Publisher server to communicate with, enter the **Windows Username** and **Password** of your Publisher administrator login, and then click **Next**.

Step 11 In the **Cisco Unified Communications Manager (CUCM)** connection details screen, type or accept the Cisco Unified Communications Manager machine **IP Address**, your **CUCM Application User ID** and **Password**, and then click **Next**.

Step 12 In both security alert messages, click **Yes**.

- Step 13 In the **Cisco TSP Information** screen, accept the settings, **and then** click **Next**.
- Step 14 In the **Call Logging** screen, select either:
- **Enable Call Logging**
 - **Disable Call Logging**
- (the current setting is selected), and then click **Next**.
- Step 15 In the **Choose Destination Location** screen, either accept the default destination folder or **Browse** to where you want to install the files, and then click **Next**.
- Step 16 In the **Start Copying Files** screen, to start copying files, click **Next**.
- The Cisco Unified Attendant Console Advanced server is installed. The database wizard then runs.
- Step 17 In the **Database Wizard**, click **Next**.
- Step 18 You are prompted to overwrite the configuration database and then the logging database:
- Click **Yes** to create a new, empty database. This will delete all of your server settings, including queues and CTI port numbers.
 - Click **No** to upgrade the existing database, retaining all of your server settings.
- Step 19 When the wizard has installed the Configuration and Logging databases, click **Finish**.
- Cisco Unified Communications Manager TSP is configured.
- Step 20 If any third-party applications that might interfere with the TSP configuration are running, you are prompted to close and then 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 21 In the Wizard Complete screen, select **Yes, I want to restart my computer now**, and then click **Finish**.
- Your computer restarts, with the Cisco Unified Communications Manager server installed.
-

**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 [Appendix F, “Updating the Cisco Unified Attendant Console Advanced Server Host Name”](#).

You need to license your system before the 5-day evaluation period expires. For more information, see [Licensing Purchased Software, page 6-6](#).

If you have installed a resilient system, set up replication on your Publisher and Subscriber servers as described in [Configuring Server Replication, page 6-54](#).



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. It contains the following main sections:

- [Backing-up Databases, page E-1](#)
- [Restoring Databases, page E-4](#)
- [Backing-up and Restoring the CUPS Configuration, page E-6](#)
- [Restoring a Subscriber Server, page E-7](#) (applies only to resilient Cisco Unified Attendant Console Advanced installations)
- [Licensing Your New Server, page E-8](#)



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. How to change the configuration is described in [Chapter 6, “Configuring and Licensing Cisco Unified Attendant Console Advanced Server”](#).
- 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. This is described in [Manually Backing-up Databases, page E-2](#).
- Automatically. This is described in [Automatically Backing-up Databases, page E-2](#). *You cannot automatically back up SQL Server Express databases.*

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 steps 3 to 6 for ATTLOG.
-

Automatically Backing-up Databases



Note

This procedure applies to SQL Server Standard and Enterprise edition only. SQL Server Express does possess the functionality to perform automatic backups.

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 2012 and 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.

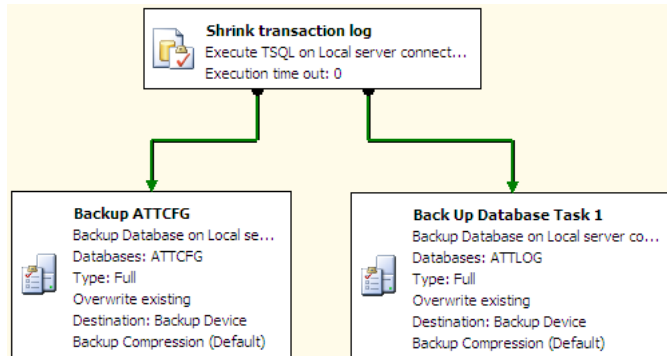


Note If you save the back up files to your server's local drive you must copy them to another location to ensure they are still available if the server fails.

- 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, page E-6](#). For instructions on how to restore a failed Subscriber server, see [Restoring a Subscriber Server, page E-7](#).

Preparing the Server

Before you can restore the databases, you must prepare the server hardware and software, and install Cisco Unified Attendant Console Advanced, as described in [Chapter 5, "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 The following points:

- 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 [Appendix F, “Updating the Cisco Unified Attendant Console Advanced Server Host Name”](#).
- 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, page E-8](#).

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

The following points:

- 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 [Appendix F, “Updating the Cisco Unified Attendant Console Advanced Server Host Name”](#).
 - 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, page E-7](#).

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 Replication, page 6-52](#).

