Cisco Unified Attendant Console Standard – Installation and Configuration Guide

Version 14.0.3
December 19, 2024

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

Text Part Number: OL-25987-01

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

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

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

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

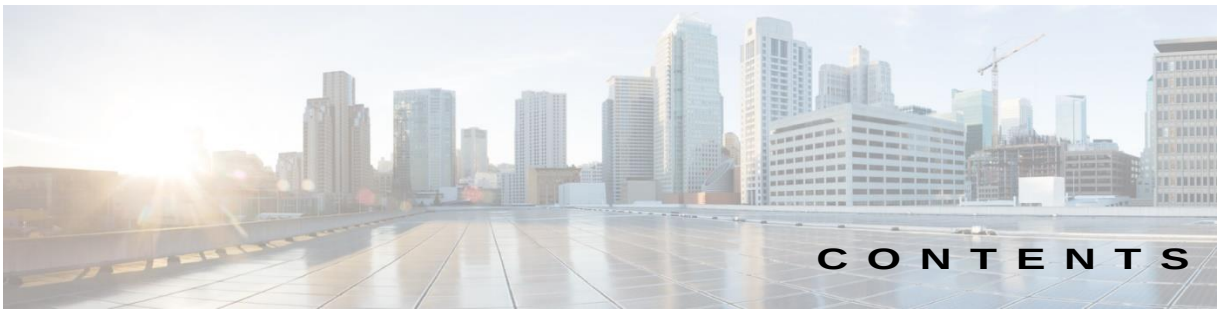
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

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

Cisco Unified Attendant Console Standard - *Installation and Configuration Guide*
© 2024 Cisco Systems, Inc. All rights reserved.



About This Guide vi
Who Should Read This Guide vi
How This Guide is Organized vi
Document Conventions vii
Obtaining Documentation and Submitting Service Requests viii

Introduction to Cisco Unified Attendant Console Standard 1
Accessibility for Users with Disabilities 1
Cisco Unified Attendant Console Standard User Interface 2
Accessing the Application Help Menu 3

License Cisco Unified Attendant Console Standard 4
Obtain Registration Code 4
Evaluation Licensing 5
Activate Evaluation Software 5
Manual Licensing 6
Upgrade Licensing 6
Activate Purchased and Upgraded Software 6
Apply License 7
Centralized Licensing 8
Create a SRV Record 8
Create a Network Shared Folder or Map Drive 10
Activate Purchased and Upgraded Software 11
Apply Licenses 12
Term-Based License Expiry and Relicensing 12
Term-Based License Expiry 12
Relicense Software 13
Obtain My Activations 13

Installing Cisco Unified Attendant Console Standard 14
Virtual Desktop Support 14
Wireshark 15
Network Requirements 15
Virus Scan Exclusions 16
Windows Folder Permissions 16
Cisco Unified Communications Manager Compatibility 17
Shared Lines and Extension Mobility 17
Configure Cisco Unified Communications Manager 18
Create an Access Control Group 18
Assign Roles to an Access Control Group 19
Create an Application User 19
Assign Devices to Application User 20
End User Account Required For Jabber Presence 21
Application Dial Rules 21
Install or Upgrade Cisco Unified Attendant Console Standard 21
Perform a Silent Installation 24
Obtain the Cisco Unified Attendant Console Standard installer and Silent Install package 24

Starting Cisco Unified Attendant Console Standard 28
Starting Cisco Unified Attendant Console Standard 28
Accessing Cisco Unified Attendant Console Standard When There Are No Valid Devices 30
Signing Out 30
Logging In to Hunt groups 31
Logging Out of Hunt groups 31
Exiting Cisco Unified Attendant Console Standard 31

Configuring Cisco Unified Attendant Console Standard 32
Preventing Access To Options Tabs 32
Making Options Tabs Accessible 33
Setting Operator Details 34
Configuring Single Sign-on 34
Configuring Presence Server 35
Modifying Presence Server Connection Details 35
Configuring Multi-Domain Presence Server 36
Configuring Single Domain Presence Server 36
Changing Cisco Unified Communications Manager directory source details 37

Primary Call Manager Detail 37
Backup Call Manager Detail 38
Setting the Operator Voicemail Prefix 39
Configuring Alerts 39
Managing Sign In Devices 40
Manually Adding Sign In Devices 40
Importing Sign In Devices 41
Deleting Sign In Devices 42

Directories 43
Directory Groups 43
Directory Synchronization 44
Synchronizing From a CSV Source File 45
Configuring Synchronization 45
Removing all contacts from CUCM directory synchronization 46
Directory Filtering 47
Creating Directory Filters 48
Directory Field Mappings 48
Destination Fields 49
Source Fields 49
Setting Directory Field Mappings 49
BLF Rules 50
Adding BLF Rules 50
Editing BLF Rules 51
Test All Rules 52
Deleting BLF Rules 52
Reordering BLF Rules 53
Directory Groups 53
Creating Directory Groups 54
Deleting Directory Groups 54
Renaming Directory Groups 55
Importing Contacts Into Directory Groups 55
Manually Adding Contacts To Directory Groups 56
Deleting Contacts From Directory Groups 57
Editing Contacts In Directory Groups and the Corporate Directory 58
Exporting Contacts From Directory Groups 58
Viewing and Using Directories 59

Changing the Directory Tab Order 60
Changing the Directory View 61
Searching For Contacts 62
Search Preferences 62
Viewing Contact Information 63
Contact Notes 64
Adding Contact Notes 64
Editing Contact Notes 64
Deleting Contact Notes 65

Call Tags 66
Contact Matching and Caller ID Pass-through 66

Keyboard Shortcuts 67
Defining and Editing Keyboard Shortcuts 69
Removing Keyboard Shortcuts 69
Resetting Shortcuts to their Default Values 70

Uninstalling Cisco Unified Attendant Console Standard 71

Application Log Configuration and Collection 72
Access the Logging Menu 72
Configuring Logging 72
Log Collection 73
Application Audit Logging 73
Disabling Audit Logging 74

Import/Export File Formats 75
XML File Format 75
Tags 76
CSV File Formats 76
CSV Files for Synchronization 76
CSV Files for Directory Import and Export 77
CSV Files for Importing Sign In Devices 79

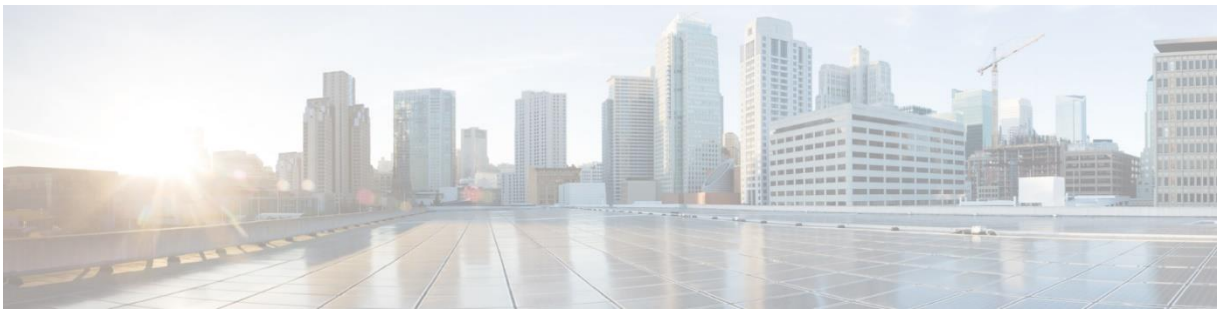
Phones Supported by Cisco Unified Attendant Console Standard 80

Manual Installation of TAPI Plug-in and Using a Cisco Unified Communications Manager TFTP server for all non-TAPI functions 83

Installation Instructions 83
Update Cisco TSP Primary CTI Manager Address, Application User and Password 84

Configuring Secure TSP 85
Secure TSP Configuration - Additional Role Requirements 85
Secure TSP Configuration - Cisco TSP Plugin Configuration 86

Security Best Practices 87
TLS Protocol Setup 88
Single Sign On 88
Directory Synchronization 88
Presence from Cisco IM & Presence 88



About This Guide

This guide describes how to install and configure Cisco Unified Attendant Console Standard.

Who Should Read This Guide

This guide is for deployment engineers, system administrators, and anyone else who installs or configures Cisco Unified Attendant Console Standard. You should have a knowledge of how to configure the Cisco Unified Communications Manager used by the application.

How This Guide is Organized

This guide contains the following sections.

Section	Contains
Introduction to Cisco Unified Attendant Console Standard	Introduction to Cisco Unified Attendant Console Standard.
License Cisco Unified Attendant Console Standard	License types and methods for acquiring and attaching licensing to Cisco Unified Attendant Console Standard.
Installing Cisco Unified Attendant Console Standard	Preparing Cisco Unified Communications Manager and installing Cisco Unified Attendant Console Standard.
Starting Cisco Unified Attendant Console Standard	Starting Cisco Unified Attendant Console Standard and configuring operator details.
Configuring Cisco Unified Attendant Console Standard	Configuring Cisco Unified Attendant Console Standard, including managing sign-in devices.
Directories	Using and controlling directories.
Call Tags	Using call tags and caller ID passthrough.
Keyboard Shortcuts	Setting up keyboard shortcuts.

Section	Contains
Uninstalling Cisco Unified Attendant Console Standard	Uninstalling Cisco Unified Attendant Console Standard.
Application Log Configuration and Collection	Configuring application logging.
Import/Export File Formats	Formats of import and export files.
Phones Supported by Cisco Unified Attendant Console Standard	List of supported Cisco phones.
Manual Installation of TAPI Plug-in and Using a Cisco Unified Communications Manager TFTP server for all non-TAPI functions	Instructions on how to configure Cisco Unified Attendant Console Standard with a TFTP server.
Configuring Secure TSP	Instructions on how to configure secure TSP.
Security Best Practices	Instructions on how to ensure security of the application.

Document Conventions

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

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

Means *reader take note*.

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

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

Obtaining Documentation and Submitting Service Requests

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

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

Introduction to Cisco Unified Attendant Console Standard

Cisco Unified Attendant Console Standard is a Microsoft Windows-based attendant console application for use with Cisco Unified Communications Manager (CUCM).

For an overview of the application features and a list of new and changed features, see the *Release Notes*.

Accessibility for Users with Disabilities

For information about the Cisco Unified Attendant Console Standard user interface and controls, see Cisco Unified Attendant Console Standard User Interface.

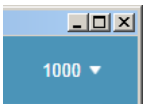
Cisco Unified Attendant Console Standard incorporates the following features to make it easier for blind and visually impaired people to use it:

- Most functions can be accessed using either the mouse or keyboard. You can define keyboard shortcuts for the most frequently used functions. For more information, see Keyboard Shortcuts.
- Set the size of call and directory text in the interface.
- A tooltip is displayed for each graphical interface control when the cursor is hovered over.

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

Cisco Unified Attendant Console Standard User Interface

The Cisco Unified Attendant Console Standard interface does all the standard operator tasks, including making calls, putting calls on hold and conferencing calls. The interface has the following main components.

Section	Contains
Main menu	Controls for using and configuring the application. Many of these controls are also available when you right-click specific parts of the interface. For example, controls relevant to the directories are displayed when you right-click in the directory pane.
	The extension used to sign into the application. You can click this to sign out of the application, or to log into and out of hunt groups.
Call Control pane	Displays the active call information on ***any*** line on the console phone, including the call status and duration, and controls for frequently used actions, such as transferring or ending the call.
Parked Calls pane	Displays active parked calls, by default in the order in which they were parked. Parked call information includes the park extension used, the identities of both the caller and the DN that parked the call, and how long the call has been parked.
Call History pane	This pane is not enabled by default; use **View > Show Call History** to enable it. When enabled, this pane displays calls completed in the current session, by default listed in reverse chronological order. You can change the order in which completed calls are listed. The **Details** column shows your call history, with the Status column showing whether the calls were dialed or received. The **Time and Date** column shows the time in *hhmm* format by default. To toggle the format between *hhmm* and *hhmmss*, right-click the column heading and either select or clear the **Include Seconds** option.
Directory pane	Displays the synchronized directory, directory groups and search results. Contact information includes line state, presence and any notes. Includes the following controls: – Unified Search box – Click to configure how searches are conducted. – Click to create a new directory group. For more information on the Directory pane, see Viewing and Using Directories.

You control the interface using both your mouse and keyboard. Many things that you can do with the mouse you can also do using your keyboard, provided that the application interface is selected.

