Cisco Unified Attendant Console Advanced Administration and Installation Guide
Version 12.0.4
February 7, 2019

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.
CONTENTS

Preface xi

CHAPTER 1
Product Overview 1-1
Features 1-1
   New Features 1-2
   Core Languages 1-3
Server High Availability 1-3
   Resilience Provided 1-4
Single Sign On 1-5
Syslog and Alert Server 1-5
Cisco Unified Attendant Console Advanced Ports 1-6
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 1-9
   AXL API 1-10
      Cisco Unified Communications Manager System Devices 1-10
      Centralized Installations and Transcoding 1-11
      TAPI Resilience 1-11
      Music on Hold 1-11
      Presence Service 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
   VMware Guest Machine Requirements 3-2
   Server Software Requirements 3-2
      SQL Server Requirements 3-3
      SQL Server Express Limitations 3-4
Contents

Additional Server Considerations 3-4
  Microsoft Windows and SQL Server Updates and Service Packs 3-4
  Data Backup 3-5
  Server Redundancy 3-5
  Antivirus Software 3-5
  Network Requirements 3-7
  Citrix Support 3-8
  Jabber Support 3-8

Cisco Unified Attendant Console Advanced Client Requirements 3-8
  PC Hardware Requirements 3-8
  Citrix Support 3-9
  PC Software Requirements 3-9
  Operator Phone Requirements 3-9

CHAPTER 4
Preparing Cisco Unified Communications Manager and Cisco Unified Presence 4-1
  Cisco Unified Communications Manager (Required) 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
  Cisco Unified Presence (Optional) 4-3
    Creating an End User for the Presence Server 4-3
    Presence states chart 4-4

CHAPTER 5
Installing Cisco Unified Attendant Console Advanced Software 5-1
  Adding Internet Information Service (IIS) 5-2
  Installing and/or configuring SQL 5-3
    Installing SQL Server 2016 5-3
    Licensing SQL Server 5-4
  Obtaining Cisco Unified Attendant Console Advanced Software 5-5
    Creating a Cisco Unified Attendant Console Advanced Downloads and Licensing Website User Account 5-5
    Downloading the Software 5-5
  High Availability (Resilient Installations) 5-6
    Export Crypto Key File 5-7
    Cisco Unified Attendant Console Advanced Server Installation Procedure 5-7
    Disabling Plug-ins that are not in use 5-10
  Installing Cisco Unified Attendant Console Advanced Client 5-11
    Installing JAWS Scripts for Visually Impaired Operation 5-12
CHAPTER 6

Cisco Unified Attendant Console Administration 6-1

Administrator Login 6-1
  Logging On 6-1
  Customized Logon Message 6-2
  Last Login Information 6-3
  Logging Out 6-3

Home Page 6-4
  Menu Options 6-4
  Toolbar 6-4
  Data Entry Fields 6-5

Accessibility for Users with Disabilities 6-6

Service Management 6-6
  Cisco Unified Attendant Server Status 6-8
  Cisco Unified Attendant LDAP Plug-in Status 6-8
  Cisco Unified Attendant Presence Plug-in Status 6-8
  Cisco Unified Attendant BLF Plug-in Status 6-9

CUCM Connectivity 6-9

Server Management 6-11
  Hostname change 6-11
    Create a Self-Signed Certificate 6-12
    Associate the new Self-Signed Certificate 6-12

Database Management 6-13
  Database Purge 6-14
    Automatic Purge 6-15

Marking Text Management 6-15

Syslog Connectivity 6-15

Realm Management 6-16

Credential Policy Management 6-17

Logging Management 6-18
  Cisco Unified Attendant Console Server Logging 6-19
  Cisco Unified Attendant LDAP Plug-in Logging 6-20
  Cisco Unified Attendant Presence Plug-in Logging 6-20
  Cisco Unified Attendant BLF Plug-in Logging 6-20

Log Collection 6-21
  Setting Up Log Collection 6-21
  Starting Log Collection 6-21
  Canceling Log Collection 6-21
  Downloading the Log Archive 6-22
Checking Log Collection Progress 6-22

CHAPTER 7  Cisco Unified Attendant Console High Availability 7-1

SQL Server Replication 7-3
  Accessing High Availability Administration Menus 7-3
    Pre-requirements for Installing and Uninstalling Replication 7-3
  Installing Replication 7-4
  Uninstalling Replication 7-7
  Re-initializing Replication 7-7
  Monitoring Replication 7-8
  Validating Replication 7-9
  Replication Report 7-10

CHAPTER 8  Configuring Cisco Unified Attendant Console 8-1

Presence Management 8-1
  Configuration 8-1
Contact Directory 8-2
  Directory Source Management 8-2
    Connecting to a Directory Source 8-3
    Directory Synchronization 8-5
    Directory Field Mapping 8-6
    Directory Rules 8-8
  Inserting, Updating and Exporting Contacts via CSV 8-9
    Inserting and Updating Contacts 8-9
      Inserting Contacts 8-9
      Updating Contacts 8-9
      Scheduling Contact Insertion and Updating 8-10
    Exporting Contacts to CSV Files 8-11
    Uploading New CSV Files 8-12
      Managing Uploaded CSV Files 8-12
Contact Management 8-13
  Adding Contacts 8-13
  Modifying Contact Information 8-14
  Deleting Contacts 8-15
Directory BLF Rules 8-15
  Creating Directory BLF Rules 8-15
  Editing Directory BLF Rules 8-16
  Deleting Directory BLF Rules 8-17
  Applying BLF Directory Rules 8-17
System Configuration Menu  8-17
  Queue Device Groups  8-18
    Creating Queue Device Groups  8-18
    Deleting Queue Device Groups  8-19
  System Device Management  8-19
  Synchronize with CUCM  8-22
Queue Management  8-25
  Creating Queues  8-26
  Deleting Queues  8-27
  Configuring Queues  8-27
  Configuring Out of Hours Routing  8-30
    Creating Out of Hours Routing Templates From Scratch  8-31
    Creating Out of Hours Routing Templates by Copying  8-32
    Deleting Out of Hours Routing Templates  8-33
    Editing Out of Hours Routing Templates  8-33
User Configuration Menu  8-33
  General Properties  8-34
  Operator Management  8-37
    Creating Operator Profiles  8-37
    Importing Operators  8-37
    Configuring Operator Profiles  8-38
    Deleting Operator Profiles  8-39
Engineering Menu  8-39
  Administrator Management  8-40

CHAPTER 9
Licensing Cisco Unified Attendant Console Advanced  9-1
  Licensing the Cisco Unified Attendant Console Advanced Software  9-1
  Activating Evaluation Software  9-2
    Activate the Software  9-2
    Activating Purchased Software  9-2
    License Expiry  9-3
  Relicensing Software  9-4

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
Backing-up and Restoring Cisco Unified Attendant Console Advanced  D-1
  Backing-up Databases  D-1
    Manually Backing-up Databases  D-2
    Automatically Backing-up Databases  D-2
  Restoring Databases  D-4
    Preparing the Servers  D-4
    Restoring the Databases  D-5
    Reconnecting a Subscriber Server to a Restored Publisher Server  D-6
  Backing-up Cryptographic Keys and Registries  D-7
    Backing-up Using Attendant Administrator  D-7
      Manually Backing-up and Restoring Cryptographic Keys and Registries  D-7
    Restoring a Subscriber Server  D-7
    Licensing Your New Server  D-8

APPENDIX E
Updating the Cisco Unified Attendant Console Advanced Server Host Name, SQL Server login name and password  E-1
  Standalone Installs Only: Prepare the Batch Files  E-2
  High Availability Installs Only: Uninstall Replication from Both Servers  E-2
  Set Cisco Unified Attendant Console Advanced and SQL Server Services Startup Type to Manual  E-2
  Modify Cisco Unified Attendant Console Advanced server host name and/or SQL Server login name and password  E-2
  Execute the Appropriate Batch Files  E-3
Modify SQL Login Name and/or Passphrase: SqlCfgChange.bat  E-3
Modify Server Hostname: ServerChange.bat  E-3
If the Conversion Fails  E-4
Set Cisco Unified Attendant Console Advanced and SQL Server services startup type to Automatic  E-5
Reinstall High Availability (If Required)  E-5
Restart Cisco Unified Attendant Console Advanced Server(s)  E-5

APPENDIX F

Performing CUCM Upgrades and Re-installing Cisco TSP  F-1
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:

<table>
<thead>
<tr>
<th>Section</th>
<th>Contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Product Overview”</td>
<td>An overview of Cisco Unified Attendant Console Advanced, including its compatibility with Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Chapter 2, “Deployment Checklist”</td>
<td>The steps to take when installing Cisco Unified Attendant Console Advanced, cross-referenced to the relevant procedures in this guide.</td>
</tr>
<tr>
<td>Chapter 3, “Hardware and Software Requirements”</td>
<td>The Cisco Unified Attendant Console Advanced server and Cisco Unified Attendant Console Advanced client hardware and software requirements.</td>
</tr>
<tr>
<td>Chapter 4, “Preparing Cisco Unified Communications Manager and Cisco Unified Presence”</td>
<td>How to configure Cisco Unified Communications Manager so that Cisco Unified Attendant Console Advanced can work with it.</td>
</tr>
<tr>
<td>Chapter 5, “Installing Cisco Unified Attendant Console Advanced Software”</td>
<td>How to download, install and license Cisco Unified Attendant Console Advanced software.</td>
</tr>
<tr>
<td>Chapter 6, “Cisco Unified Attendant Console Administration”</td>
<td>How to use the Cisco Unified Attendant Console Administration to configure the Cisco Unified Attendant Console Advanced server.</td>
</tr>
<tr>
<td>Chapter 7, “Cisco Unified Attendant Console High Availability”</td>
<td>How to provide server high availability using server replication.</td>
</tr>
<tr>
<td>Chapter 8, “Configuring Cisco Unified Attendant Console”</td>
<td>How to configure Cisco Unified Attendant Console Advanced using Cisco Unified Attendant Console Administration.</td>
</tr>
<tr>
<td>Chapter 9, “Licensing Cisco Unified Attendant Console Advanced”</td>
<td>How to license your Cisco Unified Attendant Console Advanced software.</td>
</tr>
<tr>
<td>Appendix B, “Cisco Unified Reporting”</td>
<td>How to create Cisco Unified Attendant Console Advanced Administration reports.</td>
</tr>
<tr>
<td>Appendix D, “Backing-up and Restoring Cisco Unified Attendant Console Advanced”</td>
<td>How to back up Cisco Unified Attendant Console Advanced server, and how to restore it following failures requiring a full system rebuild.</td>
</tr>
<tr>
<td>Appendix E, “Updating the Cisco Unified Attendant Console Advanced Server Host Name, SQL Server login name and password”</td>
<td>How to update the Cisco Unified Attendant Console Advanced server host name during server migration, upgrade, or rebuild.</td>
</tr>
<tr>
<td>Appendix F, “Performing CUCM Upgrades and Re-installing Cisco TSP”</td>
<td>How to perform a CUCM upgrade and re-install Cisco TSP.</td>
</tr>
</tbody>
</table>
Document Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong> font</td>
<td>Commands and keywords and user-entered text appear in <strong>bold</strong> font.</td>
</tr>
<tr>
<td><em>italic</em> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <em>italic</em> font.</td>
</tr>
</tbody>
</table>

**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:

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

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

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

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 high availability
- Directory size supported:
  - 500 speed dials per user
Features

- 125,000 full directory contacts

- Supported directory sources:
  - Active Directory
  - Cisco Unified Communications Manager
  - iPlanet Netscape

- 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


New Features

Cisco Unified Attendant Console Advanced version 12.0.4 contains the following new features:

- Defect resolution
- Reporting Data Retention Policy
- Presence Enhancements
- New Presence Driver - extending support to WebEx Messenger & Cisco IM&P
- Console user presence preferences are set at a global level
- Cisco IM&P, WebEx Messenger, and Skype for Business support for multi-domain and federated deployments.
- Bulk import, export, and update via CSV for Arabic contacts support.
- Support for 125k directory contacts
- Single Sign On for console users
- Syslog Server - Audit and Alerts
- User credential policies
- Console and Web Admin - custom login messages
- Session Idle Timeout - Web Admin and Console sessions
- BLF Enhancements - Catering to environments where directory contacts have multiple devices.
- BLF Toggle for internal contacts
- Support for Spanish JAWS scripts
Core Languages

Cisco Unified Attendant Console Advanced Server supports English only.

Server High Availability

Cisco Unified Attendant Console Advanced supports server high availability in an active/passive (hot standby) deployment, based on SQL Server replication and the synchronization of database objects across publisher and subscriber servers. For more information on how replication is implemented in Cisco Unified Attendant Console Advanced, see Chapter 7, “Cisco Unified Attendant Console High Availability”.

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

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

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

The following are installed on both server machines:

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

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

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

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

Note

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

1. Log in to Cisco Unified Attendant Console Advanced Administration and choose **Engineering > Service Management**.


If the Inter Server Communication Status is **Suspended**, the ActiveMQ service may not be running.

To check and restart the ActiveMQ service:

1. In Control Panel, click **Accessories**, and then click **Services**.

2. If the Status of the ActiveMQ service is blank (meaning that it is stopped), select the service and click **Start**.

3. Use Cisco Unified Attendant Console Advanced Administration to confirm that the Inter Server Communication Status is **Normal**.

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

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

**Resilience Provided**

The system is resilient to the following failures:

- Cisco Unified Call Manager node failure (partial failover). During normal operation, the primary Cisco Unified Attendant Console Advanced server on the Publisher server and the secondary Cisco Unified Attendant Console Advanced server on the Subscriber server connect to different **CTI Managers** within the same Cisco Unified Communications Manager cluster. For more information about CTI Manager, see **AXL Usage During Installation**. If the Cisco Unified Communications Manager node used by the primary Cisco Unified Attendant Console Advanced server fails, another Cisco Unified Communications Manager takes over and the primary Cisco Unified Attendant Console Advanced server continues to run.

- Primary CTI Manager on Publisher fails (partial failover).

- BLF Server fails (partial failover).

- If you remove all Queue DDI or CT Gateway devices using Cisco Unified Attendant Console Advanced Administration (partial failover). For example if Queue DDIs are manually removed from the TSP User Profile, the server remains active but calls follow the call forward set on Cisco Unified Communications Manager to the Subscriber. You can still update the system configuration using the Cisco Unified Attendant Console Advanced Administration on the Publisher.

- TSP failure.

- Database failure.

- Cisco Unified Attendant Console Advanced server failure (or server shut down, or failure of the communication channel between the Publisher and Subscriber servers).

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

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

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

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

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

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

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

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

Syslog and Alert Server

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

Syslogs are written for the following components:

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

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

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

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Port Type</th>
<th>Relationship *</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>389</td>
<td>TCP</td>
<td>Pub/Sub Internal or Pub/Sub&lt;-&gt;Directory source</td>
<td>Used to communicate with Microsoft Active Directory or iPlanet Netscape Directory when not using Secure Sockets Layer (SSL).</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>CUCM&lt;-&gt;Pub/Sub</td>
<td>Used by the AXL API to communicate with the Cisco Unified Communications Manager, with or without Secure Sockets Layer (SSL).</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Internal/external web browser &lt;-&gt;Pub/Sub</td>
<td>Used by the Cisco Unified Attendant Console Advanced Administration application, which is hosted on the Internet Information Services (IIS) that runs on the Cisco Unified Attendant Console Advanced server.</td>
</tr>
<tr>
<td>636</td>
<td>TCP</td>
<td>Pub/Sub Internal or Pub/Sub&lt;-&gt;Directory source</td>
<td>Used to communicate with Microsoft Active Directory or iPlanet Netscape Directory when using Secure Sockets Layer (SSL).</td>
</tr>
<tr>
<td>1433 and 1434</td>
<td>TCP</td>
<td>Pub&lt;-&gt;Sub and Opr&lt;-&gt;Pub/Sub</td>
<td>Used for SQL communication between servers and between servers and clients.</td>
</tr>
<tr>
<td>1859</td>
<td>TCP</td>
<td>Opr&lt;-&gt;Pub/Sub</td>
<td>Used by the Cisco Unified Attendant Console Advanced server and the Cisco Unified Attendant Console Advanced client to communicate across a LAN.</td>
</tr>
<tr>
<td>1862</td>
<td>TCP</td>
<td>Pub/Sub Internal</td>
<td>Used by the Cisco Unified Attendant Console Advanced LDAP Server.</td>
</tr>
<tr>
<td>1863</td>
<td>TCP</td>
<td>Opr&lt;-&gt;Pub/Sub</td>
<td>Used for communication between the Cisco Unified Attendant Presence server and the Cisco Unified Attendant Console Advanced client.</td>
</tr>
<tr>
<td>1864</td>
<td>TCP</td>
<td>Opr&lt;-&gt;Pub/Sub</td>
<td>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.</td>
</tr>
<tr>
<td>2748</td>
<td>TCP</td>
<td>CUCM&lt;-&gt;Pub/Sub</td>
<td>Used by the Cisco TSP to communicate between the Cisco Unified Attendant Console Advanced server and the Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>5222</td>
<td>TCP</td>
<td>Presence Server &lt;-&gt;IM&amp;P source Presence Server &lt;-&gt;WebEx source</td>
<td>XMPP connection between Presence Server and IM&amp;P and WebEx presence sources.</td>
</tr>
<tr>
<td>11859</td>
<td>TCP</td>
<td>Pub/Sub Internal</td>
<td>Used by the Cisco Unified Attendant Console Advanced service to communicate with the Cisco Unified Attendant Console Advanced server.</td>
</tr>
</tbody>
</table>
Integrating Cisco Unified Attendant Console Advanced with Cisco Unified Communications Manager

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

AXL Connectivity

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

AXL Usage During Installation

During Cisco Unified Attendant Console Advanced server installation you have to specify the following nodes:

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

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

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

**AXL Usage After Installation**

Part of the Cisco Unified Attendant Console Advanced BLF Plug-in service known as Device Resolution Manager (DRM) uses AXL to communicate with Cisco Unified Communications Manager. The AXL communications enable DRM to resolve the BLFs of operator and system devices, and to synchronize system devices within the Cisco Unified Communications Manager database. System device synchronization is described further in AXL API.

**Non-resilient Installation Scenarios**

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

**Scenario 1**

This scenario uses the following node IP addresses:

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

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

**Scenario 2**

This scenario uses the following node IP addresses:

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

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

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

Scenario 3
This scenario uses the following node IP addresses:
- Publisher Cisco Unified Communications Manager = 17.29.252.111
- Publisher Primary CTI Manager = 172.29.252.111
- Publisher Backup CTI Manager = 172.29.252.112
- Subscriber Cisco Unified Communications Manager = 17.29.252.111
- Subscriber Primary CTI Manager = 172.29.252.111
- Subscriber Backup CTI Manager = 172.29.252.112

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

Scenario 4
This scenario uses the following node IP addresses:
- Publisher Cisco Unified Communications Manager = 17.29.252.111
- Publisher Primary CTI Manager = 172.29.252.111
- Publisher Backup CTI Manager = 172.29.252.112
- Subscriber Cisco Unified Communications Manager = 17.29.252.112
- Subscriber Primary CTI Manager = 172.29.252.111
- Subscriber Backup CTI Manager = 172.29.252.112

DRM uses the Cisco Unified Communications Manager pointed to by both Publisher and Subscriber Cisco Unified Attendant Console Advanced servers (both 17.29.252.111 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 = 172.29.252.112
- 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 (17.29.252.111 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.
Chapter 1      Product Overview

Integrating Cisco Unified Attendant Console Advanced with Cisco Unified Communications Manager

AXL API

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

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

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

Note

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

Cisco Unified Communications Manager System Devices

Cisco Unified Attendant Console uses the following system devices:

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

The Cisco Unified Attendant Console Advanced Call Park functionality is additional to the standard Cisco Unified Communications Manager call park and directed call park functions. Operators can see what Park devices are available and choose whether to use a specific device or allow the system to select a park device for them. As these park devices are exclusive to Console attendants they are situated on the Cisco Unified Attendant Console Advanced server and require an additional range of DNs.

- Cisco Unified Attendant Console Advanced Server supports:
  - 1000 CTI Ports per server (collective total of CT gateway devices, service queues and park devices.
  - 100 CTI Route Points (Queue DDIs)

For information on configuring CTI Ports, see System Configuration Menu.
Centralized Installations and Transcoding

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

- On the Cisco Unified Attendant Console Advanced server, change the registry key HKEY_USERS/S-1-5-20/Software/Cisco Systems, Inc./RTPLib/G729PassThrough to 1 in either Hex or Dec, and then reboot the server.

- Ensure that the Device Pool and the region in which the CTI Port(s) are assigned is not restricted to G729. If it is, calls will not be processed correctly, and will be unable to be redirected to the CTI Port.

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

Note

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

TAPI Resilience

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

Music on Hold

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

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

Presence Service Integration

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

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

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

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

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

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

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.

