CONTENTS

Preface vii

chapter 1
Product Overview 1-1
Edition Feature Comparison 1-1
Core Languages 1-4
Server Resilience 1-4
Cisco Unified Attendant Console Integration with Cisco Unified Communications Manager 1-6
AXL API 1-6
Cisco Unified Communications Manager System Devices 1-6
Centralized Installations and Transcoding 1-7
TAPI Resilience 1-7
Music on Hold 1-7
Cisco Unified Presence Server Integration 1-8

chapter 2
Deployment Checklist 2-1

chapter 3
Hardware and Software Requirements 3-1
Server Requirements 3-1
Physical Server Hardware Requirements 3-1
Physical Server Software Requirements 3-2
VMware Server Requirements 3-3
VMware Guest Machine Requirements 3-4
VMware Software Requirements 3-4
Additional Server Considerations 3-4
SQL Server 2008 Limitations 3-4
SQL and Cisco Unified Attendant Console Server Resilience 3-5
Windows Updates and Service Packs 3-5
Data Backup 3-5
Server Redundancy 3-5
Antivirus Software 3-5
Network Requirements 3-6
Cisco Unified Attendant Console Client Requirements 3-6
PC Hardware Requirements 3-6
PC Software Requirements 3-7
Contents

appendix A

Uninstalling Cisco Unified Attendant Console 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
  Overflowed Calls By Date System Report  B-5

appendix C

Creating an Attendant Application User for Cisco Unified Communications Manager 7.x  C-1
  Creating an Application User  C-1
  Creating a User Group and Assigning Roles to it  C-2
  Adding the Application User to the User Group  C-2
  Adding the Application User to the Standard CCM Super Users Group  C-3

appendix D

Installing and Configuring the Cisco TSP for Cisco Unified Communications Manager 7.x  D-1
  Downloading and Installing the TSP  D-1
  Configuring the TSP  D-2
  Installing the Cisco TAPI Wave Driver  D-3

appendix E

Example Cisco Unified Attendant Console Configuration  E-1

appendix F

Upgrading Cisco Unified Attendant Console  F-1
  Upgrading Cisco Unified Attendant Console Server  F-3
Preface

This document describes how to install and configure Cisco Unified Attendant Console Premium Edition (CUACPE) – its databases, connections to Cisco Unified Communications Manager, and its system and user settings – using the Cisco Unified Attendant Admin web application.

Audience

The document is intended for:

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

This document assumes that you have knowledge of:

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

Organization

This guide includes the following sections:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Product Overview”</td>
<td>An overview of Cisco Unified Attendant Console, 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, cross-referenced to the relevant procedures in this guide.</td>
</tr>
</tbody>
</table>
Preface

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>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A non-quoted set of characters. Do not use quotation marks around the string.</td>
</tr>
<tr>
<td><strong>courier</strong> font</td>
<td>Terminal sessions and information the system displays appear in <strong>courier</strong> font.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Non-printing characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>
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 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 and Cisco Unified Communications Manager work together, see Cisco Unified Attendant Console Integration with Cisco Unified Communications Manager, page 1-6. Cisco Unified Attendant Console 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 server monitors extensions within Cisco Unified Communications Manager and routes the calls to the Cisco Unified Attendant Console clients: the attendant console applications. Calls from Cisco Unified Communications Manager enter Cisco Unified Attendant Console through Cisco Unified Communications Manager Computer Telephony Integration (CTI) Route Point devices that 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 Admin to communicate with both Cisco Unified Communications Manager, to create the required system devices, and with the Cisco Unified Attendant Console server, to configure the system parameters. Cisco Unified Attendant Console system parameters, user directory and call record logs are all stored in SQL databases on the Cisco Unified Attendant Console server.

Edition Feature Comparison

Cisco Unified Attendant Console has the following basic features:

- Call queuing engine
- Busy Lamp Field (BLF)
- Directory search capabilities that are integrated into the Cisco Unified Communications Manager directory
- Blind and consultative transfer to enterprise users

Cisco Unified Attendant Console is available in the following Editions, which differ in scale and functionality:

- Department—for team-based answering functions within large enterprises, with support for up to two operators per department and five departments per server.
- Business—for mid-sized businesses, with support for up to twelve operator clients and up to 500 Cisco Unified IP Phone users per attendant console system.
- Enterprise—for larger enterprises, with support for up to 40 operator clients and full Cisco Unified Communications Manager End User directory support.

- Premium—for larger enterprises, with support for up to 50 operator clients and up to 100,000 directory entries per attendant console system. The Premium Edition also includes server resilience and the option to use the following directory sources:
  - Active Directory 2008 R1/R2
  - iPlanet Netscape 5.0
  - iPlanet Netscape 5.1

Note: You cannot upgrade directly from one Edition of Cisco Unified Attendant Console to another: a full re-installation and a new license are required.

The table below summarizes the features of the Cisco Unified Attendant Console Editions:

Legend: ✓ = Supported, ✗ = Unsupported.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Cisco Unified Attendant Console Edition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Department</td>
</tr>
<tr>
<td>Installation</td>
<td>Web and Wizard</td>
</tr>
<tr>
<td>Configuration</td>
<td>Browser</td>
</tr>
<tr>
<td><strong>Queue Features</strong></td>
<td></td>
</tr>
<tr>
<td>Console queues supported</td>
<td>1 per instance (5 instances per server)</td>
</tr>
<tr>
<td>Configurable queue names and priority</td>
<td>✗</td>
</tr>
<tr>
<td>Show all calls in all queues option</td>
<td>✗</td>
</tr>
<tr>
<td>Configurable forced delivery timer</td>
<td>✓</td>
</tr>
<tr>
<td>Queue salutations</td>
<td>✗</td>
</tr>
<tr>
<td>Show &amp; pick calls from each queue</td>
<td>✓</td>
</tr>
<tr>
<td>Queue wait time overflow</td>
<td>✗</td>
</tr>
<tr>
<td>Queue limit overflow (number of calls)</td>
<td>✓</td>
</tr>
<tr>
<td>Operator overflow (no operators)</td>
<td>✓</td>
</tr>
<tr>
<td>Queue overflow destinations supported</td>
<td>✓</td>
</tr>
<tr>
<td>Music in queue</td>
<td>✗</td>
</tr>
<tr>
<td>Operator handset ringing</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Service Options</strong></td>
<td></td>
</tr>
<tr>
<td>Emergency mode switch</td>
<td>✗</td>
</tr>
<tr>
<td>Emergency mode destination</td>
<td>✗</td>
</tr>
<tr>
<td>Night service switch</td>
<td>✗</td>
</tr>
<tr>
<td>Night service hours/timing</td>
<td>✗</td>
</tr>
<tr>
<td>Night service destination</td>
<td>✗</td>
</tr>
<tr>
<td><strong>Directory Features</strong></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Cisco Unified Attendant Console Edition</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Department</td>
</tr>
<tr>
<td>Directory size supported</td>
<td>150 per instance (5 instances per server)</td>
</tr>
<tr>
<td>Search fields</td>
<td>3</td>
</tr>
<tr>
<td>Mobile number support</td>
<td>✓</td>
</tr>
<tr>
<td>Directory source</td>
<td>Cisco Unified Communications Manager (CUCM)</td>
</tr>
<tr>
<td>Personal directory group support</td>
<td>✓</td>
</tr>
<tr>
<td>Speed dials</td>
<td>✓</td>
</tr>
<tr>
<td>Alternative number search (hotkey)</td>
<td>✓</td>
</tr>
<tr>
<td>AND searching</td>
<td>✓</td>
</tr>
<tr>
<td>Alternate contacts search</td>
<td>✗</td>
</tr>
<tr>
<td>Cross-tab searching</td>
<td>✗</td>
</tr>
<tr>
<td>Notes against person</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Presence/Status Features</strong></td>
<td></td>
</tr>
<tr>
<td>Busy Lamp Fields (BLF)/Phone status supported</td>
<td>✓</td>
</tr>
<tr>
<td>Presence integration with Cisco Unified Presence (CUP)</td>
<td>✓</td>
</tr>
<tr>
<td>Presence integration with Microsoft OCS</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Telephony Features</strong></td>
<td></td>
</tr>
<tr>
<td>Transfer reversion (call recall)</td>
<td>✓</td>
</tr>
<tr>
<td>Hold recall</td>
<td>✓</td>
</tr>
<tr>
<td>Call toggle</td>
<td>✓</td>
</tr>
<tr>
<td>Camp on</td>
<td>✗</td>
</tr>
<tr>
<td>Call hold with notes</td>
<td>✗</td>
</tr>
<tr>
<td>Undirected call park (finds first slot)</td>
<td>✓</td>
</tr>
<tr>
<td>Directed call park (to specific park location)</td>
<td>✓</td>
</tr>
<tr>
<td>Call hold</td>
<td>✓</td>
</tr>
<tr>
<td>Park recall</td>
<td>✓</td>
</tr>
<tr>
<td>Transfer</td>
<td>✓</td>
</tr>
<tr>
<td>Conference</td>
<td>✓</td>
</tr>
<tr>
<td><strong>System Features</strong></td>
<td></td>
</tr>
<tr>
<td>Number of concurrent client logins</td>
<td>2 per instance (5 instances per server)</td>
</tr>
<tr>
<td>Keyboard driven</td>
<td>✓</td>
</tr>
<tr>
<td>System logging</td>
<td>✓</td>
</tr>
</tbody>
</table>
1 Product Overview

Edition Feature Comparison

Legend: ✓ = Supported, ✗ = Unsupported.


Core Languages

Cisco Unified Attendant Console supports English only.

Server Resilience


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

- Publisher—responsible for normal activity. All operators are logged onto the Publisher for configuration and call routing. The Publisher includes the LDAP server.
- Subscriber—the passive, secondary server (hot-stand-by backup). The information from the publisher server is replicated onto this server. If the Publisher fails, the Subscriber takes over. You cannot change the configuration through the Subscriber server.

The following are installed on both server machines:

- BLF server. Responsible for all BLF information and call activity
- Cisco Unified Presence server. Responsible for presence information. For more information, see Cisco Unified Presence Server Integration, page 1-8.

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. 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.

Note

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

1. Log in to Cisco Unified Attendant Console Web Admin 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 Web Admin to confirm that the Inter Server Communication Status is **Normal**.

You can install Cisco Unified Attendant Console Premium Edition as a single-server standalone system, with no resilience (as you do with the other Cisco Unified Attendant Console editions). If you install Cisco Unified Attendant Console Premium Edition as a standalone system, you cannot convert it to the resilient version later without performing a new, clean installation. When you install Cisco Unified Attendant Console Premium Edition in this mode, SQL Express Edition is automatically installed on the server, if no SQL Server is detected.

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 type. The Publisher requires at least SQL Server Standard to be installed, while the Subscriber can use SQL Express (which is installed when you install Cisco Unified Attendant Console Premium Edition).

**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 Premium Edition server on the Publisher server and the secondary Cisco Unified Attendant Console Premium Edition server on the Subscriber server connect to different CTI Managers (Cisco Unified Communications Manager nodes) within the same Cisco Unified Communications Manager cluster. If the Cisco Unified Communications Manager node used by the primary Cisco Unified Attendant Console Premium Edition server fails, another Cisco Unified Communications Manager takes over and the primary Cisco Unified Attendant Console Premium Edition 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 Admin (partial failover).
- TSP failure.
- Database failure.
- Cisco Unified Attendant Console server failure (or server shut down, or failure of the communication channel with the primary Cisco Unified Attendant Console server).
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 Premium Edition server on the Publisher server continues running because the TAPI-based CT Link continues working.

Cisco Unified Attendant Console Integration with Cisco Unified Communications Manager

Cisco Unified Attendant Console V9.1.1 is compatible with Cisco Unified Communications Manager versions 7.1(5) to 9.1(1).

AXL API

Cisco Unified Attendant Admin and Cisco Unified Communications Manager communicate via the AVVID XML Layer (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.
- Computer Telephony Integration (CTI) Route Points—virtual devices that can receive multiple, simultaneous calls for application-controlled redirection. They cannot terminate (answer) calls.

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

Cisco Unified Communications Manager System Devices

Cisco Unified Communications Manager uses the following system devices:

- Queue DDI (Direct Dial In)—the number dialed to route calls into a queue. Each DDI is configured on Cisco Unified Communications Manager as a CTI Route Point, and any call intended for this queue must be directed to this port, either directly or through a translation pattern.
- CT Gateway Devices—CTI Ports that are created by the Admin application when synchronized with Cisco Unified Communications Manager; they queue calls awaiting distribution to Cisco Unified Attendant Console.
- 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 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 the console attendants they are situated on the Cisco Unified Attendant Console server and require an additional range of DNs.
Centralized Installations and Transcoding

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

In Cisco Unified Communications Manager Release 7.1 and earlier, TAPI wave-enabled CTI Ports are needed for the Cisco Unified Attendant Console system to work correctly. These ports do not support the G729 codec for a connected call. Therefore, in a centralized environment where the G729 codec is being used across WAN links, a transcoder must be installed wherever the Cisco Unified Attendant Console server is located. This means that when a call crosses the WAN link to an attendant’s IP Phone as a G729 call, during any subsequent call transfer, hold or park, Cisco Unified Communications Manager changes the codec to G711 while the call is connected to the Service Queue or Call Park Device CTI Ports.

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

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

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

Note
If you start using a different Cisco Unified Communications Manager Release, access the CUCM Connectivity option and use it to validate and, if necessary, change the media driver, as described in CUCM Connectivity, page 6-13.