Backing-up and Restoring the CUPS Configuration

To back-up the CUPS configuration, do the following:

-
- Step 1 Log in to Cisco Unified Attendant Console Advanced Administration and choose **Engineering > Service Management**.
- Step 2 Stop the Cisco Unified Attendant CUPS Plug-in server.
- Step 3 On the Cisco Unified Attendant Console Advanced server make a copy of the XML file, *C:\Program Files\Cisco\CUPS\Cisco Presence Server Plug-in.exe.config*.

- Step 4 In Cisco Unified Attendant Console Advanced Administration, restart the Cisco Unified Attendant CUPS Plug-in server.
-

Restoring the CUPS Configuration

To restore the CUPS configuration, do the following:

- Step 1 Log in to Cisco Unified Attendant Console Advanced Administration and choose **Engineering > Service Management**.
- Step 2 Stop the Cisco Unified Attendant CUPS Plug-in server.
- Step 3 On the Cisco Unified Attendant Console Advanced server, overwrite the existing *C:\Program Files\Cisco\CUPS\Cisco Presence Server Plug-in.exe.config* with the copy created in the backup process.
- Step 4 In Cisco Unified Attendant Console Advanced Administration, restart the Cisco Unified Attendant CUPS Plug-in server.
-

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 [Chapter 3, “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 [Chapter 5, “Installing Cisco Unified Attendant Console Advanced Software”](#).

3. License the software, as described in [Licensing Your New Server, page E-8](#).
4. Configure replication between the Publisher and Subscriber. For more information, see [Configuring Server Replication, page 6-54](#).

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 Software, page 6-4](#).



Updating the Cisco Unified Attendant Console Advanced Server Host Name

This appendix describes how to update the Cisco Unified Attendant Console Advanced server host name during server migration, upgrade, or when you have to rebuild the server or change its domain following a failure.

To update the server, you need to complete *all* of the following steps:

1. [Updating the Server Registry with the New Host Name, page F-1.](#)
2. [Changing SQL Server Host Name, Login and Password, page F-2.](#)
3. [Updating the XML Configuration Files with the New Host Name, page F-6.](#)
4. Reboot the Cisco Unified Attendant Console Advanced server.

Updating the Server Registry with the New Host Name

The Windows registry on the Cisco Unified Attendant Console Advanced server contains several references to the server's IP address/host name, which you need to change if you migrate the server or change its host name.



Note

We recommend that when you update the registry you use the Cisco Unified Attendant Console Advancedserver hostname instead of its IP address.

To update the registry keys, do the following:

- Step 1 Back-up your registry.
- Step 2 Access Cisco Unified Attendant Console Advanced Administration, and choose **Engineering > Service Management**.
- Step 3 Stop all services.

- Step 4 Run *regedit* and use it to update the following registry keys under *HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect* so that they contain the Cisco Unified Attendant Console Advanced server host name.

<i>\Configuration</i>	<i>\Defaults</i>	<i>\Web Server</i>	
<i>\Configuration Database</i>	<i>\Server</i>		
<i>\Defaults</i>	<i>\CTI Server Name</i>		
	<i>\Last Connected Server</i>		
	<i>\Presence Server Name</i>		
	<i>\Server Name</i>		
<i>\LDAP Synchronize Server</i>	<i>\CT Connection</i>	<i>\Primary</i>	<i>\Server Name</i>
	<i>\Defaults</i>	<i>\Server Name</i>	
<i>\Logging Database</i>	<i>\Server</i>		

Changing SQL Server Host Name, Login and Password

If you are migrating Cisco Unified Attendant Console Advanced to a new server, you must change the following SQL Server information stored in the configuration database:

- the Hostname
- the SQL login and password.

You change this information using the following batch files, which run the Database Wizard:

- *ServerChange.bat*
- *SqlCfgChange.bat*



Note

If you are only changing the SQL server login name and password, run *SqlCfgChange.bat* *only*; otherwise run *both* batch files, one after the other, in any order.

Obtaining the Batch Files

How you obtain the batch files depends on the version of Cisco Unified Attendant Console you have installed.

- For *Cisco Unified Attendant Console Advanced version 10 or later*, the batch files are in the folder: *\<installation_folder>\Utility\Server and SQL Change Tool*. The default *<installation_folder>* is *Cisco*.
- For *Cisco Unified Attendant Console (Business, Department, Enterprise, and Premium Editions) version 9.1*, request the batch files from Cisco TAC, as they are not included in the default installation.
- For *Cisco Unified Attendant Console (Business, Department, and Enterprise Editions) version 9.0 and earlier*, open a case with Cisco TAC with the information specified in [If the Conversion Fails, page F-6](#).