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

3. Ensure that you have the correct versions of operating system and SQL database required by the Cisco Unified Attendant Console Advanced server and client. For more information, see:
   - VMware Guest Machine Requirements
   - Server Software Requirements
   - PC Software Requirements

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 8, “Configuring Cisco Unified Attendant Console”.

7. Install the Cisco Unified Attendant Console Advanced client. For more Information, see Installing Cisco Unified Attendant Console Advanced Client.
Hardware and Software Requirements

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

Server Requirements

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

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

Physical Server Hardware Requirements

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

- 2.2 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.
VMware Guest Machine Requirements

In a production environment, Cisco Unified Attendant Console Advanced server is supported on VMware ESXi (Vmotion included) running on a host machine that is compliant with Cisco’s UC Virtualization Supported Hardware (described at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-attendant-consoles.html).

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**

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.
- You can download an OVA template configured with the above specifications from the following location: https://cisco.com/go/ac.

Server Software Requirements

Cisco Unified Attendant Console Advanced server has the following requirements:

- Server host name length must be 15 characters or less
- One of the following activated operating systems, with Windows regional settings set to English:
  - Windows Server 2012 R2 (64-bit)
    - Update KB2919355 needs to be applied prior to installing the Cisco Unified Attendant Console Advanced server.
  - Windows Server 2016 (64-bit)
- Microsoft Visual C++ 2015 Redistributables 32-bit*
- Microsoft Visual C++ 2015 Redistributables 64-bit*
- Internet Information Service (IIS) 8.0 or later, with the Static Content role service added.
  - To install IIS on a system with Windows Server already installed, see Adding Internet Information Service (IIS).
- ASP.NET 2.0.50727 or later*
Chapter 3     Hardware and Software Requirements

Server Requirements

Note

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

- .NET Framework 4.6.1
- OpenJDK build 1.8.0.191-1 (earlier/later builds are not supported)
- One of the following databases: Microsoft SQL Server 2012, 2014 and 2016 Standard, Enterprise or Express. SQL Server Express is installed by the Cisco Unified Attendant Server installer if an existing installation of SQL Server is not detected.

SQL Server Requirements

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

Note

The following points:

- Cisco Unified Attendant Console Advanced server must be installed and operated exclusively on a supported platform.
- Windows 2012 R2 is supported only 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.

SQL Server Requirements

- Cisco Unified Attendant Console Advanced server does not support multiple SQL database instances or named instances, and requires exclusive use of and access to a local installation of SQL Server.
- If you are installing Microsoft SQL yourself, you must install it locally on the Cisco Unified Attendant Console Advanced server. Cisco Unified Attendant Console Advanced does not support the use of external SQL Servers.
- Due to security restrictions and the resource demands of a domain controller, Microsoft advises against installing SQL server on a domain controller (For more information, see 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.
- If you plan to implement Cisco Unified Attendant Console Advanced server high availability, you must ensure that the date time and time zone on your Publisher and Subscriber servers are synchronized. Both servers must be in the same time zone to ensure that any daylight-saving time changes occur simultaneously. If they are not in the same time zone, the operator console will be unable to automatically reconnect to the Publisher when it recovers from failure.
**SQL Server Express Limitations**

Microsoft SQL Server Express has the following limitations:

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

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

- More than 10 operators
- More than 500 calls per operator per day
- A directory containing more than 10,000 contacts
- Cisco Unified Attendant Console Advanced server high availability - SQL Server Express can be used on the subscriber server in high availability deployments, as long as the other criteria are not exceeded in the deployment.

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.

**Additional Server Considerations**

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

**Microsoft Windows and SQL Server Updates and Service Packs**

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

**Best Practices**

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

**Java Updates**

OpenJDK updates (manual and automatic) are not supported as they may render the system unusable. OpenJDK updates will be delivered with future Cisco Unified Attendant Console Advanced minor and major releases as required.

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

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

Data Backup

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

Instructions for setting up automatic or manual Cisco Unified Attendant Console Advanced server database backups are available in Appendix D, “Back-up and Restoring Cisco Unified Attendant Console Advanced”.

Server Redundancy

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

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

Antivirus Software

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

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

<table>
<thead>
<tr>
<th>Default Folder</th>
<th>Contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>\DBData</td>
<td>System configuration databases</td>
</tr>
<tr>
<td>\Program Files\Cisco\</td>
<td>Software and application trace files</td>
</tr>
<tr>
<td>\Apache</td>
<td>Active MQ folder</td>
</tr>
<tr>
<td>\Temp\Cisco\Trace</td>
<td>Cisco TSP trace files</td>
</tr>
<tr>
<td>%ALLUSERSPROFILE%\Cisco\CUACA</td>
<td>Cisco profile</td>
</tr>
</tbody>
</table>

The System Administrator may have set up your Cisco Unified Attendant Console Advanced server to use different folders for these files.
With any anti-virus product, configuration is a balance of scanning versus the performance of the server. The more you choose to scan, the greater the potential performance overhead. Your system administrator should determine the optimal configuration of your anti-virus application within your particular environment. Refer to your anti-virus product documentation for more detailed configuration information.

General best practices are listed below:

- Update AV software scanning engines and definition files on a regular basis, following your organization's current policies.
- Upgrade to the latest supported version of the third-party anti-virus application. Newer versions improve scanning speed over previous versions, resulting in lower overhead on servers.
- Avoid scanning of any files accessed from remote drives (such as network mappings or UNC connections). Where possible, ensure that each of these remote machines has its own anti-virus software installed, thus keeping all scanning local. With a multi-tiered antivirus strategy, scanning across the network and adding to the network load should not be required.
- Schedule full scans of systems by AV software only during scheduled maintenance windows, and when the AV scan will not interrupt other Unified Console ServerICM maintenance activities.
- Do not set AV software to run in an automatic or background mode for which all incoming data or modified files are scanned in real time.
- Due to the higher scanning overhead of heuristics scanning over traditional anti-virus scanning, use this advanced scanning option only at key points of data entry from untrusted networks (such as email and Internet gateways).
- Real-time or on-access scanning can be enabled, but only on incoming files (when writing to disk). This is the default setting for most anti-virus applications. Implementing on-access scanning on file reads will yield a higher impact on system resources than necessary in a high-performance application environment.
- While on-demand and real-time scanning of all files gives optimum protection, this configuration does have the overhead of scanning those files that cannot support malicious code (for example, ASCII text files). Cisco recommends excluding files or directories of files, in all scanning modes, that are known to present no risk to the system.
- Schedule regular disk scans only during low-usage times and at times when application activity is lowest.
- Disable the email scanner if the server does not use email.
- Additionally, set the AV software to block port 25 to block any outgoing email.
- Block IRC ports. IRC uses TCP protocol to communicate on default port 6667. It can also to connect to other TCP ports if TCP port 6667 is blocked.
- If your AV software has spy-ware detection and removal, then enable this feature. Clean infected files, or delete them (if these files cannot be cleaned).
- Enable logging in your AV application. Limit the log size to 2 MB.
- Set your AV software to scan compressed files.
- Set your AV software to not use more than 20% CPU utilization at any time.
- When a virus is found, the first action is to clean the file, the second to delete or quarantine the file.
- If it is available in your AV software, enable buffer overflow protection.
- Set your AV software to start on system startup.
TLS 1.2 Supportability

Cisco Unified Attendant Console Advanced extends TLS 1.2 compliance.

TLS 1.2 compliance:

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

Note: For TLS 1.2 supportability for the SQL Server (32-bit and 64-bit installations), please refer to Microsoft SQL Server documentation.

Network Requirements

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

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

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

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

- XenApp 7.15 (Fundamentals, Advanced, Enterprise, Platinum)
- XenDesktop 7.15 (VDI, Enterprise, Platinum)

Citrix environments support the following modes:

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

The following platforms are not supported:

- Cisco VXI Solution
- VMWare Horizon

Note

Update KB4034661 needs to be applied prior to launching seamless applications from a Server VDA running Windows Server 2016. For more information, see https://support.citrix.com/article/CTX225819.

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
Citrix Support

Cisco Unified Attendant Console Advanced Operator Client 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

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 7 with SP1
- Microsoft Windows 8.1 update 1, v. 6.3.9600 or later
  - Earlier builds will need the update KB2919355 applied prior to installing Cisco Unified Attendant Console Advanced client
- Microsoft Windows 10 (Desktop Mode)

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

- Microsoft Visual C++ 2015 Redistributable

Operator Phone Requirements

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

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

**Cisco Unified Communications Manager (Required):**
- Creating an Access Control Group
- Assigning Roles to an Access Control Group
- Creating and Assigning an Application User

**Cisco Unified Presence (Optional)**
- Creating an End User for the Presence Server

**Cisco Unified Communications Manager (Required)**

**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.
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 Calling Number Modification
- Standard CTI Allow Control of All Devices
- Standard CTI Allow Control of Phones supporting Connected Xfer and conf*
- Standard CTI Allow Control of Phones supporting Rollover Mode*
- Standard CTI Allow Reception of SRTP Key Material
- Standard CTI Enabled
- Standard SERVICEABILITY

Step 5 Click Add Selected to assign the roles.

Step 6 Click Save.

Creating and Assigning an Application User

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

Note

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

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

To create and assign an Application User:

Step 1 Log into Cisco Unified Communications Manager Administration.

Step 2 Choose User Management > Application User.

Step 3 Click Add New.
Step 4 Enter information in the following fields:
- **User ID** (a name of your choice)
- **Password**
- **Confirm Password** (this must match the Password)

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

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

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

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

---

Cisco Unified Presence (Optional)

Creating an End User for the Presence Server

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

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

To create an End User:

---

Step 1 Log into Cisco Unified Communications Manager Administration.

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

Step 3 Click **Add New**.

Step 4 Enter information in the following fields:
- **User ID** (a name of your choice)
- **Password**
- **Confirm Password** (this must match the Password)
- **Last name**
- **First Name** (optional)
- **Directory URI** (depends on the configuration)
- **Mail ID**

Step 5 Define the Service Settings:
- Select **Home Cluster** checkbox
- Select **Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)** checkbox
Step 6  Click **Save** to save the End User.

---

**Presence states chart**

**Note**  In case of multiple device scenarios, the statuses on Cisco Unified Attendant Console could be different to what is explained in the tables.

**Table 4-1  IM&P Presence States chart**

<table>
<thead>
<tr>
<th>Current State Event</th>
<th>Available</th>
<th>Away (idle)</th>
<th>On the phone</th>
<th>In a meeting</th>
<th>Available (Manual)</th>
<th>Away (Manual)</th>
<th>Do not disturb</th>
<th>Offline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>On the phone</td>
<td>In a meeting</td>
<td>Available (Manual)</td>
<td>Away (Manual)</td>
<td>Do not disturb</td>
<td>Available</td>
</tr>
<tr>
<td>Device Idle</td>
<td>Away (idle)</td>
<td>Away (idle)</td>
<td>On the phone</td>
<td>In a meeting</td>
<td>Away (idle)</td>
<td>Away (Manual)</td>
<td>Do not disturb</td>
<td>Offline</td>
</tr>
<tr>
<td>Make Call</td>
<td>On the phone</td>
<td>On the phone</td>
<td>On the phone</td>
<td>In a meeting</td>
<td>On the phone</td>
<td>Away (Manual)</td>
<td>Do not disturb</td>
<td>Offline, On the phone</td>
</tr>
<tr>
<td>Join Meeting</td>
<td>In a meeting</td>
<td>In a meeting</td>
<td>In a meeting</td>
<td>In a meeting</td>
<td>In a meeting</td>
<td>Away (Manual)</td>
<td>Do not disturb</td>
<td>Offline, In a meeting</td>
</tr>
<tr>
<td>Set Manual DND</td>
<td>Do not disturb</td>
<td>Do not disturb</td>
<td>Do not disturb</td>
<td>Do not disturb</td>
<td>Do not disturb</td>
<td>Do not disturb</td>
<td>Do not disturb</td>
<td>Do not disturb</td>
</tr>
<tr>
<td>Offline</td>
<td>Offline</td>
<td>Offline</td>
<td>Offline, On the phone</td>
<td>Offline, In a meeting</td>
<td>Offline</td>
<td>Offline</td>
<td>Offline</td>
<td>Offline</td>
</tr>
</tbody>
</table>
### Table 4-2  WebEx Presence States chart

<table>
<thead>
<tr>
<th>Current State → Event ↓</th>
<th>Available</th>
<th>Away (idle)</th>
<th>In WebEx Meeting</th>
<th>In a meeting (local outlook)</th>
<th>Available (Manual)</th>
<th>Away (Manual)</th>
<th>Do not disturb</th>
<th>Presenting</th>
<th>Offline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>In WebEx Meeting</td>
<td>In a meeting</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Available</td>
<td></td>
</tr>
<tr>
<td>Device idle</td>
<td>Away (idle)</td>
<td>Away (idle)</td>
<td>In WebEx Meeting</td>
<td>In a meeting (local outlook)</td>
<td>Away (Manual)</td>
<td>Away (Manual)</td>
<td>Do not disturb</td>
<td>Presenting</td>
<td>Offline</td>
</tr>
<tr>
<td>Join Meeting</td>
<td>In a meeting</td>
<td>In a meeting</td>
<td>In WebEx Meeting</td>
<td>In a meeting</td>
<td>Do not disturb</td>
<td>Presenting</td>
<td>Offline</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Offline</td>
<td>Offline</td>
<td>Offline</td>
<td>Offline, in a meeting</td>
<td>Offline</td>
<td>Offline</td>
<td>Offline</td>
<td>Offline</td>
<td>Offline</td>
<td></td>
</tr>
</tbody>
</table>
Installing Cisco Unified Attendant Console Advanced Software

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

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

**Step 2**  Add IIS to Server 2016, as described in Adding Internet Information Service (IIS).

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

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

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

---

**Note**

- If you have a Microsoft Windows network that uses DHCP, you must allocate a static IP address to the Cisco Unified Attendant Console Advanced server machine.
- Under Windows Server 2016 64-bit, the software must be installed in the following order:
  - **a.** Microsoft .NET framework 4.6
  - **b.** SQL Server 2016 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.
Adding Internet Information Service (IIS)

To add IIS to Windows Server 2016, do the following:

Step 1 Run Server Manager.

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

The Add Roles and Features Wizard appears.

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

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

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

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

The Add Roles and Features Wizard dialog box appears.

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

Step 8 In the Server Roles page, click Next.

Step 9 In the Features page, if they are not already installed, under .NET Framework 4.6 Features, select:

- .NET Framework 4.6
- ASP.NET 4.6

and then click Next.

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

Step 11 In the Role Services page, select:

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

and then click Next.

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

Step 13 When installation is complete, click Close.
Installing and/or configuring SQL

Before you install Cisco Unified Attendant Console Advanced server, you must manually install Microsoft SQL Server 2016 onto the Publisher machine and - if you are installing a resilient system - the Subscriber server (for more information, see Server High Availability).

Note

The instructions in this section refer to Installing SQL Server 2016 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 2016

To install SQL Server 2016:

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 and then click Next.

Step 10 In the Feature Rules page, if the rules pass, the Instance Configuration page appears.
Chapter 5 Installing Cisco Unified Attendant Console Advanced Software

Installing and/or configuring SQL

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:

- Creating a Cisco Unified Attendant Console Advanced Downloads and Licensing Website User Account
- Downloading the Software

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

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

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

Step 1 Use your internet browser to go to http://www.cisco.com/go/ac.
Step 2 Under New Users, click Register your details.
   The Register page is displayed.
Step 3 Complete the form and click Register.
Step 4 Either confirm your Reseller, or—if you are not listed—Add New Reseller.
Step 5 Click Submit to register your account.
   A confirmation screen is displayed and you are sent an e-mail containing your password to the website.

Downloading the Software

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

Step 1 Use your internet browser to go to http://www.cisco.com/go/ac.
Step 2 Enter your User Name and Password and then click Log In.
Step 3 In the navigation bar, click DOWNLOADS.
   Information about downloading, evaluating and activating software, and a list of software available for downloading is displayed.
Step 4 In the list, select the required software.
   The versions of the selected software are displayed.
Step 5 Click Download for the software you want.
Step 6 When prompted for what to do with the file, click either Open or Save. Saving the file to a local area is recommended.
High Availability (Resilient Installations)

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

To install a resilient system, do the following:

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.
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.
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.
The following points:

- Database replication is uninstalled automatically during Cisco Unified Attendant Console Advanced server installation or uninstallation. If the replication uninstall does not succeed at the first attempt, you are prompted to retry it or abort it.

- When installing or uninstalling resilient server software, both the Publisher and Subscriber server machines must be running. If either machine is turned off or inaccessible, the install or uninstall may fail.

- If the Publisher server software gets uninstalled, the Subscriber server’s software link with the Publisher server gets broken. When you reinstall the Publisher server software you must then reinstall the Subscriber server software to restore the link.

Export Crypto Key File

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

To export the cryptographic key file to your computer:

**Step 1** Log into Cisco Unified Attendant Administration.

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

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

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

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

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

Cisco Unified Attendant Console Advanced Server Installation Procedure

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

To install a Cisco Unified Attendant Console Advanced server:

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

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

**Step 3** Double-click the setup program.
Note
If they are not already installed, all required third-party applications are now automatically installed, including the Microsoft .NET Framework 4.6. If, however, the server does not have an active Internet connection, the Microsoft .NET Framework cannot be installed, and you must install it using the Microsoft Windows Deployment Image Servicing and Management (DISM) tool before continuing with the Cisco Unified Attendant Console Advanced installation. These installations may take several minutes. You are prompted to restart your computer afterwards.

Step 4
If a page listing required software appears, click Install.
The software is installed; this may take several minutes. If you are then prompted to restart your computer, click Yes.

Step 5
When your computer restarts there may be more items to install. Repeat steps 4 and 5 until all the required software is installed.
The Wizard is prepared and you are presented with the Welcome page.

Step 6
In the Wizard welcome page, click Next.

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

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

Note
• If using an account other than the sa account, it must have the sysadmin role associated to it.
• The SQL Server login password must be sufficiently complex to meet the Windows policy requirements described at http://support.microsoft.com/kb/965823.

Step 9
In the Resilient Server Mode page, click either:
• Publisher Server, to install the Publisher server, then continue from Step 12. This is the default selection. If you are installing a non-resilient system, this is the only server you need to install.
• Subscriber Server, to install the Subscriber server in a resilient installation.

Note
If you select Publisher Server, the following checks and actions are performed:
• If there is no SQL Server on the Publisher server, SQL Server Standard is installed, and a message is displayed telling you that you need to upgrade your SQL Server if you intend to have a resilient installation.
• If SQL Server Express is already installed on the Publisher server, a message is displayed telling you that you need to upgrade your SQL Server if you intend to have a resilient installation. You can either abort installation at this point, to upgrade SQL Server before installing Cisco Unified Attendant Console Advanced, or you can continue with the Cisco Unified Attendant Console Advanced installation, and then upgrade SQL Server later.
If you select Subscriber Server, and if SQL Server Express is installed on the Publisher server, the Subscriber server installation is blocked and you are prompted to upgrade the SQL Server installation on the Publisher server.
Step 10  
This step applies only when you are installing onto the Subscriber server.  
In the Server Resilience Trial page, note the information about purchasing a server resilience license, and then click Next.

Step 11  
This step applies only when you are installing onto the Subscriber server.  
In the Publisher SQL Server Information page, enter the following information about the SQL Server installed on the Publisher machine that you want to communicate with the Subscriber server you are installing:
  
  • Server Name — the machine hosting the Publisher  
  • Username — the SQL Server user name (default is sa)  
  • Password — the SQL Server password  
  
and then click Next.

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

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

Step 13  
To install a Publisher server, continue from Step 14.  
To install a Subscriber server:
  
a. When prompted to allow the Wizard to stop the services on the Publisher, click Yes.  
b. When prompted for the credentials of the Publisher server to communicate with, enter the Windows Username (computer name \ user name) and Password of your Publisher administrator login, and then click Next.

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

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

Step 15  
In both security alert messages, click Yes.

Step 16  
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 - if it is not already installed.

Step 17  
This step applies only when you are installing onto the Subscriber server.
Use the crypto key file exported from the Publisher as described in Export Crypto Key File to import it onto the Subscriber. Enter the Passphrase if necessary, Browse for the crypto key file, select it from your computer, and then click Next.

**Step 18** In the Call Logging page, select either:
- Enable Call Logging (the default)
- Disable Call Logging

and then click Next.

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

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

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

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

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

If you are upgrading the software, your system already contains a configuration database and a logging database, and you are prompted to overwrite each in turn:
- Click Yes to create a new, empty database. This will delete all of your server settings, including queues and CTI port numbers.
- Click No to upgrade the existing database, retaining all of your server settings.

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

Cisco Unified Communications Manager TSP is configured.

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

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

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

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

---

**Disabling Plug-ins that are not in use**

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

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

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

How to disable plug-ins:
1. Click Start, type services.msc, and then press Enter.
2. Right-click the related service, and then select Properties.
3. From the Startup type drop-down menu select Manual, and then click Apply.
4. Click Stop, then click OK.