Accessing the Application Help Menu

To display the Cisco Unified Attendant Console Standard Help Menu, do one of the following:

- Select **Help** > Cisco Unified Attendant Console Standard **Help**.
- Press **F1**.

The Help menu tools to search the help content:

- Text search tool
- Index
- Contents list.

License Cisco Unified Attendant Console Standard

This chapter explores the various license types and available methods for acquiring and attaching licensing to console clients. Users are encouraged to map out a licensing plan in advance of installing or upgrading the console.

Obtain Registration Code

Before you can license an application manually, you must obtain its registration code. As a local administrator, sign into each instance of Cisco Unified Attendant Console Standard that you want to license and activate, and do the following:

Step 1 Go to **Help > About** Cisco Unified Attendant Console Standard.

OR

Go to **File > Options > Licensing**.

Step 2 Note the **Registration Code**.

Tip

Users are encouraged to keep record of the registration code(s) and identifying information of the PC(s) they belong to. These codes will be subsequently used to obtain permanent licensing and will be required for any subsequent major upgrades. Centralized Licensing assists in this effort as it documents PC hostname, registration code and associated License Activation Codes.

Evaluation Licensing

Activate Evaluation Software

The software installs with a 10-day evaluation period. You have the option to extend the evaluation period to 60 days. Once the evaluation period has elapsed, the console becomes inoperable until a permanent license is applied.

Caution Evaluation licenses cannot be extended or reset.

To obtain and apply the 60-day evaluation license, do the following:

Step 1 Navigate to the *Cisco Unified Attendant Console Downloads and Licensing* website.

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 **Customer**, and then select the **Customer Site**.

Note If **Customer** or **Customer Site** do not exist, select the **Add** button, and then follow the on-screen prompts to add a new entry.

Step 5 Select the applicable **Version** and the **Product**, and then click **Next**.

Step 6 Enter the **Registration Code(s)** collected previously, and then click **Next**.

Note Click to create new fields for additional Registration Codes.

Step 7 Enter any additional email addresses where you want to receive the registration file. Separate multiple addresses with a comma, for example: *jane.doe@cisco.com,john.doe@cisco.com*. Then click **Submit**.

A registration (RGF) file is e-mailed to you. The RGF file contains activation keys and serial numbers for the 60-day evaluation period. The RGF file needs to be attached to each of the Cisco Unified Attendant Console Standard workstations whose registration codes were provided in the previous step.

Step 8 Open the email and save the RGF file to a location that can be browsed by Cisco Unified Attendant Console Standard. For information on how to apply the obtained license file, see Apply Licenses.

Manual Licensing

Manual licensing is the default licensing option.

Upgrade Licensing

The license type dictates the steps required to obtain and apply new licensing to your Cisco Unified Attendant Console Standard installation.

- Standard license type (SWSS, UCSS, à-la-carte upgrade licensing) (version-specific)
  - Users are strongly encouraged to await fulfillment of upgrade licensing order before upgrading Cisco Unified Attendant Console Standard. There are no options available to extend evaluation licensing nor are there options to apply an evaluation license to an install which has been previously fully licensed.
  - The activation process for upgrade licenses requires proof of entitlement in the form of previous activation data which can be either the prior version license activation code or associated registration code. The prior version license activation code must be activated before using to activate upgrade licensing.
  - When ready to activate upgrade licensing, see Activate Purchased and Upgraded Software.
- Term-based license type

  The steps required to license your install after upgrading depend on whether the registration code associated with your new install differs from that of your prior installation. For example, if you have migrated to a new PC or upgraded the operating system, your new installation carries a new registration code.

  If performing an in-place upgrade, which means the registration code remains the same after the upgrade, the following applies:
  - After upgrading Cisco Unified Attendant Console Standard, the only action required is to reattach the previously acquired license file. For more information about obtaining previous activation files, see Obtain My Activations.
  - After acquiring your existing licensing file (.rgf file extension), see Apply Licenses.

  If migrating to a new PC or performing an OS upgrade, which means the registration code differs following the upgrade, the following applies:
  - After upgrading Cisco Unified Attendant Console Standard, license your software. For more information, see Relicense Software.
  - Once the existing licensing has been reset, activate upgrade licensing. For more information, see Activate Purchased and Upgraded Software.

Activate Purchased and Upgraded Software

Once Cisco processes your order, you are provided with a PDF file containing one (or more) 27-digit License Activation Code (LAC).

To activate your purchased or upgraded software, do the following:

Step 1 Navigate to the *Cisco Unified Attendant Console Downloads and Licensing* website.

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 **Customer**, then click **Choose Selected Customer**.

Step 5 Select **Customer Site**, then click **Choose Selected Site**.

Note If **Customer** or **Customer Site** do not exist, select the **Add** button, and then follow the on-screen prompts to add a new entry.

Step 6 Select **License Type**, **Standard License**, then select **Choose selected license type**.

Step 7 Select the **Version**:

- **Flex Std** - This option applies to all A-Flex-3 - Named User licenses (PID - A-FLEX-CUAC-A, A-FLEX-CUAC-A-HA, and A-FLEX-CUAC-S).
- **10.x - 14.x** - For all other offerings (including perpetual licenses, upgrade licenses, Enterprise Agreement perpetual licenses, and A-Flex Enterprise Agreement licenses), select the version associated with your license activation codes.

Step 8 Select the **Product** (Cisco Unified Attendant Console Standard) that you have installed, and then click **Next**.

Step 9 You are asked if you want to activate licensing using a CSV file. Select **No** and click **Next**.

Step 10 Input **Registration Code** (one of the machine codes collected; for more information, see Manual Licensing), **License Activation Code**, *optional* **Computer Host Name** or **Location** to aid in future identification, and then select a **Term Start Date** (the date the license becomes active) for each instance. Then click **Next**.

Note Click to create new fields for additional Registration Codes.

Step 11 *This step only applies to Upgrade Licenses.*

Activating upgrade licenses requires the license activate code(s) or registration code(s) associated with the activation of the prior version. Input this data when prompted.

Step 12 In the License Request Confirmation page, provide an additional e-mail address(es) (separate multiple addresses with a comma) and click **Submit**.

A registration (RGF) file is e-mailed to you and any provided additional address(es). License request confirmation information is displayed in the web page.

Step 13 Open the email and save the registration file to a location that can be browsed by Cisco Unified Attendant Console Standard. To learn how to apply the obtained license file, see Apply Licenses.

Apply License

Step 1 In Cisco Unified Attendant Console Standard, go to **File** > **Options** > **Licensing**.

Step 2 Under **Manual Licensing Details** > **File Path**, click **Browse File** and upload the correct RGF file.

Step 3 Click **Validate**.

Centralized Licensing

Note

If centralized licensing is not configured during the installation, or changes to the centralized licensing configuration are required, do the following:

1. Open the application and go to **File > Options > Licensing**.
2. Enter the (new) **Automated Licensing Details** and click **Apply**.
3. Then close the application and relaunch it. Relaunching the application enables it to either create a populated *registration.csv* file if it didn't exist, or to populate the file with your application's information in case it did exist but was missing your information.

Caution

Currently, Centralized Licensing cannot be used to apply evaluation licensing. If you are not prepared to fully license your installation, proceed with manual licensing instructions.

As mentioned before, it is possible to license a Cisco Unified Attendant Console Standard application in multiple ways. For a single deployment, users can opt to license the application manually from a local repository. For more information, see Manual Licensing.

However, when it comes to managing multiple deployments, administrators can use **centralized licensing** to streamline the license activation, record keeping, and license installation processes. Cisco Unified Attendant Console Standard provides the following options for setting up the central license repository:

- SRV record: serving as a static alias for a local shared folder used to read and write registration and license details for Cisco Unified Attendant Console Standard. For more information, see Create a SRV Record.
- network shared locations. For more information, see Create a Network Shared Folder or Map Drive.

The advantage of using a SRV record as opposed to a Network Shared Folder or Map Drive becomes evident when the machine hosting the share is renamed or replaced.

- **SRV record**: any change requires updating the host machine name against the SRV record on the domain controller.
- **Network Shared Folder**: each installation of Cisco Unified Attendant Console Standard requires updating the **File > Options > Licensing** details.
- **Map Drive**: the new host machine needs to be mapped to each Cisco Unified Attendant Console Standard workstation.

Create a SRV Record

Tip

To achieve the greatest benefits of centralized licensing, the SRV record should be set up before installing the application. To set up a SRV record for centralized licensing, after the installation, navigate to the **File > Options > Licensing** menu.

A **SRV record** is a Domain Name System (DNS) resource record used to identify computers that host specific services. The benefit of using a SRV record for licensing is that in case of share host name changes, administrators are able to modify the SRV source record on the domain controller as opposed to modifying the user preferences of each Cisco Unified Attendant Console Standard installation.

To create a SRV record, do the following:

Step 1 Connect to the **DNS Server** and launch **DNS Manager**.

Step 2 Right-click and select **Other New Records**. Then select **Service Location (SRV)** and click **Create Record**.

Step 3 In the **New Resource Record** window, populate the following fields:

- **Domain**: pre-populated domain name.
- **Service**: the drop-down list offers pre-populated values like _http, _ftp, _ldap. However, it is recommended administrators use it to write a custom name, for example *_CUACSLicensing*.
- **Protocol**: write a custom value, for example *_tcp*.
- **Priority**: define a priority out of 10. For example, set to 0.
- **Weight**: define the weight value. For example, set to 0.
- **Port number**: enter a random port number, or a port you want to use.
- **Host offering this service**: provide the host name of the machine serving as the Centralized Licensing repository for Cisco Unified Attendant Console Standard.

Step 4 On the host offering this service, create a shared folder to which the Cisco Unified Attendant Console Standard Windows Users require read/write access.

Do the following:

a. Go to the host machine, create a New folder anywhere on it, for example on the Local Disk (C:), and name it **CUACS**.

Caution The folder name must be CUACS.

b. Right-click the folder and go to **Properties > Sharing > Advanced Sharing** and check **Share this folder**. Ensure the **Share Name** is *CUACS*.

c. Click **Permissions**, allow **Full control** for **Everyone**, click **OK** and then click **OK** again.

d. Navigate to **Properties > Security** and click **Edit** to change permissions.

e. Click **Add**, and under **Enter the object names to select**, enter **Everyone**. Click **OK**.

f. Under **Permissions for Authenticated Users**, with **Everyone** selected in the list, allow **Full control**, and click **Close**.

g. Click **Close** once more to complete the process.

Once you install Cisco Unified Attendant Console Standard using the instructions under Install or Upgrade Cisco Unified Attendant Console Standard, a file called *registration.csv* will be automatically created in this folder and used for license activation later on. For instructions on license activation, see Activate Purchased and Upgraded Software.

Create a Network Shared Folder or Map Drive

Note To achieve the greatest benefits of centralized licensing, the network shared folder or map drive should be set up before installing the application. To set up a network shared folder or map drive for centralized licensing, after the installation, navigate to the **File > Options > Licensing** menu.

Centralized licensing can be configured to reference a network shared folder or map drive. However, unlike using a SRV record, should there be changes to the network shared folder or map drive like location, host name or others, each instance of Cisco Unified Attendant Console Standard must be manually updated with the new information.

Create a Network Shared Folder

To create a network shared folder, do the following:

Step 1 Go to the host machine, create a New folder anywhere on it and give it any name, for example *Network-folder*.

Step 2 Right-click the folder and go to **Properties > Sharing > Advanced Sharing** and check **Share this folder**.

Step 3 Click **Permissions**, allow **Full control for everyone** and click **OK**.

Step 4 Go back to **Properties > Security** and click **Edit** to change permissions.

Step 5 Click **Add**, and under **Enter the object names to select**, enter **Everyone**. Click **OK**.

Step 6 Under **Permissions for Authenticated Users**, allow **Full control** and click **Close**.

Once you install Cisco Unified Attendant Console Standard using the instructions under Install or Upgrade Cisco Unified Attendant Console Standard, a file called *registration.csv* will be automatically created in this folder and used for license activation later on. For instructions on license activation, see Activate Purchased and Upgraded Software.

Create a Network Map Drive

To create a network map drive, see Create a Network Shared Folder. Then do the following:

Step 1 Go to the CUACS machine and locate the network shared folder you have just created.

Step 2 Right-click the folder and select **Map network drive**.

Step 3 Specify the drive letter and the folder that you want to connect to.

Step 4 Check the box to **Reconnect at login**. If required, check the box to **Connect using different credentials** and provide the necessary credentials to connect to the mapped drive.

Step 5 Click **Finish**.