TAPI Resilience

Cisco Unified Communications Manager enables a Telephony/TAPI Service Provider (TSP) client to communicate with a primary and backup CTI Manager to receive CTI information. This allows the Cisco Unified Attendant Console 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 supports Music on Hold (MoH) from Cisco Unified Communications Manager. Music on hold is used in the following situations:

- When an operator holds a call
- During a blind transfer
- During a re-established transfer
- When Call Arrival Mode* is set to Hold Queued Calls
* Cisco Unified Communications Manager 8.0(3) and later enables you to configure a Queue with Call Arrival Mode to **Hold Queued Calls when it arrives on the CTI Port**. This function places calls on hold so that Music on Hold can be played to the caller while they wait for an operator to answer. **If you use this mode the call is charged from the time that it is answered and put on hold on the CT Gateway.**

**Cisco Unified Presence Server Integration**

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

Cisco Unified Attendant Console can display information extracted from the Cisco Unified Presence Server from Cisco Unified Communications Manager. Cisco Unified Attendant Console V9.1.1 is compatible with Cisco Unified Presence Server versions 7.1(5) to 9.1(1). The integration is managed via the Cisco Unified Attendant CUP Plug-in directly to the Cisco Unified Attendant Admin. Cisco Unified Attendant Admin uses SIP SIMPLE to communicate with the Cisco Unified Presence server. Changes to the CUP Plug-in service are managed in real-time: you do not have to stop and restart the CUP Plug-in service for the changes to take effect.
Deployment Checklist

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

Note: If you are upgrading an existing Cisco Unified Attendant Console installation, see Appendix F, “Upgrading Cisco Unified Attendant Console”.

To install Cisco Unified Attendant Console 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 you are installing. For more information, see Cisco Unified Attendant Console Integration with Cisco Unified Communications Manager, page 1-6.

2. Determine whether the Cisco Unified Attendant Console 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. For more information, see:
   - Physical Server Hardware Requirements, page 3-1
   - VMware Server Requirements, page 3-3

3. Ensure that you have the correct versions of operating system and SQL database required by the Cisco Unified Attendant Console server and client. For more information, see:
   - Physical Server Software Requirements, page 3-2
   - Additional Server Considerations, page 3-4
   - PC Software Requirements, page 3-7

4. Configure Cisco Unified Communications Manager so that it is ready for Cisco Unified Attendant Console 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 software. For more information, see Chapter 5, “Installing Cisco Unified Attendant Console Software”.

6. Use Cisco Unified Attendant Admin to configure the Cisco Unified Attendant Console server. For more information, see Chapter 6, “Configuring and Licensing Cisco Unified Attendant Console Server”.

7. Install the Cisco Unified Attendant Console client. For more Information, see Installing Cisco Unified Attendant Console Client, page 5-10.
CHAPTER 3

Hardware and Software Requirements

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

Server Requirements

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

- Physical server, with the requirements shown below.
- VMware environment compliant with Cisco’s Specification-Based Hardware Support program. For details of the requirements, see VMware Server Requirements, page 3-3.

Physical Server Hardware Requirements

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

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

Note

The following:

- NIC teaming is not supported.
- Cisco Unified Attendant Console server is not supported in a production environment if running on a desktop PC.
- If you plan to implement Cisco Unified Attendant Console server resilience, you must ensure that the date time and time zone on your Publisher and Subscriber servers are synchronized. Both servers must be in the same time zone to ensure that any daylight-saving time changes occur simultaneously. If they are not in the same time zone, the operator console will be unable to automatically reconnect to the Publisher when it recovers from failure.
Physical Server Software Requirements

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

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

**Note**

- Cisco Unified Attendant Console server does not run under any version of Windows Server 2003.
- For non-English characters, the relevant language pack for the locale must be installed.
- Internet Information Service (IIS) 6.0 or later, with the Static Content role service added.

**Note**

- To install IIS on a system with Windows Server already installed, see Adding IIS to Installed Operating System, page 3-3.
- ASP.NET
- .Net Framework 3.5 SP1
- One of the following databases:
  - Microsoft SQL Server 2008 Express, Standard or Enterprise (32-bit or 64-bit)
  - Microsoft SQL Server 2008 R2 Express, Standard or Enterprise (32-bit or 64-bit)

**Note**

- No versions of Microsoft SQL Server 2005 are supported.
- Cisco Unified Attendant Console server does not support the Cisco Media Convergence Server (MCS) version of Windows Server.
- If the Cisco Unified Attendant Console server installer does not detect a supported version of Microsoft SQL Server, it will automatically install Microsoft SQL Server 2008 Express.
- If the Cisco Unified Attendant Console server installer detects Microsoft SQL Server 2005 Express, it automatically upgrades it to Microsoft SQL Server 2008 Express.
• If you are installing Microsoft SQL yourself, you must install it locally on the Cisco Unified Attendant Console server. Cisco Unified Attendant Console does not support the use of external SQL Servers.

• **IMPORTANT:** If you plan to implement Cisco Unified Attendant Console server resilience, you must use Microsoft SQL Server Standard or Enterprise (not Express) on the Publisher server. You can use Microsoft SQL Server Express, Standard or Enterprise on the Subscriber server. Furthermore, the Publisher and Subscriber servers must use the *same* version of Microsoft SQL Server: both must use 2005 or both must use 2008. For guidance on which SQL edition to use, see Additional Server Considerations, page 3-4.

**Adding IIS to Installed Operating System**

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

---

**Step 1** Run Server Manager, click **Roles**, and then click **Add** to use the Wizard to install Web Server (IIS).

**Step 2** Add the Required Features.

**Step 3** Select and Add the following Role Services:
- ASP.Net
- .NET Extensibility
- ISAPI Extensions
- ISAPI Filters
- Server Side Includes
- Static Content

**Step 4** Click **Install**.

---

**VMware Server Requirements**

In a production environment, Cisco Unified Attendant Console server is supported on VMware ESXi 4.x or 5.x running on a host machine that is compliant with Cisco’s Specifications-Based Hardware Support program (described at [http://docwiki.cisco.com/wiki/Specification-Based_Hardware_Support](http://docwiki.cisco.com/wiki/Specification-Based_Hardware_Support)).

**Note**

The following:
- Cisco Unified Attendant Console server is *not* supported in HyperV or any other virtualization products other than VMware.
- Cisco Unified Attendant Console *does not* run on a copy (clone) of a virtual machine.
VMware Guest Machine Requirements

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

- 1x vCPU unrestricted
- 4 GB RAM
- 40 GB of available hard disk space

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

VMware Software Requirements

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

- Windows Server 2008 R1 (32-bit)
- Windows Server 2008 R2 (64-bit)

Additional Server Considerations

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

SQL Server 2008 Limitations

Microsoft SQL Server 2008 Express has the following limitations:

- Can access only a single CPU
- Uses only 1 GB of RAM
- Has a maximum database size of 4 GB
- Cannot support server resilience

You should consider using Microsoft SQL Server Standard or Enterprise if you expect your Cisco Unified Attendant Console 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 server resilience

If a Cisco Unified Attendant Console system outgrows Microsoft SQL Server 2008 Express, you can upgrade the database to Microsoft SQL Server Standard or Enterprise. Multiple SQL databases are not supported.
SQL and Cisco Unified Attendant Console Server Resilience

Cisco Unified Attendant Console server resilience uses SQL replication, which is not available in Microsoft SQL Server Express. Therefore, if you plan to implement server resilience, you must use Microsoft SQL Server 2008 Standard or Enterprise on the Publisher server. The Subscriber server can use Microsoft SQL Server Express, Standard or Enterprise, depending on the size of your Cisco Unified Attendant Console deployment. The Publisher and Subscriber servers can be part of a Microsoft Domain, so long as they can access each other by hostname.

Note

The Publisher and Subscriber servers must use the same version of Microsoft SQL Server: 2005 or 2008. For example:

- Supported: SQL Server 2008 Standard on the Publisher and SQL Server 2008 Express on the Subscriber
- Not supported: SQL Server 2008 Standard on the Publisher and SQL Server 2005 Express on the Subscriber

Windows Updates and Service Packs

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

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

Data Backup

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

Server Redundancy

We strongly recommended that you configure your Cisco Unified Attendant Console 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

Cisco Unified Attendant Console server supports many antivirus products. You can find guidelines on antivirus software at:
The files in certain folders are constantly being accessed by the Cisco Unified Attendant Console software. Consequently, your antivirus 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>
</tbody>
</table>

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

**Network Requirements**

For Cisco Unified Attendant Console to run across a network:

- The network must support TCP/IP.
- Cisco Unified Attendant Console web administration 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 server with a static IP address.

**Cisco Unified Attendant Console Client Requirements**

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

**PC Hardware Requirements**

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

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

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

- Microsoft Windows XP Professional Service Pack 3
- Microsoft Windows Vista Professional 32-bit
- Microsoft Windows Vista Professional 64-bit (using WoW64 emulation)
- Microsoft Windows 7 32-bit
- Microsoft Windows 7 64-bit (using WoW64 emulation)

Windows Updates and Service Packs

Cisco Unified Attendant Console client supports the application of all Microsoft Windows Updates and Service Packs. Java auto-updates are not supported because they sometimes fail, rendering the system unusable.

Operator Phone Requirements

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

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

Not the following:

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

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

**Note**

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

This chapter describes how to set up Cisco Unified Communications Manager Releases 8.x and 9.x. If you have Cisco Unified Communications Manager 7.x, set it up according to the instructions in Appendix C, “Creating an Attendant Application User for Cisco Unified Communications Manager 7.x”

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

This chapter describes the following:

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

Creating a User Group

If you are using Cisco Unified Communications Manager 8.x you must create a User Group. If you are using Cisco Unified Communications Manager 9.x you must create an Access Control Group, as described in Creating an Access Control Group, page 4-2.

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

**Step 1**

Log into Cisco Unified Communications Manager Administration.
Creating an Access Control Group

If you are using Cisco Unified Communications Manager 9.x you must create an Access Control Group. If you are using Cisco Unified Communications Manager 8.x you must create a User Group, as described in Creating a User Group, page 4-1.

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

Step 1  Use your internet browser to access Cisco Unified CM Administration, and then log in.
Step 2  Choose User Management > User Settings > Access Control Group.
Step 3  Click Add New to create a new Access Control Group.
Step 4  Type a Name for the new Access Control Group.
Step 5  Click Save to save the Access Control Group.
Step 6  Assign roles to the user group, as described in Assigning Roles to a User Group or Access Control Group.

Assigning Roles to a User Group or Access Control Group

To add the roles to a User Group or Access Control Group required to enable the Cisco Unified Attendant Console 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 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
Creating and Assigning an Application User

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

Note
If you are installing a resilient system, each Cisco Unified Attendant Console server (Publisher and Subscriber) needs to have a different Application User with a different number plan for the CTI ports.

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

To create and assign an Application User:

Step 1 Log into Cisco Unified Communications Manager Administration.
Step 2 Choose User Management > Application User.
Step 3 Click Add New.
Step 4 Enter information in the following fields:
  - User ID (a name of your choice)
  - Password
  - Confirm Password (this must match the Password)
Step 5 If you are installing against Cisco Unified Communications Manager 8.x, scroll down to the Permissions Information section and click Add to User Group.
If you are installing against Cisco Unified Communications Manager 9.x, scroll down to the Permissions Information section and click Add to Access Control Group.
Step 6 Find the User Group or Access Control Group you created in the previous section and select it.
Step 7 Select Standard CCM Super Users.
Step 8 Click Add Selected.
Step 9 Click Save to save the Application User.

Configuring Access to Cisco Unified Presence Server

Cisco Unified Attendant Console is capable of integrating with Cisco Unified Presence server to display real-time presence status within the Cisco Unified Attendant Console directory.
To configure this integration, you must add the address of the Cisco Unified Attendant Console server to the firewall information on the Cisco Unified Presence server. To add the address, do the following:

**Step 1**
Use your internet browser to access Cisco Unified Presence Administration, and then choose **System > Security >Incoming ACL**.

The **Find and List Allowed Incoming Hosts** page is displayed.

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

**Step 3**
Under **Incoming ACL Information**, type a **Description** of the address, and an **IP Address Pattern**.

**Step 4**
Click **Save**.
CHAPTER 5

Installing Cisco Unified Attendant Console Software

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

1. Disable Microsoft User Account Control, as described in Disabling UAC, page 5-2.
2. Prepare SQL, if applicable, as described in Preparing SQL, page 5-2.
3. Download the Cisco Unified Attendant Console server software, as described in Obtaining Cisco Unified Attendant Console Software, page 5-4.
4. Install the Cisco Unified Attendant Console server software, as described in Installing Cisco Unified Attendant Console Server, page 5-5.
5. Install the Cisco Unified Attendant Console client software, as described in Installing Cisco Unified Attendant Console Client, page 5-10.

For how to license and configure the software, see Licensing Cisco Unified Attendant Console Software, page 6-4.

For how to uninstall the Cisco Unified Attendant Console server and its associated applications, see Appendix A, “Uninstalling Cisco Unified Attendant Console Server”.

For how to upgrade your Cisco Unified Attendant Console server and client, see Appendix F, “Upgrading Cisco Unified Attendant Console”.

The following:

- The instructions in the section refer to systems installed on Microsoft Windows Server 2008. If you are not using this, please perform the equivalent steps for your operating system.
- IIS must be installed and activated before installing Cisco Unified Attendant Console. For more information, see Physical Server Software Requirements, page 3-2.
- If you have a Microsoft Windows network that uses DHCP, you must allocate a static IP address to the Cisco Unified Attendant Console server machine.
- Access to the Cisco Unified Attendant Console server is not supported at any time via Remote Desktop (RDP), Terminal Services (TS) or any other session-based application. These applications can cause TAPI/TSP and Wave Driver instability. Only local or VNC connection is supported. For more information, see http://support.microsoft.com/kb/308405.
Disabling UAC

Cisco Unified Attendant Console server and Cisco Unified Attendant Console client will neither install nor run correctly under Windows 2008 Server, Windows Vista, or Windows 7 with Windows User Account Control (UAC) enabled. For this reason you must disable UAC on the client and server computers (in resilient installations, both the Publisher and Subscriber) before installing the software and keep it disabled while the software is running.