Installing Cisco Unified Attendant Console Advanced Client

IMPORTANT:
• If you are upgrading your software, any configured user preferences are maintained.
• If you upgrade from any older version to Cisco Unified Attendant Console Advanced 12, you will have to enter all existing administrator account and operator profile passphrases in CAPS.

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

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

To install Cisco Unified Attendant Console Advanced client:

Step 1 Login as a user with administration rights.
Step 2 Browse to the folder containing the installation files downloaded in Obtaining Cisco Unified Attendant Console Advanced Software.
Step 3 Double-click the setup program.
The Wizard is prepared and you are then presented with the Welcome page.
Installing Cisco Unified Attendant Console Advanced Client

Step 4  In the Welcome page, click Next.
Step 5  In the Choose Destination Location page, accept the default destination:
        C:\Program Files (x86)\Cisco\ 
        To install the application to a different location, click Browse and select a different location.
        Click Next to proceed.
Step 6  In the Server Information page, enter the host name of the machine running the Cisco Unified
        Attendant Console Advanced server (the Publisher server), and then click Next. If your previous
        installation used the IP address of the server, you are prompted to enter the corresponding host name.
        This information is required so that Cisco Unified Attendant Console Advanced client can talk to the
        server properly.
Step 7  In the Language Information page, select the language to use for the application, and then click Next.
Step 8  In the Icon Information page, if you want to be able to start the Console from the desktop, select Add
        Icon to Desktop to place the Cisco Unified Attendant Console Advanced icon on your desktop, and then
        click Next.
        The Start Copying Files page lets you review the information you have entered.
Step 9  If you are happy with the settings, click Next to copy the files and install the software.
Step 10 In the installation completed page, click Finish.

Installing JAWS Scripts for Visually Impaired Operation

The Cisco Unified Attendant Console Advanced client can be used with JAWS screen reading software
versions 17 and 18.
For JAWS to work correctly, do the following after installing the Cisco Unified Attendant Console
Advanced client:

Step 1  Copy the files from the following folders:
        C:\Program Files (x86)\Cisco\Attendant Console\Accessibility Scripts\<language>
        where the <language> folder is either English or Spanish.

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

Step 2  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\17.0\Settings\enu
Cisco Unified Attendant Console Administration

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

Administrator Login

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

Note

If you upgrade from any older version to Cisco Unified Attendant Console Advanced 12, you will have to enter all existing administrator account and operator profile passphrases in CAPS.

Logging On

Note

If you have upgraded from a prior release of Cisco Unified Attendant Console, you will have to enter all existing administrator account and operator profile passphrases in CAPS.

To log on to Cisco Unified Attendant Console Advanced Administration:

Step 1

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


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

Note

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

---

**Note**

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

---

**Step 2**

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

**Step 3**

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

---

**Note**

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

---

**Step 4**

Click **Login**.

The home page is displayed.

---

**Note**

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

---

**Customized Logon Message**

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

---

**Step 1**

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

**Step 2**

Click **Add New**.

**Step 3**

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

---

**Note**

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

---

**Step 4**

Enter the **Before login message**.

**Step 5**

Enter the **After login message**.

---

**Note**

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

---

**Step 6**

Click **Save**.

To edit a customized message:

---

**Step 1**

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

**Step 2**

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

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

To delete a customized message:

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

Step 2    Click **Find**.

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

Step 4    Click **Delete Selected**.

### Last Login Information

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

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

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

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

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

**Note**

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

### Logging Out

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

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

The Cisco Unified Attendant Console Advanced Administration home page contains the main menus for configuring the application, and 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 Chapter 7, “Cisco Unified Attendant Console High Availability”.
- Cisco Unified Reporting—For more information, see Appendix B, “Cisco Unified Reporting”.

Note

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

Menu Options

The Cisco Unified Attendant Console Advanced Administration menus are:

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

Toolbar

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="+" alt="Add" /></td>
<td>Add or install an item</td>
</tr>
<tr>
<td><img src="%E2%88%92" alt="Remove" /></td>
<td>Remove or uninstall an item</td>
</tr>
<tr>
<td><img src="%E2%97%98" alt="Save" /></td>
<td>Save</td>
</tr>
<tr>
<td><img src="%E2%97%98" alt="Reset Passphrase" /></td>
<td>Reset Passphrase</td>
</tr>
<tr>
<td><img src="%E2%97%98" alt="Test Connection or Validate Replication" /></td>
<td>Test Connection or Validate Replication</td>
</tr>
<tr>
<td><img src="%E2%97%98" alt="Monitor Replication" /></td>
<td>Monitor Replication</td>
</tr>
<tr>
<td>Icon</td>
<td>Function</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="Repair Database" /></td>
<td>Repair Database or Repair and Purge Database</td>
</tr>
<tr>
<td><img src="image" alt="Directory Field Mappings" /></td>
<td>Directory Field Mappings</td>
</tr>
<tr>
<td><img src="image" alt="Directory Rules" /></td>
<td>Directory Rules</td>
</tr>
<tr>
<td><img src="image" alt="Database Repair Report or Replication Report" /></td>
<td>Database Repair Report or Replication Report</td>
</tr>
<tr>
<td><img src="image" alt="Select All (on page) or Select All In Search (including any other pages of results)" /></td>
<td>Select All (on page) or Select All In Search (including any other pages of results)</td>
</tr>
<tr>
<td><img src="image" alt="Clear All (on page) or Clear All In Search (including any other pages of results)" /></td>
<td>Clear All (on page) or Clear All In Search (including any other pages of results)</td>
</tr>
<tr>
<td><img src="image" alt="Delete Selected (Queue/operator Management)" /></td>
<td>Delete Selected (Queue/operator Management)</td>
</tr>
<tr>
<td><img src="image" alt="Calendar" /></td>
<td>Calendar (select a date).</td>
</tr>
<tr>
<td><img src="image" alt="Start Server" /></td>
<td>Start Server</td>
</tr>
<tr>
<td><img src="image" alt="Stop Server" /></td>
<td>Stop Server</td>
</tr>
<tr>
<td><img src="image" alt="View information for a service." /></td>
<td>View information for a service.</td>
</tr>
<tr>
<td><img src="image" alt="Refresh service display" /></td>
<td>Refresh service display</td>
</tr>
<tr>
<td><img src="image" alt="Synchronize directory with Cisco Unified Communications Manager or Re-initialize Replication." /></td>
<td>Synchronize directory with Cisco Unified Communications Manager or Re-initialize Replication.</td>
</tr>
<tr>
<td><img src="image" alt="Set out of hours routing for a queue." /></td>
<td>Set out of hours routing for a queue.</td>
</tr>
</tbody>
</table>

### 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 8, “Configuring Cisco Unified Attendant Console”
- 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.

For more information on the Cisco Accessibility Program visit http://www.cisco.com/web/about/responsibility/accessibility/contact.html

Service Management

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

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

Note

If you are not using LDAP or Presence, you can harden the Cisco Unified Attendant Console Advanced system by disabling the plug-ins using the Service Control Manager (SCM). However, you should set these services to start automatically in case you decide to use them later. If the services are disabled and you try to start them from Web Admin, you will see an error.

To manage a service:

Step 1 Choose Engineering > Service Management.
**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>
<thead>
<tr>
<th>Control</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Server</td>
<td><img src="image" alt="Start" /></td>
<td>Start the server.</td>
</tr>
<tr>
<td>Stop Server</td>
<td><img src="image" alt="Stop" /></td>
<td>Stop the server.</td>
</tr>
<tr>
<td>Information</td>
<td><img src="image" alt="Info" /></td>
<td>View the server activity and status.</td>
</tr>
<tr>
<td>Refresh</td>
<td><img src="image" alt="Refresh" /></td>
<td>Update the page.</td>
</tr>
</tbody>
</table>

**Information Displayed**

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

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>The server and databases are connected.</td>
</tr>
</tbody>
</table>
The data displayed depends on which server you choose.

### Cisco Unified Attendant Server Status

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

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

### Cisco Unified Attendant LDAP Plug-in Status

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

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

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

### Cisco Unified Attendant Presence Plug-in Status

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

- The Server Activity, consisting of active presence Subscriptions and Connected Users (Console clients and Web Admin itself).
- The status of the Unified CM server and the WebEx server.
- Comms — the Presence server port status
Database — the configuration database connectivity status

If your Cisco Unified Attendant Console Advanced is running in resilient mode, the Inter Server Communication Status is also shown (the status of the link between the Publisher and Subscriber servers).

Cisco Unified Attendant BLF Plug-in Status

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

- The Server Activity of Subscriptions and Connected Users
- The status of the following servers is displayed:
  - CT Link
  - DRM
  - Comms
  - Database — the configuration database connectivity status

If your Cisco Unified Attendant Console Advanced is running in resilient mode, the Inter Server Communication Status is also shown (the status of the link between the Publisher and Subscriber servers).

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:
Chapter 6  Cisco Unified Attendant Console Administration

CUCM Connectivity

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

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

  Follow the instructions in the message.

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

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

  Follow the instructions in the message.

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

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

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

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

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

**Note**

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

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

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

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

- If the media driver setting of the selected server is correct and Attendant Server is not running, the following message appears:
Update Complete. Please restart Attendant Console services of selected Cisco UAC Advanced server for this change to take effect.

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

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

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

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

---

**Server Management**

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

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

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

To change server details:

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

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

**Step 3** Enter the following values:

- **Reconnection Delay (msecs)**—reconnection delay in milliseconds. Default Value 90000. You must enter a value.

- **Buffer Duration (secs)**—buffer duration in seconds. Default Value 259200. You must enter a value.

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

---

**Hostname change**

If the hostname of the Cisco Unified Attendant Console Advanced Server machine is changed, you will need to perform the following steps to manage HTTPS:

**Step 1** Create a Self-Signed Certificate.

**Step 2** Associate the new Self-Signed Certificate.
Create a Self-Signed Certificate

To create a Self-Signed Certificate, do the following:

Step 1: On your computer, open the **Server Manager** and go to **Tools > Internet Information Services (IIS) Manager**. Internet Information Services (IIS) Manager window opens.

Step 2: Under **Connections**, click your server.

Step 3: Under **IIS**, double-click **Server Certificates**.

Step 4: In **Actions**, click **Create Self-Signed Certificate**.

Step 5: Under **Specify a friendly name for the certificate**, type the name you want to use for your domain.

Step 6: Under **Select a certificate store for the new certificate**, select **Personal**.

Step 7: Click **OK** and the new certificate will appear in the list of **Server Certificates**.

Associate the new Self-Signed Certificate

To associate the new Self-Signed Certificate, do the following:

Step 1: On your computer, open the **Server Manager** and go to **Tools > Internet Information Services (IIS) Manager**. Internet Information Services (IIS) Manager window opens.

Step 2: Under **Connections**, click the arrow next to your server, and then under **Sites** click **Default Web Site**.

Step 3: In **Actions**, under Edit Site, click **Bindings**. The **Site Bindings** window opens.

Step 4: If an https binding **does not already exist**, do the following:

a. Click **Add**. The **Add Site Binding** window opens.

b. Set your binding settings:
   - Type: https
   - IP address: All Unassigned
   - Port: 443
   - Host name: the FQDN of the machine or localhost

OR

If an https binding **already exists**, do the following:

a. In **Site Bindings**, click the HTTPS (port 443) binding, and the click **Edit**. The Edit Site Binding window appears.

b. Under **SSL certificate**, from the drop-down menu select the Self-Signed Certificate you created previously (as described in **Create a Self-Signed Certificate**).

c. Click **Select**. The **Select Certificate** window appears.

d. Click the certificate you want to use, and click **OK**.

e. In the **Edit Site Binding** window, click **OK** and close all other windows.
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**.

**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 effect. Select the option to restart the server immediately.

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

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

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

- Database Name
- SQL Server
- Activity Start Date
- Activity End Date
- Status
- Error Code
Database Purge

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

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

Note

The following points:

- We recommend that before purging the database you stop all Cisco Unified Attendant Console Services; this will free server resources for the purge process and lessen the impact on the live production environment.
- For best results, purge data in groups of 1-3 months, depending on the amount of data to be purged.

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 the calendar and select it from there.

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

Step 4  Click Purge Database.

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

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

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

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

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

⚠️ Caution  If auto-purge is enabled, do not schedule directory synchronization to execute at midnight, because auto-purge runs at midnight every day. If auto-purge is disabled, directory synchronization can be run at midnight.

Marking Text Management

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

To manage marking text:

**Step 1** Choose Engineering > Marking Text Management.

The Marking Text Management page appears.

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

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

**Step 4** Click Save.

Syslog Connectivity

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

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

**Step 1** Choose Engineering > Syslog Connectivity > Syslog Server Connectivity.

*The information on this page is read only when logged into the Subscriber server.*

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

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

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

The Realm Management option enables you to specify which domains have access to the single sign-on (SSO) Home Realm on a Cisco Unified Attendant Console Advanced server. If no domains are assigned to the Home Realm, all SSO users have access to it. If you specify one or more domains for the realm, only users in those domains have access to the realm and to SSO.

Note
You can configure the Home Realm only when logged into the Publisher server.

To configure a Home Realm or assign domains to it:

Step 1 Choose User Configuration > Realm Management. The Realm Management page appears.
Step 2 If you have a resilient installation, in Server Details, select the Publisher or Subscriber server, as appropriate.
Step 3 Under Realm Management, click Select alongside the Home Realm to manage (Default SSO Home Realm).
Step 4 Under SSO Connectivity, in CUCM name or IP, type the IP address or FQDN of the Cisco Unified Communications Manager providing SSO.
Step 5 If required, change the CUCM port (default, 443) and then click Save.

To test the SSO connection, click Test SSO. The connection is tested and the result displayed.
To view, add, edit or delete the domains assigned to the realm, click Add Domain; the Domain Configuration page appears. This lists the domains currently assigned to the realm, and enables you to add others. You can only add domains that are valid on the selected server.

To add a new domain to the realm:

**Step 1**  
Click Add New.

**Step 2**  
Under General, type a Domain Name, and then click Save.

To edit a domain, under Select Domain, click Select alongside the domain, change the Domain Name, and then click Save.

To delete a domain, under Select Domain, select the appropriate check box, and then click Delete Selected.

## Credential Policy Management

The Credential Policy Management feature enables you to define the lifetimes of the passphrases used by Console Client users when they log in, and the conditions under which the Cisco Unified Attendant Console Advanced server locks out Console Client users to prevent Denial of Service (DOS) attacks on the system.

This policy also applies to Web Administration accounts, however such an account cannot get locked out as it is a system account.

Passphrases identify authorized users. This feature enables you to define, system-wide:

- How long before a user passphrase must be changed - users are prompted to change their passphrases before they are due to expire.
- How long before a new user passphrase can be changed - this prevents frequent changes of legitimate passphrases, as might be attempted by a bogus user.
- How long before an old user passphrase can be reused - to ensure that users enter new passphrases rather than simply re-use old ones.
- How many of the most recent passphrases cannot be re-used - to ensure that users enter new passphrases rather than simply re-use old ones.
- The composition of passphrases: their minimum length and the minimum numbers of the following character types they must contain:
  - Numeric
  - Special

**Note**  
Certain combinations of special and normal characters are not allowed as they resemble malicious code used in attacks on the Web Administration application. If you choose such a combination, for example, “<“ followed by a character, an error message is displayed.

- Lower case letters
- Upper case letters
Note

- The minimum number of any of these character types must not be greater than the minimum passphrase length.
- Minimum upper and lower case letter check will not work for the following languages: Arabic, Chinese (simplified), Chinese (traditional), Hebrew, traditional Cantonese, Japanese, Korean.

- Whether passphrases in the passphrase dictionary can be used. The passphrase dictionary is a database containing a list of common passphrases that might be used by dictionary attack software.

Console Client user lockout (when a user is locked out, the server does not respond to login requests) is configured with the following parameters:

- The number of failed login attempts by a user before the account is locked.
- The period after a failed login attempt during which further failed attempts may lock the account.
- How long an account can remain inactive (no logins) before it is locked out.
- How long before their passphrase expires that the server starts sending change warnings to users.
- The number of expiry warnings that can be dismissed by a user before the account is locked.
- How long after their passphrase expires before a user’s account is locked.

Note

If a user account is locked due to passphrase expiry and the administrator unlocks the user account from the Web Admin application without changing the passphrase, the account will be locked again when the user tries to login. To avoid this, the administrator must change the passphrase after unlocking the account.

To configure the login credential policy, do the following:

Step 1 Choose User Configuration > Credential Policy Management.
Step 2 Type the Passphrase Lifetime and Passphrase Content parameters.
Step 3 Type the Account Lockout parameters.
Step 4 Click Save.

Logging Management

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

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

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

To manage logging:

---

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

The **Logging Management** page appears.

**Step 2**
As required, do the following:

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

---

**Cisco Unified Attendant Console Server Logging**

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

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

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

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

To manage Cisco Unified Attendant Console Advanced server logging:

**Step 1**
Select the process(es) to log.

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

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

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

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

**Step 6**
Click **Save** to save the changes.
Cisco Unified Attendant LDAP Plug-in Logging

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

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

To manage Cisco Unified Attendant LDAP Plug-in logging:

Step 1 Select the Logging Level. One of: Detailed (default), Advanced, Minimum, Full.
Step 2 View the Logging path & file name. This field is read-only.
Step 3 Specify the Number of files that can be created in the logging folder. The default is 10.
Step 4 Specify the Lines per file. The number of lines each log file can contain. The default is 200000.
Step 5 Click Save to save the changes.

Cisco Unified Attendant Presence Plug-in Logging

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

To manage Cisco Unified Attendant Presence Plug-in logging:

Step 1 Select the Logging Level. One of: Detailed (default), Advanced, Minimum, Full.
Step 2 View the Logging path & file name. This field is read-only.
Step 3 Specify the Number of files that can be created in the logging folder. The default is 10.
Step 4 Specify the Lines per file. The number of lines each log file can contain. The default is 10000.
Step 5 Click Save to save the changes.

Cisco Unified Attendant BLF Plug-in Logging

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

To manage Cisco Unified Attendant BLF Plug-in logging:

Step 1 Select the Logging Level. One of: Detailed (default), Advanced, Minimum, Full.
Step 2 View the Logging path & file name. This field is read-only.
Step 3 Specify the Number of files that can be created in the logging folder. The default is 100.
Step 4 Specify the Lines per file. The number of lines each log file can contain. The default is 100000.
Log Collection

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

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

Setting Up Log Collection

To set up log collection:

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

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

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

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

a. Select Password protected.

b. Type the Password required to view the files in the archive.

c. Confirm the passphrase.

Starting Log Collection

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

Canceling Log Collection

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

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

## Checking Log Collection Progress

To check how log collection is proceeding, click Log Collection Report. The Log Collection Report page shows you the status of the current or most recent log collection, and any errors encountered. During archive file creation the percentage complete is displayed and this is updated regularly; you can manually update the report page by clicking Refresh.

![Example Replication Report](Image)

### Figure 6-2 Example Replication Report

<table>
<thead>
<tr>
<th>Replication Report</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Task</strong></td>
</tr>
<tr>
<td>Verify SQL Server Edition</td>
</tr>
<tr>
<td>Verify Replication Feature</td>
</tr>
<tr>
<td>Stop windows service &quot;SQLServerAgent&quot; at &quot;PAK-A3H-7&quot;</td>
</tr>
<tr>
<td>Start windows service &quot;SQLServerAgent&quot; at &quot;PAK-A3H-7&quot;</td>
</tr>
<tr>
<td>Stop windows service &quot;M3TC&quot; at &quot;PAK-A3H-7&quot;</td>
</tr>
<tr>
<td>Start windows service &quot;M3TC&quot; at &quot;PAK-A3H-7&quot;</td>
</tr>
<tr>
<td>Stop windows service &quot;Cisco Unified Attendant Server&quot; at &quot;PAK-A3H-7&quot;</td>
</tr>
<tr>
<td>Stop windows service &quot;Cisco Unified Attendant LDAP Plug-in&quot; at &quot;PAK-A3H-7&quot;</td>
</tr>
<tr>
<td>Stop windows service &quot;Cisco Unified Attendant Server&quot; at &quot;PAK-A3H-7&quot;</td>
</tr>
<tr>
<td>Start windows service &quot;Cisco Unified Attendant LDAP Plug-in&quot; at &quot;PAK-A3H-7&quot;</td>
</tr>
<tr>
<td>Configure Distribution</td>
</tr>
<tr>
<td>Add Publication</td>
</tr>
<tr>
<td>Add article for table &quot;Agent_Details&quot;</td>
</tr>
<tr>
<td>Add article for table &quot;Agent_Options&quot;</td>
</tr>
<tr>
<td>Add article for table &quot;Agent_Skills&quot;</td>
</tr>
</tbody>
</table>

### Step 5
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 6
To return to the Replication Management page, click Go next to Related link: Back to Replication Management.
Cisco Unified Attendant Console High Availability

Cisco Unified Attendant Console Advanced server high availability is provided partly by server replication. For more information on high availability, see Server High Availability.