Once you install Cisco Unified Attendant Console Standard using the instructions under Install or Upgrade Cisco Unified Attendant Console Standard, a file called *registration.csv* will be automatically created in this folder and used for license activation later on. For instructions on license activation, see Activate Purchased and Upgraded Software.

Activate Purchased and Upgraded Software

Prepare the registration.csv file

Once Cisco processes your order, you are provided with a PDF file containing one (or more) 27-digit License Activation Code (LAC).

In case of bulk licensing, the administrator can use the information from the PDF to populate the *registration.csv* file that was automatically created during installation. To prepare the *registration.csv* file, do the following:

- open the *registration.csv* file and enter the correct information in the **LAC** column using the PDF provided by Cisco.
- in case of an upgrade, and if the registration code changes, enter the **OldRegistrationCode**.

Activate licenses

Before proceeding, see Upgrade Licensing for details pertaining to upgrade licensing. To activate your licenses, do the following:

Step 1 Navigate to the *Cisco Unified Attendant Console Downloads and Licensing* website.

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 **Customer**, then click **Choose Selected Customer**.

Step 5 Select **Customer Site**, then click **Choose Selected Site**.

Note If **Customer** or **Customer Site** do not exist, select the **Add** button, and then follow the on-screen prompts to add a new entry.

Step 6 Select **License Type**, **Standard License**, then select **Choose selected license type**.

Step 7 Select the **Version**:

- **Flex Std** - This option applies to all A-Flex-3 - Named User licenses (PID - A-FLEX-CUAC-A, A-FLEX-CUAC-A-HA, and A-FLEX-CUAC-S).
- **10.x - 14.x** - For all other offerings (including perpetual licenses, upgrade licenses, Enterprise Agreement perpetual licenses, and A-Flex Enterprise Agreement licenses), select the version associated with your license activation codes.

Step 8 Select the **Product** (Cisco Unified Attendant Console Standard) that you have installed, and then click **Next**.

Step 9 You are asked if you want to activate licensing using a CSV file. Select **Yes**, then click **Choose File** and upload the *registration.csv* file you have previously updated. Click **Next** to see the populated license details according to the file you have uploaded, and then click **Next** again to go to the next step.

Step 10 In the **License Request Confirmation** page, provide an additional email address(es) (separate multiple addresses with a comma) and click **Submit**.

A zipped file called *CSVRegistration.zip* containing registration (RGF) files and a *registration.csv* file is emailed to you and any provided additional address(es). License request confirmation information is displayed in the web page.

Step 11 Apply your licenses. For more information, see Apply Licenses.

Apply Licenses

In order to apply the licenses, unzip and save the RGF files and the *registration.csv* file you have received by email to the same location the registration.csv file was first created. This is either a local shared folder, a network shared folder or a network map drive depending on your configuration. Replace the existing *registration.csv* file with the emailed one.

If the user has all the necessary access credentials, the application silently and automatically synchronizes the license from a shared location on application launch. However, if license synchronization fails, the user has several options:

- A window asking for **Access Credentials** pops up on application launch. The user can enter the correct access credentials here in order to synchronize the license.
- The user can skip the process above and instead log into the application and synchronize the license at **File > Options > Licensing > Sync License**.

Note Once a license has successfully synchronized with the console, attempting to trigger a subsequent manual sync with the same license file presents the error *Invalid License File*.

Term-Based License Expiry and Relicensing

Term-Based License Expiry

Beginning 30 days prior to license expiration date, Cisco Unified Attendant Console Standard will display the following license status alerts and warnings:

- 30 days prior to and the day of expiration:
  - Application **Title** bar: *License expires in X days*.
- 30-day grace period, beginning the day after the expiration date:
  - At application launch: *License expired on MM/DD/YYYY. Request that your System Administrator applies a new license before MM/DD/YYYY to avoid service interruption*. Click **OK** to proceed.
  - Application **Title** bar: *License expired*.
  - In the **Help > About** Cisco Unified Attendant Console Standard box: *X-year subscription expired. Apply new license within Y day(s) to avoid service interruption*.

Relicense Software

The following scenarios may remove the license from your install or change the Cisco Unified Attendant Console Standard registration code. In the event the registration code is changed, the existing license needs to be reset and subsequently activated against the new registration code.

Prior to executing any of the following actions, retrieve the existing registration code from the console client **Help > About** Cisco Unified Attendant Console Standard, or under **File > Options > Licensing**.

- Reinstall or upgrade the operating system on the same hardware
- Add or remove hardware (such as an NIC card or primary hard drive)
- Change the machine name (join or leave a domain)

To reset the Cisco Unified Attendant Console Standard license, contact Cisco Global Licensing Operations and request a re-host. You need to provide them with the original Cisco Unified Attendant Console Standard Registration Code or associated License Activation Codes.

Obtain My Activations

Step 1 Navigate to the *Cisco Unified Attendant Console Downloads and Licensing* website.

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

Step 3 From the left navigation pane, select **My Activations** or **My 60 Day Activations**.

Step 4 Locate and select the license file(s) you require.

Step 5 Provide any additional email addresses to send the files to, separating multiple addresses with a comma.

Step 6 Select **Resend**.

Installing Cisco Unified Attendant Console Standard

To install Cisco Unified Attendant Console Standard, do the following:

1. Validate that the PC satisfies the minimum hardware and software requirements. For more information, see the *Release Notes*.
2. Within Cisco Unified Communications Manager, create an Access Control Group, Application User, and associate any user devices and contact devices required.

   If you are working in a non-SSO environment and intend to use the Presence facility within Cisco Unified Attendant Console Standard, you must also set up an End User. For more information about setting up an end user, see End User Account Required For Jabber Presence. For more information about SSO, see Starting Cisco Unified Attendant Console Standard.
3. Install the Cisco Unified Attendant Console Standard software. For instructions, see Install or Upgrade Cisco Unified Attendant Console Standard.

   Optionally, perform a silent install instead. For instructions, see Perform a Silent Installation.
4. License your product. For instructions, see License Cisco Unified Attendant Console Standard.

Note Before proceeding with the installation, see Security Best Practices.

Virtual Desktop Support

Cisco Unified Attendant Console Standard supports **Persistent** and **Dedicated** Virtual Desktop infrastructures, including:

- Citrix Virtual Desktops (Standard, Advanced, and Premium) version 7.19, which requires Persistent and Dedicated configuration; see the Citrix product documentation.
- VMware Horizon (Standard, Advanced, and Enterprise), which requires Persistent and Dedicated configuration; see the VMware Horizon documentation.

Support is not extended to virtual application infrastructures, non-persistent virtual desktops, or to shared/floating user profiles. To review testing environment details, test criteria and test output, see the *CUAC Standard VDI Interoperability Guide*.

Wireshark

Caution If Wireshark needs to be installed on a Cisco Unified Attendant Console Standard workstation, it must be installed using the default settings with the exception of deselecting the **Npcap** component. If Npcap is a requirement, deselect the **Legacy loopback support for Nmap** option during Npcap setup instead. If Npcap is installed, it is known to cause issues with Cisco Unified Attendant Console Standard licensing.

Network Requirements

Cisco Unified Attendant Console Standard is a client application within the Cisco Unified Communications Manager (CUCM) infrastructure, and does not establish any listeners, being only a consumer of CUCM services.

The computer running Cisco Unified Attendant Console Standard must support TCP/IPv4 and permit access to the Cisco Unified Communications Manager and the Cisco Unified IM&P Server. By default, these connections leverage the following:

Component	Port type	Direction	Port number	Use
Cisco Unified Communication Manager	TCP	Bidirectional	443	AXL communication between Cisco Unified Attendant Console Standard and Communication Manager
Cisco Unified IM&P Server	TCP	Bidirectional	5222	XMPP communication between Cisco Unified Attendant Console Standard and IM&P Server
TSP	TCP	Bidirectional	2748	CTI communication between Cisco TSP and Communication Manager
TSP Media Driver	UDP	Bidirectional	50000 - 54000	Media ports

If you have a firewall on your computer, you must configure firewall exceptions for these ports or for any alternatives you may use in your installation.

Note Consider the default dynamic port range appropriate to your computer's operating system when defining firewall exceptions, as described at *https://support.microsoft.com/en-us/kb/832017*.

Round Trip Time

The maximum Round Trip Time (RTT) for TAPI communication between Cisco Unified Attendant Console Standard and Cisco Unified Communications Manager is 80ms. For more information, see the *Cisco Solution Reference Network Design*.

Virus Scan Exclusions

To prevent key system files from being quarantined by anti-virus software, add the following folders to the virus scan exclusions:

- *Program Files (x86)**Cisco*\Cisco Unified Attendant Console Standard
- *Users*\<*windows_user_name*>*AppData**Roaming**CUACSLayout*
- *ProgramData**CUACS*

Windows Folder Permissions

The following folders require the permissions outlined below:

- \Program Files (x86)\Cisco\Cisco Unified Attendant Console Standard\Users\<windows_user_name>\AppData\Roaming\CUACSLayout\Users\<windows_user_name>\AppData\Roaming\CUACSLogging\ProgramData\CUACS
  - Modify
  - Read & execute
  - List folder contents
  - Read
  - Write
  - Special permissions

Directory Contact Jabber Presence

Cisco Unified Attendant Console Standard can retrieve Jabber presence status for directory contacts.

You can leverage a single user account for multiple installations. We recommend that no more than 100 Cisco Unified Attendant Console Standard installations share a single user account.

Supported authentication methods:

- Cisco IM and Presence Server: supports Cisco Unified Communications Manager End User and Single Sign On (SSO) authentication.

Cisco Unified Communications Manager Compatibility

For more information about the operating system and Cisco Unified Communications Manager (CUCM) version compatibility matrix, see the *Release Notes*.

Shared Lines and Extension Mobility

Console User Devices and Lines

A shared line is any line that is presented on two or more devices.

Shared Lines on a Cisco Unified Attendant Console user's login device are supported, but with several caveats.

- The Call Control panel will only display active calls belonging to the device used to sign in to the application. However, the presence indicator belonging to the shared line within the Call Control panel will show line status across all instances of the line.
- Calls in a ringing state on the shared line will be presented within the Call Control panel.
- Held calls on the shared line will be presented within the Call Control panel, regardless of which device was used to place the call on hold.

For example:

  - Device A and Device B both display extension 1000.
  - User signs in to Cisco Unified Attendant Console Standard with Device A and sees extension 1000 presented in the Call Control panel.
  - A call comes in to extension 1000 displaying as a ringing call within the console user’s Call Control panel.
  - Device B answers the call. The call is no longer visible on the console user’s screen, but the console user’s extension 1000 presence indicator will show an active call.
  - Device B places the call on hold. The call appears in the Call Control panel as a held call, which the console user can now resume if desired.

Extension Mobility allows users to temporarily use another phone as their own, during which time that phone adopts the user’s configuration profile.

Cisco Extension Mobility users must sign in to their device prior to launching Cisco Unified Attendant Console Standard. Extension mobility devices must be associated with the application user, just as any other supported end point.

If the requirement is to have multiple operators using Cisco Unified Attendant Console Standard to answer calls ringing into a single destination (for example, an office’s main phone number), rather than relying on Shared Lines for call distribution, configure a hunt group (where each operator has a unique directory number associated with the Line Group) in Cisco Unified Communications Manager, using **Hunt Pilot > Hunt Group > Line Group**. This will prevent call control race conditions that could arise when multiple answer requests for a single call are simultaneously sent to Cisco Unified Communications Manager, and which could result in one request being fulfilled while the others return call control failures.

Directory Contact Devices and Lines

Directory contact extensions that are shared with multiple devices and/or extension mobility profiles are supported but carry the following caveats:

- For a device to be eligible for BLF status monitoring, it must be listed as a Controlled Device against the Cisco Unified Attendant Console Standard Application User account. See Assign Devices to Application User for device association instructions.
- Shared line and/or extension mobility BLF status extends to a single partition. If shared lines exist in multiple partitions, and all devices are assigned to the Application User, BLF status will be inaccurately presented within the contact directory.
- Busy Lamp Field (BLF) Status - Cisco Unified Attendant Console Standard will monitor a shared extension on a single, registered, device. Any activity on a shared line, regardless of the device being monitored, will impact BLF status. Device selection criteria consists of the following descending items:
  - Line Priority - devices are ranked based on the shared line position, with the line 1 position ranking the highest. If there is a tie, the next criterium is evaluated.
  - Device Name - devices are ranked alphanumerically, in ascending order.
- Registration Status - Cisco Unified Attendant Console Standard will monitor device registration status. If at any point a monitored device remains unregistered for 30 or more seconds, the device selection process will restart.
- Do Not Disturb is a device function, as opposed to a line state. Therefore, Do Not Disturb will only be presented in the contact directory, if the monitored device sets Do Not Disturb. Any other device, with the shared line, that enables Do Not Disturb will not impact contact directory BLF for any given shared line.