Note
The exact steps to do this vary between Windows versions.

To disable UAC:

Step 1 Log into the server machine with local administrator rights.
Step 2 In Control Panel, open User Accounts.
Step 3 Click Turn User Account Control on or off (in Windows 7, click Change User Account Control Settings).
Step 4 De-select Use User Account Control (UAC) to help protect your computer (in Windows 7, move the User Account Control Settings slider to Never notify), then click OK.
Step 5 Restart your machine for the change to take affect.

Preparing SQL

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

However, if you are installing a resilient Cisco Unified Attendant Console Premium Edition system (for more information, see Server Resilience, page 1-4), the Publisher server requires either SQL Server Standard or Enterprise edition to be installed: SQL Server Express is inadequate. Furthermore, if you have more than ten operators, you should also install SQL Server Standard or Enterprise edition on the Subscriber server.

Note
The instructions in this section refer to using SQL Server 2008 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 server. Cisco Unified Attendant Console does not support external SQL Servers.

To install SQL Server:

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

Preparing SQL

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

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

The standard setup support rules are listed.

Step 4 Click Next.

Step 5 Enter the product key, then click Next.

Step 6 Accept the license terms, then click Next.

Step 7 Install the Setup Support Files.

Step 8 In the Setup Support Rules page, select All Features With Defaults, and then click Next.

Step 9 In the Feature Selection page, select:

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

Then click Next.

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

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

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

- SQL Server Agent runs under the NT Authority\System account.
  Set the Startup Type to Automatic.
- SQL Server Database Engine runs under the NT Authority\Network Services account.
  Set the Startup Type to Automatic.

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

Step 13 In Database Engine Configuration page:

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

Then click Next.

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

Step 15 In the Installation Rules page, click Next.

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

Step 17 When the setup process is complete, click Next.
Obtaining Cisco Unified Attendant Console Software

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

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

Evaluating Cisco Unified Attendant Console Software

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

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

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

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

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

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

Before you can install the Cisco Unified Attendant Console software, you must download it as described in Obtaining Cisco Unified Attendant Console Software, page 5-4.

Resilient Installation Prerequisites

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

Before installing a resilient system, do the following:

1. Ensure that the Console Client, Publisher and Subscriber machines are accessible using their hostname or NetBIOS name, and that these can be resolved to the correct IP Address. You can add the servers to a Windows domain if you want.
2. Log into the Publisher machine.
3. Ensure that the machine date, time and time zone are correct.
4. If you have a firewall on the Publisher server, configure Firewall Exceptions for:
   - Windows Management Instrumentation (WMI)
   - Distributed Transaction Coordinator (MSDTC)
   - Port 1433 (used by the SQL Server)
   - Port 1859 (used for communication between the Cisco Unified Attendant Console client and server)
   - Port 1864 (used by the BLF Plug-in)
   - Ports 61616 and 61618, to enable messages to pass between the servers
5. Install the Cisco Unified Attendant Console server on the Publisher, as described in Installation Procedure, page 5-7.

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:
   - Windows Management Instrumentation (WMI)
   - Distributed Transaction Coordinator (MSDTC)
   - Port 1433 (used by the SQL Server)
   - Port 1859 (used for communication between the Cisco Unified Attendant Console client and server)
   - Port 1864 (used by the BLF Plug-in)
   - Ports 61616 and 61618, to enable messages to pass between the servers.

9. Install the Cisco Unified Attendant Console server on the Subscriber, as described in Installation Procedure, page 5-7.

The following:

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

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

To install a Cisco Unified Attendant Console server:

1. Log in to the machine hosting the server, using a login with local administrator rights.
2. Browse to the folder where the downloaded installation files are saved.
3. Double-click the setup program.

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

If they are not already installed, all required third-party applications are now installed, including the Microsoft .NET Framework 3.5, and a Microsoft SQL Server (Microsoft SQL Server Express gets installed automatically). Any such installations may take several minutes. You are prompted to restart your computer afterwards.

4. In the Wizard welcome screen, click Next.
5. In the Registration Information screen, type or accept the license holder Name and Company Name, and then click Next.
6. In the SQL Server Login Information screen, type the SQL Server Username (default is sa) and Password (default is Z1ppyf0rever), then click Next.

Note

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

The Installation Mode screen is displayed.

7. To install a standalone system, do the following:
   a. In the Installation Mode screen, click Standalone Solution.
   b. Click Yes to confirm that you want to continue.
   c. In the Server Information screen, type the Cisco Unified Attendant Server Machine Name / IP Address onto which you are installing the software, and then click Next.
   d. Continue from Step 10.

To install a resilient system, do the following:

a. In the Installation Mode screen, click Resilient Solution.

b. In the Resilient Server Mode screen, click either:
   - Publisher Server, to install the Publisher server, then continue from Step 8.
   - Subscriber Server, to install the Subscriber server.

c. This step applies only when you are installing onto the Subscriber server.

To install a resilient system, do the following:

a. In the Server Information screen, type the Cisco Unified Attendant Server Machine Name / IP Address onto which you are installing the software, and then click Next.

b. In the Publisher SQL Server Information screen, enter the following information about the SQL Server installed on the Publisher machine that you want to communicate with the Subscriber server you are installing:
- **Server Name** — the machine hosting the Publisher
- **Username** — the SQL Server user name (default is sa)
- **Password** — the SQL Server password

and then click **Next**.

If the servers are unable to communicate, verify that the Windows firewall is either off or configured as described in step 4 on page 5-5.

**Step 8**  
In the **Server Information** screen, type the Cisco Unified Attendant Console **Server Machine Name** onto which you are installing the software, and then click **Next**.

**Step 9**  
To install a Publisher server, continue from **Step 10**.

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 10**  
In the Cisco Unified Communications Manager (CUCM) connection details screen, type the Cisco Unified Communications Manager machine **IP Address**, your **CUCM Application User ID** and **Password**, and then click **Next**.

**Note**  
The Application User account specified by the User ID must already exist on the Cisco Unified Communications Manager. Creating a Cisco Unified Communications Manager User ID is described in **Creating and Assigning an Application User, page 4-3**.

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

**Step 11**  
In both security alert messages, click **Yes**.

**Step 12**  
In the **Cisco TSP Information** screen, select and enter either the **IP Address** or **Host Name** of the Primary CTI Manager. If you have one, enter the details for the **Backup CTI Manager**, and then click **Next**.

**Note**  
If you are connecting to Cisco Unified Communications Manager 8.x or later, the installation process automatically installs the Cisco TSP version appropriate. If you are connecting to Cisco Unified Communications Manager 7.x, you must manually install and configure the Cisco TSP as described in **Appendix D, “Installing and Configuring the Cisco TSP for Cisco Unified Communications Manager 7.x”**.

**Step 13**  
In the **Choose Destination Location** screen, either accept the default destination folder or **Browse** to where you want to install the files, and then click **Next**.

**Step 14**  
In the **Start Copying Files** screen, click **Next**.

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

**Step 15**  
In the **Database Wizard**, click **Next**.
During database creation, the server driver media setting is set according to the CUCM version passed 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 16**
When the wizard has installed the Configuration and Logging databases, click **Finish**.
Cisco Unified Communications Manager TSP is configured.

**Step 17**
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 18**
In the Wizard Complete screen, select **Yes, I want to restart my computer now**, and then click **Finish**.
Your computer restarts, with the Cisco Unified Communications Manager server installed.

You need to license your system before the 5-day evaluation period expires. For more information, see **Licensing Purchased Software, page 6-5**.
If you have installed a resilient system, set up replication on your Publisher and Subscriber servers as described in **Cisco Unified Replication, page 6-37**.

**Disabling Remote Access Connection Manager Service**

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

**Step 1**
In Control Panel, open **Administrative Tools**, and then double-click **Services**.

**Step 2**
Right-click the **Remote Access Connection Manager** service, and then click **Properties**.

**Step 3**
In the dialog box **General** tab set **Startup type** to **Disabled**, and then click **OK**.

**Step 4**
Restart your machine for the change to take effect.
Installing Cisco Unified Attendant Console Client

Note

Note the following prerequisites:

- To complete this procedure you need administration rights.
- 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 server)
  - Port 1863 (used by the CUP server)
  - Port 1864 (used by the BLF Plug-in)
  - Port 5060 as an incoming and outgoing UDP port (used by the CUP server)

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

- Before proceeding, 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.

Note

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

To install Cisco Unified Attendant Console client:

Step 1
Browse to the folder containing the installation files downloaded in Obtaining Cisco Unified Attendant Console Software, page 5-4.

Step 2
Double-click the setup program.

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

Step 3
In the Welcome screen, click Next.

Note

Click Back on any Wizard screen to go back to the previous one.

Step 4
In the Registration Information screen type the Name of the registered owner of the software and their Company, and then click Next.

Step 5
In the Choose Destination Location screen, accept the default destination:

C:\Program Files\Cisco\

To install the application to a different location, click Browse and select a different location.

Click Next to proceed.

Step 6
In Server Type screen, select Standalone (the default) or Resilient, to match your server installation, and then click Next.
Installing Cisco Unified Attendant Console Software

Step 7 If you selected Resilient in step Step 6, note the message about using the Publisher Server name in the next step, and then click OK.

Step 8 In the Server Information screen, enter the name of the machine running the Cisco Unified Attendant Console server (the Publisher Server in resilient installations), and then click Next. If you are performing a resilient installation, you can only enter the server host name in this field. This information is required so that Cisco Unified Attendant Console can talk to the server properly.

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

Where a DNS Server is not present on the network or the Server Machine Name cannot be resolved, you must amend the Hosts file (WINDOWS\system32\drivers\etc\) to reflect the Server IP Address and Server Machine Name. Please ensure that the installation prerequisites have been satisfied.

Step 9 In the Presence Information screen, select the type of presence required:
- Microsoft Presence Status
- Cisco Presence Status
- None
and then click Next.

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

Step 10 In the Language Information screen, select the language to use for the application, and then click Next.

Step 11 In the Visually Impaired Operator Support screen, select Yes or No (the default), and then click Next.

Step 12 In the Icon Information screen, select Add Icon to Desktop to place the Cisco Unified Attendant Console icon on your desktop, and then click Next.

A summary of the information you have entered is displayed.

Step 13 If you are happy with the settings, click Next to copy the files and install the software.

Step 14 In the installation completed screen, click Finish.

Setting Data Execution Prevention

Note To perform this procedure, you need to have administration rights.

If you are installing Cisco Unified Attendant Console client on any of these operating systems:
- Windows Vista Professional (32 bit and WoW64)
- Windows 7 (32 bit and WoW64)

you must set Data Execution Prevention (DEP) to a less restrictive setting than the default. To do this perform the following steps—or their equivalent under your operating system:

Step 1 Right-click My Computer and select Properties.
Step 2 In the window, select Advanced system settings.
Step 3 In the System properties window, select the Advanced tab.
Step 4 Under Performance, click Settings.
Step 5 In the Performance Options dialog box, select the Data Execution Prevention tab.
Step 6 Select Turn on DEP for essential windows programs and services only, then click OK.
Step 7 In the System properties window, click OK.
Configuring and Licensing Cisco Unified Attendant Console Server

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

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

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

- Administrator Login, page 6-1
- Home Page, page 6-2
- Licensing Cisco Unified Attendant Console Software, page 6-4
- Engineering Menu, page 6-7
- System Configuration Menu, page 6-18
- User Configuration Menu, page 6-31
- Cisco Unified Replication, page 6-37

Example Configuration
For examples of the parameters you use to set up a resilient Cisco Unified Attendant Console Premium Edition installation, see Appendix E, “Example Cisco Unified Attendant Console Configuration”.

Administrator Login

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

To log on to Cisco Unified Attendant Admin:
Step 1 In an internet browser, enter the URL specified by your network administrator to access Cisco Unified Attendant Admin. This has the format: http://<<ip address of Cisco Unified Attendant Console server>>/WebAdmin/login.aspx.


The Login page opens.

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

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

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

Step 4 Click Login.

The home page is displayed.

---

Home Page

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

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

- Cisco Unified Replication—For more information, see Cisco Unified Replication, page 6-37.
- Cisco Unified Reporting—For more information, see Appendix B, “Cisco Unified Reporting”.

Menu Options

The Cisco Unified Attendant Admin menus are:

- **Engineering**—control and configure connectivity and support management. For more information, see Engineering Menu, page 6-7.
- **System Configuration**—manage synchronization of devices and queues with Cisco Unified Communications Manager. For more information, see System Configuration Menu, page 6-18.
- **User Configuration**—manage Cisco Unified Attendant Console configuration. For more information, see User Configuration Menu, page 6-31.
- **Help**—view help on Cisco Unified Attendant Admin and licensing the applications. For more information about licensing the software, see Licensing Cisco Unified Attendant Console Software, page 6-4.
Toolbar

When you select a menu option a new page is displayed where you configure that aspect of the Cisco Unified Attendant Console 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>![+]</td>
<td>Add or install an item</td>
</tr>
<tr>
<td>![−]</td>
<td>Remove or uninstall an item</td>
</tr>
<tr>
<td>![文件]</td>
<td>Save</td>
</tr>
<tr>
<td>![重置]</td>
<td>Reset Password</td>
</tr>
<tr>
<td>![测试]</td>
<td>Test Connection or Validate Replication</td>
</tr>
<tr>
<td>![修复]</td>
<td>Repair Database or Repair and Purge Database</td>
</tr>
<tr>
<td>![日历]</td>
<td>Calendar (select a date).</td>
</tr>
<tr>
<td>![开始]</td>
<td>Start Server</td>
</tr>
<tr>
<td>![停止]</td>
<td>Stop Server</td>
</tr>
<tr>
<td>![服务]</td>
<td>View information for a service.</td>
</tr>
<tr>
<td>![刷新]</td>
<td>Refresh</td>
</tr>
<tr>
<td>![同步]</td>
<td>Synchronize with Cisco Unified Communications Manager or Re-initialize Replication.</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.