Cisco Unified Attendant Console Advanced contains two databases:

- Configuration database, ATTCFG, which contains all user configurations and the contacts directory.
- Logging database, ATTLOG, which is responsible for logging.

The Configuration database is synchronized between the Publisher and Subscriber server using SQL Server replication and the synchronization of database objects across multiple database servers. The configuration database can be updated only on the Publisher server. The copy on the Subscriber server is read-only.

The Logging database is synchronized between Publisher and Subscriber using Microsoft DTC. Log information is replicated both ways between the SQL databases on the servers, with the log on each containing a full record of call transactions on both servers. The copy on the Subscriber server allows limited adding, amending and deleting of user/call-related real-time activities when the Publisher logging database is unavailable.
The connections between Publisher and Subscriber required for high availability are summarized in this figure:

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.

- **Do not** install Cisco Unified Replication during SQL Server installation, and do not manually configure it using SQL Server Feature Selection. Set up server high availability through Cisco Unified Replication only. If you do install or configure Cisco Unified Replication within SQL Server, you may experience unexpected results and other problems.
Chapter 7      Cisco Unified Attendant Console High Availability

SQL Server Replication

SQL Server replication involves these types of replication:

- Snapshot replication
- Transactional replication

Snapshot replication makes an exact copy (snapshot) of the Publisher and distributes it to the Subscriber; this includes queue and operator details, and the contact directory. It does not monitor for updates to the data. Snapshot replication is used to provide the initial data set for transactional replication; and it can also be used to completely refresh the data on the subscriber. After the initial snapshot, the Subscriber is kept up to date with the Publisher using transactional replication. Subsequent data transactions (INSERTed, UPDATED, and DELETED data) in the Publisher are captured by the transaction log and then stored in the distribution database, which acts as a data queue. The changes are then propagated and applied to the Subscriber in the order in which they occurred.

SQL Server replication uses standalone programs called agents to track changes and distribute data between databases. The agents are:

- SQL Server Agent—executes scheduled administrative tasks or jobs consisting of one or more job steps. Job information is stored in the SQL Server. The other agents run as directed by this agent; and it is required for the Publisher and Subscriber to be able to talk to each other.
- Distributor Agent—moves the snapshot and transactions from Publisher to Subscriber.
- Q Reader—a SQL Server agent that handles the data queues.
- Snapshot Agent—prepares snapshot files containing schema and data of published tables and database objects, stores the files in the snapshot folder, and records synchronization jobs in the distribution database.
- Log Agent—monitors the transaction log of each database configured for transactional replication, and copies the transactions marked for replication from the transaction log into the distribution database.

You can check how the agents are running using the Monitor Replication function, described in Monitoring Replication.

Accessing High Availability Administration Menus

Pre-requisites for Installing and Uninstalling Replication

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

- Full replication functionality is available only if a current high availability license and SQL Server Standard or Enterprise edition are installed on the Publisher server.
- If the license has expired, or if there is no high availability license installed, you can only uninstall any existing replication.

Note

The following points:

- When you have installed a Publisher or Subscriber server you cannot convert it into the other type.
The date, time and time zone on the Publisher and Subscriber machines must be the same, otherwise Console users will not be notified that the Publisher has become available after recovering from a failure, and will be unable to switch from the Subscriber back to the Publisher. One way to achieve this is to synchronize the time of both servers with the same time server.

To access the Replication Management menus do the following:

**Step 1** On the Publisher server, in Cisco Unified Attendant Console Advanced Administration, use the Navigation control at the right-hand end of the banner to select Cisco Unified Replication and click Go. The Cisco Unified Replication home page is displayed.

**Step 2** Click Replication Management. The Replication Management page is displayed. This lists the databases on the selected server:
- ATTCFG—the configuration database
- ATTLOG—the logging database

The Publication Name is a unique name used by SQL Server during replication. It has the format <Server_Name>_ <Database_Name>. A database with a Publication name (a publication) has replication configured.

**Step 3** Under Server Details, select the server to check or configure.

**Step 4** Under Replication Management, click Select alongside the database to check or configure. The Information for that database is displayed, below which are the following control buttons:
- Install Replication. For more information, see Installing Replication.
- Uninstall Replication. For more information, see Uninstalling Replication.
- Reinitialize Replication. For more information, see Re-initializing Replication.
- Monitor Replication. For more information, see Monitoring Replication.
- Validate Replication. For more information, see Validating Replication.
- Replication Report. For more information, see Replication Report.

## Installing Replication

**Note**

The following point:

- The information in this section refers to using SQL Server 2016 Standard Edition. If you are using a different version or edition the information may be slightly different. The equivalent information is described in your SQL Server user documentation.

- The CT and LDAP servers on the Publisher and the CT server on the Subscriber are stopped when you install, uninstall or re-initialize replication.

- **IMPORTANT**: Installing replication shuts down both servers. Consequently, after installing replication you must either restart your computer or restart the services as described in Service Management.
Before installing or un installing replication, you must ensure that the SQL Server network uses the correct protocols and settings:

- On both the Publisher and Subscriber, the SQL Server Service (MSSQLSERVER) must be running under the Network Service account.
- On the Publisher, the SQL Agent Service must be running under the Local System account.
- On both Publisher and Subscriber, MSSQLSERVER and the Clients must have TCP/IP, Shared Memory, and Named Pipes protocols enabled.

How to do these is explained below.

**Ensuring that MSSQLSERVER is running under the Network Service account**

On both the Publisher and Subscriber, do the following:

**Step 1** Click the **Start** button, and then, in the **Start** menu, choose **Administrative Tools > Component Services**.

The **Component Services** window appears.

**Step 2** In the navigation pane, select **Services (Local)**.

**Step 3** In the list of services, right-click **SQL Server (MSSQLSERVER)**, and then select **Properties**.

The **SQL Server (MSSQLSERVER) Properties** dialog box appears.

**Step 4** Click the **Log On** tab.

**Step 5** Select **This account**, and then click **Browse**.

**Step 6** In **Enter the object name to select**, type **Network Service**, and then click **OK**.

**Step 7** In the **SQL Server (MSSQLSERVER) Properties** dialog box, click **OK**.

**Ensuring that the SQL Agent Service is running under the Local System account**

On the Publisher, do the following:

**Step 1** Click the **Start** button, and then, in the **Start** menu, choose **Administrative Tools > Component Services**.

The **Component Services** window appears.

**Step 2** In the navigation pane, select **Services (Local)**.

**Step 3** In the list of services, right-click **SQL Server Agent (MSSQLSERVER)**, and then select **Properties**.

The **SQL Server Agent (MSSQLSERVER) Properties** dialog box appears.

**Step 4** Click the **Log On** tab.

**Step 5** Select **Local System account**, and then click **OK**.

**Ensuring that MSSQLSERVER has TCP/IP, Shared Memory, and Named Pipes protocols enabled**

On both the Publisher and Subscriber, do the following:

**Step 1** Click the **Start** button, and then, in the **Start** menu, choose **All Programs > Microsoft SQL Server <version> > Configuration Tools > SQL Server Configuration Manager**.
**Step 2** In the navigation pane, expand **SQL Server Network Configuration**, and then select **Protocols for MSSQLSERVER**.

**Step 3** In the list of protocols, do the following:

- Double-click **TCP/IP** to display its properties; then, under the **Protocol** tab, set **Enabled** to **Yes**, and then click **OK**.
- Double-click **Shared Memory** to display its properties; then, under the **Protocol** tab, set **Enabled** to **Yes**, and then click **OK**.
- Double-click **Named Pipes** to display its properties; then, under the **Protocol** tab, set **Enabled** to **Yes**, and then click **OK**.

Before installing or uninstalling replication you must also:

- Close SQL Management studio and all SQL connections. If you do not, the installation or uninstallation may fail.
- If you have a firewall on the Publisher or Subscriber server, on the affected servers configure Firewall Exceptions for:
  - Windows Management Instrumentation (WMI)
  - Distributed Transaction Coordinator (MSDTC)
  - Port 1433 (used by the SQL Server)
  - Port 1864 (used by the BLF plug-in)
  - Ports 61616 and 61618, to enable messages to pass between the servers

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

**Installing Replication on a Specific Database**

You must install replication on both the ATTCFG and ATT LOG databases on both the Publisher and the Subscriber. Configure the Publisher databases before configuring the Subscriber databases.

To install replication on a specific database:

**Step 1** On the Publisher server, select the database as described on page 7-4.

**Step 2** Under **Server Credentials (<server_name>)**, type the **Windows username** (domain name\username, fully qualified domain name\username, or server name\username as required by your local and group security policies) and **Password** of a user with local administrator rights to the opposite server.

**Step 3** Click **Install Replication**.

**Step 4** In the message, click **OK** to confirm that you want to install replication on that database.

Replication is installed. You can check the progress of the installation by clicking **Replication Report**. For more information, see **Replication Report**.

When replication has been installed for that server and database, click **Go** next to **Related Link: Back to Replication** and repeat this procedure for each remaining databases.
Uninstalling Replication

Before uninstalling replication, perform the checks and procedures at the start of Installing Replication.

To uninstall replication:

**Step 1** On the Publisher server, in Cisco Unified Attendant Console Administration, use the Navigation control at the right-hand end of the banner to select Cisco Unified Replication, and then click Go.

The Cisco Unified Replication home page is displayed.

**Step 2** Click Replication Management.

The Replication Management page is displayed.

---

Note Replication must be uninstalled from the Subscriber server first; then from the Publisher server.

**Step 3** Under Server Details, select the Subscriber server.

**Step 4** In the ATTCFG row, click Select.

**Step 5** Type the user credentials.

**Step 6** Select Uninstall Replication, and then click OK to confirm that you want to uninstall replication.

Replication is uninstalled for the ATTCFG database.

**Step 7** Click Replication Report or Monitor Replication to check progress of the uninstallation.

For details of using these controls, see Replication Report and Monitoring Replication.

**Step 8** When replication has been uninstalled for ATTCFG, repeat 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.

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 7-4.

**Step 2** Click Reinitialize Replication.

**Step 3** Click OK to confirm that you want to reinitialize replication.
Monitoring Replication

To monitor how replication is proceeding for a server and database selected as described on page 7-4:

**Step 1** In the Replication Management page, select the database as described on page 7-4.

**Step 2** Click Monitor Replication.

The Monitor Replication page is displayed. It contains details of the following:

- The Publisher and Subscriber servers
- The replication latency—the time delay between transaction at the Publisher resulting in a corresponding transaction at the Subscriber
- The throughput—the bandwidth of the replication—the data transfer rate in database rows per second
- The states of the replication agents

**Step 3** To update the display, click Refresh.

**Step 4** To validate that replication is working correctly, click Validate Replication. This summarizes the differences between the Publisher and Subscriber copies of each database.
Validating Replication

You can check whether replication is working and is up to date by creating a validation report, which lists the main database tables, along with their status, a comparison of the number of records in the Publisher and Subscriber, and a summary of any errors.

To validate replication for a selected database on a selected server:

**Step 1** In the Replication Management page, select the database as described on page 7-4.

**Step 2** Click Validate Replication.

The Validation Report is displayed. For example:

*Figure 7-1 Example Validation Report*

<table>
<thead>
<tr>
<th>Publication Name</th>
<th>Article Name</th>
<th>Status</th>
<th>Difference</th>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAK-KSHAHZAD-7_ATTCFG</td>
<td>ValidateCTIPorts</td>
<td>Success</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAK-KSHAHZAD-7_ATTCFG</td>
<td>ValidateOverflow</td>
<td>Success</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAK-KSHAHZAD-7_ATTCFG</td>
<td>ValidateNightService</td>
<td>Success</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAK-KSHAHZAD-7_ATTCFG</td>
<td>ValidateDirEntries</td>
<td>Success</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAK-KSHAHZAD-7_ATTCFG</td>
<td>ValidateResourceGrp</td>
<td>Success</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 7-4.

**Step 2** Click Replication Report.

The Replication Report is displayed.

**Figure 7-2 Example Replication Report**

<table>
<thead>
<tr>
<th>Task</th>
<th>Publication Name</th>
<th>Task Date</th>
<th>Status</th>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Publication</td>
<td>PK-AISHAH-7_ATTIFG</td>
<td>2021-11-17 10:26:04.50</td>
<td>Completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verify SQL Server Edition</td>
<td>PK-AISHAH-7_ATTIFG</td>
<td>2021-11-17 10:26:04.51</td>
<td>Completed</td>
<td></td>
<td>Unified</td>
</tr>
<tr>
<td>Verify Replication Feature</td>
<td>PK-AISHAH-7_ATTIFG</td>
<td>2021-11-17 10:26:04.53</td>
<td>Completed</td>
<td></td>
<td>Installed</td>
</tr>
<tr>
<td>Set startup type for windows service &quot;SQLServerAgent&quot; at &quot;PAK-AISHAH-7&quot;</td>
<td>PK-AISHAH-7_ATTIFG</td>
<td>2021-11-17 10:26:04.55</td>
<td>Completed</td>
<td></td>
<td>Already set to automatic</td>
</tr>
<tr>
<td>Set startup type for windows service &quot;MSDTC&quot; at &quot;PAK-AISHAH-7&quot;</td>
<td>PK-AISHAH-7_ATTIFG</td>
<td>2021-11-17 10:26:08.25</td>
<td>Completed</td>
<td></td>
<td>Already set to automatic</td>
</tr>
<tr>
<td>Start windows service &quot;SQLServerAgent&quot; at &quot;PAK-AISHAH-7&quot;</td>
<td>PK-AISHAH-7_ATTIFG</td>
<td>2021-11-17 10:26:08.40</td>
<td>Completed</td>
<td></td>
<td>Already started</td>
</tr>
<tr>
<td>Start windows service &quot;MSDTC&quot; at &quot;PAK-AISHAH-7&quot;</td>
<td>PK-AISHAH-7_ATTIFG</td>
<td>2021-11-17 10:26:05.65</td>
<td>Completed</td>
<td></td>
<td>Already started</td>
</tr>
<tr>
<td>Stop windows service &quot;Cisco Unified Attendant Server&quot; at &quot;PAK-AISHAH-7&quot;</td>
<td>PK-AISHAH-7_ATTIFG</td>
<td>2021-11-17 10:26:05.94</td>
<td>Completed</td>
<td></td>
<td>Stopped</td>
</tr>
<tr>
<td>Stop windows service &quot;Cisco Unified Attendant LDAP Plugin&quot; at &quot;PAK-AISHAH-7&quot;</td>
<td>PK-AISHAH-7_ATTIFG</td>
<td>2021-11-17 10:26:08.38</td>
<td>Completed</td>
<td></td>
<td>Stopped</td>
</tr>
<tr>
<td>Stop windows service &quot;Cisco Unified Attendant Server&quot; at &quot;PAK-2003MAY-WEB&quot;</td>
<td>PK-AISHAH-7_ATTIFG</td>
<td>2021-11-17 10:26:06.86</td>
<td>Completed</td>
<td></td>
<td>Stopped</td>
</tr>
<tr>
<td>Stop windows service &quot;Cisco Unified Attendant LDAP Plugin&quot; at &quot;PAK-2003MAY-WEB&quot;</td>
<td>PK-AISHAH-7_ATTIFG</td>
<td>2021-11-17 10:26:07.08</td>
<td>Completed</td>
<td></td>
<td>Stopped</td>
</tr>
<tr>
<td>Configure Distribution</td>
<td>PK-AISHAH-7_ATTIFG</td>
<td>2021-11-17 10:26:07.28</td>
<td>Completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add Publication</td>
<td>PK-AISHAH-7_ATTIFG</td>
<td>2021-11-17 10:26:07.37</td>
<td>Completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add article for table &quot;Agent_Details&quot;</td>
<td>PK-AISHAH-7_ATTIFG</td>
<td>2021-11-17 10:26:14.57</td>
<td>Completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add article for table &quot;Agent_Options&quot;</td>
<td>PK-AISHAH-7_ATTIFG</td>
<td>2021-11-17 10:26:17.17</td>
<td>Completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add article for table &quot;Agent_Skills&quot;</td>
<td>PK-AISHAH-7_ATTIFG</td>
<td>2021-11-17 10:26:17.35</td>
<td>Completed</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.
Configuring Cisco Unified Attendant Console

Presence Management

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

Configuration

To configure a presence source:

Step 1
Choose Engineering > Presence Management.
The Presence Management page is displayed, listing all the presence drivers that satisfy the Find filter.

Step 2
If required, Find the presence source to configure.
These drivers are available:
- Unified CM (IM and Presence)
- WebEx (IM and Presence)
- Skype Local
An ID in the Presence User ID column shows that the driver has been configured and is connected to the presence server.
A Yes in the Default Driver column shows which (if any) of the drivers is providing all the clients with their default presence data.

Note
The following:
- IMPORTANT—If you are using Cisco Unified CM (IM&P) the Cisco Unified Attendant Presence Plug-in has to be added to the firewall information on the Communications Manager.
- If you are not using Presence data, you can make your Cisco Unified Attendant Console Advanced system more secure by disabling the associated plug-in using Service Management, as described on page 6-6.

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

Directory Source Management

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

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

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.
- Directory Field Mappings. This is described in Directory Field Mapping.
- Directory Rules. This is described in Directory Rules.
In addition to populating your contacts database (also known as the full directory) from an external source directory, you can also:

- Manually add contacts to your contacts database, as described in Contact Management.
- Import contacts from CSV files and export contacts to CSV files, as described in Inserting, Updating and Exporting Contacts via CSV.

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

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

---

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

---

### Connecting to a Directory Source

To connect to a directory source do the following:

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

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

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

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

**Step 3** Set the following parameters:

- **General**
  - Source Name—The name of the source directory
  - Directory platform—The name of the selected external directory (read only)
  - Enable synchronization—Select to enable synchronization

- **Connection**
  - Host name or IP—The host name or IP address of the source directory server
Contact Directory

- **Host port**—The port number, which depends on the type of source directory you select and whether you use secure sockets layer (SSL):

<table>
<thead>
<tr>
<th>Directory Source</th>
<th>SSL</th>
<th>Host Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Active Directory</td>
<td>Selected</td>
<td>636</td>
</tr>
<tr>
<td>Microsoft Active Directory</td>
<td>Not Selected</td>
<td>389</td>
</tr>
<tr>
<td>iPlanet Netscape Directory</td>
<td>Selected</td>
<td>636</td>
</tr>
<tr>
<td>iPlanet Netscape Directory</td>
<td>Not Selected</td>
<td>389</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>Selected</td>
<td>443</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>Not Selected</td>
<td>443</td>
</tr>
</tbody>
</table>

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

- **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.

- **Notifications**
  - **Monitor Change Notifications**—Check this option if you want any changes in the directory server to be instantaneously reflected in the database. If this option is not selected, the database will be updated at the next synchronization.

**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 Directory Synchronization.
- Access the **Directory Field Mapping** functionality. For more information, see Directory Field Mapping.
- Access the **Directory Rules** functionality. For more information, see Directory Rules.
Directory Synchronization

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

⚠️ **Caution**

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

⚠️ **Caution**

If auto-purge is enabled, do not schedule directory synchronization to execute at midnight, because auto-purge runs at midnight every day. If auto-purge is disabled, directory synchronization can be run at midnight.

To configure directory synchronization do the following:

**Step 1**

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

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

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

**Step 2**

Set the Directory Synchronization parameters.
Chapter 8      Configuring Cisco Unified Attendant Console

Contact Directory

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

### Directory Field Mapping

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

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

To map a field:

---

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

The mappings are listed.

**Step 2**  
Click **Add New**.

The **Field Mapping Information** is displayed.

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

**Step 4**  
Select a **Destination field** in the contacts database.

**Note**  
If you are mapping CUCM fields and select Extension as your Destination field, you will not be able to delete the mapping.

**Step 5**  
If you are mapping:

- Microsoft Active Directory
- iPlanet Netscape Directory
- CUCM and your Destination field is anything other than Extension

Type a Default value, which is written to the Destination field if the Source field is empty.

If you are mapping CUCM fields and your Destination field is Extension, you cannot type a Default value.