Configure Cisco Unified Communications Manager

Prior to installing Cisco Unified Attendant Console Standard, configure Cisco Unified Communications Manager by performing the steps described in this section.

Note If Cisco Unified Communications Manager was enabled for but not properly configured for secure TSP configurations, implementing the steps described in this section breaks communication between the Cisco Unified Attendant Console Standard and Cisco Unified Communications Manager. To configure Cisco Unified Communication secure TSP, see Configuring Secure TSP.

Create an Access Control Group

Access Control Groups define the roles and permissions available to the designated Application Users. To create an Access Control Group, do the following:

Step 1 Access Cisco Unified CM Administration.

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

Step 3 Click **Add New**.

Step 4 Type a **Name**.

Step 5 Click **Save**.

Assign Roles to an Access Control Group

Add roles to the Cisco Unified Attendant Console Standard Access Control Group by doing the following:

Step 1 Access Cisco Unified CM Administration.

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

Step 3 Search for the Cisco Unified Attendant Console Standard **User Group**.

Step 4 Click the **Roles** icon to the right of the group name.

Step 5 Click **Assign Role to Group**, and then click **Find**.

Step 6 Select the following roles:

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

Note

- Any divergence from the noted roles will break the solution.
- For more information on how to configure secure TSP, see Configuring Secure TSP.

Step 7 Click **Add Selected** to assign the roles.

Step 8 Click **Save**.

Create an Application User

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

- Each install requires an Application User with all console user devices and directory contact devices assigned to it.
- Multiple installs, using the same login devices and monitoring the same directory contact BLF states, require a single Application User with all console user devices and directory contact devices assigned to it.
- Multiple installs, using different login devices and/or monitoring different directory contact BLF states, require multiple Application Users. Each Application User would have its unique subset of controlled devices.
- You can associate up to 5000 lines (not phones) with the Application User.

To create an Application User and assign it to the Access Control Group, do the following:

Step 1 Access Cisco Unified CM Administration.

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

Step 3 Click **Add New**.

Step 4 Enter information in the following fields:

- **User ID**
- **Password**
- **Confirm Password**

Step 5 Under **Permissions Information**, select **Add to Access Control Group**.

Step 6 Search for and select the Cisco Unified Attendant Console Standard **Access Control Group**, and then click **Add Selected**.

Step 7 Click **Save**.

Assign Devices to Application User

To sign into Cisco Unified Attendant Console Standard and monitor Busy Lamp Status of directory contacts, the following related devices must be assigned to the Application User:

- The operator device
- Contact devices - so that you can see their line states in the directory

To determine the maximum number of devices that can be assigned to Cisco Unified Attendant Console Standard Application User(s), see **Scalability** in the *Release Notes*.

To associate devices with an Application User, do the following:

Step 1 Access Cisco Unified CM Administration.

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

Step 3 Search for the Cisco Unified Attendant Console Standard **Application User**, and then click the **User ID**.

Step 4 Under **Device Information**, find **Available Devices** and click **Device Association**.

Step 5 Search for and then select all relevant devices.

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

End User Account Required For Jabber Presence

Configuring the Cisco IM&P source for each install requires an End User account with presence enabled. This section pertains only to those installs that intend to present Jabber presence status within the Cisco Unified Attendant Console Standard contact directory.

If the Cisco Unified Attendant Console Standard users already have End User accounts configured against the presence sources, there is no requirement to create new accounts.

Supported authentication methods:

- Cisco IM and Presence Server: supports Cisco Unified Communications Manager End User and Single Sign On (SSO) authentication.

Application Dial Rules

Cisco Unified Communications Manager uses Application Dial Rules to add or remove digits from dialed numbers. Cisco Unified Attendant Console Standard synchronizes the rules from Cisco Unified Communications Manager at login. Application Dial Rules are applied to all outbound calls initiated by the user via the client.

If there are multiple rules, they are executed in the order defined in Cisco Unified Communications Manager. If the login synchronization fails, dial rules will not be applied.

During rule synchronization:

- New rules are added to the client repository.
- Existing rules in the client repository are updated as required.
- Rules deleted at a source level are removed from the client repository.

Note

- Rule modifications made following user login will not be reflected until the Cisco Unified Attendant Console Standard client is relaunched.
- Ensure that Call Park extensions do not conflict with Application Dial Rules. Conflicting extensions will prevent users from retrieving parked calls.
- Cisco Unified Attendant Console Standard will remove non-dialable characters (dialable characters include: *, +, 0-9, #) prior to processing Application Dial Rules.

Install or Upgrade Cisco Unified Attendant Console Standard

These instructions apply to new installs and in-place upgrades. To execute an in-place upgrade, the new installer can be executed without uninstalling the existing version.

When upgrading from one major version to another (for example, from version 11.x to 12.x), licensing resets to a 10-day evaluation license. For further licensing instructions, see License Cisco Unified Attendant Console Standard.

If the required third-party applications are not in place before executing the Cisco Unified Attendant Console Standard installer, the installation wizard first installs those which may cause the PC to restart. After restarting, the installation wizard automatically resumes.

To install Cisco Unified Attendant Console Standard, do the following:

Step 1 Confirm Cisco Unified Communications Manager compatibility. For more information, see **Cisco Unified Communications Manager Compatibility** in the *Release Notes*.

Step 2 Confirm that the Application User roles and device assignments align with their requirements. For more information, see Configure Cisco Unified Communications Manager.

Step 3 Log in to the Windows PC as a user with local administrator rights.

Step 4 Launch *CUACS_Setup.exe*. The installation wizard appears.

Step 5 In the **Welcome** page, click **Next**.

Step 6 In the **Cisco Unified Communications Manager Connection Details** page, type the Cisco Unified Communications Manager machine **IP Address**, your **CUCM Application User ID** and **Password**.

If you would like to skip the TSP download and installation, check **Skip TSP Download and Installation** and then click **Next**. A pop-up shows up to confirm you want to skip TSP.

If the connection fails, click Cancel. Validate the connection details or opt to **Skip TSP Download and Installation**, and then click **Next**.

Note

- Port 443 is used for the Cisco Unified Communications Manager connection by default. The Cisco Unified Communications Manager configuration can be changed following the installation. For instructions, see Changing Cisco Unified Communications Manager directory source details.
- *If you have downloaded and installed TSP, note the following*: The Cisco TSP Primary CTI Manager will match the provided Host Name, FQDN, or IP Address. This value can be modified following the installation as required. For instructions, see Update Cisco TSP Primary CTI Manager Address, Application User and Password. If you want to use a different node as the Primary CTI Manager, you can do this through the Cisco TSP configuration after installing Cisco Unified Attendant Console Standard.
- The Cisco Unified Communications Manager credentials are stored in the configuration file using AES-256 encryption.
- To configure Cisco Unified Attendant Console Standard with a TFTP server, see Manual Installation of TAPI Plug-in and Using a Cisco Unified Communications Manager TFTP server for all non-TAPI functions.

Step 7 In the two **Security Alert** messages, click **Yes**.

Step 8 In the **Language Information** page, select the required language, and then click **Next**.

Step 9 In the **Cisco Unified Presence Server Connection Information** page, type the following:

- **Server Address** of the Cisco IM&P server
- **Domain** containing the server
- **Cisco Unified Presence User Name**
- **Cisco Unified Presence Password**

Step 10 Click **Next**.

Note

- If you are working in a Cisco Single Sign On (SSO) environment, the SSO End User provides the Presence information, and the User defined here is not used.
- Port 5222 is used by default. You can change the Presence configuration after you have installed Cisco Unified Attendant Console Standard. For instructions, see Configuring Presence Server.
- The Presence credentials are stored in the configuration file using AES-256 encryption.

Step 11 In the **License Repository Options** page, select the appropriate licensing option.

a. Local licensing: the default option is to license locally by selecting **Local Repository**. If you select this option, proceed to Step 14.

b. Centralized licensing: to license from one central location, select either **SRV Record** or **Network Shared Location** depending on your configuration. If you select either one of these options, proceed to Step 12.

Note

For either option, the installer checks if a *registration.csv* file exists. If not, the installer creates it, either locally at *C:\ProgramData\CUACS* or at the specified centralized licensing location.

Step 12 *This step only applies to centralized licensing*.

Note

In order to use centralized licensing, administrators must go through these steps before installing the application. Otherwise, users can switch to centralized licensing via the **File > Options > Licensing** menu after the installation.

- If you have selected **SRV Record** in the previous step, in the **Central License Repository Connection Details** page, enter the **SRV Record Name** created by the administrator, for example *_CUACSLicensing*. For more information, see Create a SRV Record.
- If you have selected **Network Shared Location** in the previous step, in the **Central License Repository Connection Details** page, enter the network shared location or map drive created by the administrator. For more information, see Create a Network Shared Folder or Map Drive.

Step 13 Click **Next**.

- If the Windows user account executing the installer has access to the specified centralized licensing location, the installer continues to the next screen.
- If the Windows user account executing the installer does not have access to the specified centralized licensing location, the user is prompted to provide the **Username**, **Password** and **Domain** (if applicable) of an account with read/write permissions. Click **OK** on the prompt, provide the credentials, and then click **Next**.

  However, if the referenced repository or SRV record name does not exist, leave the credentials blank and proceed with the next step. The credentials can be provided after the application has been installed.

Step 14 In the **Choose Destination Location** page, either accept the default folder (recommended) or **Browse** to the folder in which to install the application, and then click **Next**.

Step 15 In the **Start Copying Files** page, if the details are correct, click **Next**. If not, click **Back** and correct the information. Cisco Unified Attendant Console Standard is installed.

Step 16 In the **InstallShield Wizard Complete** page, select *Yes, I want to restart my computer now*, and then click **Finish**.

Note

If the installation wizard is unable to download the TSP, you can fix the problem by doing the following:

1. In your web browser, under **Tools**, select **Internet Options**.
2. In the dialog box, select the **Advanced** tab.
3. Under **Security**, deselect (uncheck) **Check for publisher's certificate revocation**.
4. Under **Security**, deselect (uncheck) **Check for server certificate revocation.**
5. Click **OK**.

Perform a Silent Installation

Optionally, you can perform a silent installation instead. Follow the instructions in this section to build and execute a silent installation package.

Note

When performing a silent installation, all the prerequisites are automatically installed with no user interaction.

Obtain the Cisco Unified Attendant Console Standard installer and Silent Install package

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

Step 2 Create an account or login.

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

Step 4 Select Cisco Unified Attendant Console Standard.

Step 5 Download the required version.

Step 6 Download the silent install package *CUACS_Silent_Deployment*.

Step 1 - Unzip and Prepare Silent Install Repository

This is the package that you use to create the silent install answer file, as well as to subsequently deploy the package.

Step 1 Unzip the *CUACS_Silent_Deployment* package and move the enclosed **CUACS_Silent_Install** repository to the parent drive (default C:\) on the workstation used to create the answer file.

Step 2 Unzip the Cisco Unified Attendant Console Standard package and move the *CUACS_Setup.exe* file to the enclosed folder at *C:\CUACS_Silent_Install* (default).

Step 2 - Create Answer File

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

Note If you are using a repository other than the default *C:\CUACS_Silent_Install*, you must edit the repositories in the *createISS.bat* file before moving forward by right-clicking *createISS.bat*, selecting **Edit** and editing the location of the repository. Further instructions will refer to the default location of *C:\CUACS_Silent_Install* for simplicity purposes.

Step 1 Using full administrative rights, open Command Prompt/Powershell.

Step 2 Navigate to the *C:\CUACS_Silent_Install* folder.

Step 3 Type the command *createISS.bat* in the command window and press **Enter** to execute the batch file.

Step 4 This launches the installer. Provide the inputs required for the subsequent silent installs.

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

Step 3 - Prepare Cisco TAPI Plugin

If **Skip TSP Download and Installation** was selected when creating your ISS file, skip to Step 4 - Readiness Review.

If unsure whether **Skip TSP Download and Installation** was selected during install, right-click the *CUACS_Opr_New.iss* file in the *C:\CUACS_Silent_Install* repository and select **Edit**. Search for **Skip TSP**.