Accessibility for Users with Disabilities

Cisco Unified Attendant Admin includes features that make it easier for blind and visually impaired users.
Licensing Cisco Unified Attendant Console Software

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

- Licensing Evaluation Software
- Licensing Purchased Software
- Relicensing Software

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

You need a valid license to be able to perform a major upgrade. When you install a major upgrade your existing license information is erased and the five day evaluation period is restarted. To continue using the application after this time you must obtain a new license.

Licensing Evaluation Software

You can use downloaded software for 5 days before you must license it. Licensing the software enables you to evaluate it for 60 more days. If you do not license the download, you will be unable to use it after the fifth day. If you intend to install the software in a resilient configuration (with separate Publisher and Subscriber servers), you require a separate license for each server.

**Note**
You cannot extend the 60-day evaluation period or apply a second 60-day evaluation license. If you need more evaluation time, you must reinstall your system from the operating system level, and then apply a new 60-day evaluation license.

To license the evaluation software, do the following:

**Step 1**

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

**Step 3**
In the navigation bar, click **ACTIVATE EVALUATION SOFTWARE**.

**Step 4**
Select your **Reseller**, **Customer** and **Customer Site**.
**Licensing Cisco Unified Attendant Console Software**

**Note**  If your reseller, customer or site are not available, choose the options to add them.

**Step 5**  Enter your Cisco Unified Attendant Console **Registration Code**.

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

**Step 6**  Select the **Product** that you have installed.

**Step 7**  Select the **Version** of the product you have installed.

**Step 8**  Click **Next**.

A registration (.RGF) file is e-mailed to you, and a message to this effect is displayed in the web page.

**Step 9**  Open the email and save the registration file to a location that can be browsed by the Cisco Unified Attendant Console server.

**Step 10**  Log into Cisco Unified Attendant Console Web Admin and choose **Help > Licensing**.

**Step 11**  In the **License Management** page, select **Registration File**.

**Step 12**  Click **Browse** and then open the Registration File.

**Step 13**  Click **Submit** to complete license activation.

**Step 14**  Stop and then restart the services, as described in “Service Management” on page 6-10.

---

**Licensing Purchased Software**

You can purchase the software at any time in the evaluation periods, giving you unlimited use. When you purchase the software Cisco provide you with a 27-digit license activation code (LAC). After activating the software, you cannot revert to the trial version.

To activate your purchased software, do the following:

**Step 1**  Use your internet browser to go to [http://www.cisco.com/go/ac](http://www.cisco.com/go/ac).

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

**Step 3**  In the navigation bar, click **ACTIVATE PURCHASED SOFTWARE**.

**Step 4**  Select your **Reseller**, **Customer** and **Customer Site**.

**Note**  If your reseller, customer or site are not available, choose the options to add them.

**Step 5**  Enter the **Registration Code** of the Publisher server, and then click **Submit**.

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

**Step 6**  Enter at least one License Activation Code and then click **Submit**.
Step 7  If the license activation code you entered is for Cisco Unified Attendant Console Premium Edition, the first time you follow this procedure you are prompted to confirm whether you intend to install the software in a resilient configuration (with separate Publisher and Subscriber servers, each of which requires a separate license).

To install a resilient system, click **Yes**. For a non-resilient system, click **No**. If you choose **Yes**, the following happens:

- The License Activation Code is used to license the Publisher Server.
- A License Activation Code is generated for the Subscriber Server and e-mailed to you.

Step 8  In the License Request Confirmation page, optionally enter an additional e-mail address and click **Submit**. If you want to change the License Activation Code you entered in Step 6 before proceeding, click **Revise License Request**.

A registration (.RGF) file is e-mailed to you, and license request confirmation information is displayed in the web page.

Step 9  If you have chosen to install a resilient Cisco Unified Attendant Console Premium Edition system, the registration file sent to you is for your Publisher server. Also e-mailed to you is a License Access Code for your Subscriber server. To license your Subscriber server you need to repeat Steps 1 to 8 using this License Access Code and the Registration Code from your Subscriber server.

Step 10  Open the email and save the registration file to a location that can be browsed by the Cisco Unified Attendant Console server.

Step 11  Log into Cisco Unified Attendant Console Web Admin and choose **Help > Licensing**.

Step 12  In the **License Management** page, select **Registration File**.

Step 13  Click **Browse** and then open the Registration File.

Step 14  Click **Submit** to complete the registration.

Step 15  Stop and then restart the services, as described in “Service Management” on page 6-10.

---

**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 software

And within a VM Environment:

- Copy the VM image
- Perform a major upgrade of the Cisco Unified Attendant Console software

All these cause the license to expire, and the System and User Configuration menus to disappear from Cisco Unified Attendant Admin.
To re-license a server, contact Cisco TAC and request a re-host. You will need to provide them with either the original license activation codes or the SO number of your purchase.

**Engineering Menu**

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

- **Administrator Management** (not available when logged in to Subscriber server). This is described in *Administrator Management*, page 6-7.
- **Server Management**. This is described in *Server Management*, page 6-8.
- **Database Management** (cannot be changed if you have a resilient installation). This is described in *Database Management*, page 6-8.
- **Database Purge**. This is described in *Database Purge*, page 6-9.
- **Service Management**. This is described in *Service Management*, page 6-10.
- **CUCM Connectivity**. This is described in *CUCM Connectivity*, page 6-13.
- **CUPS Connectivity**. This is described in *CUPS Connectivity*, page 6-15.
- **Logging Management**. This is described in *Logging Management*, page 6-15.

**Administrator Management**

The *Administration Management* option enables you to change or reset the administrator password used when logging into the Web Admin application. This option is not available on a resilient system if you are logged into the Subscriber server.

*Note*
The password is not case sensitive.

To change the password:

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

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

**Step 3** Enter *New Password*.

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

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

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

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

Note
This Engineering menu option is not available if you have a standalone installation.

The databases in the Publisher and Subscriber server machines contain a Server Details table. If you have a resilience license, you can change some of these details using the Server Management option.

To change server details:

Step 1 Choose Engineering > Server Management.
Step 2 The Server Management page is displayed.
Step 3 Under Server Details, select the server to manage.
Step 4 Enter the following values:
   • Reconnection Delay (msecs)—reconnection delay in milliseconds. Default Value 90000. You must enter a value.
   • Buffer Duration (secs)—buffer duration in seconds. Default Value 259200. You must enter a value.
Step 5 Click Save to save the settings.

Database Management

The configuration database is created when you install the Cisco Unified Attendant Console 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 Admin 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 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 server Installation Wizard, the password is Z1ppyf0rever.
Note

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

Step 6

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

Note

There is no Save button in a resilient Cisco Unified Attendant Admin Premium installation.

Step 7

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

Test the Database

To test the specified database, click Test Connection.

Repair the Database

To repair the specified database, click Repair Database.

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

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

Database Purge

The Database Purge option enables you to purge old call logging and operator session information from the database. Customers using SQL Server Express may need to do this because their database size is limited to 4 GB. If the logging database becomes full, some features and services may fail.

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

To purge the database:

Step 1

Choose Engineering > Database Purge.

Step 2

Enter a Start Date either by entering it in the format yyyy-mm-dd (year-month-date) or by selecting it from the calendar.

Step 3

Enter an End Date either by entering it in the format yyyy-mm-dd (year-month-date) or by selecting it from the calendar.
Step 4  Click **Purge the Database**.
Cisco Unified Attendant Admin stops the server and purges the database. You must manually restart the server service.

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

- Database Name
- SQL Server
- Activity Date
- Purge Start Date
- Purge End Date
- Table Name
- Number of Records effected
- Status
- Error Code
- Error Description

**Service Management**

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

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

To manage a server:

Step 1  Choose **Engineering > Service Management**.
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="Play" /></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="Information" /></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>
<tr>
<td>Not Connected</td>
<td>The server and databases are not connected.</td>
</tr>
<tr>
<td>Standby</td>
<td><strong>Logging Database only.</strong> The connection between the service and the Logging Database is not in use.</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
  - If your Cisco Unified Attendant Console is running in resilient mode, the Inter Server Communication Status is also shown.
- The Resilience Status (only with resilient installations):
  - The Inter Server Communication Status shows the status of the link between the Publisher and Subscriber servers.
  - The Publisher Failover Status shows the status of the Publisher server.
  - The Subscriber Failover Status shows the status of the Subscriber server.

**Cisco Unified Attendant LDAP Plug-in Status**

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

The following are displayed for the Cisco Unified Attendant LDAP Plug-in:
- The Server Activity of Active Sources and Active Synchs
- The status of the following servers:
  - Primary Server
  - Configuration Database

**Cisco Unified Attendant CUPS Plug-in Status**

The following are displayed for the Cisco Unified Attendant CUPS Plug-in:
- The Server Activity of User Activity and Active Subscriptions
- The status of the Primary Server

**Cisco Unified Attendant BLF Plug-in Status**

The following are displayed for the Cisco Unified Attendant BLF Plug-in:
- The Server Activity of Subscriptions and Connected Users
- The status of the following servers is displayed for the Cisco Unified Attendant Plug-in:
- CT Link
- DRM
- COMMS
- Database — the configuration database connectivity status
- If your Cisco Unified Attendant Console is running in resilient mode, the Inter Server Communication Status is also shown.

- The Inter Server Communication Status shows the status of the link between the Publisher and Subscriber servers.

### CUCM Connectivity

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

Cisco Unified Attendant Console supports the Legacy Driver for Cisco Unified Communications Manager Release 7.1(5) but uses the New Media Driver when connected to Cisco Unified Communications Manager Release 8.0 and later. If the media driver configuration does not match the Cisco Unified Communications Manager version, the Cisco Unified Attendant Console Server will not start and the BLF Plug-in will not be able to establish a CTI channel.

The **CUCM Connectivity** option enables you to set up and test the Cisco Unified Communications Manager connection. You can access the **CUCM Connectivity** option even when Cisco Unified Attendant Console Server is not running.

---

**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 Server validates its internal driver settings against the Cisco Unified Communications Manager Release.

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

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

- If you have a resilient Cisco Unified Attendant Admin Premium Edition installation and are logged in to the Publisher, the message says:

  
  *Attendant Admin has detected that the media driver configuration for the selected CUAC server does not match your CUCM version. Please click the Save button so the Attendant Admin can correct the media driver configuration for the selected CUAC Server. You also need to click on other CUAC servers to make sure that the media driver configuration for other servers is correct.*

  Follow the instructions in the message.

- If you have a resilient Cisco Unified Attendant Admin Premium Edition installation and are logged in to the Subscriber, the message says:
Attendant Admin has detected that the media driver configuration for the selected CUAC server does not match your CUCM version. Please use Publisher Attendant Admin to correct the media driver configuration for the selected CUAC Server. You also need to click on other CUAC 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 Admin Premium Edition 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 a **CUCM name or IP**, the name or IP address of the machine where Cisco Unified Communications Manager is installed.

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

**Step 6** Enter **User name**, the Cisco Unified Communications Manager application user ID. For more information about application users, see Creating and Assigning an Application User, page 4-3.

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

**Note** The Username and Password are case-sensitive. Make sure you enter the information in these fields in correct case.

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

**Step 8** If you have a resilient Cisco Unified Attendant Admin Premium Edition 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 Admin 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 CUAC 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 CUAC 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 CUAC server for this change to take effect.*

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

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

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

To manage connectivity details:

Step 1. Choose Engineering > CUPS Connectivity.

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

Step 3. Type the CUPS Port to connect to. This is set to 5060 by default (when not using TLS).

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

Step 5. Type the TLS port. The Transport Layer Security Port. By default this is -1, indicating that TLS is switched off. To enable TLS, specify a port number (Normally either 5061 or 5062).

Step 6. If TLS is enabled, type the Certificate nickname (used to identify the correct certificate in the certificate database) and the Certificate database password (to validate the nickname and provide access to the database).

Step 7. To save, click Save.

Step 8. To test, click Test Connection.

Note

IMPORTANT—The Cisco Unified Attendant CUPS Plug-in has to be added to the firewall information on the Communications Manager. See section Configuring Access to Cisco Unified Presence Server, page 4-3.

Logging Management

When you install Cisco Unified Attendant Console, 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
- Cisco Unified Attendant CUPS Plug-in
- Cisco Unified Attendant BLF Plug-in

Note

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

To manage logging:
## Engineering Menu

**Step 1**

Choose **Engineering > Logging Management**.