**Step 6**  
Click **Save** to add the mapping.
### Mapping Cisco Unified Attendant Console Advanced Fields to an LDAP Directory Source

The following Cisco Unified Attendant Console Advanced fields can be mapped to an LDAP data source:

<table>
<thead>
<tr>
<th>Cisco Unified Attendant Console Advanced Field</th>
<th>Number of Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absent Message</td>
<td>4000</td>
</tr>
<tr>
<td>Alternate Department</td>
<td>100</td>
</tr>
<tr>
<td>Alternate First Name</td>
<td>40</td>
</tr>
<tr>
<td>Alternate Last Name</td>
<td>50</td>
</tr>
<tr>
<td>Business 1</td>
<td>40</td>
</tr>
<tr>
<td>Business 2</td>
<td>40</td>
</tr>
<tr>
<td>Company Name</td>
<td>100</td>
</tr>
<tr>
<td>Cost Center</td>
<td>100</td>
</tr>
<tr>
<td>Department</td>
<td>100</td>
</tr>
<tr>
<td>Email</td>
<td>100</td>
</tr>
<tr>
<td>Email 2</td>
<td>100</td>
</tr>
<tr>
<td>Email 3</td>
<td>100</td>
</tr>
<tr>
<td>Extension</td>
<td>40</td>
</tr>
<tr>
<td>Fax</td>
<td>40</td>
</tr>
<tr>
<td>First Name</td>
<td>40</td>
</tr>
<tr>
<td>Full Job Title</td>
<td>255</td>
</tr>
<tr>
<td>Full Name</td>
<td>100</td>
</tr>
<tr>
<td>Home</td>
<td>40</td>
</tr>
<tr>
<td>Home Address Line 1</td>
<td>50</td>
</tr>
<tr>
<td>Home Address Line 2</td>
<td>50</td>
</tr>
<tr>
<td>Home Address Line 3</td>
<td>50</td>
</tr>
<tr>
<td>Home Address Line 4</td>
<td>50</td>
</tr>
<tr>
<td>Home Post Code</td>
<td>50</td>
</tr>
<tr>
<td>Initials</td>
<td>40</td>
</tr>
<tr>
<td>Job Title</td>
<td>3</td>
</tr>
<tr>
<td>Keyword</td>
<td>100</td>
</tr>
<tr>
<td>Last Name</td>
<td>50</td>
</tr>
<tr>
<td>Location</td>
<td>100</td>
</tr>
<tr>
<td>MAC Address</td>
<td>255</td>
</tr>
<tr>
<td>Middle Name</td>
<td>40</td>
</tr>
<tr>
<td>Mobile</td>
<td>40</td>
</tr>
<tr>
<td>Pager</td>
<td>40</td>
</tr>
<tr>
<td>Notes</td>
<td>4000</td>
</tr>
<tr>
<td>Room Name</td>
<td>50</td>
</tr>
</tbody>
</table>
Contact Directory

Directory Rules

Use Directory Rules to manage the filters to use when importing information from your selected directory to the Cisco Unified Attendant Console Advanced server. The filters are built into rules. You can have multiple filters in a rule, and apply multiple rules.

Note

If contacts in the LDAP source contain directory numbers associated with Cisco Unified Communications Manager CTI Route Points, you must exclude them from directory synchronization using Directory Rules, and then manually add them to the directory as External contacts, as described in Contact Management.

Tip

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

If you have multiple rules, each containing a single filter, the rules/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 an existing rule, Select the rule and continue from Step 4.

Step 3

Enter a Rule Name, and then click Save.

Step 4

To add a filter to the rule, click Add New.

Step 5

Select a Source field, against which the filter Value is matched.

Step 6

Select an Operator, which determines how the Value is matched in the Source field. Choose one of: Equal to, Approx. Equal to, Less and Equal to (<=), Greater and Equal to (>=).

Step 7

Enter the Value to match against the Source field using the Operator.
Inserting, Updating and Exporting Contacts via CSV

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.

Note
Files containing non-English/Unicode characters must be in UTF8 format.

Inserting Contacts

To insert contacts from a CSV file, do the following:

Step 1
Choose Bulk Administration > Insert Contacts.
The Insert Contacts Configuration page appears.

Step 2
Under Insert Contacts, select a file. Only files of the correct type are offered. You can use each CSV file in only one job.
If you want, you can view the contents of the file (click View File) or the contents of a sample file (click View Sample File).

Step 3
If required, edit the Job Description to give it a unique identity.

Step 4
Select either Run immediately, to run the job when you click Save (Step 5), or Run Later, to run the job using the Job Scheduler, as described in Scheduling Contact Insertion and Updating.

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).
Chapter 8  Configuring Cisco Unified Attendant Console

Inserting, Updating and Exporting Contacts via CSV

**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**.

**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**, 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):

<table>
<thead>
<tr>
<th>Job Status</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inactive</td>
<td>Job not activated and never run.</td>
</tr>
<tr>
<td>Pending</td>
<td>Job activated and scheduled to run.</td>
</tr>
<tr>
<td>Processing</td>
<td>Job running. You can stop the job by selecting it and then deactivating it using the controls.</td>
</tr>
<tr>
<td>Failed</td>
<td>Job failed because of:</td>
</tr>
<tr>
<td></td>
<td>• File not found or can't be opened.</td>
</tr>
<tr>
<td></td>
<td>• Unique reference not found</td>
</tr>
<tr>
<td></td>
<td>• File has invalid format.</td>
</tr>
<tr>
<td>Expired</td>
<td>Job not activated and run before its configured date and time.</td>
</tr>
<tr>
<td>Stopped</td>
<td>Job deactivated by user or LDAP server stopped it during shut down.</td>
</tr>
<tr>
<td>Suspended</td>
<td>Link to one of the following has failed: Arc Server, Configuration database, CSV driver.</td>
</tr>
<tr>
<td>Completed</td>
<td>Job completed successfully.</td>
</tr>
</tbody>
</table>

Matching jobs are listed.

**Step 3**  Select the relevant job from the list. Either select the check box, or use the **Select All, Clear All, Select All In Search** and **Clear All In Search** controls, as required.

**Note**  You cannot reconfigure or re-schedule completed jobs.

**Step 4**  Within the job to schedule, click **Select**.

**Step 5**  Under **Scheduled Date/Time**, enter or select a **Date**, then enter or select a **Time** in the formats indicated. If you do not set the date and time, the job will be configured to run immediately.

**Step 6**  Click **Save** to save your changes.
Step 7  Saved jobs will not be processed until you activate them. To activate the job, ready for processing, click Activate Job. You can deactivate an activated job by clicking Deactivate Job. You can use Activate Selected and De-activate Selected to activate or deactivate all selected jobs. If a job has completed, you cannot activate or deactivate it.

Note  When a job has been run you cannot reconfigure it.

Exporting Contacts to CSV Files

You can export selected contacts into a CSV file for archiving or sharing. You cannot schedule the exporting of contacts.

To export contacts to a CSV file, do the following:

Step 1  Choose Bulk Administration > Export Contacts.

The Export Contacts page appears.

Step 2  Find contacts to export by matching against one of the following:
  • First name
  • Last name
  • Department
  • Extension
  • Locations
  • Business 1
  • Full Job Title
  • Mobile
  • User field 1

Matching contacts are listed.

Note  You can apply multiple filters to select just those contacts you want to export.

Step 3  Click Next.

Step 4  Under General, enter the name of the CSV file to contain the contacts. The file name can be up to 11 characters long.

Step 5  Click Save.

The contacts are exported. You cannot export one set of contacts until the last export has completed.

Step 6  If you are exporting large numbers of contacts, you can check how it is progressing by clicking Export Contact Report.

You can list and access the exported file under Bulk Administration > Upload/Download Files.
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**.
Contact Management

The Contact Management menu allows you to add, modify*, delete** and view*** contacts in the full directory. Contacts belonging to the full directory will be visible to all console users.

*Mapped LDAP source contact fields cannot be modified by Cisco Unified Attendant Console Advanced users or administrators. Sync fields will appear unavailable in the Contact Details window within the console and in the Contact Management menu of the Web Administration. Field modifications must be made at a source level.

**LDAP source contacts cannot be deleted via the Contact Management menu. To remove synchronized contacts, you must exclude them from directory synchronization using Directory Rules (see Directory Rules).

***Private Personal Directory Group contacts (created by end users) will not be visible in the Contact Management menu.

Note

Internal contacts cannot have Extensions associated with Cisco Unified Communications Manager CTI Route Points. To designate a CTI Route Point number for a contact, the contact must be deleted and recreated as an external contact. If the contact belongs to a sync source, then it must be excluded using a Directory Rule (see Directory Rules).

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, including numbers and company details.

**Limit BLF to Device Name** defines how Cisco Unified Attendant Console Advanced obtains the BLF for the new contact. If the contact has only a single phone, we recommend that you select **Limit BLF to Device Name**. If you know the contact's CUCM device name, type it in **Device Name**, and the system will attempt to get the BLF using it. If you don't know the CUCM device name, leave **Device Name** blank; if it has permission to update the record, the Console will insert the **Device Name** once the user appears in its directory with a BLF status, after it has determined the best device from which to obtain it. If the contact is using Extension Mobility, or uses their extension number across multiple devices, we recommend that you clear **Limit BLF to Device Name** to let the system find the best device from which to obtain BLF using the device selection algorithm described in the *Cisco Unified Attendant Console Advanced Design Guide*.

**Device Name** is case-sensitive, and is inactive if **Limit BLF to Device Name** is not selected. Specify the default **Limit BLF to Device Name** setting in **General Properties** (for more information, see **General Properties**).

**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**.
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.

Step 2
Create a filter to Find the contacts to delete.

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.

Step 2
Click Add New.

Step 3
Under General, type the Name of the new rule.
Configuring Cisco Unified Attendant Console Directory BLF Rules

Step 4 Optionally, under Select Directory Numbers, specify the directory numbers to convert by selecting either:

- **Number Begins with**, and then typing a pattern to match the start of the numbers.
- **Regular Expression**, and then typing the expression to use.

Step 5 If you want to remove certain non-numeric characters from the telephone number, select Remove Non-numeric Characters – which will remove all the non-numeric characters – and then specify the Exceptions that you want to keep.

Step 6 Optionally, under Remove/Replace Digits, define how to convert the start of the number string by selecting either:

- **Total Digits to be Removed**, and then typing the number of digits to remove from the start of the string. If you want to replace the digits with some others, type these into the corresponding Replace with field.
- **Regular Expression**, and then typing the expression to use. If you want to replace the digits with some others, type these into the corresponding Replace with field.

Step 7 Optionally, under Add to String, specify a Prefix and Suffix to add to the number string.

Step 8 To test your new rule, under Test Directory BLF Rule, type a Sample Directory Number to convert, and then click Test Rule. If the number that appears in the Result is not what you expect, modify the rules and try again. Otherwise, click Save to save the rule in the database. The new rule appears in the Directory BLF Rules Priority list.

Step 9 To change the position of a rule in the list, and hence the processing order, click the Up or Down arrows as required, and then click Save.

## Editing Directory BLF Rules

To edit a Directory BLF Rule:

Step 1 Choose System Configuration > Directory BLF Rules.

The Directory BLF Rules page is displayed, with the rules listed that satisfy the Find filter, which consists of:

- The rule property. You can select either Name or Sample Number.
- A condition of the rule property, such as begins with. This part of the filter is displayed only if you select the Name property.
- A string to compare to the rule property under that condition. If you select the Name property, type a string; all the rules with matching names are listed.

If you select the Sample Number property, type a sample phone number; all the rules with Select Directory Numbers regular expressions that match the format of this number are listed.

You can add filters (up to a maximum of 10) using the plus (+) control; thereby narrowing the search.

Step 2 If necessary, Find the rule.

Step 3 Click Select to display that rule’s parameters.

Step 4 Edit the rule’s parameters, and then click Save.
Deleting Directory BLF Rules

To delete a Directory BLF Rule:

**Step 1** Choose System Configuration > Directory BLF Rules.

The Directory BLF Rules page is displayed, with the rules that satisfy the Find filter listed.

**Step 2** If necessary, Find the rule.

**Step 3** Select the check box at the start of each rule to delete. Click Select All to select all the rules for deletion.

**Step 4** Click Delete Selected.

Applying BLF Directory Rules

BLF Directory Rules are applied when you create or amend contacts using the Cisco Unified Attendant Console Advanced client, Cisco Unified Attendant Console Advanced Administration, or via LDAP import. You can also manually apply the rules to update contacts as follows:

**Step 1** Choose Bulk Administration > Job Scheduler.

The Job Scheduler page appears.

**Step 2** Find the BLF Subscription Number conversion job, and then Select it.

The General section is read-only.

**Step 3** Under Scheduled Date/Time, enter or select a Date, then enter or select a Time. If you do not set the date and time, the job will run immediately.

**Step 4** Activate the job, ready for processing, by clicking Activate Job. You can deactivate an activated job by clicking De-activate Job.

**Step 5** Click Save to save your changes, and run the job at the specified time.

The contact BLF subscription numbers are updated; you can view them in the Contact Numbers section of the Contact Management page.

For more information about scheduling updates, see Scheduling Contact Insertion and Updating.

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, and to add and manage system devices, as described in System Device Management.

- **Synchronize with CUCM.** This includes the CUCM Sync Report, and is described in Synchronize with CUCM.

- **Directory Source Management.** This is described in Queue Management.
• **Contact Management.** This is described in [Contact Management](#).
• **Directory BLF Rules.** This is described in [Directory BLF Rules](#).

## 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.

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

### Note

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

## Creating Queue Device Groups

To create a queue device group:

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

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

**Step 2** Either

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

- **Find** a Queue Device Group to configure:
  
  a. Specify a filter: a string to search for and where to search for it:

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

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

  b. Click **Find**.

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

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

  Another Queue Device Groups page is displayed.

  **Step 4** Use this page to change the name of the selected group or to manage the system devices in the group:
To change the name of the queue device group, under **General** edit the text in the field, and then click **Save**.

To access the System Device Management page so that you can manage the system devices in the group, under **System Devices** select the appropriate server. For the full procedure, see **System Device Management**.

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

**Deleting Queue Device Groups**

You cannot delete a Queue Device Group until all devices in it have been removed.

To delete a Queue Device Group, do the following:

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

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

**Step 2** **Find** the Queue Device Group to delete.

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

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

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

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

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

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

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

**System Device Management**

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

**Note**
If you have a resilient installation:

- You must create the same numbers of each type of system device on both the Publisher and Subscriber
- You cannot configure system devices when logged into the Subscriber server
To configure system devices and synchronize device ranges with Cisco Unified Communications server:

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

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

**Step 2** Under **Select queue device group profile**, click **Select** alongside the Queue Device Group to configure. Another **Queue Device Groups** page is displayed.

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

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

<table>
<thead>
<tr>
<th>Field or Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue Device Group</td>
<td>The name of the queue device group for this server.</td>
</tr>
<tr>
<td>Template Device</td>
<td>You can create a template CTI device with custom settings in Cisco Unified Communications Manager, and use it as a quick way of assigning these settings to your Cisco Unified Attendant Console Advanced devices. If you do not have a template, default values are assigned to your devices. All the properties of the Template Device, such as device pool, partition, and Calling Search Space (CSS), are mapped onto any new devices you create. Click <strong>Find Template Device</strong> to search for a template.</td>
</tr>
</tbody>
</table>

**Notes:**

- The Music On Hold (MOH) source configured against Cisco Unified Attendant Console Advanced CTI ports must be set to unicast, otherwise call control issues may arise. *CTI devices do not support the multicast MOH feature.*

- The template device should be based on an end point (a phone) or a CTI Port. *Do not use a CTI Route Point as a template device.*

- If under **Protocol Specific Information** a Subscribe Calling Search Space is configured, then under **Device Information** an Owner User ID must also be configured, otherwise an error occurs when you synchronize the CTI ports with Cisco Unified Communications Manager.

- If a template device is specified for a Queue DDI it must outline the Calling Search Space (CSS) for the following:
  - Forward on CTI Failure
  - Forward Unregistered Internal
  - Forward Unregistered External
  Set these within Cisco Unified Communications Manager, under **Directory Number Configuration > Call Forward and Call Pickup Settings**.

**Copy all device properties from this device**

**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.

**Service Devices**

**Note:** The Music On Hold (MOH) source configured against Cisco Unified Attendant Console Advanced CTI ports must be set to unicast, otherwise call control issues may arise. *CTI devices do not support the multicast MOH feature.*
Step 4  Click **Find Template Device** to list and search for template devices to use.

Define the search filter:

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

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

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

---

**Tip**

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

---

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

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

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

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

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

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

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

---

**Note**

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

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

You can only add ranges of up to 100 devices.

b. Click **Save**.

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

Step 7  Click **Save**.

---

**Note**

Each time you change devices you must synchronize Cisco Unified Attendant Console Advanced with Cisco Unified Communications Manager.
Step 8  Click **Synchronize with CUCM** to display the **Synchronize with CUCM** page, as described 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check box</td>
<td>Click to select/clear that Queue Device Group.</td>
</tr>
<tr>
<td><em>Queue Device Group</em></td>
<td>The Queue Device Group name.</td>
</tr>
<tr>
<td><em>Publisher Devices</em> (&lt;server_name&gt;)</td>
<td>The number of devices in that group that are on the Publisher server.</td>
</tr>
<tr>
<td><em>Subscriber Devices</em> (&lt;server_name&gt;)</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

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

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

**Step 4**  Click **Synchronize with CUCM**.

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

**Step 5**  If you are satisfied with the time required to synchronize, click **Yes**.
Cisco Unified Attendant Console Advanced Administration synchronizes the devices with Cisco Unified Communications Manager. You do not have to login to Cisco Unified Communications Manager administration.

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

---

The report contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sync Status</strong></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Synchronization status; one of:</td>
</tr>
<tr>
<td></td>
<td>- Associating</td>
</tr>
<tr>
<td></td>
<td>- Completed</td>
</tr>
<tr>
<td></td>
<td>- Creating</td>
</tr>
<tr>
<td></td>
<td>- Deleting</td>
</tr>
<tr>
<td></td>
<td>- Validating</td>
</tr>
<tr>
<td>Ignore call forward settings</td>
<td>Whether <strong>Ignore call forward</strong> is set.</td>
</tr>
<tr>
<td>Started At</td>
<td>The date and time when Cisco Unified Communications Manager synchronization started. For example, 2015-04-12 16:08:52.</td>
</tr>
<tr>
<td>Ended At</td>
<td>The date and time when Cisco Unified Communications Manager synchronization ended. For example, 2015-04-12 16:10:52.</td>
</tr>
</tbody>
</table>

**CUCM Connection Validation**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The Cisco Unified Communications Manager Application User profile ID.</td>
</tr>
<tr>
<td>Server Name</td>
<td>The name of the server hosting Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the connection validation; one of:</td>
</tr>
<tr>
<td></td>
<td>- Completed</td>
</tr>
<tr>
<td></td>
<td>- Error</td>
</tr>
<tr>
<td></td>
<td>- Validating</td>
</tr>
<tr>
<td>Error Code</td>
<td>The code of the error that has been encountered. For example, 9400.</td>
</tr>
<tr>
<td>Error Description</td>
<td>This field gives a brief description of the error that has been encountered. For example, HTTP/1.1 503 Service Unavailable.</td>
</tr>
</tbody>
</table>

**Template Device Validation**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue Device Group</td>
<td>A Queue Device Group.</td>
</tr>
<tr>
<td>Template Device Pkid</td>
<td>The unique ID of the Queue Device Group from Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the template device validation; one of:</td>
</tr>
<tr>
<td></td>
<td>- Completed</td>
</tr>
<tr>
<td></td>
<td>- Error</td>
</tr>
<tr>
<td></td>
<td>- Validating</td>
</tr>
</tbody>
</table>
### System Configuration Menu

#### Chapter 8 Configuring Cisco Unified Attendant Console

The following errors may occur during CUCM synchronization.

**Table 8-1**

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Error Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco Errors</strong></td>
<td></td>
</tr>
<tr>
<td>Less than 5000</td>
<td>These errors correspond to DBL exception error codes.</td>
</tr>
<tr>
<td>5000</td>
<td>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.</td>
</tr>
<tr>
<td>5002</td>
<td>Unknown Request Error—the user agent saves a request that is unknown to the API.</td>
</tr>
<tr>
<td>5003</td>
<td>Invalid Value Exception—an invalid value is detected in the XML request.</td>
</tr>
<tr>
<td>5007</td>
<td>Item Not Valid Error—the system identified the specified item does not exist or was specified incorrectly at input.</td>
</tr>
<tr>
<td>599</td>
<td>Schema Not Supported—there has been an AXL request error because the schema is not supported.</td>
</tr>
<tr>
<td><strong>Internal Errors</strong></td>
<td></td>
</tr>
<tr>
<td>9000</td>
<td>Exception in AXL component—an unknown error occurred while processing the AXL component.</td>
</tr>
<tr>
<td>9100</td>
<td>Function parameter error—the parameter value is empty or null.</td>
</tr>
<tr>
<td>9200</td>
<td>Device already created—the device being synchronized already exists in Cisco Unified Communications Manager and is synchronized with the client.</td>
</tr>
<tr>
<td>9300</td>
<td>Template device not found—the template device that you have selected does not exist.</td>
</tr>
</tbody>
</table>
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

The following:

- For how to best set up queue overflow see Queue Overflow - Best Practice in the Cisco Unified Attendant Console Advanced Design Guide.
- If you have a resilient system and you are logged into the Subscriber server, you cannot change any of the Queue Management parameters.