- If value = 1, then **Skip TSP Download and Installation** was selected. Therefore, you may skip this section and move to **Deploying Software**.
- If value = 0, then **Skip TSP Download and Installation** was not selected. Therefore, you must follow the instructions below.

Download TAPI installer from UCM

Step 1 Login to **Cisco Unified CM Administration**.

Step 2 Navigate to **Applications > Plugins**.

Step 3 Search for **Name + Begins with + Cisco TAPI**.

Step 4 Download the 64-bit **Cisco TAPI** plugin.

You must place the Cisco TAPI plugin in the designated **Default Repository** or recommended **Alternate Repository**.

- Plugin file: *CiscoTSPx64.exe*
- Default Repository: *C:\Users\Public\Desktop*

  If you wish to leverage the default repository, no edits are needed in the answer file. To proceed, ensure that the *CiscoTSPx64.exe* file resides in the defined repository on any target machine.
- Alternate Repository (recommended):

1. Navigate to the *C:\CUACS_Silent_Install* repository.
2. Right-click the *CUACS_Opr_New.iss* file and select **Edit**.
3. Locate **Alternate TSP Path=' '**.
4. Replace existing value (' ') with the absolute path for the *CiscoTSPx64.exe*.

   It is recommended you use **Alternate TSP Path=C:\CUACS_Silent_Install** because it results in having to manage a single repository for all things related to the silent deployment of Cisco Unified Attendant Console Standard.
5. Copy the *CiscoTSPx64.exe* file to the designated **Alternate TSP Path**.

Step 4 - Readiness Review

At this point, the **CUACS_Silent_Install** folder should contain, at a minimum, the following files:

- *createISS.bat*
- *CUACS_Opr_New.iss*
- *CUACS_Setup.exe*
- *CiscoTSPx64.exe* (if you are leveraging the recommended Alternate TSP Path)
- *runSilent.bat*

This complete package is used to execute silent installations.

Note The generated *.log* files are not necessary for successful installation if everything else is in the same folder.

Step 5 - Executing Silent Install

Step 1 Copy the packaged **CUACS_Silent_Install** repository to the parent drive of the target machine, default *:C*.

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

Step 2 Execute the *RunSilent.bat* batch file using full administrative rights, for example:

- Group Policy
- Command Prompt/Powershell

Step 3 Using full administrative rights, open Command Prompt/Powershell.

a. Navigate to the **C:\CUACS_Silent_Install** folder.

b. Type the command *RunSilent.bat* in the command window and press **Enter** to force start the batch file.

Note

- Following the installation of Cisco TSP, either as part of the Cisco Unified Attendant Console Standard silent install or manual install via alternative effort, the workstation is automatically restarted.
- If the **Skip TSP Download and Installation** option was enabled, Cisco TSP must be manually installed on the workstation prior to launching Cisco Unified Attendant Console Standard.

Starting Cisco Unified Attendant Console Standard

Starting Cisco Unified Attendant Console Standard

To start the Cisco Unified Attendant Console Standard client:

Step 1 Double-click the desktop icon. A splash screen appears.

Step 2 Cisco Unified Attendant Console Standard provides SSO and non-SSO mode for the application. The Cisco Unified Attendant Console Standard Sign In screen appears if one of the following is true:

- You are working in a non-SSO environment; therefore, the application does not need any additional credentials to log in but instead runs under the logged in user profile.
- You are working in an SSO environment but have not yet configured Cisco Unified Attendant Console Standard to use it. For information on how to configure the application, see Configuring Single Sign-on.
- You have configured Cisco Unified Attendant Console Standard to use the SSO environment and have already logged into it through another application, such as Jabber.

The Cisco Unified Attendant Console Standard Sign In screen contains either the number of the last attendant phone used to sign in, or the text Extension, showing that you need to enter an attendant phone number. Continue at Step 3.

Alternatively, if you are working in an SSO environment, but have not yet logged into any Cisco Unified Communications application, do the following:

a. If security alerts are displayed, click **Yes** in each.

b. In the SSO credentials web page, enter your **User Name** and **Password**, and then click **Log In**.

Note If the login details are invalid, a message appears and the application closes. Either try to log in again using correct SSO details, or contact your network administrator.

The Cisco Unified Attendant Console Standard Sign In screen appears, containing either the number of the last attendant phone used to sign in, or the text Extension, showing that you need to enter an attendant phone number.

Step 3 In the Cisco Unified Attendant Console Standard Sign In screen: To use the number in the field, proceed to Step 4. To use a new extension number:

a. Type the number into the field. As you type, the application lists those devices available for signing in that match the number. For more information on defining devices, see Managing Sign In Devices. The more you type, the shorter the list becomes. The list contains the name and extension number for each matching device.

Note If the Device List under the **File > Options > Device List** tab is empty, all devices associated with the application user are available for signing into Cisco Unified Attendant Console Standard. For more information, see Assign Devices to Application User.

If the Device List contains one or more devices, you can sign in using one of them. If all the devices in the Device List are invalid, you will be unable to sign in without the assistance of a system administrator. For more information, see Accessing Cisco Unified Attendant Console Standard When There Are No Valid Devices.

b. Select a number in the list by either double-clicking it, or by highlighting it and then pressing **Enter**. You can close the list and clear the selection by pressing **Esc**.

Step 4 If the sign in extension is part of one or more hunt groups, and you want the application to log you into them during sign in, select **Log in to hunt groups at sign in**.

Note
- If you are already logged into your hunt groups, you do not need to set **Log in to hunt groups at sign in**.
- You cannot log in to a hunt group using an extension that is already being used by another Cisco Unified Attendant Console Standard user.

Step 5 Click **Sign In** or press **Enter**. The number you are trying to sign in with is checked against the list of valid extensions.

Step 6 Depending on the devices available, you may need to do one of the following

- If there are no valid devices, a message is displayed requesting that you contact your system administrator to create a valid device. For more information, see Accessing Cisco Unified Attendant Console Standard When There Are No Valid Devices.
- If several valid devices have the same extension number, or if one or more valid devices has multiple lines, a list of the devices and lines is displayed. Select the device and line to use, and then click **OK**.

The main application user interface appears, ready for you to use.

If there was no device list and you entered the extension number of a valid Cisco device, that device and all its lines is added to the device list.

Note If the partition of the line used to sign into the console is changed while the console is in use, the user must sign out and sign back into the console.

While the application is running, you can change the attendant console operator directory number (DN). For more information, see Setting Operator Details.

Accessing Cisco Unified Attendant Console Standard When There Are No Valid Devices

If there are no valid devices in the Device List, the system administrator must create at least one - or clear the Device List.

To access Cisco Unified Attendant Console Standard when no valid device is available in the Device List, the system administrator must do the following:

Step 1 In the Sign In screen invalid extension message, click **Administrative Override**.

Note The **Administrative Override** link appears only when there is a Device List containing at least one device.

Step 2 Do one of the following:

- When an **Options Password** has not been set, the **Options** window appears, with the **Device List** tab displayed. Clear all devices from the list or add one or more new devices. For more information, see Manually Adding Sign In Devices.
- When an **Options Password** has been set, the **Options** window appears, with the **Options Password** tab displayed.
  - **a.** Make the Device List tab accessible. For more information, see Making Options Tabs Accessible.
  - **b.** Clear all devices from the list or add one or more new devices. For more information, see Manually Adding Sign In Devices.

Step 3 Close the **Options** window.

Signing Out

To sign out an attendant console session, do either of the following:

- In the main menu, click the extension number at the top right of the interface, and then select **Sign out of application**.
- Use the **Ctrl+S** keyboard shortcut.

The sign in screen is displayed.

Note

- Active synchronizations of the directory at the time of sign out will continue in the background unless the application is closed.
- At sign out, active hunt group logins are logged out.

Logging In to Hunt groups

A *hunt group* is a group of extensions configured so that an unanswered call to any extension gets forwarded to one of the other lines in the group. Cisco Unified Communications Manager supports hunt groups, and Cisco Unified Attendant Console Standard enables you to sign in using a device that is part of one or more hunt groups, so that calls to the groups can be received through your operator phone.

If you are logged out from any hunt groups, you will not receive any calls through the groups.

If you are not logged in to the hunt groups of which your extension is part, you can either log in to them when you sign in to the application (for more information, see Starting Cisco Unified Attendant Console Standard), or you can click the extension number at the top right of the interface, and then select **Login to hunt groups**.

While you are logging in to the hunt group (which may take a few seconds) you will not be able to receive any new calls, but current calls will continue unaffected, and you will be logged in at the end of the current call.

Logging Out of Hunt groups

If you are logged in to a hunt group, to log out do either of the following:

- Click the extension number at the top right of the interface, and then select **Log out of hunt groups**.
- User the **Ctrl+I** keyboard shortcut.

When you sign out, you are automatically logged out of any hunt groups to which you belong.

While you are logging out you cannot take calls, but current calls will continue unaffected. You will be logged out at the end of the current call.

Exiting Cisco Unified Attendant Console Standard

To exit Cisco Unified Attendant Console Standard, do one of the following:

- In the main menu, choose **File > Exit**.
- Use the keyboard shortcut you have defined. For more information, see Defining and Editing Keyboard Shortcuts.
- Click the window close button.

Configuring Cisco Unified Attendant Console Standard

This chapter describes how to configure Cisco Unified Attendant Console Standard.

All the configuration functions are contained within tabbed pages of the **Options** window, which you access by choosing **File > Options**. You can password-protect the following **Options** tabs:

- Directory Filters
- Directory Mappings
- BLF Rules
- Device List
- Logging

This chapter provides information about enabling and disabling password protection, and it describes various configuration procedures and synchronization configuration with Cisco Unified Communications Manager.

Preventing Access To Options Tabs

In the application's default state, all the Options tabs are accessible by any user. You can use the **Options Password** to prevent access to the password-protected Options tabs listed under Configuring Cisco Unified Attendant Console Standard.

To prevent access to the password-protected Options tabs:

Step 1 In the main menu, choose **File > Options**. The **Options** window appears.

Step 2 Click the **Options Password** tab.

Step 3 Select **Password Protection**.

Step 4 Type the **Application Password** (the Cisco Unified Communications Manager Application User password specified in the **CUCM Configuration** tab. For more information, see Changing Cisco Unified Communications Manager directory source details.

Step 5 Click **Apply**.

Step 6 Click **Cancel** to close the Options window.

The password-protected Options tabs are now inaccessible.

Making Options Tabs Accessible

You can regain access to the Options tabs listed under Configuring Cisco Unified Attendant Console Standard by entering the correct **Options Password**. To regain access to the password-protected Options tabs:

Step 1 In the main menu, choose **File > Options**. The **Options** window appears.

Step 2 Click the **Options Password** tab.

Step 3 Type the **Application Password** (the Cisco Unified Communications Manager Application User password specified in the **CUCM Configuration** tab. For more information, see Changing Cisco Unified Communications Manager directory source details.

Step 4 Click **Authenticate**.

If you have entered the password incorrectly, the **Application Password** field is highlighted, otherwise the **Password Protection** and **Application Password** controls appear.

You now have temporary access to the password-protected Options tabs, and you can make and apply changes to their settings. To keep the Options tabs password-protected after you finish modifying the settings, click **Cancel** to close the Options window, and then skip the rest of this procedure.

Step 5 Clear **Password Protection**.

Step 6 Type the **Application Password.**

Step 7 Click **Apply**.

Step 8 Click **Cancel** to close the Options window.

Password protection is disabled and all the Options tabs are now accessible.

Note

If you forget the Options Password, you can either:

- change the password of the existing Cisco Unified Communications Manager Application User,
- create a new Application User with a new password,

and then validate the credentials under the CUCM Configuration tab, and enter the new password under the Options Password tab.

Setting Operator Details

You set your operator details either when you start Cisco Unified Attendant Console Standard or while it is running.

To set the operator details while Cisco Unified Attendant Console Standard is running, do the following:

Step 1 In the main menu, choose **File > Options**. The **Options** window appears.

Note You can configure a keyboard shortcut to do this. For instructions, see Keyboard Shortcuts.

Step 2 Click the **Operator Details** tab.

Step 3 Under **Operator Details**, type the **Extension** of the attendant console operator.

Note If a **Device List** is defined, the same restrictions as on the sign in extension apply, but the list is not displayed when you start typing. For more information, see Managing Sign In Devices.

Step 4 Then, under **When a Call is Forwarded or Diverted**, set which number to show in case a call has been forwarded or diverted. You can select either **First redirected number** or **Last redirected number**. This information is shown in the Call Control pane, within the active call information, and Call History pane, in the Details column.