The fields in the form are described below:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco Unified Attendant Console server</strong></td>
<td></td>
</tr>
<tr>
<td>Main process</td>
<td>Log the main process.</td>
</tr>
<tr>
<td>CTI process</td>
<td>Log the CTI process.</td>
</tr>
<tr>
<td>Communication process</td>
<td>Log the communication process.</td>
</tr>
<tr>
<td>Router process</td>
<td>Log the router process.</td>
</tr>
<tr>
<td>Database process</td>
<td>Log the database process.</td>
</tr>
<tr>
<td>Logging path &amp; file name</td>
<td>The logging file path and name. For example, C:\Program Files\Cisco\Attendant Server\Log\ICD.txt.</td>
</tr>
<tr>
<td>Number of files</td>
<td>The number of log files that can be created in the logging folder. The default is 10.</td>
</tr>
<tr>
<td>Lines per file</td>
<td>The number of lines each log file can contain. The default is 10000.</td>
</tr>
<tr>
<td>Service logging path &amp; file name</td>
<td>The service logging file path and name. For example, C:\Program Files\Cisco\Attendant Server\Log\ICD1.txt.</td>
</tr>
<tr>
<td><strong>Cisco Unified Attendant LDAP Plug-in</strong></td>
<td></td>
</tr>
<tr>
<td>Logging level</td>
<td>One of: Detailed (default), Advanced, Minimum, Full.</td>
</tr>
<tr>
<td>Logging path &amp; file name</td>
<td>The LDAP Plug-in logging file path and name. For example, C:\Program Files\Cisco\LDAP Plug-in\Log\log.txt.</td>
</tr>
<tr>
<td>Number of files</td>
<td>The number of log files that can be created in the logging folder. The default is 10.</td>
</tr>
<tr>
<td>Lines per file</td>
<td>The number of lines each log file can contain. The default is 200000.</td>
</tr>
<tr>
<td><strong>Cisco Unified Attendant CUPS Plug-in</strong></td>
<td></td>
</tr>
<tr>
<td>Logging level</td>
<td>One of: Detailed (default), Advanced, Minimum, Full.</td>
</tr>
<tr>
<td>Logging path &amp; file name</td>
<td>The CUPS Plug-in logging file path and name. For example, C:\Program Files\Cisco\CUPS Plug-in\Log\log.txt.</td>
</tr>
<tr>
<td>Number of files</td>
<td>The number of log files that can be created in the logging folder. The default is 10.</td>
</tr>
<tr>
<td>Lines per file</td>
<td>The number of lines each log file can contain. The default is 10000.</td>
</tr>
<tr>
<td><strong>Cisco Unified Attendant BLF Plug-in</strong></td>
<td></td>
</tr>
<tr>
<td>Logging level</td>
<td>One of: Detailed (default), Advanced, Minimum, Full.</td>
</tr>
<tr>
<td>Logging path &amp; file name</td>
<td>The BLF Plug-in logging file path and name. For example, C:\Program Files\Cisco\BLF Plug-in\Log\log.txt.</td>
</tr>
<tr>
<td>Number of files</td>
<td>The number of log files that can be created in the logging folder. The default is 100.</td>
</tr>
<tr>
<td>Lines per file</td>
<td>The number of lines each log file can contain. The default is 100000.</td>
</tr>
</tbody>
</table>

**Step 2**

Enter Cisco Unified Attendant Console Server Logging Management details, as described in *Cisco Unified Attendant Console Server Logging*, page 6-17.
Step 3 Enter Cisco Unified Attendant LDAP Plug-in Logging Management details, as described in Cisco Unified Attendant LDAP Plug-in Logging, page 6-17.

Step 4 Enter Cisco Unified Attendant CUPS Plug-in Logging Management details, as described in Cisco Unified Attendant CUPS Plug-in Logging, page 6-18.

Step 5 Enter Cisco Unified Attendant BLF Plug-in Logging Management details, as described in Cisco Unified Attendant BLF Plug-in Logging, page 6-18.

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

---

**Cisco Unified Attendant Console Server Logging**

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

- Main Process
- Router Process
- CTI Process
- Database Process
- Communication Process

By default, the Main and Router processes are selected for logging. To keep the log file to a manageable size, log the fewest processes possible.

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

To manage Cisco Unified Attendant Console server logging:

Step 1 Select the process(es) to log.

Step 2 Specify the **Logging path** and **file name**.

Step 3 Specify the **Number of files** to create.

Step 4 Specify the **Lines per file** to which to restrict the file.

Step 5 Specify the **Service logging path** and **file name** to maintain log of the Cisco Unified Attendant Console server service.

---

**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 Admin 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**.

Step 2 Specify the **Logging path** and **file name**.
Step 3 Specify the Number of files to create.
Step 4 Specify the Lines per file to which to restrict the file.

Cisco Unified Attendant CUPS Plug-in Logging

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

To manage Cisco Unified Attendant CUPS Plug-in logging:

Step 1 Select the Logging Level.
Step 2 Specify the Logging path and file name.
Step 3 Specify the Number of files to create.
Step 4 Specify the Lines per file to which to restrict the file.

Cisco Unified Attendant BLF Plug-in Logging

Cisco Unified Attendant Admin 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.
Step 2 Specify the Logging path and file name.
Step 3 Specify the Number of files to create.
Step 4 Specify the Lines per file to which to restrict the file.

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, as described in Queue Device Groups, page 6-20, and to add and manage system devices, as described in System Device Management, page 6-19.
- **Synchronize with CUCM.** This includes the CUCM Sync Report, and is described in Synchronize with CUCM, page 6-22.
- **Directory Source Management.** This is described in Directory Source Management, page 6-25.
System Device Management

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

**Step 1**
Choose **System Configuration > Queue Device Groups**, and select the server as described in **Queue Device Groups**, page 6-20.

The System Device Management page lists the devices on the selected server.

**Step 2**
In **Server Details**, select the Publisher or Subscriber server, as appropriate.

**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.

The remaining fields in the System Device Management page are described below:

<table>
<thead>
<tr>
<th>Field</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><strong>Template Device</strong></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 devices. If you do not have a template, default values are assigned to your devices. Click <strong>Find Template Device</strong> to search for a template.</td>
</tr>
<tr>
<td>CT Gateway Devices</td>
<td>From: The number of the first device in the range to configure. For example 6301.</td>
</tr>
<tr>
<td></td>
<td>To: The number of the last device in the range to configure. For example 6302.</td>
</tr>
<tr>
<td>Service Devices</td>
<td>From: The number of the first device in the range to configure. For example 6401.</td>
</tr>
<tr>
<td></td>
<td>To: The number of the last device in the range to configure. For example 6402.</td>
</tr>
<tr>
<td>Park Devices</td>
<td>From: The number of the first device in the range to configure. For example 6501.</td>
</tr>
<tr>
<td></td>
<td>To: The number of the last device in the range to configure. For example 6502.</td>
</tr>
</tbody>
</table>

**Note:** 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. We recommend that you use the **Application User ID** allocated for Cisco Unified Attendant Console for the **Owner User ID**.
All the properties of the Template Device, such as device pool, partition, and calling search space, are mapped onto any new devices you create.

**Step 3**  
Click **Find Template Device** to list and search for template devices to use.  
Define the search filter:  
- The device property—such as **Device Name**, **Description**, or **Directory Number**—to check.  
- A condition of the device property, such as **is not empty**, or how to compare the property with a string, such as **begins with**.  
- A string to compare to the device property in the specified way (used only with **begins with**, **ends with**, **contains** and **is exactly**).  
You can also add search filters (up to a maximum of 10) using the plus (+) and minus (-) controls; thereby narrowing the search.

**Step 4**  
Select a template device and click **Save**.  

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

**Step 5**  
Enter a device range for each CT Gateway Device, Service Device and Park Device (for descriptions of these devices, see *Cisco Unified Communications Manager System Devices*, page 1-6).

**Note**  
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**.

**Step 6**  
Click **Save** to save the data.  
**Step 7**  
Click **Synchronize with CUCM** to display the **Synchronize with CUCM** page, as described in *Synchronize with CUCM*, page 6-22.

---

**Queue Device Groups**

The Queue Device Groups option enables you to create and configure 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 provides access to the **Queue Device Groups** page, which you use to configure the pooled devices as described in *System Device Management*, page 6-19.

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

**Note**  
If you have a resilient system and you are logged into the Subscriber server, you cannot change any of the Queue Device Groups,

**Step 1**  
Choose **System Configuration > Queue Device Groups**.
A page listing all the queue device groups that satisfy the **Find** filter is displayed.

**Step 2**
Either

Click **Add New**, to create a new queue device group,

or

**Find** a Queue Device Group to configure:

a. Specify a filter: a string to search for and where to search for it.
   - Accept **Queue Device Group** to search the queue device group names.
   - 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**.
   - 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** **Select** the Queue Device Group to configure.

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

**Step 4** To change the name of the queue device group, edit the text in the field and click **Save**.

**Step 5** To access the System Device Management page so that you can manage system devices, select the appropriate server under **System Devices**. For the rest of the procedure, see **System Device Management**, page 6-19.

**Note** Each time you change devices you must synchronize Cisco Unified Attendant Console with Cisco Unified Communications Manager, as described in the next section.

---

**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.
Configuring and Licensing Cisco Unified Attendant Console Server

System Configuration Menu

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

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 option 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.

Step 2
If you have a resilient installation, in Server Details, select the Publisher or Subscriber server, as appropriate.

The devices and queue locations are listed.

Note
If you have installed a standalone (non-resilient) system, the page is headed by a Synchronization Properties, Ignore call forwarding settings checkbox.

Each list contains the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device DN</td>
<td>The directory number of each configured device. For example, 2000.</td>
</tr>
<tr>
<td>Device Type</td>
<td>The type of device. For example, CTI Route Point.</td>
</tr>
<tr>
<td>Queue Device Group</td>
<td>The Queue Device Group containing the device.</td>
</tr>
<tr>
<td>Server Name</td>
<td>The server for which the Queue Device Group is configured.</td>
</tr>
</tbody>
</table>

Step 3
To ignore any call forwarding settings that have been set against a template device, select Ignore call forwarding settings.

Note
This checkbox is not displayed in a resilient Cisco Unified Attendant Console Premium Edition installation.

Step 4
Click Synchronize with CUCM.
Cisco Unified Attendant Admin automatically synchronizes the devices with Cisco Unified Communications Manager. You do not have to login to the Cisco Unified Communications Manager administration.

Synchronization may take several minutes to complete. 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 state; 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 Ignore call forward is set.</td>
</tr>
<tr>
<td>Started At</td>
<td>The date and time when Cisco Unified Communications Manager synchronization started. For example, 2012-04-12 16:08:52.</td>
</tr>
<tr>
<td>Ended At</td>
<td>The date and time when Cisco Unified Communications Manager synchronization ended. For example, 2012-04-12 16:10:52.</td>
</tr>
<tr>
<td><strong>CUCM Connection Validation</strong></td>
<td></td>
</tr>
<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. The error codes are described in the table on page 6-24.</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>
</tbody>
</table>
The following errors may occur during CUCM synchronization.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></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>
<tr>
<td><strong>Error Code</strong></td>
<td>The code of any error encountered while validating a device. For example 9300. The error codes are described in the table on page 6-24.</td>
</tr>
<tr>
<td><strong>Error Description</strong></td>
<td>The description of the error. For example, Template device not found.</td>
</tr>
</tbody>
</table>

**Device Sync**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Name</strong></td>
<td>The server for which the Queue Device Group is configured.</td>
</tr>
<tr>
<td><strong>Queue Device Group</strong></td>
<td>The Queue Device Group containing the device.</td>
</tr>
<tr>
<td><strong>Device DN</strong></td>
<td>The number of the device being synchronized. For example, 6101.</td>
</tr>
<tr>
<td><strong>Device Type</strong></td>
<td>The type of device being synchronized. For example, CT Gateway Device.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>The status of the device synchronization; one of:</td>
</tr>
<tr>
<td></td>
<td>• Completed</td>
</tr>
<tr>
<td></td>
<td>• Error</td>
</tr>
<tr>
<td></td>
<td>• Inprogress</td>
</tr>
<tr>
<td><strong>Error Code</strong></td>
<td>The code of any error encountered while synchronizing a device. For example 9550. The error codes are described in the table below.</td>
</tr>
<tr>
<td><strong>Error Description</strong></td>
<td>The description of the error. For example, HTTP/1.1 403 Access to the requested resource has been denied.</td>
</tr>
</tbody>
</table>

### Error Code | Error Description
--- | ---
**Cisco Errors**

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

**Internal Errors**

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>
Directory Source Management

Cisco Unified Attendant Admin can synchronize simultaneously to one external source directory of each of these kinds:

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

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

- **Directory Synchronization.** This is described in Directory Synchronization, page 6-28.
- **Directory Field Mappings.** This is described in Directory Field Mapping, page 6-29.
- **Directory Rules.** This is described in Directory Rules, page 6-30.

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 Premium Edition’s 100K limit). Because of this, a warning message is displayed when you have more than one directory source enabled.

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

---

**Caution**

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

---

### Mapping Cisco Unified Attendant Console Fields to an LDAP Directory Source

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

<table>
<thead>
<tr>
<th>Cisco Unified Attendant Console 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>
</tbody>
</table>
Connecting to a Directory Source

To connect to a directory source do the following:

**Step 1** Choose System Configuration > Directory Source Management.
The Directory Source Management page is displayed, listing the directory sources available to you.

**Step 2** Select the directory source to manage.
The page changes to show information about the directory source and your connection to it.