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Error Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9400</td>
<td>HTTP/1.1 503 Service Unavailable—the AXL service is unavailable.</td>
</tr>
<tr>
<td>9500</td>
<td>HTTP/1.1 401 Unauthorized—the user authentication credentials are invalid.</td>
</tr>
<tr>
<td>9550</td>
<td>HTTP/1.1 403 Access to the requested resource has been denied—access denied error from AXL response.</td>
</tr>
<tr>
<td>9555</td>
<td>HTTP/1.1 404—there is an invalid header location in the SOAP Request.</td>
</tr>
<tr>
<td>9600</td>
<td>Call Manager OS not recognized—the operating system returned by Cisco Unified Communications Manager is neither Linux nor Windows.</td>
</tr>
<tr>
<td>9650</td>
<td>Call Manager Version not detected—the AXL Response from Cisco Unified Communications Manager did not provide the version.</td>
</tr>
<tr>
<td>9700</td>
<td>Socket error—there are network problems.</td>
</tr>
<tr>
<td>9750</td>
<td>Connection refused—the server did not respond or the request has been posted to an invalid URL.</td>
</tr>
<tr>
<td>9755</td>
<td>Read Timeout—the server did not respond.</td>
</tr>
<tr>
<td>9800</td>
<td>Normal Exit—normal exit on completion.</td>
</tr>
<tr>
<td>10000</td>
<td>Connection timeout—connection timeout from the server.</td>
</tr>
</tbody>
</table>
Creating Queues

To create a queue:

**Step 1** Choose **User Configuration > Queue Management**.

The **Queue Management** page is displayed.

**Step 2** Click **Add New**.

**Step 3** Under **General**, set the following:

- **Name**—type the name of the queue.
- **Priority**—specify the priority of the selected queue's calls in relation to calls belonging to other queues (1 highest - 99 lowest):
  - Calls in queue are prioritized from top (highest priority) to bottom (lowest priority) based on delivery queue, followed by wait time within that queue.
  - If all queues have the same priority (such as the default value - 99), then calls are arranged and/or delivered based on wait time and delivery method as opposed to delivery queue.
  - Forced delivery calls always take priority over broadcast delivery calls, irrespective of the priority specification.
- **Salutation**—optionally type a greeting to be displayed in a pop-up for the operator to use. This is the same for all servers.
- **Queue device group**—select the queue device group to use.

**Step 4** Specify the **Call Delivery Method**:

- **Broadcast**—select this so that all logged-in operators can see the call in their Queued Incoming Calls (F8) pane, and any can pick up the call. This is the default queue type.
- **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.

**Note** *The Call Delivery Method cannot be modified after the queue is created.* If you need to change the Call Delivery Method for a queue, you must delete the queue and then recreate it with the new method.

**Step 5** Click **Save**.

You can now set the queue DDI and configure the Full CTI Failure, Emergency, Overflow and Out of House routing properties, as described in **Configuring Queues**, below.
Deleting Queues

To delete a queue:

**Step 1** Choose User Configuration > Queue Management.
The Queue Management page is displayed.

**Step 2** Click Find to see the list of available queues.

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

**Step 4** Click Delete Selected.

Configuring Queues

To configure a queue (if you are viewing the Queue Management page 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 8-29.

**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).

**Step 8** Set the following properties:
• **Full CTI Failure device**—(only in resilient installations). Type the name of the device to use if there is a full CTI failure. Calls get forwarded to this device when both servers are down and are unable to take any calls.

If, in Cisco Unified Communications Manager, you have specified destinations for the following Call Forward and Call Pickup Settings:

- Forward on CTI Failure
- Forward Unregistered Internal

and you have:

- Configured a resilient Cisco Unified Attendant Console Advanced Administration installation
- Assigned Publisher and Subscriber DDIs
- Created a Queue and configured a Full CTI Failure device on the queue
- Used Cisco Unified Attendant Console Advanced Administration to synchronize the device

Then an AXL SOAP request synchronizes the devices on Cisco Unified Communications Manager. This sets the queue's Subscriber DDI as the forwarding destination of the queue's Publisher DDI, and the Full CTI failure device is made the forwarding destination of the queue's Subscriber DDI.

**Note**

If you change the Full CTI Failure device or Queue DDI you must re-[Synchronize with CUCM](#) to update the Cisco Unified Communications Manager device configuration. For instructions on how to do this, see [Synchronize with CUCM](#).

• **Emergency**—the destination calls must be forwarded to when the queue is in emergency mode.

  - **Destination type**—select:
    - **Device** (then type a DDI number in the Emergency destination),
    - **Queue** (then find and select a Queue as the Emergency destination) or
    - **None**, to disable the forwarding of Emergency calls.

  If you select Queue, the Find Queue button is displayed next to the destination field; click this to display the Queue Selection page.

  Use the Find controls to list particular queues (find by Name, DDI or Queue Type), click a radio button to select the required queue, and then click Save.

  - **Emergency destination**—the destination DDI (if Destination type is Device), or Queue Name (if the Destination type is Queue) to which to send calls when the queue is in emergency mode.

• **Overflow**—This controls the routing (overflow) of calls from a queue when certain parameters are exceeded. It contains these properties:

  - **Maximum calls**—The maximum number of calls that can wait in the queue. Additional calls are routed to the Maximum calls destination.

  - **Destination type**—select:
    - **Device** (then type a DDI number in the Maximum calls destination),
    - **Queue** (then find and select a Queue as the Maximum calls destination) or
    - **None**, to disable the Maximum calls overflow.

  If you select Queue, click Find Queue to select a queue from the Queue Selection page, as described for the Emergency destination.

  - **Maximum calls destination**—the destination DDI (if Destination type is Device), or Queue Name (if the Destination type is Queue) to which to route calls when the Maximum calls parameter is exceeded.
Chapter 8   Configuring Cisco Unified Attendant Console

Queue Management

- **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, 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.

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**.

---

### Configuring Out of Hours Routing

The out of hours routing feature enables you to define destinations (numbers or queues) to which calls to a queue are routed outside office hours or during staff breaks. Each queue can have its own out of hours routing configuration.

**Note**

The out of hours configuration refers to the date and time on the server hosting the queue. It is not defined for other time zones.

Out of hours routing is defined using named **templates**, which you apply to your queues, as described in **Configuring Queues**. The template’s **profile** defines the out of hours date and time period(s) and the destination to receive the calls during that period.

**Note**

A queue’s out of hours routing configuration is set at the instant a template is applied. If you change a template after it has been applied to a queue, those changes do not affect the queue.

You can create out of hours routing templates either from scratch (you define *all* properties of the template) or by copying an existing template and then editing its properties.

This section describes the following:

- Creating Out of Hours Routing Templates From Scratch
- Creating Out of Hours Routing Templates by Copying
- Deleting Out of Hours Routing Templates
- Editing Out of Hours Routing Templates

**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**.
- Change existing out of hours date and time periods, as described in **Editing Out of Hours Routing Templates**.
Deleting Out of Hours Routing Templates

To delete an out of hours routing template, do the following:

**Step 1** Choose User Configuration > Templates > Out of Hours Routing.

The Out of Hours Routing Template page appears.

**Step 2** If necessary, Find the template(s) to delete.

**Step 3** Click the appropriate check boxes on the left or use the Select All (on page) or Select All In Search (including any other pages of results) to select the template(s) to delete.

**Step 4** Click Delete Selected.

Editing Out of Hours Routing Templates

To edit an out of hours routing template, do the following:

**Step 1** Choose User Configuration > Templates > Out of Hours Routing.

The Out of Hours Routing Template page appears.

**Step 2** If necessary, Find the template(s) to edit.

**Step 3** Click Select next to the template to edit.

**Step 4** If you want to change the name of the template, under General, type the new Template name, and then click Update.

**Step 5** Do the following as required:

- To add a new time period configuration (Specific Dates or Days of the Week) follow the instructions in Creating Out of Hours Routing Templates From Scratch.
- To edit an existing time period configuration, click Select alongside, change the configuration, and then click Save.
- To remove time period configurations from your template, select the corresponding check boxes on the left, and then click Delete Selected.

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.
- **Queue Management.** This is described in Queue Management.
- **Operator Management.** This is described in Operator Management.
- **Realm Management.** This is described in Realm Management.
- **Credential Policy Management.** This is described in Credential Policy Management.
- **Templates.** This is described in Configuring Out of Hours Routing.
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. (See note for requirements.)
- 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. (See note for requirements.)

Note
International Dialing Requirements

- Use of the External International Access Number requires that contact numbers be in E.164 format (for example, +1 555 555 5555).
- External Area Code must be formatted as +<country code>. The <bold>+<bold> pre-fixed External Area Code is required for the External International Access Number to go in to effect. Otherwise, outbound calls will default to the External Access Number.

- Default FAC and CMC Settings—Forced Authorization Codes (FAC) and Client Matter Codes (CMC) are configured in Cisco Unified Communications Manager, and they must be added in Cisco Unified Attendant Console Administrator if the system performs the following actions on calls:
  - Overflows
  - Night Service destination
  - Attendant Operators perform a Blind Transfer
If the destination number is an **External Number** (external to your organization or CUCM), the system may require you to provide FAC and CMC information to perform the above actions. If the information is configured in Cisco Unified Attendant Console Administrator under General Properties, the system will automatically append this information when requested by CTI during its call operation.

If this information is not configured in Cisco Unified Attendant Console Administrator but is required to make an external call, then any calls initiated by the user (Attendant Operator) will be prompted with a FAC and CMC dialog box. However, system transfers like overflows, night service and emergency overflows will fail.

To configure FAC and CMC, refer to the documentation available here:


**Note**

Client Matter Code (CMC) is used to provide extra call logging facilities within the Cisco Unified Communications Manager. The user has to enter their CMC Code before their external consult transfer can proceed. The CMC code is written into the call detail records, which can then be used to charge calls to different cost centers.

**Note**

Forced Authorization Code (FAC) is used to provide security in the Cisco Unified Communications Manager for dialing “Route Patterns”. In some call centers, some callers are only allowed to make external consult transfers if they first enter a FAC. If they fail to enter a FAC or enter an incorrect FAC the transfer fails.

---

**Recall Timers**—these properties are used to set the duration of each type of recall:

- **Hold recall**—the maximum time a call put on hold by an operator remains on hold before an audible alert is played
- **Transfer recall**—the maximum time before an unanswered operator-transferred call is returned to that operator
- **Park recall**—the maximum time before an unanswered parked call is returned to the operator. The call can still be picked up by the intended recipient once the Parked timeout has happened.
- **Camp On recall**—the maximum time an unanswered call remains camped-on before it is returned to the operator.

**Default Queue Device Group**—select the system default queue device group: the group of devices to use to route the call if the system is otherwise unable to attach a device group to it.

**Call Arrival Mode**—Select to enable **Hold queued calls** mode, which is used to trigger Music on Hold (MoH) within the Cisco Unified Communications Manager.

**Note**

Cisco Unified Communications Manager enables you to configure a queue to hold queued calls when they arrive on the CTI Port, and play Music on Hold to the caller while they wait for an operator to answer. **If you use this mode the call is charged from the time that it is answered and put on hold on the CT Gateway.**

**Contact Directory Setting**—The Cisco Unified Communications Manager device name is used to retrieve a contact’s BLF information. This device name is either:
User Configuration Menu

- Part of the contact's details, entered manually when the contact is created in the Contact Management page (see Contact Management).
- Automatically found by Cisco Unified Attendant Console Advanced using the device selection algorithm described in the Cisco Unified Attendant Console Advanced Design Guide.

The Limit BLF to Device Name setting determines which of these is used by default when you create new contacts in the Contact Management page. If most of your directory contacts have a single phone, select Limit BLF to Device Name, otherwise clear it.

- **Call Logging Setting**—Select Call Logging to enable call logging, clear it to disable call logging.

  **Note**
  After disabling call logging, you can remove old logging data using Engineering > Database Purge. For more information, see Database Purge.

- **Login Rate Settings**—Select this to protect the system against denial of service (DOS) attacks.
  
  The login rate is checked at these levels:
  
  - **User Level**—This applies only to non-SSO users, and only when a correct login name is used with an incorrect password. If the login name is incorrect, the Session Level setting applies.
  
  - **Session Level**—This setting applies to both SSO and non-SSO users, and concerns the use of incorrect login names that are not in the system cash and cannot then be found in the system’s list of authorized users.

  In both cases, the user has 60 seconds from first attempt in which to log in successfully. During this time, if the user login attempt fails because of either an invalid login name or invalid password on three consecutive occasions, on the fourth attempt (irrespective of whether correct credentials are provided) the server makes the user wait for 60 seconds before they can try again. After this time, the server is reset, counts and timers are zeroed, and the check repeated, and so on until the user either logs in or gives up.

  Once the Login Rate has struck, the console GUI will be greyed out and not usable until the application is restarted. In the case of Web Admin, when Login Rate has struck, it will display Online Login Failure Message.

  Successfully logging in resets the timers and counts to zero.

  On a resilient system the Publisher and Subscriber do not share a cache - each has its own - meaning that more bogus logins than configured could be attempted during system failover.

- **Session Idle Setting**—Select this to decide how long the user can be idle before being logged off. Enter between 0 and 60 minutes, or leave empty to disable the function.

**Step 3**

Click **Save** to save the changes.
Operator Management

The Operator Management option enables you to create and configure operator profiles, including associating queues with profiles. You can also import users as operators from the Cisco Unified Communications Manager or other LDAP-compliant directory servers, and convert non-SSO users to SSO users.

Creating Operator Profiles

To create an operator profile:

**Step 1** Choose User Configuration > Operator Management.
A list of existing operators appears.

**Step 2** Click Add New.

**Step 3** Under General, do the following:

- **a.** Enter a Login name.
- **b.** Enter a Passphrase, and then re-enter it to confirm it.
- **c.** In Role, select either:
  - Standard
  - VIOC – enables attendant operators who are blind or have low vision to use the Console with the help of the JAWS screen reader. For more information, see Accessibility for Users with Disabilities.
- **d.** To force a non-SSO user to change their passphrase when they next log in, select Account Reset. This setting is cleared when the user changes their passphrase.
- **e.** To lock the account of a non-SSO user, select Account Locked. To unlock a locked account, clear the checkbox. For a list of situations in which an account is locked, see Credential Policy Management.

The Last Login Date/Time (UTC) shows the date and time that the operator last successfully logged in.

**Step 4** Click Save.

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

Importing Operators

You can import LDAP contacts as operators with these user characteristics:

- Cisco Single Sign-on (SSO) Users
- Local Users – who do not use SSO and can be logged in without federation authentication. You can convert these users to SSO users by linking them to existing SSO users.

The number of contacts you can import in one go is restricted by the number specified under your Cisco Unified Attendant Console Advanced license, with a maximum of 50.

To import contacts:
**User Configuration Menu**

---

**Step 1**  
Choose **User Configuration > Operator Management**.

The Operator Management page listing existing operators appears.

**Step 2**  
Click **Import**.

The Import Contact page appears, listing the contacts you can import from Cisco Unified Communications Manager.

**Step 3**  
For each contact to import, select the check box in the left-hand column. All the contacts you select are imported with the Role that you choose in the next step.

**Step 4**  
In **User Type**, select either **Local** or **SSO**.

**Step 5**  
In **Role**, select either **Standard** or **VIOC**.

**Step 6**  
Click **Save Selected/Changes**.

The imported operators are added to the list on the Operator Management page.

---

**Configuring Operator Profiles**

You can configure operator profiles, including linking local users with SSO users so that they can use SSO.

To configure an operator profile:

**Step 1**  
Choose **User Configuration > Operator Management**.

**Step 2**  
**Find** an operator profile to manage. Specify a filter: a string to search for and where to search for it.

- Select **Login Name**.
- A condition of the login name, such as **is not empty**, or how to compare the login name with a string, such as **begins with**.
- A string to compare to the login name in the specified way (used only with **begins with**, **ends with**, **contains** and **is exactly**).

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

**Step 3**  
Click **Find**.

**Step 4**  
**Select** the operator profile you want to configure or link.

The profile information is displayed.

If any queues are associated with the operator, they are listed in **Associated Queues**.

**Step 5**  
If required, under **General**, edit the **Login name**, **Passphrase**, and then **Confirm passphrase**.

**Step 6**  
Under the **Role**, select either **Standard** or **VIOC** (for blind people and people with low vision).

**Step 7**  
To force the user to change their passphrase when they next log in, select **Account Reset**.

**Step 8**  
To associate the profile with a queue, under **Queue Association**, click **Queue Association**.

You can use **Find** to search for a specific queue if it is not displayed.

**Step 9**  
Select the queue(s) to associate with the profile and clear any already-associated queues you do not want associated.

**Step 10**  
To convert the user profile to use SSO by linking it to an SSO User, click **Link** (if **Link** is not displayed the profile already uses SSO).
The Link Contact page appears.

**Step 11** Select the control in the left-hand column of the row containing the contact to link to, and then click **Save Selected/Changes**.

The contact User Profile data name now matches that of the linked operator.

**Step 12** Click **Save** to save the changes.

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

---

### Deleting Operator Profiles

To delete an operator profile:

**Step 1** Choose **User Configuration > Operator Management**. The **Operator Management** page is displayed.

**Step 2** Click **Find** to see the list of available operator profiles.

**Step 3** Select the checkbox of the operator profile(s) you want to delete.

**Step 4** Click **Delete Selected**.

---

### 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*.
- **Server Management**. This is described in *Server Management*.
- **Database Management** (cannot be changed if you have a resilient installation). This is described in *Database Management*.
- **Database Purge**. This is described in *Database Purge*.
- **Service Management**. This is described in *Service Management*.
- **Presence Management**. This is described in *Presence Management*.
- **CUCM Connectivity**. This is described in *System Configuration Menu*.
- **Syslog Connectivity**. This is described in *Syslog Connectivity*.
- **Logging Management**. This is described in *Logging Management*.
- **Marking Text Management**. This is described in *Marking Text Management*.
Administrator Management

The Administrator Management option enables you to change or reset the administrator login name and passphrase 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. In a resilient system, if you change the Administrator account user login name on the Publisher, the change doesn’t get reflected on the Subscriber until you log out and then in again.

To change the login name and passphrase:

---

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

**Step 2**
Type a new **Login name**.

**Step 3**
Type the **Old passphrase**. The current passphrase.

**Step 4**
Type the **New passphrase**.

It is good practice to have a strong passphrase that utilizes both numeric and alpha characters. The Cisco Unified Attendant Console Advanced server allows up to a maximum of 20 characters including the use of Special Characters such as %,$,£,&.

**Note**
The passphrase is case sensitive.

**Step 5**
Re-enter the new passphrase in **Confirm new passphrase**.

**Step 6**
Under **Session Management**, type the **Number of Sessions** - concurrent Web Administration log in sessions - in the range 1 to 5 (the default), or unlimited (type 0).

**Step 7**
Click **Save** to save changes.
Licensing Cisco Unified Attendant Console Advanced

Licensing the Cisco Unified Attendant Console Advanced Software

Note
If you want to install a resilient Cisco Unified Attendant Console Advanced system, you need to license it separately from the server and user licenses. High availability functionality is available to use in both the 5-day and 60-day evaluation mode.

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

- Activating Evaluation Software
- Activating Purchased Software
- Relicensing Software

The instructions assume that you have logged into the Cisco Unified Attendant Console Downloads and Licensing website.

Note
- Once a system is fully licensed you cannot 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.
Activating Evaluation Software

You can use downloaded software for 5 days before you must license it. Licensing the software enables you to evaluate it for 60 more days. If you do not license the download, you will be unable to use it after the fifth day.

**Note**
You cannot extend the 60-day evaluation period or apply a second 60-day evaluation license. If you need more evaluation time, you must reinstall your system from the operating system level, and then apply a new 60-day evaluation license.

Activate the Software

Before starting, log into Cisco Unified Attendant Console Administration, choose Help > Licensing, and make a note of the Registration Code. Then, in the Cisco Unified Attendant Console Downloads and Licensing website, Activate Evaluation Software page:

**Step 1**
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 options to add them.

**Step 2**
Select the Version and the Product that you have installed, and then click Next.

**Step 3**
Enter your Registration Code.
A registration (.RGF) file is e-mailed to you, and a message to this effect is displayed in the web page.

**Step 4**
Open the email and save the registration file to a location that can be browsed by the Cisco Unified Attendant Console Advanced server.

**Step 5**
Log into Cisco Unified Attendant Console Administration and choose Help > Licensing.

**Step 6**
In the License Management page, select Registration File.

**Step 7**
Click Browse and then open the Registration File.

**Step 8**
Click Submit to complete license activation.

**Step 9**
Stop and then restart the services, as described in Service Management. If you have configured a resilient server, you need to stop then restart the services once the Publisher server services are restored.

Activating Purchased Software

You can purchase the software at any time in the evaluation periods, giving you unlimited use. When you purchase the software Cisco provide you with a 27-digit license activation code (LAC). After activating the software, you cannot revert to the trial version.

**Note**
If you have purchased à la carte upgrade licenses, or requested UCSS upgrade licenses through the Cisco Product Upgrade Tool, you must ensure that the previous version’s 27-digit LACs are activated before activating the upgrade LACs. If you do not do this the upgrade activation will fail.
In resilient installation, all licensing information is held on the Publisher server, and then replicated to
the Subscriber. You only need to license the Publisher - the Subscriber inherits this information via
replication.