Step 5 Click **Apply**.

Configuring Single Sign-on

Cisco Single Sign On (SSO) is a facility designed to help users who run multiple Cisco Unified Communications applications in a work session. Once a user signs in to any one configured application, they do not need to subsequently sign into other applications.

Cisco Unified Attendant Console Standard supports the following single sign-on Identity Providers:

- Microsoft Active Directory Federation Services (ADFS)
- OpenAM
- Ping

Leveraging Single Sign-On authentication introduces the following user experiences:

- SSO runs for a configurable length of time. If the session expires while Cisco Unified Attendant Console Standard is running, the user is prompted to re-authenticate.
- The application will not start until the user authenticates via SSO.
- If a user signs in using SSO for another Cisco Unified Communications application, prior to launching Cisco Unified Attendant Console Standard, the user will not be prompted to sign in again.
- If a user has not previously signed into another Cisco Unified Communications application, prior to launching Cisco Unified Attendant Console Standard, the user will be presented with a SSO login screen.

To configure Single Sign On, do the following:

Step 1 In the main menu, choose **File > Options**. The **Options** window appears.

Note You can configure a keyboard shortcut to do this. For instructions, see Keyboard Shortcuts.

Step 2 Click the **Operator Details** tab.

Step 3 Under **Presence Details**, select **Use Single Sign-On**.

Note
- If Cisco Unified Attendant Console Standard is running in a non-SSO environment, this control is disabled.
- If you have already entered valid SSO credentials, this control will already be selected.
- You do not need to click Apply to save and apply the Use Single Sign-On setting.

To stop using Cisco Unified Attendant Console Standard with SSO, repeat the above procedure but clear **Use Single Sign-On**. If you want to display Presence information outside of the SSO environment, you must define which Presence Server to use, as described in the next section.

Configuring Presence Server

Modifying Presence Server Connection Details

To add or modify Cisco Presence server connection details, do the following:

Step 1 In the main menu, choose **File > Options**. The **Options** window appears.

Note You can configure a keyboard shortcut to do this. For instructions, see Keyboard Shortcuts.

Step 2 Click the **Operator Details** tab.

Step 3 Under **Presence Details**, edit the following as required:

- Select or clear **Use Single Sign-On**.
  - This control is disabled if Cisco Unified Attendant Console Standard is not running in a SSO environment. Select this to use the End User accessed through the SSO login web page to provide Presence information.
- **Presence Server Address** or URL required for hosted presence.
- **Presence Server Port** number. By default, this is 5222.

- **Domain** containing the Presence Server:
  - Configuring Multi-Domain Presence Server
  - Configuring Single Domain Presence Server
- **Presence Server User** name.
  - If you are using SSO, this will be the user name chosen for SSO validation, and you will be unable to edit it.
- Corresponding user **Password**.
  - If you are using SSO, this will be blank and you will not be able to edit it.

Note The Presence credentials are stored in the configuration file using AES-256 encryption.

Step 4 Click **Apply**. The application validates the connection. If this fails, it prompts you for the correct connection details.

Step 5 Perform a search to refresh the contact and display the correct presence state.

Configuring Multi-Domain Presence Server

If your Presence server supports multi-domains, do the following:

Step 1 In the main menu, choose **File > Options**. The **Options** window appears.

Step 2 Click the **Operator Details** tab.

Step 3 Under **Presence Details**, edit the following:

- Delete the **Domain** value.
- Type the **User ID** (formatted as full URI).

Note Contact User IDs must be formatted as full URIs. Subscription request will pass the unmodified contact URI to the Presence Server.

Configuring Single Domain Presence Server

If your Presence server supports a single domain, do the following:

Step 1 In the main menu, choose **File > Options**. The **Options** window appears.

Step 2 Click the **Operator Details** tab.

Step 3 Under **Presence Details**, edit the following:

- Type the **Domain** value.
- Type the **User ID** without affixing the domain.

Note

Cisco Unified Attendant Console Standard will affix the specified domain to unmatched contacts. For example:

- Configured Domain = cisco.com
- Contact User ID in directory = john.doe@acme.com. Subscription request will be made for john.doe@acme.com@cisco.com.
- Configured Domain = cisco.com
- Contact User ID in directory = john.doe@cisco.com. Subscription request will be made for john.doe@cisco.com.

Changing Cisco Unified Communications Manager directory source details

Note

- Cisco Unified Communications Manager version must match the existing version.
- Certain menus may require a password to unlock. For more information, see Preventing Access To Options Tabs.

Primary Call Manager Detail

To change the Cisco Unified Communications Manager directory source details, do the following:

Step 1 In the main menu, choose **File** > **Options**. The **Options** window appears.

Step 2 Click the **CUCM Configuration** tab.

Step 3 Under **Primary Call Manager Detail**, edit the following as required:

- The Cisco Unified Communications Manager **Server Address**.
- The Cisco Unified Communications Manager **Port** number. By default, this is 443.
- The Cisco Unified Communications Manager **Application Username**. The Application User must have assigned roles. For more information, see Assign Roles to an Access Control Group.
- The **Application Password** that corresponds with the Username.

Note

The Cisco Unified Communications Manager credentials are stored in a database using AES-256 encryption.

Step 4 Click **Apply**.

If the new CUCM version does not match the currently configured CUCM version, a warning message appears.

Step 5 Exit and then restart Cisco Unified Attendant Console Standard for the changes to take effect.

Backup Call Manager Detail

Setting up backup Call Manager details is optional. If you set up a backup CUCM, Cisco Unified Attendant Console Standard will still prioritize the primary CUCM but will attempt to connect to the backup if the primary is unavailable.

If you do not want to use it, leave the Server Address field empty. Otherwise, do the following:

Step 1 In the main menu, choose **File** > **Options**. The **Options** window appears.

Step 2 Click the **CUCM Configuration** tab.

Step 3 Under **Backup Call Manager Detail**, edit the following as required:

- The Cisco Unified Communications Manager **Server Address**.
- The Cisco Unified Communications Manager **Port** number. By default, this is 443.
- The Cisco Unified Communications Manager **Application Username**. The Application User must have assigned roles. For more information, see Assign Roles to an Access Control Group.
- The **Application Password** that corresponds with the Username.

Note The Cisco Unified Communications Manager credentials are stored in a database using AES-256 encryption.

Step 4 Click **Apply**.

If the new CUCM version does not match the currently configured CUCM version, a warning message appears.

Step 5 Exit and then restart Cisco Unified Attendant Console Standard for the changes to take effect.

Setting the Operator Voicemail Prefix

Note Access to the functions described in this section may be restricted by your system administrator, and you may need a password to access the necessary Options tab. For more information, see Preventing Access To Options Tabs.

If your operator uses a separate voicemail number, you define its prefix. To set the operator voicemail prefix, do the following:

Step 1 In the main menu, choose **File > Options**. The **Options** window appears.

Note You can configure a keyboard shortcut to do this. For instructions, see Keyboard Shortcuts.

Step 2 Click the **CUCM Configuration** tab.

Step 3 Under **Transfer to Voicemail Option**, type the attendant console operator **Voicemail Prefix**.

Step 4 Click **Apply**.

Configuring Alerts

Cisco Unified Attendant Console Standard alerts you when the following events occur (listed in order of precedence):

1. Call is ended (not by console)
2. Device is in service (the console device)
3. Call is ringing at primary device
4. Call is ringing at secondary device
5. Device is out of service (the console device)
6. A system error has occurred

If two or more alerts occur simultaneously, you are alerted about the one with the highest precedence. Cisco Unified Attendant Console Standard can produce the following visual alerts:

- If the application is not the active window, it becomes the active window and is placed in front of any other open window, ready for you to interact with it.
- If the application is not the active window, then in the Windows taskbar the application icon flashes.

To configure alerts, do the following:

Step 1 In the main menu, choose **File > Options**. The **Options** window appears.

Note You can configure a keyboard shortcut to do this. For instructions, see Keyboard Shortcuts.

Step 2 Click the **Alerts** tab.

Step 3 Under **Alerts Detail**, for each event, do the following:

- Select the **Taskbar** checkbox if you want the application icon in the Windows taskbar to flash when that event occurs.
- Select the **Pop to Front** checkbox if you want the application window to be displayed in front of all others on the desktop when it is minimized to the taskbar or hidden at the time of the event.

Step 4 Click **Apply**.

Managing Sign In Devices

Attendants can only sign into Cisco Unified Attendant Console Standard using a valid Cisco device, with a device name, extension, and line number. For attendants to be able to make calls, the device must also be associated with the Application User/End user configured in the Cisco TSP.

System administrators define which devices are available for attendants to use; these devices constitute the **Device List**, which is accessible using **File > Options > Device List**. At start-up and during execution, the application checks whether the devices in the Device List are associated with the Application User/End User configured in the Cisco TSP.

- If they are not, they are marked as invalid. These have a lighter color in the list, and attendants cannot make calls using them.
- If they were previously marked as invalid but are now associated with the Application/End user, they are marked as valid, and attendants can make calls using them.

Administrators can either manually add devices to the list or import them from CSV files.

While importing sign in devices from a CSV file, the application checks that each device is associated with the Application/End User configured in the Cisco TSP. If a device is not associated, it is shown as invalid in the Device List.

If additional lines are later associated with a sign in device (using Cisco Unified Communications Manager), they get added to the Device List. After these changes, attendants will still be able to sign in using the old extension.

Manually Adding Sign In Devices

Note Access to the functions described in this section may be restricted by your system administrator, and you may need a password to access the necessary Options tab. For more information, see Preventing Access To Options Tabs.

To manually add devices:

Step 1 Choose **File > Options > Device List**. The **Device List** appears.

Step 2 Under **Device List**, click **Add Devices**.

Step 3 In **Search Devices**, type a device name. All devices matching what you type are listed; and the more characters you type, the shorter the list becomes. Non-Cisco devices are not listed.

Step 4 For each device you want to add, select the **Add** checkbox.

Note If there are multiple lines on the selected device, all the lines are selected and added to device list.

Step 5 Click **Apply**.

The devices are added to the Device List.

Importing Sign In Devices

Note Access to the functions described in this section may be restricted by your system administrator, and you may need a password to access the necessary Options tab. For more information, see Preventing Access To Options Tabs.

You can import sign in devices from a CSV file. For more information, see CSV Files for Importing Sign In Devices.

To import devices from a CSV file:

Step 1 Choose **File** > **Options** > **Device List**.

Step 2 Under **Import From CSV**, click **Browse** and select the file to import.

The file name and path are displayed under **File Location**.

Note If you click **View Sample** you can view the required format of the CSV file for importing login devices.

Step 3 Click **Import Devices**.

The file format is validated, and if any devices in the file are non-Cisco, you are informed that they will not be imported, and then you are prompted to continue. To import the Cisco devices from the file, click **Yes**. To abort the process, click **No**.

The devices are imported and added to the Device List. As the devices are imported, they are checked against those already listed and any matching devices are ignored.

Deleting Sign In Devices

Note Access to the functions described in this section may be restricted by your system administrator, and you may need a password to access the necessary Options tab. For more information, see Preventing Access To Options Tabs.

To remove devices:

Step 1 Choose **File > Options > Device List**.

In the Device List, click the corresponding **X** in the **Delete** column.

Note If a device has multiple lines, all are deleted from the list. The device remains in the database.

Step 2 In the confirmation message, click **Yes**.

Directories

Cisco Unified Attendant Console Standard displays one or more directories of contacts. Always displayed is your corporate directory (shown in the interface as **Directory**), which is copied from one or more of the following sources:

- Cisco Unified Communications Manager
- A comma-separated-variable (CSV) file. CSV file names have the *.csv* extension.

Note The CSV file can be on any shared network location to which Cisco Unified Attendant Console Standard has read access.

Cisco Unified Communications Manager is the usual source of your corporate directory. Up to date contact information is copied from the source into Cisco Unified Attendant Console Standard by the synchronization process. For a description of this, see Directory Synchronization.