**Step 3** Set the following parameters:

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

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

<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>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Cisco Unified Attendant Console Field</th>
<th>Number of Characters</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Section</td>
<td>50</td>
</tr>
<tr>
<td>Title</td>
<td>4</td>
</tr>
<tr>
<td>User Field 1</td>
<td>100</td>
</tr>
<tr>
<td>User Field 2</td>
<td>100</td>
</tr>
<tr>
<td>User Field 3</td>
<td>100</td>
</tr>
<tr>
<td>User Profile</td>
<td>255</td>
</tr>
</tbody>
</table>
System Configuration Menu

- Use SSL—Select to use SSL

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

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

• Container (displayed only with Microsoft Active Directory or iPlanet Netscape Directory sources)
  - Base DN—The top level of the LDAP directory tree
  - Object class—The object class of the base DN (the default for Microsoft Active Directory is contact; the default for iPlanet Netscape Directory is inetOrgPerson)
  - Scope—Select either One Level or Sub Tree Level (default). With One Level the data is searched to one level below the specified Object class and Base DN. With Sub Tree Level the data is searched in all levels below the specified Object class and Base DN.

Step 4
Click Save to save your changes.

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

• Test the connection to the directory. Click Test Connection; the system tells you whether the connection to the directory works.

• Access the Directory Synchronization functionality. For a description of this functionality, see Directory Synchronization, page 6-28.

• Access the Directory Field Mapping functionality. For a description of this functionality, see Directory Field Mapping, page 6-29.

• Access the Directory Rules functionality. For a description of this functionality, see Directory Rules, page 6-30.

Directory Synchronization

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

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

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

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

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

**Step 2**  
Set the Directory Synchronization parameters.

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

---

**Directory Field Mapping**

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

To map a field:

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

The mappings are listed.
Step 2  Click Add New.
The Field Mapping Information is displayed.

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

Step 4  Select a Destination field in the contacts database.

Step 5  Enter a Default value, which is written to the Destination field if the Source field is empty.

Step 6  Click Save to add the mapping.

Directory Rules

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

Tip
Multiple filters within a rule are combined with a logical AND. For example, 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 last name 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.

Step 8  Click Save to save the filter in the rule.
User Configuration Menu

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

- **General Properties.** This is described in General Properties, page 6-31.
- **Queue Management.** This is described in Queue Management, page 6-32.
- **Operator Management.** This is described in Operator Management, page 6-36.

General Properties

The General Properties option enables you to manage the Cisco Unified Attendant Console 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:

**Step 1** Choose User Configuration > General Properties.

**Step 2** Enter the General Properties:

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

**Note**

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

- **External access number**—the prefix that enables you to call external numbers
- **External international access number**—the prefix that enables you to call international external numbers
- **External area code**—the Country Code of the Cisco Unified Communications Manager location. International numbers that include this country code are dialed as domestic calls.

**Default FAC and CMC Settings**—If Forced Authorization Codes (FAC) and/or Client Matter Codes (CMC) are configured in Cisco Unified Communications Manager, these may be needed when the system makes Attendant calls or transfers. For example, a blind transfer where the final outbound call is made from a Service Queue CTI port. If an external call is made from the operator’s handset, the operator is presented with a FAC or CMC dialog box in which they manually enter the code from their application.
Client Matter Code (CMC) is used to provide extra call logging facilities within the Communications Manager. The user has to enter their CMC Code before their external consult transfer can proceed. The CMC code is written into the call detail records, which can then be used to charge calls to different cost centers.

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

Recall Timers—these properties are used to set the duration of each type of recall:
- Hold recall—the maximum time a call put on hold by an operator remains on hold before an audible alert is played
- Transfer recall—the maximum time before an unanswered operator-transferred call is returned to that operator
- Park recall—the maximum time before an unanswered parked call is returned to the operator. The call can still be picked up by the intended recipient once the Parked timeout has happened.
- Camp On recall—the maximum time an unanswered call remains camped-on before it is returned to the operator.

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

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

Working Days—Set the days and hours that the Cisco Unified Attendant Console queues are active. Specify the following:
- The days the queues are active
- The Working hours from time and Working hours to time: the periods the queues are active on the specified days

Working Days is a global setting, and may not be suitable in a situation where Queues are specific to offices that are in different time zones. In this case, use No Operator Overflow in User Configuration > Queue Management. This enables you to push calls to a specific destination if no operators are logged into the queue (this does not apply to a queue where an operator is unavailable or busy).

For more information on time of day routing, see the Cisco Unified Attendant Console Design Guide.

Step 3
Click Save to save the changes.

Queue Management

Depending on the number of incoming calls and staffing levels, operator queues may receive more calls than they can handle. For this reason, you must define what to do with these calls when the following overflow conditions exist for your queues:
• Maximum number of calls waiting to be answered exceeded
• Maximum call wait time exceeded
• No operator

If you want, overflowed calls can be simply discarded, but it is better to route them to an overflow destination. You must define a destination for each overflow condition, which can be different for each.

In a similar way, when a queue is in emergency mode you can route calls made to it to another destination. In both cases, this destination is either an overflow number (DDI) or an overflow queue. The overflow number cannot be the same as that of the overflow queue, and you cannot overflow a queue to itself.

The Queue Management option enables you to create and configure operator queues, including the overflow destinations.

### 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** Enter the General properties:

- **Name**—the name of the queue.
- **Priority**—the priority of the queue when calls are being routed. This is used to manage the order in which calls in different queues are handled. A queue with a high priority has its calls processed before those in queues with a lower priority. This is the same for all servers.
- **Salutation**—a greeting displayed in a pop-up for the operator to use. This is the same for all servers.
- **Queue device group**—select the queue device group to use.

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

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

- **Forced Delivery**—select this to make the queue a forced delivery queue. This causes an enquiry call to be made from the CTI Port to the next attendant handset in a circular, round-robin pattern. Attendants receive calls in the order in which they log in, and after the last attendant receives a call, the first receives the next one. Attendants are skipped if they are still busy on a previous call.

- **Forced delivery answer time (secs)**—the length of time that a forced delivery call rings at an attendant’s extension before it gets routed to the next available attendant.

**Step 5** Click Save.

You can now set the queue DDI and configure the Full CTI Failure, Emergency, Overflow and Night Service properties, as described in Configuring Queues, below.

---

**Note**
If you have a resilient system and you are logged into the Subscriber server, you cannot change any of the Queue Management parameters.
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 Night Service 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.

Step 6 Enter a queue DDI, click Save, and then, in the Related Link field, select Back to Queue, and then click Go.

Step 7 If required, in the Queue Management page, modify the General properties, which are described in Creating Queues, page 6-33.

Step 8 In the Queue Management page, 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 Call 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 Admin installation
- Assigned Publisher and Subscriber DDIs
- Created a Queue and configured a Full CTI Failure device on the queue
- Used Cisco Unified Attendant Admin to synchronize the device
Then an AXL SOAP request synchronizes the devices on Cisco Unified Call 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 Call Manager device configuration. For instructions on how to do this, see Synchronize with CUCM, page 6-22.

- **Emergency**—the destination calls must be forwarded to when the queue is in emergency mode.
  - **Destination type**—select:
    - *Device* (then type a DDI number in the **Emergency destination**)
    - *Queue* (then find and select a Queue as the **Emergency destination**) or
    - *None*, to disable the forwarding of Emergency calls.

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

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

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

- **Overflow**—This controls the routing (overflow) of calls from a queue when certain parameters are exceeded. It contains these properties:
  - **Maximum calls**—The maximum number of calls that can wait in the queue. Additional calls are routed to the **Maximum calls destination**.

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

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

  - **Maximum calls destination**—the destination DDI (if **Destination type** is **Device**), or Queue Name (if the **Destination type** is **Queue**) to which to route calls when the Maximum calls parameter is exceeded.

  - **Wait time**—The maximum time a call can wait in the queue before being routed to the **Wait time destination**. This has the format **hours:Minutes:Seconds**, with a maximum of 23:59:59.

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

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

  - **Wait time destination**—the destination DDI (if **Destination type** is **Device**), or Queue Name (if the **Destination type** is **Queue**) to which to route calls when the Wait time parameter is exceeded.
User Configuration Menu

- **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.

  - **Night Service**—This enables you to specify a Night service destination. Calls made outside the Working Days general property are routed to this destination. Night service enables you to take a queue out of operation for periods, during which calls are routed elsewhere. It contains these properties:
    
    - **Destination type**—select:
      
      - **Device** (then type a DDI number in the Night service destination),
      - **Queue** (then find and select a Queue as the Night service destination) or
      - **None**, to disable the Night service overflow.

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

    - **Night service destination**—the destination DDI (if Destination type is Device), or Queue Name (if the Destination type is Queue) to which to route calls outside of normal working hours.

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

**Step 10** Click **Synchronize with CUCM** to access the Synchronize with CUCM page. For more information, see Synchronize with CUCM, page 6-22.

---

**Operator Management**

The Operator Management option enables you to create and configure operator profiles, including associating queues with profiles.

**Creating Operator Profiles**

To create an operator profile:

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

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

**Step 3** Enter a **Login name**.

**Step 4** Enter a **Password**, and then re-enter it to confirm it.

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

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

To configure an operator profile:

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

**Step 2** Find an operator profile to manage. Specify a filter: a string to search for and where to search for it.
- Select **Login Name**.
- A condition of the login name, such as **is not empty**, or how to compare the login name with a string, such as **begins with**.
- A string to compare to the login name in the specified way (used only with **begins with**, **ends with**, **contains** and **is exactly**).

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

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

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

The profile information is displayed.

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

**Step 5** If required, edit the **Login name**, **Password**, and then **Confirm password**.

**Step 6** To associate the profile with a queue, click **Queue Association**.

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

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

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

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

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

---

Cisco Unified Replication

Cisco Unified Attendant Console server resilience is partly provided by server replication. For more information on resilience, see **Server Resilience, page 1-4**.

Cisco Unified Attendant Console Premium Edition contains two databases:

- Configuration database—contains all user configurations and the contacts directory
- Logging database—responsible for logging

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

The Log database is synchronized between Publisher and Subscriber using Microsoft DTC. 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.
Note

The following:

- Cisco Unified Attendant Console does not run on a copy (clone) of a Virtual machine. For more information about VMware requirements, visit:

- Database replication is uninstalled automatically during Cisco Unified Attendant Console 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 replication during SQL Server installation, and do not manually configure replication within SQL Server. Set up server resilience through Cisco Unified Replication only. If you do install or configure replication within SQL Server, you will be unable to manage it—for example, you will be unable to uninstall it—using Cisco Unified Replication.

---

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

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

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

You can check how the agents are running using the Monitor Replication function, described in Monitoring Replication, page 6-41.
Configuring Server Replication

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

You can configure, validate and monitor replication, and troubleshoot and fix the database using Cisco Unified Replication.

Note
The following:

- You must configure replication for both the ATTCFG and ATTLOG databases on both the Publisher and the Subscriber. Configure the Publisher databases before configuring the Subscriber databases. (the Subscriber communicates with the Publisher). When you have installed a Publisher or Subscriber server you cannot convert it into the other type. The Publisher requires at least SQL Server Standard to be installed, while the Subscriber can use SQL Express (which is installed when you install Cisco Unified Attendant Console Premium Edition).
- The date, time and time zone on the Publisher and Subscriber machines must be the same, otherwise Console users will not be notified that the Publisher has become available after recovering from a failure, and will be unable to switch from the Subscriber back to the Publisher. One way to achieve this is to synchronize the time of both servers with the same time server.
- The CT and LDAP servers on the Publisher and the CT server on the Subscriber are stopped when you install, uninstall or re-initialize replication, and are started again afterwards.

Before you can configure Cisco Unified Replication, you must do the following:

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

The Cisco Unified Replication home page is displayed.

Step 2
Click Replication Management.

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

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

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

Step 4
Under Replication Management, click Select alongside the database to check or configure.

The Information for that database is displayed, below which are the following control buttons:
- Install Replication. For more information, see Installing Replication, page 6-40.
- Uninstall Replication. For more information, see Uninstalling Replication, page 6-41.
- Reinitialize Replication. For more information, see Re-initializing Replication, page 6-41.
- Monitor Replication. For more information, see Monitoring Replication, page 6-41.
• **Validate Replication.** For more information, see Validating Replication, page 6-42.
• **Replication Report.** For more information, see Replication Report, page 6-43.

---

### Installing Replication

**Note**
The information in this section refers to using SQL Server 2008 Standard Edition. If you are using a different version or edition the information may be slightly different. The equivalent information is described in your SQL Server user documentation.

Before installing or uninstalling replication:

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

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

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

To install replication on a specific database:

**Step 1**
On the Publisher server, select the database as described on page 6-39.

**Step 2**
Under **Server Credentials (<server_name>)**, type the **Windows username** (domain name\username or server name\username) and **Password** of a user with administrator rights to the Subscriber server.

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

**Step 4**
In the message, click **OK** to confirm that you want to install replication on that database.
Replication is installed. You can check the progress of the installation by clicking Replication Report. For more information, see Replication Report, page 6-43.

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

---

**Note**  
Important: Installing replication shuts down both servers. Consequently, after installing replication you must either restart your computer or restart the services as described in Service Management, page 6-10.

---

### Uninstalling Replication

Before uninstalling replication, perform the checks and procedures at the start of Installing Replication, page 6-40.

To uninstall replication:

**Step 1**  
On the Publisher server, select the database as described on page 6-39.

**Step 2**  
Click Uninstall Replication.

**Step 3**  
Click OK to confirm that you want to uninstall replication.

Replication is uninstalled.

You can check the progress of the uninstallation by clicking Monitor Replication or Replication Report.

---

### Re-initializing Replication

If replication has been suspended as a result of a Publisher-Server communication failure, you can re-initialize it. Re-initialization restores the Publisher snapshot to the Subscriber and re-starts transactional replication.

**Note**  
If replication has been dropped you must install replication again, as described in Installing Replication, page 6-40.

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

**Step 1**  
In the Replication Management page, select the select the database as described on page 6-39.

**Step 2**  
Click Reinitialize Replication.

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

---

### Monitoring Replication

To monitor how replication is proceeding for a server and database selected as described on page 6-39:
Cisco Unified Replication

Step 1
In the Replication Management page, select the database as described on page 6-39.