In the Cisco Unified Attendant Console Downloads and Licensing website, Activate Purchased
Software page:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select your Reseller, then select your Customer, and then select your Customer Site.</td>
</tr>
<tr>
<td>Note</td>
<td>If your reseller, customer or site are not available, click the control to add them.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select the Version and the Product that you have installed, and then click Next.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the Registration Code from the server, and then click Next.</td>
</tr>
<tr>
<td>Note</td>
<td>To find your Registration Code, log into Cisco Unified Attendant Console Administration and choose Help &gt; Licensing.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter at least one License Activation Code and then click SUBMIT.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Enter at least one License Activation Code and then click SUBMIT. If you want to change the License Activation Code you entered in Step 4 before proceeding, click Back.</td>
</tr>
<tr>
<td></td>
<td>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 high availability the Subscriber remains under evaluation mode and will cease to work at the end of the evaluation period.</td>
</tr>
<tr>
<td></td>
<td>A registration (.RGF) file is e-mailed to you, and license request confirmation information is displayed in the web page.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Open the email and save the registration file to a location that can be browsed by the Cisco Unified Attendant Console Advanced server.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Log into Cisco Unified Attendant Console Administration and choose Help &gt; Licensing.</td>
</tr>
<tr>
<td>Step 8</td>
<td>In the License Management page, select Registration File.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Click Browse and then open the Registration File.</td>
</tr>
<tr>
<td>Step 10</td>
<td>Click Submit to complete the registration.</td>
</tr>
<tr>
<td>Step 11</td>
<td>Stop and then restart the services, as described in Service Management. If you have configured a resilient server, you need to stop then restart the services once the Publisher server services are restored.</td>
</tr>
</tbody>
</table>

License Expiry

Cisco Unified Attendant Console Administration will display license expiry alerts beginning 30 days
prior to the date of expiration. Following expiration, users are warned that the license(s) have expired but are given a 30-day grace period to act before experiencing service interruption. Once the grace period elapses, the license(s) will deactivate.
Cisco Unified Attendant Console Administration presents the following licensing status messages:

- Alert messages are presented at login for licenses set to expire within 30 days. License type alerts appear as follows:
  - User license(s) are approaching expiration, refer to License Management. Take action now to prevent service interruption.
  - High Availability license is approaching expiration, refer to License Management. Take action now to prevent service interruption.

- Warning messages are presented at login and in the License Management menu, on the date of expiration and for the duration of the 30-day grace period that follows. License type warnings appear as follows:
  - At login:
    - User license(s) are approaching expiration, refer to License Management. Take action now to prevent service interruption.
    - High Availability license is approaching expiration, refer to License Management. Take action now to prevent service interruption.
  - In Help > Licensing > License Management:
    - The license line item(s) are displayed in bold red text.
  - Following grace period expiration, in Help > Licensing > License Management menu:
    - The fully expired license line item(s) are displayed in gray with a status of inactive - expired.

## Relicensing Software

If you do any of the following to the server environment you must re-license the software with a new registration code:

- Reinstall the operating system on the same hardware
- Install a different operating system 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

**Note**

In case of a major version upgrade (for example, 10.x to 12.x or 11.x to 12.x), the Subscriber server will say “UNLICENSED COPY” on Web Admin and the server will not be usable. To fix this, you will need to install replication. Once replication is installed, the copy will become licensed and the server will be usable.

And within a VM Environment:

- Copy the VM image
- Perform a major upgrade of the Cisco Unified Attendant Console Advanced software
Note

In case of a major version upgrade (for example, 10.x to 12.x or 11.x to 12.x), the Subscriber server will say “UNLICENSED COPY” on Web Admin and the server will not be usable. To fix this, you will need to install replication. Once replication is installed, the copy will become licensed and the server will be usable.

All these cause the license to expire, and the System and User Configuration menus to disappear from Cisco Unified Attendant Console Administration.

To re-license a server, contact Cisco 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.
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 or uninstallation. If the replication uninstall does not succeed at the first attempt, you are prompted to retry it or abort it.
- When installing or uninstalling resilient server software, both the Publisher and Subscriber server machines must be running. If either machine is turned off or inaccessible, the install or uninstall may fail.
- If the Publisher server software gets uninstalled, the Subscriber server’s software link with the Publisher server gets broken. When you reinstall the Publisher server software you must then reinstall the Subscriber server software to restore the link.

When you uninstall a resilient system, it doesn’t matter whether you start with the Publisher or the Subscriber.

To uninstall Cisco Unified Attendant Console Advanced server (the exact steps depend on the operating system of the host system):

**Step 1** Choose **Start > Control Panel**, and then double-click **Add/Remove Programs**.

**Step 2** From the list, select **Cisco Unified Attendant Server**, and then click **Remove**.

The Wizard prepares to (un)install the server application.

**Step 3** When you are prompted to confirm that you want to remove Cisco Unified Attendant Console Advanced server from your machine, click **Yes**.

**Step 4** If you have a resilient installation and both servers are running, you are prompted that the services on the other server (Subscriber or Publisher, as appropriate) need to be stopped. In the message click **Yes** to stop the services. In the Server screen, enter the **Username** and **Passphrase** of the administrative account on the other server.

The server application is uninstalled.
Uninstalling Microsoft SQL Server

To uninstall the Microsoft SQL Server from your Cisco Unified Attendant Console Advanced server:

**Step 1** Choose Start > Control Panel, and then double-click Add/Remove Programs.

**Step 2** From the list, select Microsoft SQL Server, and then click Remove.

The server instances are listed.

**Step 3** Select the instance to remove, and then click Next.

You are asked to confirm that you want to uninstall the selected instance.

**Step 4** Click Finish to remove the components. Click Back to go back and change any of the information.

While the components are being uninstalled the Setup Progress is displayed.

**Step 5** When all the components have been removed, click Finish.

**Step 6** When you have uninstalled Microsoft SQL Server, delete the C:\DBdata\ folder and the databases it contains.

Uninstalling the .NET Framework

**Caution** If you uninstall the .NET Framework Cisco Unified Attendant Console Advanced will not function.

To uninstall the .NET Framework:

**Step 1** Choose Start > Control Panel, and then double-click Add/Remove Programs.

**Step 2** From the list, select whatever .NET you have installed, and then click Remove.

You are prompted to either Repair or Uninstall the .NET Framework.

**Step 3** Select Uninstall, and then click Next.

**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. It will be available only if you enabled it during installation.

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

To access Cisco Unified Reporting:

**Step 1** Log in to Cisco Unified Attendant Console Advanced Administration, as described in Administrator Login.

The Cisco Unified Attendant Console Advanced Administration home page is described. For more information, see Home Page.

**Step 2** In Navigation at the top right of the home page, select Cisco Unified Reporting, and then click Go.

The Cisco Unified Reporting home page is displayed. This contains the System Reports menu from which you can run the following reports:

- Incoming Calls by Date and Time. For more information, see Incoming Calls by Date and Time System Report.
- Operator Calls by Time. For more information, see Operator Calls by Time System Report.
- Operator Calls by Queue. For more information, see Operator Calls by Queue System Report.
- Operator Availability. For more information, see Operator Availability Report.
- Overflowed Calls by Date. For more information, see Overflowed Calls By Date System Report.
### Toolbar

At the top of each system report is a toolbar containing the following for controlling the report:

<table>
<thead>
<tr>
<th>Control</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Related Links: Back to System Reports Go" /></td>
<td>Click Go to return to the System Reports home page.</td>
</tr>
<tr>
<td><img src="image" alt="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." /></td>
<td>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.</td>
</tr>
<tr>
<td><img src="image" alt="Select a format Export" /></td>
<td>Export a copy of the report. First select the format from Excel (.XLS) or Acrobat (.PDF).</td>
</tr>
<tr>
<td><img src="image" alt="Refresh the Report screen." /></td>
<td>Refresh the Report screen.</td>
</tr>
<tr>
<td><img src="image" alt="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." /></td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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

Most of the reports require you to select a **From** date, and some also require a **To** date so that the report covers the range of specified dates. You can restrict a date range to a single day by specifying the same **From** and **To** dates. The *Operator Calls by Time* report only covers a single date; so a range is not required. You can select the date by clicking the calendar control.

### Time Range

Most of the reports require you to select a **From** time and a **To** time. These times have the format **hh:mm:ss**, where **hh** uses a 24 hour clock. Both times are compared to the start time of the calls on that day. For example, with a **From** time of 09:00:00, calls starting at 08:59:59 or earlier are omitted from the report. With a **To** time of 17:00:00, calls starting at 17:00:01 or later are omitted from the report.
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Calls</td>
<td>Number of calls reaching the Cisco Unified Attendant Console Advanced.</td>
</tr>
<tr>
<td>Answered Calls</td>
<td>Number of calls answered.</td>
</tr>
<tr>
<td>Abandoned Calls</td>
<td>Number of calls abandoned.</td>
</tr>
<tr>
<td>Overflowed Calls</td>
<td>Number of calls overflowed to a queue, device or external number.</td>
</tr>
<tr>
<td>% Answered</td>
<td>Percentage of calls answered.</td>
</tr>
<tr>
<td>% Abandoned</td>
<td>Percentage of calls abandoned.</td>
</tr>
<tr>
<td>% Overflowed</td>
<td>Percentage of calls overflowed.</td>
</tr>
<tr>
<td>Average Answered Wait</td>
<td>Average time calls wait before being answered.</td>
</tr>
<tr>
<td>Average Answered Talk Time</td>
<td>Average talk time for answered calls.</td>
</tr>
<tr>
<td>Average Abandoned Wait</td>
<td>Average time a caller waits before the call is abandoned.</td>
</tr>
<tr>
<td>Answer Time Profile</td>
<td>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.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Longest Wait</td>
<td>The longest time a caller had to wait to be answered.</td>
</tr>
<tr>
<td>Break Hour</td>
<td>Break hours.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator</td>
<td>Operator name.</td>
</tr>
<tr>
<td>Total Calls</td>
<td>Total number of inbound calls to the attendant operator.</td>
</tr>
<tr>
<td>Console</td>
<td>Total number of calls to the queue attended by the attendant operator, including:</td>
</tr>
<tr>
<td></td>
<td>• Incoming queue calls</td>
</tr>
<tr>
<td></td>
<td>• Retrieved calls from F5</td>
</tr>
<tr>
<td></td>
<td>• Calls retrieved from park by double-clicking the Park DN on the screen</td>
</tr>
<tr>
<td>Others</td>
<td>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.</td>
</tr>
<tr>
<td>Inbound Total talk time</td>
<td>Total talk time for the inbound queue calls only.</td>
</tr>
<tr>
<td>Inbound Average talk time</td>
<td>Average talk time for the inbound queue calls only.</td>
</tr>
<tr>
<td>Inbound Longest talk time</td>
<td>Longest talk time for the inbound queue calls.</td>
</tr>
<tr>
<td>Total Outbound Calls</td>
<td>Total number of outbound calls made by the operator, including:</td>
</tr>
<tr>
<td></td>
<td>• Normal outbound calls</td>
</tr>
<tr>
<td></td>
<td>• Consult transfer enquiry calls</td>
</tr>
<tr>
<td></td>
<td>• Conference enquiry calls</td>
</tr>
<tr>
<td></td>
<td>• Park calls retrieved by dialing the park DN</td>
</tr>
<tr>
<td></td>
<td>• Abandoned calls</td>
</tr>
<tr>
<td>Outbound Total talk time</td>
<td>Total talk time for outbound answered calls.</td>
</tr>
<tr>
<td>Outbound Average talk time</td>
<td>Average talk time for outbound answered calls.</td>
</tr>
<tr>
<td>Outbound Longest talk time</td>
<td>Longest talk time for outbound answered calls.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator</td>
<td>Logged in attendant operator’s name.</td>
</tr>
<tr>
<td>Queue</td>
<td>The queue assigned to that attendant operator.</td>
</tr>
<tr>
<td>No. of calls</td>
<td>Total number of queue calls answered within that queue.</td>
</tr>
<tr>
<td>Total Talk</td>
<td>The total talk time by the operator on inbound calls from that queue.</td>
</tr>
<tr>
<td>Average Talk</td>
<td>Average talk time on answered calls on that queue.</td>
</tr>
<tr>
<td>Longest Talk</td>
<td>Longest talk time for answered calls on that queue.</td>
</tr>
</tbody>
</table>

Operator Availability Report

The Operator Availability report shows the daily availability of one or more operators between the start and end date. Statistics are displayed for each logged in period, with totals for each day.

Specify the following parameters before running this report:

- Start and End Date
- Operator

- Duration of the report cannot exceed one year.
- You can only select one operator at a time.

The report contains the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator</td>
<td>Logged in attendant operator’s name.</td>
</tr>
<tr>
<td>Logged In</td>
<td>Times the specified operator logged in on that day.</td>
</tr>
<tr>
<td>Logged Out</td>
<td>Times the specified operator logged out on that day.</td>
</tr>
<tr>
<td>Time Logged In</td>
<td>Duration of the logged in period.</td>
</tr>
<tr>
<td>Time Available</td>
<td>Amount of time in the logged in period that the operator was available.</td>
</tr>
<tr>
<td>Number of Calls</td>
<td>Number of calls handled during the logged in period.</td>
</tr>
<tr>
<td>Avg Call Duration</td>
<td>Average length of calls handled during the logged in period.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue</td>
<td>The Queue(s) for which the report is generated.</td>
</tr>
<tr>
<td>Total Queue Calls</td>
<td>The total number of incoming calls at the Queue.</td>
</tr>
<tr>
<td>Total Overflow In</td>
<td>The total number of calls overflowed from the Queue.</td>
</tr>
<tr>
<td>Overflow In</td>
<td>The number of calls overflowed into the Queue from other Queues during business hours.</td>
</tr>
<tr>
<td>Night Service In</td>
<td>The number of calls overflowed into the Queue during break hours.</td>
</tr>
<tr>
<td>Overflow out Time Limit</td>
<td>The number of calls that overflowed because the maximum call waiting time was exceeded.</td>
</tr>
<tr>
<td>Overflow out No Operators</td>
<td>The number of calls that overflowed because no attendant operator was logged into the queue.</td>
</tr>
<tr>
<td>Emergency</td>
<td>The number of calls that overflowed because the queue was in emergency mode.</td>
</tr>
<tr>
<td>Overflow out Destination Time Limit</td>
<td>The destination for calls overflowed for exceeding the maximum wait time.</td>
</tr>
<tr>
<td>Overflow out Destination No Operators</td>
<td>The destination for calls overflowed when no operator was logged into the queue.</td>
</tr>
<tr>
<td>Emergency</td>
<td>The destination for calls overflowed when the queue was in emergency mode.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>% In</td>
<td>The percentage of incoming calls that had overflowed from another queue.</td>
</tr>
<tr>
<td>% Out</td>
<td>The percentage of incoming calls that overflowed from the queue.</td>
</tr>
</tbody>
</table>
Example Cisco Unified Attendant Console Advanced Configuration

This appendix contains an example resilient Cisco Unified Attendant Console Advanced system configuration.

**Publisher:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example Value</th>
<th>For more information...</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSP application user</td>
<td>CUACAPUB01</td>
<td>See Creating and Assigning an Application User.</td>
</tr>
<tr>
<td>Machine Name</td>
<td>CUACAPUB01</td>
<td></td>
</tr>
<tr>
<td>CT Gateway</td>
<td>1600 - 1609</td>
<td>See Device Groups.</td>
</tr>
<tr>
<td>Service Device</td>
<td>1610 - 1619</td>
<td></td>
</tr>
<tr>
<td>Park Device</td>
<td>1620 - 1629</td>
<td></td>
</tr>
<tr>
<td>Queue DDI</td>
<td>1630 - 1639</td>
<td></td>
</tr>
</tbody>
</table>

**Subscriber**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSP application user</td>
<td>CUACASUB01</td>
<td>See Creating and Assigning an Application User.</td>
</tr>
<tr>
<td>Machine Name</td>
<td>CUACASUB01</td>
<td></td>
</tr>
<tr>
<td>CT Gateway</td>
<td>1650 - 1659</td>
<td>See Device Groups.</td>
</tr>
<tr>
<td>Service Device</td>
<td>1660 - 1669</td>
<td></td>
</tr>
<tr>
<td>Park Device</td>
<td>1670 - 1679</td>
<td></td>
</tr>
<tr>
<td>Queue DDI</td>
<td>1680 - 1689</td>
<td></td>
</tr>
</tbody>
</table>
Device Groups
For a description of how to define device groups and the devices in them, see System Device Management.
For a description of how to create queues and define queue DDIs, see Queue Management.

<table>
<thead>
<tr>
<th>Name</th>
<th>Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFAULT</td>
<td><strong>Primary (Publisher)</strong></td>
</tr>
<tr>
<td></td>
<td>CT Gateway 1600 - 1604</td>
</tr>
<tr>
<td></td>
<td>Service Device 1610 - 1614</td>
</tr>
<tr>
<td></td>
<td>Park Device 1620 - 1624</td>
</tr>
<tr>
<td></td>
<td>Queue DDI 1630 - 1634</td>
</tr>
<tr>
<td>DEVELOPMENT</td>
<td><strong>Primary (Publisher)</strong></td>
</tr>
<tr>
<td></td>
<td>CT Gateway 1605 - 1609</td>
</tr>
<tr>
<td></td>
<td>Service Device 1615 - 1619</td>
</tr>
<tr>
<td></td>
<td>Park Device 1625 - 1629</td>
</tr>
<tr>
<td></td>
<td>Queue DDI 1635 - 1639</td>
</tr>
</tbody>
</table>

Attendant Operators
For a description of how to create and configure attendant operators, see Operator Management.

<table>
<thead>
<tr>
<th>Name</th>
<th>Passphrase</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPERATOR1</td>
<td>cisco</td>
</tr>
<tr>
<td>TESTOP</td>
<td>&lt;BLANK&gt;</td>
</tr>
</tbody>
</table>

Attendant Queues

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Primary DDI (Publisher)</th>
<th>Secondary DDI (Subscriber)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BROADCAST</td>
<td>Broadcast</td>
<td>1630</td>
<td>1680</td>
</tr>
<tr>
<td>CONSOLE - FORCE</td>
<td>Forced delivery</td>
<td>1631</td>
<td>1681</td>
</tr>
</tbody>
</table>
Back-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
- Restoring Databases
- Backing-up Cryptographic Keys and Registries
- Restoring a Subscriber Server (applies only to resilient Cisco Unified Attendant Console Advanced installations)
- Licensing Your New Server

Note: The instructions in this appendix are for SQL Server 2008 databases. The procedures may vary slightly for other versions.

Back-up and Restoring Cisco Unified Attendant Console Advanced

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 8, “Configuring Cisco Unified Attendant Console”.
- 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.
- Automatically. This is described in Automatically Backing-up 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:

When the backup is complete, the following messages is displayed:

**Step 6** In the message, click **OK**.

**Step 7** Repeat steps 3 to 6 for **ATTLOG**.

Automatically Backing-up Databases

SQL enables you to create a *maintenance plan* that automatically backs-up specified databases.

The following procedure creates a maintenance plan for an automatic back up that runs according to a specific schedule; it overwrites the backup file created the previous day, and shrinks the database transaction logs. You should modify the settings to meet your specific requirements.

To create a maintenance plan do the following:

**Step 1** Start Microsoft SQL Server Management Studio and connect to the server.

**Step 2** In the Object Explorer, expand **Management**.

**Step 3** Right-click **Maintenance Plans** and select **New Maintenance Plan**.

**Step 4** Type a name for the Maintenance Plan and then click **OK**.

The new plan is created and listed in the design view in the right-hand half of the interface. The Maintenance Plan Tasks toolbox is displayed in the lower left-hand corner of the interface.

**Step 5** Optionally, type a plan **Description**.

**Step 6** Double-click **Subplan_1**.

**Step 7** In the Subplan Properties dialog box, enter a meaningful **Name** and **Description**, and click the **Schedule** calendar icon.

**Step 8** In the Job Schedule Properties dialog box, select or specify the following:
- A **Schedule type**
- The job **Frequency**
Back-up and Restoring Cisco Unified Attendant Console Advanced

Appendix D

Backing-up Databases

Backing-up Databases

- The **Daily frequency** (times) when the job must run.

**Note**

We strongly recommend that you schedule this task to run out of working hours.

**Step 9**

Click **OK**.

**Step 10**

In the Subplan Properties dialog box, click **OK**.

**Step 11**

Drag an **Execute T-SQL Statement Task** from the Maintenance Plan Tasks toolbox and drop it into the lower right-hand corner of the interface. You will use this task to shrink the transaction logs of both databases.

**Step 12**

Click the task and rename it as required.

**Step 13**

Right-click the task and choose **Edit**, then enter the following into the **T-SQL statement** field:

**Note**

For SQL 2014 databases, substitute the following for the lines in red:

- ALTER DATABASE ATTCFG SET RECOVERY SIMPLE
- ALTER DATABASE ATTLOG SET RECOVERY SIMPLE

Use ATTCFG

EXEC sp_dboption 'ATTCFG','trunc. log on chkpt.', 'true'
CHECKPOINT
DBCC SHRINKFILE (ATTCFG_log, 1,TRUNCATEONLY)

Use ATTLOG

EXEC sp_dboption 'ATTLOG','trunc. log on chkpt.', 'true'
CHECKPOINT
DBCC SHRINKFILE (ATTLOG_log, 1,TRUNCATEONLY)

**Step 14**

Click **OK**.