Preparing the Batch Files For Standalone Installation

By default, the batch files are configured for use with resilient installations only. If you wish to use them in standalone installations you must first edit their XML configuration files.

To edit the configuration files:

-
- | | |
|--------|--|
| Step 1 | Navigate to <code> <installation_folder>\Utility\Server and SQL Change Tool</code> . |
| Step 2 | Use a text editor to open <code>SQLCfgChangeXML</code> . |
| Step 3 | Change the <code>AllConnectedServers</code> key to <code>No</code> . |
| Step 4 | Save and then close the file. |
| Step 5 | Repeat Step 2 to Step 4 for <code>ServerChangeXML</code> . |
-

Before Running the Batch Files

Before running the batch files, do the following on the server(s).



Note

If you have a resilient system, you need to do steps 1. and 2. below on *both* servers, even if you only want to change one server.

1. Stop the following services:
 - ActiveMQ
 - BLF Plug-in
 - Cisco Unified Attendant LDAP Plug-in (Primary server only)
 - Cisco Unified Attendant Server
 - CUPS Plug-in service
2. Set the start-up type of all of these services to Manual.
 - a. From **Control Panel**, select **Administrative Tools**.
 - b. Select **Services**.
 - c. For each of the above services, select the service, right-click, and then select **Properties**.
 - d. In the **Properties** dialog box, click the **General** tab, set the **Startup type** to **Manual**, and then click **OK**.
3. If you have a resilient installation, uninstall replication.
 - a. On the Publisher server, run **Cisco Unified Attendant Console Advanced Administration**.
 - b. Use the **Navigation** control at the right side of the banner to select **Cisco Unified Replication**, and then click **Go**.

The Cisco Unified Replication home page is displayed.
 - c. Click **Replication Management**.

The Replication Management page is displayed.
 - d. Under **Server Details**, select the server to check or configure.



Note The uninstall must be completed first on the subscriber server, then on the publisher server.

- e. Under **Replication Management**, click **Select** alongside the database to uninstall.
 - f. Click **Uninstall Replication**.
 - g. Click **OK** to confirm that you want to uninstall replication.
4. Add a new user or change the existing user password within SQL Studio Manager.

Running the Batch Files



Note The following:

- If you are only changing the SQL server login name and password, run `SqlCfgChange.bat` *only*; otherwise run *both* batch files, one after the other, in any order.
 - Use the batch files to update one server at a time: finish updating one before updating the other.
-

Running 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 with all fields populated with the current data from the registry.

Step 2 In **User Name**, type the new user name.

Step 3 In **Password**, type a new password.



Note The new user must have the necessary privileges and access rights as mentioned in the Cisco Unified Attendant Console Advanced installation instructions.

Step 4 Click **Test Connection**.

Step 5 If the message **Connected Successfully** appears, click **OK**.
If the message **Connection Failed** appears, re-type the user name and password and try again.

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 `SqlCfgChange.bat` file again using valid data. Details of any errors are displayed on the **Errors** tab.

Step 7 Click **Finish**.

Running ServerChange.bat

To change the server host name, do the following:

-
- Step 1** Double-click **ServerChange.bat**.
- The **SQL Server Connection** page appears with all fields populated with the current data from the registry.
- Step 2** Type the new **Server** name.
- Step 3** Click **Test Connection**.
- Step 4** If the message **Connected Successfully** appears, click **OK**.
If the message **Connection Failed** appears, re-type 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 `SqlCfgChange.bat` file again using valid data. Details of any errors are displayed on the **Errors** tab.
- Step 7** Click **Finish**.
- Step 8** Make any necessary changes to your network to ensure that the server is accessible using the new host name.
- Step 9** From within SQL Server Management Studio, run the following script to fix the SQL Server local server name:
- ```
<installation_folder>\Utility\Server and SQL Change Tool\SQLServerChange.sql
```
- Step 10** 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.
- 

## After Changing the Servers

After updating all affected servers, on each do the following:

1. Set the start-up type of all services to **Automatic**.
2. Re-start both the server machines. This restarts the SQL server services.
3. If you have a resilient installation, re-install replication using Attendant Admin.

## If the Conversion Fails

The batch files log everything they do in the file:

`|<installation_folder>\Utility\Server and SQL Change Tool\DBInstallationLog.txt.`

If the conversion fails, please supply Cisco TAC support with a copy of this 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 `Cisco Presence Server Plug-in.exe.config` from the CTI and CUPS Server folders.

## Updating the XML Configuration Files with the New Host Name

You need to edit the XML configuration files for the CUP server, CTI server and Database.