Step 2
Click Monitor Replication.

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

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

Step 3
To update the display, click Refresh.

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

Validating Replication

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

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

Step 1
In the Replication Management page, select the database as described on page 6-39.

Step 2
Click Validate Replication.

The Validation Report is displayed. For example:
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 select the database as described on page 6-39.
Step 2  Click Replication Report.

The Replication Report is displayed.
Step 3  Use the Rows Per Page control to change the number of lines displayed, and the controls at the bottom right of the report to display specific pages.

Step 4  To return to the Replication Management page, click Go next to Related link: Back to Replication Management.
Uninstalling Cisco Unified Attendant Console Server

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

Note

The following:

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

When you uninstall a resilient system, it doesn’t matter whether you start with the Publisher or the Subscriber.

To uninstall Cisco Unified Attendant Console 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**.

Step 3  When you are prompted to confirm that you want to remove Cisco Unified Attendant Console server from your machine, click **Yes**.

Step 4  If you have a resilient installation and both servers are running, you are prompted that the services on the other server (Subscriber or Publisher, as appropriate) need to be stopped. In the message click **Yes** to stop the services. In the Server screen, enter the **Username** and **Password** of the administrative account on the other server.

The server application is uninstalled.
The page contains instructions for uninstalling components of a system. The instructions include:

**Uninstalling Microsoft SQL Server**

To uninstall the Microsoft SQL Server from your Cisco Unified Attendant Console 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.

**Step 3** Select the instance to remove, and then click Next.

**Step 4** Click Finish to remove the components. Click Back to go back and change any of the information.

**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**

To uninstall the .NET Framework:

**Step 1** Choose Start > Control Panel, and then double-click Add/Remove Programs.

**Step 2** From the list, select Microsoft .NET Framework 3.5, and then click Remove.

**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.

**Step 6** When all the components have been removed, click Finish.
Uninstalling Cisco TSP

If you need to uninstall the Cisco TSP follow the instructions in ciscotsp.txt, which was created when the TSP was installed. The file’s default location is C:\Program Files\Cisco.
Cisco Unified Reporting

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

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

To access Cisco Unified Reporting:

**Step 1**  
Log in to Cisco Unified Attendant Admin, as described in Administrator Login, page 6-1. The Cisco Unified Attendant Admin home page is described. For more information, see Home Page, page 6-2.

**Step 2**  
In Navigation at the top right of the home page, select **Cisco Unified Reporting**, and then click Go. The Cisco Unified Reporting home page is displayed. This contains the System Reports menu from which you can run the following reports:

- Incoming Calls by Date and Time. For more information, see Incoming Calls by Date and Time System Report, page B-3.
- Operator Calls by Time. For more information, see Operator Calls by Time System Report, page B-4.
- Operator Calls by Queue. For more information, see Operator Calls by Queue System Report, page B-5.
- Overflowed Calls by Date. For more information, see Overflowed Calls By Date System Report, page B-5.
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" /></td>
<td>Click Go to return to the System Reports home page.</td>
</tr>
<tr>
<td>![Go]</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>![Select a format]</td>
<td>Export a copy of the report. First select the format from Excel (.XLS) or Acrobat (.PDF).</td>
</tr>
<tr>
<td>![Print]</td>
<td>Refresh the Report screen.</td>
</tr>
<tr>
<td>![Print]</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

All the reports require you to select a From date, and some also require a To date so that the report covers the range of specified dates. You can restrict a date range to a single day by specifying the same From and To dates. You can also select the date by clicking the calendar control.

Time Range

All the reports require you to select a From time and a To time. These times have the format \texttt{hh:mm:ss}, where \texttt{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. 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 and time.

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.</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>
</tbody>
</table>
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>Answer Time Profile</td>
<td>The percentage of calls answered within the specified number of seconds.</td>
</tr>
<tr>
<td></td>
<td>..10: % Calls answered in less than 10 seconds.</td>
</tr>
<tr>
<td></td>
<td>..20: % Calls answered between 10 to 19 seconds.</td>
</tr>
<tr>
<td></td>
<td>..30: % Calls answered between 20 to 29 seconds.</td>
</tr>
<tr>
<td></td>
<td>..40: % Calls answered between 30 to 39 seconds.</td>
</tr>
<tr>
<td></td>
<td>..40+: % Calls answered after 40 or more seconds.</td>
</tr>
<tr>
<td>Longest Wait</td>
<td>The longest time a caller had to wait to be answered.</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>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>
</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>Total Outbound Calls</td>
<td>Total number of outbound calls made by the operator. Includes:</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>

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)

<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>
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 an attendant operators was not 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>
<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>
Creating an Attendant Application User for Cisco Unified Communications Manager 7.x

This appendix describes how to create and configure an Application User within Cisco Unified Communications Manager 7.x so that Cisco Unified Attendant Console can communicate with it via TSP. The application user profile provides the roles and privileges you need to be able to modify and synchronize information.

To create and configure an Application User, follow these steps:

1. **Creating an Application User**.
2. **Creating a User Group and Assigning Roles to it**, page C-2.

### Creating an Application User

To create an Application User, do the following:

**Step 1**
On the server machine, use your internet browser to access Cisco Unified Communications Manager Administration, and then choose User Management > Application User.

**Step 2**
Click Add New.

**Step 3**
Type the following:

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

**Step 4**
Select a **Presence Group**.

**Step 5**
Click **Save** to save the Application User.

**Note**
If you are using Active Directory to synchronize with the Cisco Unified Communications Manager, the Application User profile must also exist in Active Directory.
Creating a User Group and Assigning Roles to it

You must now associate your new Application User with a User Group, which contains the roles that govern what the user can do.

To create a User Group, do the following:

Step 1: On the server machine, use your internet browser to access Cisco Unified Communications Manager Administration, and then choose User Management > User Groups.

Step 2: Click Add New to create a new User Group.

Step 3: Type a Name for the new User Group.

Step 4: Click Save to save the User Group.

Step 5: On the Find and List User Groups page, Find the User Group you just created.

Step 6: In the Search Results, click Roles for the User Group.

Step 7: Click Assign Role to Group.

The roles that can be assigned are listed.

Step 8: Select the following roles:
- Standard CTI Allow Call Park Monitoring
- Standard CTI Allow Calling Number Modification
- Standard CTI Allow Control of All Devices
- Standard CTI Allow Reception of SRTP Key Material
- Standard CTI Enabled
- Standard AXL API Access

Step 9: If your environment uses phone models 69xx, 7931, 7965, 89xx or 99xx, you must also select:
- Standard CTI Allow Control of Phones supporting Rollover Mode
- Standard CTI Allow Control of Phones supporting Connected Xfer and conf

Step 10: Click Add Selected to assign the roles.

Step 11: Click Save.

Adding the Application User to the User Group

To add the Application User to the User Group, do the following:

Step 1: On the server machine, use your internet browser to access Cisco Unified Communications Manager Administration, and then choose User Management > User Groups.

Step 2: On the Find and List User Groups page, Find the User Group you just created, and then select it in the results.

Step 3: Click Add App Users to Group.

The Application Users are listed.
Adding the Application User to the Standard CCM Super Users Group

The Standard CCM Super Users group is a User Group with full access permission to all named roles. After you have added the Application User to your newly created User Group, you must also add it to the Standard CCM Super Users group.

To add your Application User to Standard CCM Super User, do the following:

**Step 1** On the server machine, use your internet browser to access Cisco Unified Communications Manager Administration, and then choose User Management > User Groups.

**Step 2** On the Find and List User Groups page, search for Standard CCM Super Users.

**Step 3** On the Find and List User Groups page, Find Standard CCM Super Users, and then select it in the results.

**Step 4** Click Add App Users to Group.

The Application Users are listed.

**Step 5** Select the check box to the left of your newly-created Application User, and then click Add Selected.
Creating an Attendant Application User for Cisco Unified Communications Manager 7.x

Adding the Application User to the Standard CCM Super Users Group
Installing and Configuring the Cisco TSP forCisco Unified Communications Manager 7.x

The Cisco TAPI (or Telephony) Service Provider (TSP) enables the Cisco Unified Attendant Console Server to communicate with the Cisco Unified Communications Manager CTI Manager service, which provides call control.

Cisco Unified Attendant Console installation also automatically installs the Cisco TSP appropriate to your Cisco Unified Communications Manager—unless you are using Cisco Unified Communications Manager Release 7.x, in which case you must manually install the Cisco TSP for that release.

This appendix describes the following steps:

1. Downloading and Installing the TSP.

If you need to uninstall the Cisco TSP, follow the instructions in the file C:\Program Files\Cisco\CiscoTSP.txt, which is created when the TSP is installed. This file also includes instructions for installing the Cisco TAPI Wave driver.

**Downloading and Installing the TSP**

To download and install the Cisco TSP, do the following:

**Step 1**
On the server machine, use your internet browser to access Cisco Unified Communications Manager Administration, and then choose **Application > Plug ins.**

**Step 2**
Find the Cisco Telephony Service Provider using the search field (Figure D-1).

**Step 3**
In the **Search Results**, click **Download** on the Cisco Telephony Service Provider line.
Configuring the TSP

To configure TSP, do the following:

**Step 1**  Click the **Start** button, and then in the **Start** menu, choose **Settings** > **Control Panel** > **Phone and Modem Options**.

**Step 2**  Select the **Advanced** tab.

**Step 3**  Select `CiscoTSP001.tsp`.

**Step 4**  Click **Configure**, and then select the **User** tab.

**Step 5**  In **User Name**, type the User ID of the Cisco Unified Communications Manager Application User created in Appendix C, “Creating an Attendant Application User for Cisco Unified Communications Manager 7.x”.

**Step 6**  Type the **Password**, and then again in **Verify Password**.

**Step 7**  Select the **CTI Manager** tab.

**Step 8**  Under **Primary CTI Manager Location**, select and then type either the **IP Address** or **Host Name** of the CTI Manager to connect to. If a second CTI Manager is available, you can optionally specify a **Backup CTI Manager Location**.

**Note**  The CTI Manager service runs on each CUCM node in a cluster. Your primary CTI Manager should be on the Cisco Unified Communications Manager publisher, and your Backup CTI Manager on the subscriber.

**Step 9**  Select the **Wave** tab.

**Step 10**  Type the **Desired number of possible Automated Voice lines**. Specify sufficient to allow *all* your CTI Ports to be monitored by this TSP. You may want to specify a larger number to cater for future expansion. If you wish to change the number at a future date, you will have to uninstall and reinstall the Cisco TAPI Wave driver.

**Step 11**  Click **OK**.

**Step 12**  Select the **Advanced** tab.

**Step 13**  In **Provider Open Completed Timeout (secs)**, type 300.

**Step 14**  Click **OK**.

**Step 15**  Reboot the machine.

You now need to install the Cisco TAPI Wave driver.
Installing the Cisco TAPI Wave Driver

These instructions are for a Windows 2008 Server. If you have a different operating system, perform the equivalent steps.

To install the Cisco TAPI Wave driver, do the following:

---

Step 1
In Control Panel, double-click Add Hardware.

Step 2
In the Add Hardware wizard, click Next.

Step 3
Select Install the hardware that I manually select from a list, and then click Next.

Step 4
From the list of Common hardware types, select Sound, video and game controllers, and then click Next.

Step 5
When prompted to select the device driver, click Have Disk.

Step 6
In the Install From Disk dialog box, Browse to C:\Program Files\Cisco Systems\Wave Drivers, select the file oemsetup.inf, and then click Open.

Step 7
Click OK.

Step 8
In the Select the device driver you want to install page, select the Cisco TAPI Wave Driver, and then click Next.

Step 9
In the Wizard is ready to install your hardware page, click Next.

Step 10
If prompted for Digital signature Not Found, click Continue Anyway.

Step 11
When prompted to Install from disk 1 for file avaudio32.dll, Browse to C:\Program Files\Cisco\Wave Drivers, and then click Open.

Step 12
When prompted, reboot the server.
Installing the Cisco TAPI Wave Driver
Example Cisco Unified Attendant Console Configuration

This appendix contains an example resilient Cisco Unified Attendant Console Premium Edition Version 9.1.1 system configuration.

**Publisher:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSP application user</td>
<td>CUACPUB01</td>
<td>See Creating and Assigning an Application User, page 4-3.</td>
</tr>
<tr>
<td>Machine Name</td>
<td>CUACPUB01</td>
<td></td>
</tr>
<tr>
<td>CT Gateway</td>
<td>1600 - 1609</td>
<td>See Device Groups, page E-2.</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>CUACSUB01</td>
<td>See Creating and Assigning an Application User, page 4-3.</td>
</tr>
<tr>
<td>Machine Name</td>
<td>CUACSUB01</td>
<td></td>
</tr>
<tr>
<td>CT Gateway</td>
<td>1650 - 1659</td>
<td>See Device Groups, page E-2.</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, page 6-19.

For a description of how to create queues and define queue DDIs, see Queue Management, page 6-32.