Directory Groups

You can also view and connect to contacts that are not in your synchronized directory but which you want to be able to select quickly. These directory groups can contain any combination of the following:

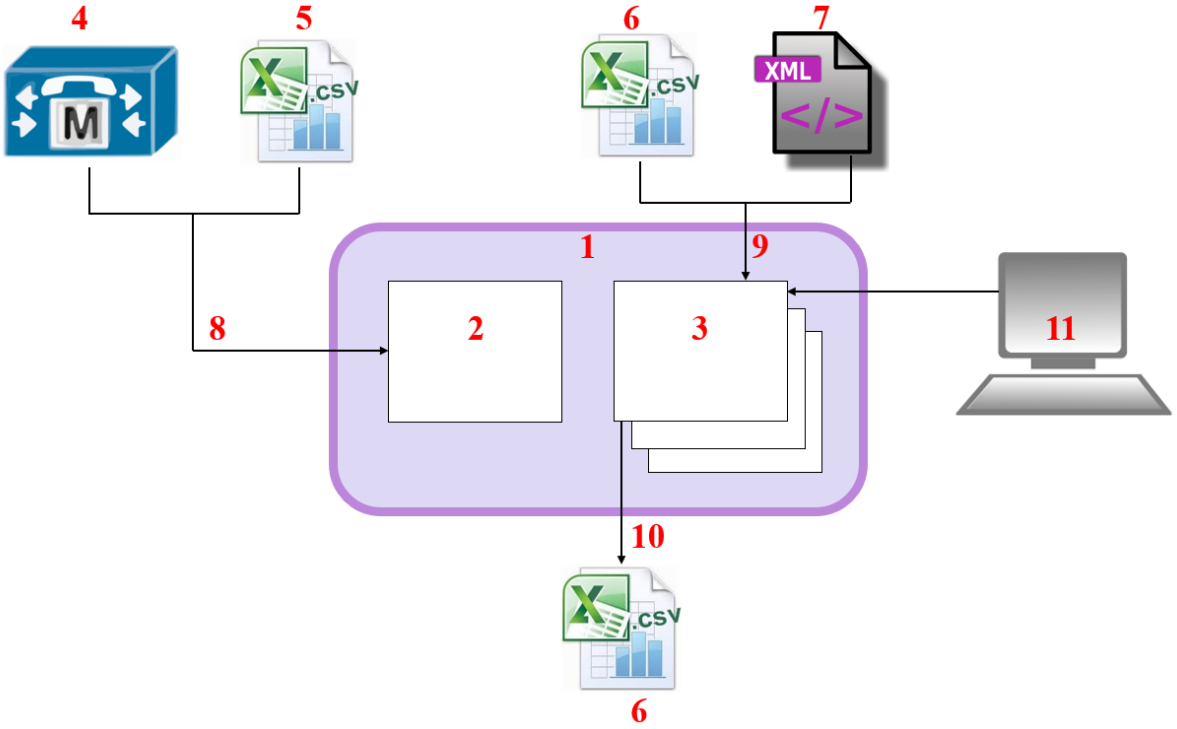
- Contacts imported (copied) from sources other than those listed above. These sources are either CSV files or Extensible Markup Language (XML) files. For more information, see Importing Contacts Into Directory Groups.
- Contacts you enter yourself. For more information, see Manually Adding Contacts To Directory Groups.

As well as importing contacts into directory groups, you can also export (copy) directory groups to CSV files, so that they can be used by other attendants or even in other applications.

Note The format of CSV files imported/exported is different from that of CSV files used for synchronization.

For more information, see Directory Groups.

The relationships between directories and external information is summarized below.



1. Cisco Unified Attendant Console Standard.
2. Corporate directory.
3. Directory groups.
4. Cisco Unified Communications Manager.
5. CSV file for synchronization. For details of the format, see CSV File Formats.
6. CSV file for importing and exporting. For details of the format, see CSV File Formats.
7. XML file.
8. Synchronize contacts. Includes applying Directory Filter, Directory Mapping Rules and BLF rules.
9. Import contacts.
10. Export contacts.
11. Manually entered contact.

Directory Synchronization

The process of copying contacts from your source directories into Cisco Unified Attendant Console Standard is known as synchronization because the information in the source and internal directories is identical at the instant of copying. When synchronization occurs, the contacts from both the Cisco Unified Communications Manager and the CSV file (if you specify one) are copied into Cisco Unified Attendant Console Standard. The actual data that is displayed in your corporate directory depends not only on what is in your sources but also on any directory field mappings, directory filters or BLF rules you have configured.

If synchronization detects that a contact it is copying is already in Cisco Unified Attendant Console Standard, it first validates the information (checks that it is correct) and then updates Cisco Unified Attendant Console Standard with any information that has changed since the last synchronization. If a synchronization fails mid-process – for example, because of a network failure – it starts again from the beginning.

The synchronization process needs to know what contact data to copy from the source to your corporate directory, and it gets this information from directory field mappings; for more information, including how to set the mappings, see Directory Field Mappings.

You can choose to copy only certain contacts to Cisco Unified Attendant Console Standard by applying a directory filter, this ensures that only those contacts that have the characteristics you specify in a series of directory rules are added to the corporate directory. For example, you can synchronize the contacts from only a specific department. For more information, see Directory Filtering.

During synchronization you can modify the first part of your contact telephone numbers, so that the numbers in your corporate directory differ from those in your source directory. For example, you might have telephone number stored in Cisco Unified Communications Manager as 01189728567, but in the corporate directory you want to see it as 8567. You achieve this number conversion by creating BLF Rules, which are applied during synchronization. For more information, see BLF Rules.

Note

- The converted numbers must match the DNs monitored in TAPI, otherwise the line state will not be displayed in the directories.
- These converted numbers are used by Cisco Unified Attendant Console Standard when it dials. If you set up BLF rules, you also need to set up translations in Cisco Unified Communications Manager to convert the numbers in Cisco Unified Attendant Console Standard back to the originals, so that you can call those numbers.

Directory synchronization takes place at regular intervals that you define, and you can also configure Cisco Unified Attendant Console Standard to synchronize with the source directory when you start the application (this is the default situation). Additionally, you can manually start synchronization. For more information, see Configuring Synchronization.

Synchronizing From a CSV Source File

When you synchronize from a CSV file, the file structure is first validated. The format of CSV files imported/exported is different from that of CSV files used for synchronization. For more information on valid CSV file formats, see CSV File Formats.

Configuring Synchronization

Note

Access to the functions described in this section may be restricted by your system administrator, and you may need a password to access the necessary Options tab. For more information, see Preventing Access To Options Tabs.

When you install Cisco Unified Attendant Console Standard, a set of default synchronization parameters are created, which should work for your installation. However, you can change these parameters to the values you require. Additionally, if you want to manually synchronize your system after changing its configuration, use this procedure.

To configure synchronization, do the following:

Step 1 In the main menu, choose **File > Options**. The **Options** window appears.

Step 2 Click the **General** tab.

Step 3 Under **Sync Detail**, do the following:

- To synchronize when the application starts, select the **Auto Synch Startup** check box.
- To define the interval in hours between automatic synchronizations, in **Sync Interval (In Hours)**, type a number. The default is zero, which means that synchronization is not scheduled to run again.
- To synchronize your directory now, click **Sync Now**. This control is disabled if there is already a synchronization in process.

Step 4 To synchronize to a CSV file source, under **CSV Detail**, **Browse** to the **File Location** of your CSV source, and either type its name or select it, and then click **OK**.

If you specify a CSV file source, the application synchronizes to both it and any specified Cisco Unified Communications Manager when you restart the application. For more information on specifying or changing CUCM details, see Changing Cisco Unified Communications Manager directory source details.

If you do not have a CSV source, click **Clear** to clear this field.

To view a sample CSV file, click **View Sample**.

Step 5 Click **Apply**.

Removing all contacts from CUCM directory synchronization

During the Cisco Unified Attendant Console Standard install, directory synchronization with CUCM is configured. There isn't an option to disable the CUCM directory synchronization source, but you can prevent contacts from syncing by creating a directory filter. For more information, see Directory Filtering.

To remove all contacts belonging to the CUCM directory source, and to prevent future contact imports, create a filter that matches no contacts.

For example, no contacts in CUCM have the Department name ABCD1234. Therefore, you should create a directory filter: Department <> is exactly <> ABCD1234. After applying the filter and executing a directory sync, any existing contacts not matching the filter are removed and no contacts that do not match the filter are subsequently imported.

Directory Filtering

Note

Directory filters are applied exclusively to the directory synchronization source, Cisco Unified Communications Manager.

A directory filter consists of a series of directory rules that are applied during synchronization to ensure that only certain contacts are copied to the corporate directory.

Each directory rule can compare one of the following contact details to a text string:

- Department
- Telephone
- Location

The rule makes the comparison according to one of the following conditions:

- Begins with
- Contains
- Is exactly
- Ends with
- Is not empty
- Does not contain

So, for example, you might only want to copy contacts whose *Department Is exactly Sales*. This would, however, exclude anyone whose department is *Sales America*, for example. Or maybe you want to synchronize those contacts whose *Department Ends with ing*, which would copy the contacts from both *Marketing* and *Engineering* (and any other department ending in those letters).

Directory filters can consist of any number of directory rules, combined using these logical operators:

- AND
- OR

So, for example, you might have a rule that synchronizes only those contacts whose *Department Is exactly Sales* AND their *Location Ends with America*, so that your corporate directory contains all the new world sales staff. When you use more than two rules, the AND operator has precedence over OR; so a rule with the structure X AND Y OR Z is equivalent to (X AND Y) OR Z.

Creating Directory Filters

Note

- Access to the functions described in this section may be restricted by your system administrator, and you may need a password to access the necessary Options tab. For more information, see Preventing Access To Options Tabs.
- Directory filters are applied exclusively to the directory synchronization source, Cisco Unified Communications Manager.

To create a directory filter, do the following:

Step 1 In the main menu, choose **File > Options**. The **Options** window appears.

Note You can configure a keyboard shortcut to do this. For instructions, see Keyboard Shortcuts.

Step 2 Click the **Directory Filters** tab.

Step 3 Do the following, as many times as required until your filter is complete:

a. If this is not the first rule in the filter, select the **Link** (Logical Operation) to apply between the previous rule and the one you are about to define.

b. Select the contact **Field** to compare.

c. Select the **Condition** to use in the comparison.

d. In **Value**, type the text to compare with the Field.

e. Click **Add**.

Step 4 Click **Apply** to save the changes.

Step 5 In the **Options** window, select the **Configuration** tab, and then, under **Sync Detail**, click **Sync Now** (this control is disabled if there is already a synchronization in process). The filter is applied and only those contacts satisfying the filter are copied to the corporate directory.

Directory Field Mappings

Before you synchronize contacts into Cisco Unified Attendant Console Standard the application needs to know which contact data fields (source fields) to import from Cisco Unified Communications Manager or a CSV file, and what destination fields within the application to populate with the data. This is called defining the directory field mappings. Contact data synchronized according to these mappings cannot be edited, but you can edit non-mapped fields.

You can specify separate directory field mappings for the data from your Cisco Unified Communications Manager and from a CSV file; so, for example, you could import your sales contacts from Cisco Unified Communications Manager, and your marketing contacts from a CSV file.

When you install Cisco Unified Attendant Console Standard default directory field mappings are defined for you. You can, however, change these mappings or define your own. For more information, see Setting Directory Field Mappings.

Destination Fields

Cisco Unified Attendant Console Standard supports the following contact destination fields:

- Department
- Directory URI
- Email
- First Name
- Home Phone
- Last Name
- Location
- Manager
- Middle Name
- Mobile
- Telephone (automatically mapped from source)
- User Field 1
- User Field 2

Source Fields

By default, Cisco Unified Attendant Console Standard has mappings set up for synchronizing contacts from Cisco Unified Communications Manager (CUCM) and CSV files. However, you may wish to change the default mappings, or define your own.

Setting Directory Field Mappings

Note Access to the functions described in this section may be restricted by your system administrator, and you may need a password to access the necessary Options tab. For more information, see Preventing Access To Options Tabs.

To set the directory field mappings, do the following:

Step 1 In the main menu, choose **File > Options**. The **Options** window appears.

Note You can configure a keyboard shortcut to do this. For instructions, see Keyboard Shortcuts.

Step 2 Click the **Directory Mappings** tab.

Step 3 Select a **Directory Source: CUCM** or **CSV**.

Step 4 Do the following, as required:

- To add a mapping, select the **Source Field**, **Destination Field**, and then click **Add**.
- To delete a mapping, click the corresponding **Delete** symbol, and then in the confirmation message, click **Yes**.

Step 5 Click **Apply**.

The next time you synchronize with your source, the mappings are applied.

BLF Rules

BLF rules are applied during synchronization to convert directory numbers to a different format by searching for and replacing specific number prefixes. You can define sets of multiple rules to be applied one after the other during synchronization, and you can define different sets of rules for synchronizing from Cisco Unified Communications Manager and CSV files.