### Updating the CTI Server Configuration File

To update the CTI server configuration file, do the following:

- 
- Step 1 Using Windows Explorer, open the CTI server configuration file `C:\Program Files\Cisco\CTI Server\CTI Server.exe`.
- Step 2 Edit the value of the following key so that it contains the new server host name:  
`<add key="ServerIP" value="new_server_host_name" / >`
- Step 3 Save and close the file.
- 

### Updating the CUP Server Configuration File

To update the CUP server configuration file, do the following:

- 
- Step 1 Using Windows Explorer, open the CUP server configuration file `C:\Program Files\Cisco\CUPS\Cisco Presence Server Plug-in.exe`.
- Step 2 Edit the value of the following key so that it contains the new server host name:  
`<add key="ServerIP" value="new_server_host_name" / >`
- Step 3 Save and close the file.
- 

### Updating the Database Configuration File

To update the Database configuration file, do the following:

- 
- Step 1** Using Windows Explorer, open the Database configuration file *C:\Program Files\Cisco\Utilities\Config.DB*.
- Step 2** Edit the values of the following keys so that they contain the new server host name:  
ATTCFG, Configuration DB, "*new\_server\_host\_name*", sa , )hh > (j]n]j)  
ATTLOG, Logging DB , "*new\_server\_host\_name*" , sa , )hh > (j]n]j)
- Step 3** Save and close the file.
- 



**Note** When you have completed updating the Server Registry, the SQL Database Tables, and the XML Configuration Files, reboot the Cisco Unified Attendant Console Advanced server.

---

■ Updating the XML Configuration Files with the New Host Name



---

## A

access control group, creating and assigning roles [4-1](#)  
access numbers [6-37](#)  
Active MQ service, checking [1-3](#)  
agents (SQL Server replication) [6-54](#)  
antivirus software [3-7](#)  
application user, creating [4-2](#)  
archiving logs [6-18](#)  
AXL API [1-9](#)

---

## B

backing-up data [3-7](#)  
backup up and restoring the server [E-1 to E-8](#)  
BLF subscription number [6-35](#)

---

## C

call arrival mode [6-38](#)  
Calling Search Space (CSS) [6-22](#)  
call logging database, purging [6-10](#)  
call parking [1-10](#)  
Cisco TSP, uninstalling [A-3](#)  
Cisco Unified Attendant BLF Plug-in  
    logging [6-17](#)  
    starting/stopping [6-11](#)  
    status [6-13](#)  
Cisco Unified Attendant Console  
    evaluating [5-7](#)  
    evaluation software, activating [6-5](#)  
    relicensing software [6-7](#)  
Cisco Unified Attendant Console Advanced

configuration management [6-37](#)  
features [1-1](#)  
integrating with Cisco Unified Communications Manager [1-7](#)  
language support [1-2](#)  
licensing software [6-4](#)  
overview [1-1 to 1-11](#)  
upgrading [D-1 to D-5](#)

### Cisco Unified Attendant Console Advanced Administration [1-1](#)

administrator password, changing [6-7](#)  
Bulk Administration menu [6-48 to 6-52](#)  
Engineering menu [6-7 to 6-19](#)  
home page [6-2, 6-48](#)  
logging-in [6-1](#)  
System Configuration menu [6-19 to 6-32](#)  
User Configuration menu [6-37 to 6-61](#)

### Cisco Unified Attendant Console Advanced client [1-1](#)

installing [5-13](#)  
requirements [3-10](#)

### Cisco Unified Attendant Console Advanced server

configuring [6-1 to 6-61](#)  
example configuration [C-1 to C-2](#)  
installing [5-1](#)  
logging [6-16](#)  
prerequisites [5-9](#)  
redundancy and resilience [3-7](#)  
requirements [3-1](#)  
starting/stopping [6-10](#)  
status [6-12](#)  
uninstalling [A-1 to A-3](#)

### Cisco Unified Attendant Console Downloads and Licensing website user account, creating [5-7](#)

### Cisco Unified Attendant CUPS Plug-in

connection, configuring 6-15  
 logging 6-17  
 starting/stopping 6-11  
 status 6-13

**Cisco Unified Attendant LDAP Plug-in**  
 logging 6-17  
 starting/stopping 6-10  
 status 6-12

**Cisco Unified Communications Manager**  
 connection, setting-up and testing 6-13  
 integration with Cisco Unified Attendant Console Advanced 1-7  
 preparing 4-1 to 4-3  
 synchronizing device configurations 6-23