<table>
<thead>
<tr>
<th>Name</th>
<th>Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFAULT</td>
<td>Primary (Publisher)</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></td>
<td>Secondary (Subscriber)</td>
</tr>
<tr>
<td></td>
<td>CT Gateway 1650 - 1654</td>
</tr>
<tr>
<td></td>
<td>Service Device 1660 - 1664</td>
</tr>
<tr>
<td></td>
<td>Park Device 1670 - 1674</td>
</tr>
<tr>
<td></td>
<td>Queue DDI 1680 - 1684</td>
</tr>
<tr>
<td>DEVELOPMENT</td>
<td>Primary (Publisher)</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>
<tr>
<td></td>
<td>Secondary (Subscriber)</td>
</tr>
<tr>
<td></td>
<td>CT Gateway 1655 - 1659</td>
</tr>
<tr>
<td></td>
<td>Service Device 1665 - 1669</td>
</tr>
<tr>
<td></td>
<td>Park Device 1675 - 1679</td>
</tr>
<tr>
<td></td>
<td>Queue DDI 1685 - 1689</td>
</tr>
</tbody>
</table>

Attendant Operators
For a description of how to create and configure attendant operators, see Operator Management, page 6-36.

<table>
<thead>
<tr>
<th>Name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPERATOR1</td>
<td>cisco</td>
</tr>
<tr>
<td>TESTOP</td>
<td>[BLANK]</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>
Upgrading Cisco Unified Attendant Console

This section describes how to upgrade your Cisco Unified Attendant Console server and client. Use the following table to determine whether your current Cisco Unified Attendant Console version can be upgraded to version 9.1.1,

<table>
<thead>
<tr>
<th>Your Cisco Unified Attendant Console version</th>
<th>Can be directly upgraded to version 9.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.(x)</td>
<td>No</td>
</tr>
<tr>
<td>2.0.1.(x)</td>
<td>No</td>
</tr>
<tr>
<td>3.1.1.(x)</td>
<td>No, Must first upgrade to version 8.0.0.(x)</td>
</tr>
<tr>
<td>8.0.0.(x)</td>
<td>Yes</td>
</tr>
<tr>
<td>8.0.3.(x)</td>
<td>Yes</td>
</tr>
<tr>
<td>8.6.1.(x)</td>
<td>Yes</td>
</tr>
<tr>
<td>8.6.2.(x)</td>
<td>Yes</td>
</tr>
<tr>
<td>9.0.1(x)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The following:

- Cisco Unified Attendant Console runs under Microsoft SQL Server 2008 only.
- You cannot change the edition of your Cisco Unified Attendant Console during an upgrade. To change the edition—for example from Business Edition to Enterprise Edition—you must perform a complete, clean re-installation and obtain a license for the new edition.
- If you upgrade the Cisco Unified Attendant Console server you also need to upgrade the Cisco Unified Attendant Console. If you do not, differences between the databases may cause inconsistent system performance.
When upgrading resilient server software, both the Publisher and Subscriber server machines must be running. If either machine is turned off or inaccessible, the upgrade may fail.

To upgrade Cisco Unified Attendant Console:

1. Ensure that your Cisco Unified Communications Manager version is compatible with the version of Cisco Unified Attendant Console you are upgrading to. For more information, see Cisco Unified Attendant Console Integration with Cisco Unified Communications Manager, page 1-6.

2. Ensure that you have the correct version of operating system and SQL database engine required by the Cisco Unified Attendant Console version. For more information, see:
   - Physical Server Software Requirements, page 3-2
   - VMware Software Requirements, page 3-4

3. Ensure that you are using an Application User account for integration with Cisco Unified Communications Manager.
   Cisco Unified Attendant Console version 8.0.0.5 and earlier used an End User account to communicate with Cisco Unified Communications Manager. Cisco Unified Attendant Console 8.0.3 and later uses an Application User instead of an End User. For details of how to create an Application User, see Creating and Assigning an Application User, page 4-3.

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

4. Download the Cisco Unified Attendant Console software. For more information, see Downloading the Software, page 5-4.

5. Sometimes you will need to re-license your Cisco Unified Attendant Console server. Each release of Cisco Unified Attendant Console has a three-part build number; for example: 8.0.3, where 8 is the major release number, 0 is the minor release number, and 3 is the maintenance release number.
   During major release upgrades—for example, upgrading from version 8.0.3 to version 9.0.1—the permanent licensing gets removed and your server reverts to a 5-day evaluation period. If you have a valid UCSS contract, you can request a new license activation code by visiting http://www.cisco.com/upgrade and using the tool there. You will need your service contract number to use this tool and order the upgrade.
   If you do not have a valid UCSS contract, you can purchase an à la carte upgrade. The following table shows the product number you will need to order. You need to order as many upgrades as you have licenses on your Cisco Unified Attendant Console server.

<table>
<thead>
<tr>
<th>Product</th>
<th>À La Carte Upgrade Product Number</th>
<th>Delivery Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Attendant Console Department Edition</td>
<td>L-CUACD9X-U-AC=</td>
<td>Electronic</td>
</tr>
<tr>
<td></td>
<td>CUACD9X-U-AC=</td>
<td>Paper</td>
</tr>
<tr>
<td>Cisco Unified Attendant Console Business Edition</td>
<td>L-CUACB9X-U-AC=</td>
<td>Electronic</td>
</tr>
<tr>
<td></td>
<td>CUACB9X-U-AC=</td>
<td>Paper</td>
</tr>
<tr>
<td>Cisco Unified Attendant Console Enterprise Edition</td>
<td>L-CUACE9X-U-AC=</td>
<td>Electronic</td>
</tr>
<tr>
<td></td>
<td>CUACE9X-U-AC=</td>
<td>Paper</td>
</tr>
</tbody>
</table>
Upgrading Cisco Unified Attendant Console Server

To upgrade a Cisco Unified Attendant Console server:

Step 1 Log in to the machine hosting the server, using a login with local administrator rights.
Step 2 Browse to the folder where the downloaded installation files are saved.
Step 3 Double-click the setup program.

The Wizard is prepared and you are presented with the Welcome screen.
Step 4 In the Wizard welcome screen, click Next.
Step 5 In the License Confirmation screen, click Next.

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

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

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

If you are upgrading to a new minor or maintenance release, for example from version 8.0.3 to 8.6.2, a new license file is required only if you are:

- Renaming your server
- Using new hardware
- Using a new virtual machine
- Upgrading from version 8.0.3 to a later release when already running in a virtual machine

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

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

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

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

7. License your Cisco Unified Attendant Console server, as described in Licensing Cisco Unified Attendant Console Software, page 6-4.

8. Install the Cisco Unified Attendant Console client over the existing installation. For more information, see Installing Cisco Unified Attendant Console Client, page 5-10.
Step 7  In the **SQL Server Login Information** screen, accept the SQL Server Username (default is `sa`) and type the Password (If you are using the SQL Express that was installed with the Cisco Unified Attendant Console software, the default password for the `sa` account is `Z1ppyf0rever`), and then click **Next**. This information is required to connect to the SQL databases.

### Note
The SQL Server login password must be sufficiently complex to meet the Windows policy requirements described at [http://support.microsoft.com/kb/965823](http://support.microsoft.com/kb/965823).

Step 8  If you have a resilient system and are upgrading the Subscriber server, in the **Publisher SQL Server Information** screen type the Publisher **Server Name**, **SQL User Name** and **Password**, and then click **Next**.

Step 9  In the **Server Information** screen accept the Cisco Unified Attendant Console **Server Machine Name / IP Address**, and then click **Next**.

Step 10  Do one of the following:
- If you are upgrading a standalone system, continue at **Step 11**.
- If you have a resilient system and are upgrading the Publisher server, you are prompted to allow the Wizard to stop the services on the Subscriber. Click **Yes** to continue. When prompted for the credentials of the Subscriber server to stop, enter the **Windows Username** and **Password**, and then click **Next**.
- If you have a resilient system and are upgrading the Subscriber server, you are prompted to allow the Wizard to stop the services on the Publisher. Click **Yes** to continue. When prompted for the credentials of the Publisher server to communicate with, enter the **Windows Username** and **Password** of your Publisher administrator login, and then click **Next**.

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

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

Step 13  In the **Cisco TSP Information** screen, accept the settings, and then click **Next**.

Step 14  In the **Choose Destination Location** screen, either accept the default destination folder or **Browse** to where you want to install the files, and then click **Next**.

Step 15  In the **Start Copying Files** screen, to start copying files, click **Next**.

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

Step 16  In the **Database Wizard**, click **Next**.

Step 17  You are prompted to overwrite the configuration database and then the logging database:
- Click **Yes** to create a new, empty database. This will delete all of your server settings, including queues and CTI port numbers.
- Click **No** to upgrade the existing database, retaining all of your server settings.

Step 18  When the wizard has installed the Configuration and Logging databases, click **Finish**.

Cisco Unified Communications Manager TSP is configured.

Step 19  If any third-party applications that might interfere with the TSP configuration are running, you are prompted to close and then automatically restart them. Accept this option and click **OK**.

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

Step 20  In the **Wizard Complete** screen, select **Yes, I want to restart my computer now**, and then click **Finish**.
Your computer restarts, with the Cisco Unified Communications Manager server installed.

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

If you have installed a resilient system, set up replication on your Publisher and Subscriber servers as described in Configuring Server Replication, page 6-39.
INDEX

A
access control group, creating and assigning roles 4-2
access numbers 6-31
Active MQ service, checking 1-4
agents (SQL Server replication) 6-38
antivirus software 3-5
application user, creating 4-3
AXL API 1-6

B
backing-up data 3-5

C
call arrival mode 6-32
call logging database, purging 6-9
call parking 1-6
Cisco TSP, uninstalling A-3
Cisco Unified Attendant Admin 1-1
  administrator password, changing 6-7
  Engineering menu 6-7–6-18
  home page 6-2
  logging-in 6-1
  System Configuration menu 6-18–6-30
  User Configuration menu 6-31–6-44
Cisco Unified Attendant BLF Plug-in
  logging 6-18
  starting/stopping 6-10
  status 6-12
Cisco Unified Attendant Console
  configuration management 6-31
  editions 1-1
  evaluating 5-4
  evaluation software, activating 6-4
  features 1-1
  integrating with Cisco Unified Communications Manager 1-6
  language support 1-4
  licensing software 6-4
  overview 1-1–1-8
  relicensing software 6-6
  upgrading F-1–F-5
Cisco Unified Attendant Console client 1-1
  installing 5-10
  requirements 3-6
Cisco Unified Attendant Console Downloads and Licensing website user account, creating 5-4
Cisco Unified Attendant Console server
  configuring 6-1–6-44
  example configuration E-1–E-2
  installing 5-1
  logging 6-17
  prerequisites 5-5
  redundancy and resilience 3-5
  requirements 3-1
  starting/stopping 6-10
  status 6-12
  uninstalling A-1–A-3
Cisco Unified Attendant CUPS Plug-in
  connection, configuring 6-15
  logging 6-18
  starting/stopping 6-10
  status 6-12
Cisco Unified Attendant LDAP Plug-in
logging 6-17
starting/stopping 6-10
status 6-12
Cisco Unified Communications Manager
connection, setting up and testing 6-13
integration with Cisco Unified Attendant Console 1-6
preparing 4-1–4-4
synchronizing device configurations 6-22
system devices 1-6
Cisco Unified Presence (CUP)
preparing 4-1
server (CUPS)
access, configuring 4-3
integration 1-8
Cisco Unified Replication 6-37–6-44
Cisco Unified Reporting 8-1–8-6
Client Matter Codes (CMC) 6-31
contacts database, synchronizing with source 6-28
CTI Manager D-2
CUCM, see Cisco Unified Communications Manager
CUPS, see Cisco Unified Presence server

D
Data Execution Prevention (DEP), setting 5-11
database
configuration 6-37
managing 6-8
logging 6-37
replication, uninstalling 5-6
deployment checklist 2-1
device configuration, synchronizing with Cisco Unified Communications Manager 6-22
directory
connection, testing 6-28
external, synchronization 6-25
field mapping 6-29
filtering during importing 6-30
source, connecting 6-27
.NET Framework, uninstalling A-2

E
emergency destination 6-35
exclusions for antivirus software 3-6

F
firewall exceptions 5-5
course client 5-10
for replication 6-40
Forced Authorization Codes (FAC) 6-31
full CTI failure device 6-34

H
hardware and software requirements 3-1–3-7

I
importing
directory information 6-30
installing the software 5-1
iPlanet Netscape Directory 6-25

L
logging servers and plug-ins, managing 6-15

M
Microsoft Active Directory 6-25
Microsoft SQL Server
Express 5-2
preparing 5-2
uninstalling A-2
Microsoft Windows Updates and Service Packs 3-7
Microsoft Windows Updates and Service Packs (on server) 3-5
music on hold (MoH) 1-7

N
network requirements 3-6
night service 6-36

O
operator phone requirements 3-7
operator profiles, creating and configuring 6-36
operator queues, creating and configuring 6-33

P
parking calls 1-6
publisher server 1-4
details, changing 6-8

Q
queue device groups 6-20
deleting 6-21
queue overflows 6-35

R
recall timers 6-32
Remote Access Connection Manager Service, disabling 5-9
replication 6-37–6-44
configuring 6-39
installing 6-40
monitoring 6-41
preparing 6-39
reinitializing 6-41
report 6-43
uninstalling 6-41
validating 6-42
reports B-1–B-6
report parameters B-2
resilience
inter-server communication link, checking 1-4
server 1-4
TAPI 1-7
rules (filters) for directory importing 6-30

S
search filter (Find) 6-20
server replication, see replication
server resilience 1-4
software requirements 3-1
SQL Server
2008 limitations 3-4
replication 1-4, 6-38
standalone installation 1-5
Standard Super Cisco Unified Communications Manager
User C-3
subscriber server 1-4
details, changing 6-8
synchronization errors 6-24
system reports B-1–B-6

T
TAPI D-1, D-2
TAPI resilience 1-7

U
upgrading the software F-1
User Account Control (UAC), disabling 5-2
User Group C-2
user group
assigning roles 4-2
creating 4-1
V

VMware server requirements 3-3

W

working days (working hours) 6-32