**Step 15**

Do the following for the configuration database (ATTCFG) and then repeat for the logging database (ATTLOG):

a. Drag a **Back Up Database Task** from the Maintenance Plan Tasks toolbox and drop it below the Execute T-SQL Statement Task.

b. Click the task and rename it as required.

c. Right-click the task and choose **Edit**.

d. We recommend applying the following settings:

- Set **Backup Type** to **Full**.
- In **Database(s)**, click the down-arrow and select ATTCFG or ATTLOG, as appropriate.
- In **Back up databases across one or more files**, enter a file path and name.

**Note**

If you save the 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**.
Restoring Databases

This section describes how to restore the server and databases for the following installations of Cisco Unified Attendant Console Advanced:

- Non-resilient installations
- The Publisher server on resilient installations. If you have to rebuild and restore your Publisher server, you will then need to reconnect it to your existing Subscriber server, as described in Reconnecting a Subscriber Server to a Restored Publisher Server. For instructions on how to restore a failed Subscriber server, see Restoring a Subscriber Server.

Preparing the Servers

Before you can restore the databases, you must prepare the server hardware and software, and install Cisco Unified Attendant Console Advanced.

Step 1  Install the Publisher, as described in Chapter 5, “Installing Cisco Unified Attendant Console Advanced Software”.

Step 2  Back-up the cryptographic keys and registries, as described in Backing-up Cryptographic Keys and Registries.

Step 3  Install the Subscriber, as described in 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:

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.
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 E, “Updating the Cisco Unified Attendant Console Advanced Server Host Name, SQL Server login name and password”.

If you are installing a Cisco Unified Attendant Console Advanced Publisher server, ensure that you select Publisher when prompted.

After installing the Cisco Unified Attendant Console Advanced software on your new server, you must license it, as described in Licensing Your New Server.

**Restoring the Databases**

When you have installed Cisco Unified Attendant Console Advanced you can restore your backed-up databases.

To restore the databases, do the following:

**Step 1** In Control Panel, open Administrative Tools, and then double-click **Services**.

**Step 2** Stop the following services:
- BLF Plug-in
- Cisco Unified Attendant LDAP Plug-in
- Cisco Unified Attendant Server

**Step 3** Restart the SQL Server (MSSQLSERVER) service. This will also restart the SQL Server Agent service, if it is running.

**Step 4** Start Microsoft SQL Server Management Studio and connect to the server.

**Step 5** In the Object Explorer, expand **Databases**.

**Step 6** Do the following for the configuration database (ATTCFG) and then repeat for the logging database (ATTLOG):

a. Right-click the appropriate database and choose **Tasks > Restore > Database**.

b. In the Restore Database dialog box, select the **General** page.

c. Under **Source for restore**, select **From device**.

d. Browse to the file at the **Backup location**.

e. Select the **Backup sets to restore**.

f. In the Restore Database dialog box, select the **Options** page.

g. Select **Overwrite the existing database (WITH REPLACE)**.

h. Click **OK**.

The database is restored. When the restore has completed successfully a message is displayed.

i. In the message, click **OK**.
Restoring Databases

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 E, “Updating the Cisco Unified Attendant Console Advanced Server Host Name, SQL Server login name and password”.

- If you are using the same System Devices (CT Gateway, Service, and Park Devices) and queue DDIs on the new or re-imaged server as were used with the backed-up server, you must access Cisco Unified Communications Manager and delete the associated Devices, CTI Route Points and Device Names before using the Cisco Unified Attendant Console Advanced Administration Configuration > Synchronize with CUCM function.

---

Reconnecting a Subscriber Server to a Restored Publisher Server

**Note**

This section applies only to resilient Cisco Unified Attendant Console Advanced installations where you have restored a failed Publisher Server. For how to rebuild and restore a failed Subscriber server, see Reconnecting a Subscriber Server.

To reconnect your existing Subscriber server to your restored Publisher server, do the following:

1. Uninstall the software on the Subscriber server.
2. Re-install the software on the Subscriber server.

**Note**

You must install the same version of software you were using before the failure. If you install a different version your database will have an incorrect schema and will be unable to accept replicated data from the Publisher.

3. Configure replication between the Publisher and Subscriber.

For more information on how to perform any of these steps, see Chapter 7, “Cisco Unified Attendant Console High Availability”.

---

Cisco Unified Attendant Console Advanced - Administration and Installation Guide

OL-29383-01
Backing-up Cryptographic Keys and Registries

Before installing the Subscriber you must back-up the Publisher’s cryptographic keys and registries, and copy them to the Subscriber, otherwise the latter will not function correctly.

Backing-up Using Attendant Administrator

You can use Cisco Unified Attendant Administration to back-up the Publisher’s cryptographic keys and registries. This is described in Export Crypto Key File. The backup-up key archive should be copied to Subscriber.

Manually Backing-up and Restoring Cryptographic Keys and Registries

To back-up the keys and registries manually:

Step 1
On the Publisher, use regedit to export the key:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Arc Solutions\Call Connect\Crypto

to a disk file.

Step 2
Note the folder name in the HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Arc Solutions\Call Connect\Crypto\Security\KeyFilePath registry value, and then copy the aesKey.dat file from that folder.

To restore the keys and registries to the Subscriber:

Step 1
Copy the disk file from Step 1 in the back-up procedure to the Subscriber machine, double-click the file on the Subscriber, and then respond to all the prompts to merge the exported keys into the Subscriber registry.

Step 2
Copy the aesKey.dat file from Step 2 in the back-up procedure to the same folder on the Subscriber machine that contained it on the Publisher.

You can now restore the Subscriber.

Restoring a Subscriber Server

Note
This section applies only to resilient Cisco Unified Attendant Console Advanced installations where the Subscriber server has failed.

If your Subscriber server fails and you have had to build a new one, do the following:

1. Prepare the Subscriber server hardware and software. For more information, see Chapter 3, “Hardware and Software Requirements”.

2. Install the Cisco Unified Attendant Console Advanced software on the Subscriber server. During installation, do the following:

...
Appendix D  Backing-up and Restoring Cisco Unified Attendant Console Advanced

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 the Cisco Unified Attendant Console Advanced Software.
Updating the Cisco Unified Attendant Console Advanced Server Host Name, SQL Server login name and password

This appendix describes how to update the Cisco Unified Attendant Console Advanced server host name and SQL Server connection details of an existing installation.

There are two utilities in the Cisco Unified Attendant Console Advanced server program files.

- Modify pre-existing installation, server host name: ServerChange.bat
- Modify SQL Server credentials used by Cisco Unified Attendant Console Advanced: SqlCfgChange.bat

Complete the following steps in entirety for each server that is modified. You must execute all of the following steps for a publisher, and then subscriber if using high availability. It is imperative that all changes be made in entirety to one server at a time.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>Standalone installs only:</strong> prepare the batch files.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>High Availability installs only:</strong> uninstall replication from both servers.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Set Cisco Unified Attendant Console Advanced and SQL Server Services startup type to <strong>Manual</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Modify Cisco Unified Attendant Console Advanced server host name and/or SQL Server login name and password.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Execute the appropriate batch file(s).</td>
</tr>
<tr>
<td>Step 6</td>
<td>Set Cisco Unified Attendant Console Advanced and SQL Server services startup type to <strong>Automatic</strong>.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Reinstall High Availability if required.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Restart Cisco Unified Attendant Console Advanced server(s).</td>
</tr>
</tbody>
</table>
Standalone Installs Only: Prepare the Batch Files

Edit the configuration files associated with the host name and SQL server credentials change utilities. To edit the configuration files:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Navigate to Program Files (x86)\Cisco\Utilities\Server and SQL Change Tool.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Use a text editor to open the relevant configuration file(s):</td>
</tr>
<tr>
<td></td>
<td>• Modify SQL login name and/or passphrase: SQLCfgChange.bat.</td>
</tr>
<tr>
<td></td>
<td>• Modify server hostname: ServerChange.bat.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Change the AllConnectedServers key to No.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Save and then close the file.</td>
</tr>
</tbody>
</table>

High Availability Installs Only: Uninstall Replication from Both Servers

High Availability must be uninstalled before implementing any changes and before executing the database update utilities. See Uninstalling Replication.

Set Cisco Unified Attendant Console Advanced and SQL Server Services Startup Type to Manual

1. Navigate to Control Panel, and then select Administrative Tools.
2. Select Services.
3. Stop the following services:
   - ActiveMQ
   - BLF Plug-in
   - Cisco Unified Attendant LDAP Plug-in (Primary server only)
   - Cisco Unified Attendant Server
   - Cisco Unified Attendant Presence Plug-in
4. Set the start-up type of the services listed above to Manual.
   a. Right-click the service name, and then select Properties.
   b. In the Properties dialog box, click the General tab, set the Startup type to Manual, and then click OK.

Modify Cisco Unified Attendant Console Advanced server host name and/or SQL Server login name and password

High Availability installs only: as previously noted, it is imperative that changes are made to one server at a time. Once the steps have been completed for the first server, follow the same steps for the second server. Implementing changes to both servers at the same time will break the solution.
Execute the Appropriate Batch Files

Follow the instruction relevant to the change being made to the Cisco Unified Attendant Console Advanced servers.

The order in which the batch files are executed is not important. If you want to modify the details associated with a publisher and subscriber, the order in which the changes are made is not important.

Modify SQL Login Name and/or Passphrase: SqlCfgChange.bat

To change the SQL Server user name and password, do the following:

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Double-click SqlCfgChange.bat. The SQL Server Connection page appears.</td>
</tr>
<tr>
<td>2</td>
<td>In User Name, type the new user name.</td>
</tr>
<tr>
<td>3</td>
<td>In Password, type a new password.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Confirm that the Server name matches the current server name.</td>
</tr>
<tr>
<td>5</td>
<td>Click Test Connection.</td>
</tr>
<tr>
<td>6</td>
<td>If the message Connected Successfully appears, click OK. Retype the password. If the message Connection Failed appears, retype the user name and password and try again.</td>
</tr>
<tr>
<td>7</td>
<td>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.</td>
</tr>
<tr>
<td>8</td>
<td>Click Finish.</td>
</tr>
</tbody>
</table>

Modify Server Hostname: ServerChange.bat

To change the server host name, do the following:

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Double-click ServerChange.bat. The SQL Server Connection page appears.</td>
</tr>
<tr>
<td>2</td>
<td>Type the new Server name, SQL username and password.</td>
</tr>
<tr>
<td>3</td>
<td>Click Test Connection.</td>
</tr>
<tr>
<td>4</td>
<td>If the message Connected Successfully appears, click OK. Retype SQL password. If the message Connection Failed appears, retype the user name and password and try again.</td>
</tr>
<tr>
<td>5</td>
<td>Click Next.</td>
</tr>
</tbody>
</table>
Appendix E  Updating the Cisco Unified Attendant Console Advanced Server Host Name, SQL Server login name and Host Machine Name

The Host Machine Name page appears, containing the Machine Name configured in the database and Host Name of your machine.

Step 6  Click Next.

The Installation Progress page appears. If a cross appears alongside any progress message it means that stage of the update has failed; you must run the ServerChange.bat file again using valid data. Details of any errors are displayed on the Errors tab.

Step 7  Click Finish.

Step 8  Launch SQL Server Management Studio and log in with SA account.

a. Click File > Open > File.

b. Navigate to and open \Program Files (x86)\Cisco\Utilities\Server and SQL Change Tool\SQLServerChange.sql.

c. Click Execute.

d. Exit SQL Management Studio after the script successfully executes.

Step 9  If you have a resilient system and have changed the Publisher host name, log in to the Subscriber server and use a text editor to open the C:\Apache\ActiveMQ\conf\credentials.properties file; change the line starting:

othernode=

to specify the new publisher host name. For example:

othernode=PAK-SZA-WIN2009

and then save the file.

If the Conversion Fails

The batch files log everything they do in the folder:

%programdata%\Cisco\CUACA\Server\Logging\DBW\.

If the conversion fails, please supply Cisco TAC support with a copy of this folder and the following files:

- The .bat and .xml files from the folder \<installation_folder>\Utility\Server and SQL Change Tool\.
- The Arc Solutions registry
- The databases
- The files CTI Server.exe.config and PresenceServer.exe.config from the CTI and Presence Server folders.
Set Cisco Unified Attendant Console Advanced and SQL Server services startup type to Automatic

After updating all affected servers, on each do the following:
1. Navigate to Control Panel, and then select Administrative Tools.
2. Select Services.
3. Set the start-up type of the following services to Automatic:
   - BLF Plug-in
   - ActiveMQ
   - Cisco Unified Attendant Server
   - Cisco Unified Presence Server
   - Cisco Unified Attendant LDAP Plug-in (Publisher Only)

Reinstall High Availability (If Required)

If leveraging high availability, install replication. See Installing Replication.

Restart Cisco Unified Attendant Console Advanced Server(s)

For changes to take effect, restart Cisco Unified Attendant Console Advanced server(s).
Performing CUCM Upgrades and Re-installing Cisco TSP

To perform a CUCM upgrade and re-install Cisco TSP, do the following:

Step 1: Launch Cisco TSP Media Driver Configuration and take note of the **Starting** and **Ending** ports.

Step 2: Launch Cisco TSP Configuration, and click **Configure**.

Step 3: Select the **General** tab and take note of the **Auto Update Information** settings.

Step 4: Select the **User** tab and take note of the application user ID and password.

Step 5: Select the CTI Manager tab and take note of the **Primary** and **Backup** CTI Manager locations.

Step 6: Take note of the configurations under the **Security** and **Advanced** tabs.

Step 7: Login to CUCM Administration, select **Application > Plug-ins**. Download the relevant Cisco TAPI client.

Step 8: Stop all CUAC Services.

Step 9: Uninstall Cisco TSP.

Step 10: Restart server.

Step 11: Login as a local administrator, then stop all CUACA Services.

Step 12: Navigate to **Program Files (x86 - if 64-bit)/Cisco/CTI Server/**. Delete the **Driver Instance** folder.

Step 13: Install Cisco TAPI client using the configuration from steps 1 through 6. If something is missed during the install, you can launch the configuration screens post install to modify.

Step 14: Restart server.
<table>
<thead>
<tr>
<th>A</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>access control</td>
<td>group, creating and assigning</td>
<td>4-1</td>
</tr>
<tr>
<td>access numbers</td>
<td>8-34</td>
<td></td>
</tr>
<tr>
<td>account locking</td>
<td>unlocking</td>
<td>8-37</td>
</tr>
<tr>
<td>Active MQ</td>
<td>service, checking</td>
<td>1-3</td>
</tr>
<tr>
<td>agents</td>
<td>(SQL Server replication)</td>
<td>7-3</td>
</tr>
<tr>
<td>antivirus software</td>
<td>3-5</td>
<td></td>
</tr>
<tr>
<td>application user</td>
<td>creating</td>
<td>4-2</td>
</tr>
<tr>
<td>archiving logs</td>
<td>6-21</td>
<td></td>
</tr>
<tr>
<td>audit server</td>
<td>connecting</td>
<td>6-15</td>
</tr>
<tr>
<td>AXL API</td>
<td>1-10</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>backing-up data</td>
<td>3-5</td>
<td></td>
</tr>
<tr>
<td>backup up and</td>
<td>restoring the server</td>
<td>D-1 to D-8</td>
</tr>
<tr>
<td>BLF subscription</td>
<td>number</td>
<td>8-15</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>call arrival</td>
<td>mode</td>
<td>8-35</td>
</tr>
<tr>
<td>Calling Search</td>
<td>Space (CSS)</td>
<td>8-20</td>
</tr>
<tr>
<td>call logging</td>
<td>database, purging</td>
<td>6-14</td>
</tr>
<tr>
<td>call parking</td>
<td>1-10</td>
<td></td>
</tr>
<tr>
<td>Cisco TSP,</td>
<td>uninstalling</td>
<td>A-3</td>
</tr>
<tr>
<td>Cisco Unified</td>
<td>Attendant BLF Plug-in</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified</td>
<td>Attendant CUPS Plug-in</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified</td>
<td>Attendant LDAP Plug-in</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attendant Console Advanced</td>
<td></td>
</tr>
<tr>
<td>configure</td>
<td>6-1 to 6-22, 8-1 to 8-2</td>
<td></td>
</tr>
<tr>
<td>example</td>
<td>configuration</td>
<td>C-1 to C-2</td>
</tr>
<tr>
<td>installing</td>
<td>5-1</td>
<td></td>
</tr>
<tr>
<td>logging</td>
<td>6-19</td>
<td></td>
</tr>
<tr>
<td>logging</td>
<td>redundancy and resilience</td>
<td>3-5</td>
</tr>
<tr>
<td>logging</td>
<td>6-19</td>
<td></td>
</tr>
<tr>
<td>logging</td>
<td>status</td>
<td>6-8</td>
</tr>
<tr>
<td>logging</td>
<td>6-20</td>
<td></td>
</tr>
<tr>
<td>logging</td>
<td>status</td>
<td>6-8</td>
</tr>
<tr>
<td>logging</td>
<td>6-20</td>
<td></td>
</tr>
<tr>
<td>logging</td>
<td>status</td>
<td>6-8</td>
</tr>
</tbody>
</table>
starting/stopping 6-6
status 6-8
Cisco Unified Communications Manager
  connection, setting-up and testing 6-9
  integration with Cisco Unified Attendant Console Advanced 1-7
  preparing 4-1 to 4-4
  synchronizing device configurations 8-22
Cisco Unified Presence (CUP)
  preparing 4-1
  server (CUPS)
    integration 1-11
Cisco Unified Replication 7-3 to 7-10
Cisco Unified Reporting B-1 to B-6
Citrix support 3-8
Client Matter Codes (CMC) 8-34
collecting logs 6-21
console client
  lockout 6-17
  login credentials 6-17
contacts
  exporting to CSV Files 8-11
  inserting and updating from CSV files 8-9
  uploading from CSV files 8-12
contacts database, synchronizing with source 8-5
credentials for console client login 6-17
cryptographic keys, backing-up and restoring D-7
CSV files of contacts, managing and uploading 8-12
CTI Manager 1-8
CUCM, see Cisco Unified Communications Manager

deployment checklist 2-1
device configuration, synchronizing with Cisco Unified Communications Manager 8-22
Device Resolution Manager (DRM) 1-8
directory
  connection, testing 8-4
  external, synchronization 8-2
  field mapping 8-6
  filtering during importing 8-8
  source, connecting 8-3
Directory BLF Rules 8-15
domains 6-16
.NET Framework, uninstalling A-2

E
E.164 numbers 8-15
emergency destination 8-28

F
firewall exceptions 5-6
  console client 5-11
  for replication 7-6
Forced Authorization Codes (FAC) 8-34
full CTI failure device 8-28

H
hardware and software requirements 3-1
home realm 6-16

I
importing
  operators 8-37
installing the software 5-1
iPlanet Netscape Directory 8-2
Index

J
Jabber support 3-8
JAWS scripts 5-12
Job Scheduler 8-10

L
licensing software 9-1
linking to SSO users 8-38
log archive 6-21
log collection 6-21
logging in 6-1
last log in information 6-3
logging off 6-3
logging servers and plug-ins, managing 6-18

M
mapping
directory information 8-8
marking text, managing 6-15
Microsoft Active Directory 8-2
Microsoft SQL Server
preparing 5-3
uninstalling A-2
Microsoft Windows Updates and Service Packs 3-9
Microsoft Windows Updates and Service Packs (on server) 3-4
music on hold (MoH) 1-11

N
network requirements 3-7
non-resilient installation 1-4

O
operator phone requirements 3-9
operator profiles, creating and configuring 8-37
operator queues, creating and configuring 8-25
operators, importing 8-37
out of hours routing
configuring 8-30
setting up queue 8-29

P
parking calls 1-10
passphrase 6-17
presence source management 8-1
publisher server 1-3
details, changing 6-11
purge database 6-14

Q
queue
out of hours routing 8-29
overflows 8-28
queue device groups 8-18
deleting 8-19

R
realms 6-16
recall timers 8-35
replication
installing 7-4
monitoring 7-8
reinitializing 7-7
report 7-10
uninstalling 7-7
validating 7-9
reports B-1 to B-6
report parameters B-2
resilience
inter-server communication link, checking 1-3
server 1-3
TAPI 1-11
rules (filters) for directory importing 8-8

S
scheduling contact insertion and updating 8-10
search filter (Find) 8-21
server
   backing up and restoring D-1 to D-8
   migrating E-1
   resilience 1-3
   updating the host name E-1
software requirements 3-1
SQL Server
   licensing 5-4
   replication 1-3, 7-3
SQL Server 2014, installing 5-3
subscriber server 1-3
   details, changing 6-11
synchronization errors 8-24
system reports B-1 to B-6

T
TAPI resilience 1-11
template device 8-20

V
VIOC role in operator profile 8-37
VMware server requirements 3-2