**Cisco Unified Presence (CUP)**  
 preparing 4-1  
 server (CUPS)  
   access, configuring 4-3  
   integration 1-11

**Cisco Unified Replication 6-52 to 6-61**

**Cisco Unified Reporting B-1 to B-6**

**Citrix support 3-9**

**Client Matter Codes (CMC) 6-38**

collecting logs 6-18

**contacts**  
   exporting to CSV Files 6-51  
   importing and exporting 6-48  
   inserting and updating from CSV files 6-49  
   uploading from CSV files 6-48

contacts database, synchronizing with source 6-30

contacts in full directory, adding, deleting and modifying 6-33

CSV files of contacts, managing and uploading 6-48

**CTI Manager 1-7**

CUCM, see Cisco Unified Communications Manager

CUPS, see Cisco Unified Presence server

---

## D

**database**  
   configuration 6-52  
   managing 6-8  
   logging 6-52  
   replication, uninstalling 5-10

**deployment checklist 2-1**

device configuration, synchronizing with Cisco Unified Communications Manager 6-23

**Device Resolution Manager (DRM) 1-8**

**directory**  
   connection, testing 6-30  
   external, synchronization 6-27  
   field mapping 6-31  
   filtering during importing 6-32  
   source, connecting 6-29

**Directory BLF Rules 6-35**

.NET Framework, uninstalling A-2

---

## E

E.164 numbers 6-35

emergency destination 6-41

---

## F

**firewall exceptions 5-9**  
   console client 5-13  
   for replication 6-57

**Forced Authorization Codes (FAC) 6-38**

full CTI failure device 6-41

---

## H

hardware and software requirements 3-1 to 3-11

## I

## importing

- contacts [6-48](#)

- installing the software [5-1](#)

- iPlanet Netscape Directory [6-27](#)

## J

- Jabber support [3-10](#)

- JAWS scripts [5-15](#)

- Job Scheduler [6-50](#)

## L

- licensing software [6-4](#)

- log archive [6-18](#)

- log collection [6-18](#)

- logging servers and plug-ins, managing [6-16](#)

## M

## mapping

- directory information [6-32](#)

- Microsoft Active Directory [6-27](#)

## Microsoft SQL Server

- Express [5-2](#)

- preparing [5-2](#)

- uninstalling [A-2](#)

- Microsoft Windows Updates and Service Packs [3-11](#)

- Microsoft Windows Updates and Service Packs (on server) [3-7](#)

- music on hold (MoH) [1-11](#)

## N

- network requirements [3-9](#)

- non-resilient installation [1-3](#)

## O

- operator phone requirements [3-11](#)

- operator profiles, creating and configuring [6-43](#)

- operator queues, creating and configuring [6-39](#)

## out of hours routing

- configuring [6-44](#)

- setting up queue [6-42](#)

## P

- parking calls [1-10](#)

- publisher server [1-2](#)

- details, changing [6-8](#)

## Q

## queue

- out of hours routing [6-42](#)

- overflows [6-41](#)

- queue device groups [6-19](#)

- deleting [6-20](#)

## R

- recall timers [6-38](#)

- Remote Access Connection Manager Service, disabling [5-13](#)

- replication [6-52 to 6-61](#)

- configuring [6-54](#)

- installing [6-56](#)

- monitoring [6-59](#)

- preparing [6-54](#)

- reinitializing [6-59](#)

- report [6-60](#)

- uninstalling [6-58](#)

- validating [6-59](#)

- reports [B-1 to B-6](#)

- report parameters [B-2](#)

## resilience

- inter-server communication link, checking [1-3](#)
- server [1-2](#)
- TAPI [1-11](#)

rules (filters) for directory importing [6-32](#)

---

**S**

scheduling contact insertion and updating [6-50](#)

search filter (Find) [6-22](#)

## server

- backing up and restoring [E-1 to E-8](#)
- migrating [F-1 to F-7](#)
- replication, *See* replication
- resilience [1-2](#)
- updating the host name [F-1 to F-7](#)

software requirements [3-1](#)

## SQL Server

- 2008 limitations [3-6](#)
- licensing [5-6](#)
- replication [1-2, 6-54](#)

SQL Server 2008, installing [5-2](#)

SQL Server 2012, installing [5-3](#)

SQL Server 2014, installing [5-5](#)

subscriber server [1-3](#)

- details, changing [6-8](#)

synchronization errors [6-26](#)

system reports [B-1 to B-6](#)

---

**T**

TAPI resilience [1-11](#)

template device [6-22](#)

---

**U**

upgrading the software [D-1](#)

---

**V**

VIOC role in operator profile [6-43](#)

VMware server requirements [3-5](#)