BLF rules are applied in the order they are listed in the BLF rules List. For example, if the first rule modifies the number from 01189597895 to 8957, the next rule is applied to the modified number. By moving rules up or down in the list, you change the order in which they are applied

Note BLF rules will only be applied to contacts synchronized from CUCM, CSV or ALL, but not to imported or manually added contacts.

Adding BLF Rules

Note Access to the functions described in this section may be restricted by your system administrator, and you may need a password to access the necessary Options tab. For more information, see Preventing Access To Options Tabs.

To add a BLF rule, do the following:

Step 1 In the main menu, choose **File > Options**. The **Options** window appears.

Note You can configure a keyboard shortcut to do this. For instructions, see Keyboard Shortcuts.

Step 2 Click the **BLF rules** tab. A list of all existing BLF rules is displayed. By default, no rules are defined.

Step 3 Click **New Rule**. The **BLF Rule Detail** page appears.

Step 4 Type a **Rule Name**.

Step 5 Define the **Selection Criteria**.

a. **Directory Source**: select either CUCM, CSV or All.

b. **Length**: optionally, enter that the rule applies to numbers that match a certain length - if no length is specified then the rule will apply to all numbers.

c. **Begins With**: optionally, enter that the rule applies to numbers that begin with a specified value - if no value is specified then the rule will apply to all numbers.

Step 6 Define the **Transformation Criteria**.

a. **Ignore Characters**: optionally, remove non-digit characters (such as +) from the number by typing them here (with no separators).

b. **Remove Non-Digit Characters**: optionally, select if you want the rule to remove non-digit characters.

c. **Number of Characters to Remove from Beginning**: optionally, enter that the rule removes a certain amount of characters from the beginning of the number.

d. **Add Prefix**: optionally, enter that the rule adds a prefix to the start of the number.

Step 7 Before applying the criteria, you can **Test BLF Rules**.

a. **Pre-Transformation Number**: type in any number, and then click Run Test.

b. Check that the number displayed in **Test Results** matches your expectations. If not, revise the rule settings.

Step 8 If you are satisfied with the rule, click **Apply**. If not, click **Cancel** to cancel any changes you have entered. This will take you back to the main application screen without making any changes.

After you apply a rule, the BLF Rules page appears, and you can continue adding, editing or deleting BLF rules.

Editing BLF Rules

Note Access to the functions described in this section may be restricted by your system administrator, and you may need a password to access the necessary Options tab. For more information, see Preventing Access To Options Tabs.

To edit an existing BLF rule, do the following:

Step 1 In the main menu, choose **File > Options**. The **Options** window appears.

Note You can configure a keyboard shortcut to do this. For instructions, see Keyboard Shortcuts.

Step 2 Click the **BLF rules** tab. A list of all existing BLF rules is displayed.

Step 3 Select the rule to edit.

Step 4 Click **Edit Rule** to display the **BLF Rule Detail** page.

Step 5 Edit the fields, as required. For more information, see Adding BLF Rules.

Step 6 Test the rule, as required.

Step 7 Click **Apply**.

Test All Rules

To test all the rules at the same time, do the following:

Step 1 In the main menu, choose **File > Options**. The **Options** window appears.

Step 2 Click the **BLF Rules** tab.

Step 3 Click **Test All Rules**.

Step 4 In the pop-up window, enter the **Pre-Transformation Number** on which to test your rules.

Step 5 Select the **Directory Source** (All, CUCM or CSV).

Step 6 Click **Run Test** to see **Test Results**.

Step 7 Once you are done, click **Close** to go back.

Note When multiple BLF rules are configured, the output of the first rule will become the input of the second rule. If you are not satisfied with the final result of your transformed number, you may need to review individual BLF rules or their order.

Deleting BLF Rules

Note Access to the functions described in this section may be restricted by your system administrator, and you may need a password to access the necessary Options tab. For more information, see Preventing Access To Options Tabs.

To delete a BLF rule, do the following:

Step 1 In the main menu, choose **File > Options**. The **Options** window appears.

Note You can configure a keyboard shortcut to do this. For instructions, see Keyboard Shortcuts.

Step 2 Click the **BLF Rules** tab. A list of all existing BLF rules is displayed.

Step 3 Select the rule to delete.

Step 4 Click **Delete Rule**.

Step 5 Click **Apply**.

Reordering BLF Rules

Note Access to the functions described in this section may be restricted by your system administrator, and you may need a password to access the necessary Options tab. For more information, see Preventing Access To Options Tabs.

To change the order in which BLF rules are applied during synchronization, do the following:

Step 1 In the main menu, choose **File > Options**. The **Options** window appears.

Note You can configure a keyboard shortcut to do this. For instructions, see Keyboard Shortcuts.

Step 2 Click the **BLF Rules** tab. A list of all existing BLF rules is displayed.

Step 3 On each rule to move, do the following, as required:

a. Select the rule.

b. To move the rule towards the top of the list, click **Move Up**.

c. To move the rule towards the bottom of the list, click **Move Down**.

Step 4 Click **Apply**.

Directory Groups

Directory groups contains special contacts – including contacts not in your source directory – that you want to be able to select quickly. You must create your directory group before adding contacts to it. For details of how to do this, see Creating Directory Groups.

You add contacts to directory groups by either of the following methods:

- Importing contacts from CSV files or XML files; see Importing Contacts Into Directory Groups.
- Manually creating contacts; see Manually Adding Contacts To Directory Groups.

You can amend the name of a directory group, and the details of any contact in the group. You can also export the contacts from directory groups to CSV files.

Creating Directory Groups

You need to create directory groups before you can import data to them. To create a directory group, do the following:

Step 1 Do one of the following:

- Click the **Add Directory Group** (+) control.
- In the main menu, choose **Edit > Add directory group**.
- Use the keyboard shortcut you have defined; see Defining and Editing Keyboard Shortcuts.

The **New Directory Group** dialog box appears.

Step 2 Type a **Directory Group Name**, and then either click **Save** or press **Enter**.

The directory group is added as a new tab in the directory display.

Deleting Directory Groups

Note You cannot delete directory groups while synchronization is in process.

To delete a directory group, do one of the following:

Step 1 Right-click the directory group tab.

Step 2 Select **Delete Directory Group**.

Step 3 In the confirmation message, click **Yes**.

or

Step 1 Select the directory group, and then do one of the following:

- In the main menu, choose **Edit > Delete directory group**.
- Use the keyboard shortcut you have defined; see Defining and Editing Keyboard Shortcuts.

Renaming Directory Groups

To rename a directory group, do one of the following:

Step 1 Right-click the directory group tab.

Step 2 Select **Edit Directory Group**.

Step 3 In the dialog box, type the new group name, and then click **Save**.

or

Step 1 Do one of the following:

- In the main menu, choose **Edit > Edit directory group**.
- Use the keyboard shortcut you have defined; see Defining and Editing Keyboard Shortcuts.

Step 2 In the dialog box, type the new group name, and then click **Save**.

Importing Contacts Into Directory Groups

You can import contacts from the following types of files into an existing directory group.

- XML – for example, one previously exported from Cisco Attendant Console (CAC)
- CSV

For details of the formats of these files, see Import/Export File Formats.

Note

- You cannot import contacts into a directory group while the application is synchronizing to the corporate directory.
- The format of CSV files imported/exported is different from that of CSV files used for synchronization.

When importing contacts into the main directory, the information of a contact that already exists is amended. New contacts cannot be created in the main directory through import.

However, when importing into speed dial directories, duplication may occur in several scenarios:

- if the same contact was created by different users on different applications and CSV files are exchanged between these users, the contact is duplicated.
- if the unique ContactID is missing from the import file and cannot, therefore, be matched to the ContactID of existing contacts, the contacts are duplicated as many times as the user imports the file; the ContactID may be missing because you are using an old version import/export files, or if it has been manually edited out.

To avoid duplication, create contacts within a single Cisco Unified Attendant Console Standard installation, then export a CSV file and use it to import contacts on all other installations. This way, all contacts share the same ContactID.

At the start of the import process Cisco Unified Attendant Console Standard validates the file structure and format. If either is incorrect, you are alerted to the fact and the process is aborted.

You can only import contacts into an existing directory group – either one that already contains contacts, or a new one created especially for the purpose. See Creating Directory Groups.

To import contacts into a directory group, do the following:

Step 1 Do one of the following:

- In the main menu, choose **File > Import Contacts**.
- In the main menu, choose **File > Options**. In the **Options** window, click the **Import/Export** tab.
- Right-click in any directory group, and then select **Import Contacts**.
- Use the keyboard shortcut you have defined; see Defining and Editing Keyboard Shortcuts.

Step 2 Then do the following:

a. In **File Name**, click **Browse** and select the file to import.

Note You cannot type a file name or edit the name of a selected file.

b. Select the **File Type**.

c. If the **Directory Group** to receive the contacts is not correct, select the correct one.

d. Click **Import Contacts**.

e. The import progress is displayed.

Step 3 When the import is complete, close the dialog box.

Manually Adding Contacts To Directory Groups

You can manually add contacts to directory groups.

Note You cannot manually add contacts to your corporate directory.

To add a contact to the displayed directory group, do the following:

Step 1 Do one of the following:

- Right-click the directory group contact listing, and then select **Add Contact**.
- Select the directory group and do either of the following:
  - In the main menu, choose **Edit > Contacts > Add Contact**.
  - Use the keyboard shortcut you have defined; see Defining and Editing Keyboard Shortcuts.

The **Contact** dialog box appears.

Step 2 Type the contact information; see Destination Fields. You can also enter a contact **Note**.

Step 3 Click **Save**.

Step 4 In the confirmation message, click **OK**.

Step 5 When you have finished adding contacts, close the **Contact** dialog box.

Alternatively, you can drag (copy) contacts from the corporate directory or another directory group, and then drop them into the target directory group.

Note

- This creates a duplicate contact in the directory group. Take care not to create multiple duplicates.
- When editing contact properties or adding/editing a note, the changes will only occur for the directory group contact against which you make the changes. That is, the changes will not copy from the duplicate to the original or the other way around.

To drag contacts into a directory group:

Step 1 Display the directory containing the contact to copy.

Step 2 Select the contact and then, holding the mouse button, drag the contact over the appropriate directory group tab to list its contents.

Step 3 Drag the contact into the list, and then drop it.

Deleting Contacts From Directory Groups

You can delete contacts from directory groups.

Note You cannot delete contacts from your corporate directory.

To delete a contact from the displayed directory group, do the following:

Step 1 Select the contact to delete.

Step 2 Do one of the following:

- Right-click and then select **Delete Contact**.
- In the main menu, choose **Edit > Contacts > Delete Contact**.
- Use the keyboard shortcut you have defined; see Defining and Editing Keyboard Shortcuts.

Step 3 In the confirmation message, click **Yes**.

Editing Contacts In Directory Groups and the Corporate Directory

You can edit all the information belonging to a contact in a directory group and some of the information for a contact synchronized into the corporate directory.

Note You can edit any fields in manually added contacts, but you can only edit unmapped fields in contacts that have been synchronized into the corporate directory; the edited data is retained when the contact is synchronized. Should the field become mapped, the edited contact data in the corporate directory will be overwritten during synchronization with the data mapped from the Call Manager.

To edit a contact, do the following:

Step 1 Open the relevant directory and display the contact.

Step 2 Do one of the following:

- Right-click the contact, and then select **View/Edit Contact**.
- In the main menu, choose **Edit > Contacts > View/Edit Contact**.
- Use the keyboard shortcut you have defined; see Defining and Editing Keyboard Shortcuts.

The **Contact** dialog box appears.

Step 3 Edit the contact information; see Destination Fields.

Note You can edit the data in the white fields, but not in the shaded fields.

Step 4 Click Save.

Step 5 In the confirmation message, click OK.

Exporting Contacts From Directory Groups

You can export a directory group into a preexisting CSV file. To export a directory group, do the following:

Step 1 Do one of the following:

- In the main menu, choose **File > Export Contacts**.
- In the main menu, choose **File > Options**. In the **Options** window, click the **Import/Export** tab.
- Right-click in any directory group, and then select **Export Contacts**.
- Use the keyboard shortcut you have defined; see Defining and Editing Keyboard Shortcuts.

Step 2 Then do the following:

a. In **File Name**, click **Browse** and navigate to the target folder.

b. Either type a file name (to create a new CSV file) or select an existing file to export to. If you select an existing file, you are prompted to overwrite it; click **Yes** to overwrite the file.

Note The format of CSV files imported/exported is different from that of CSV files used for synchronization.

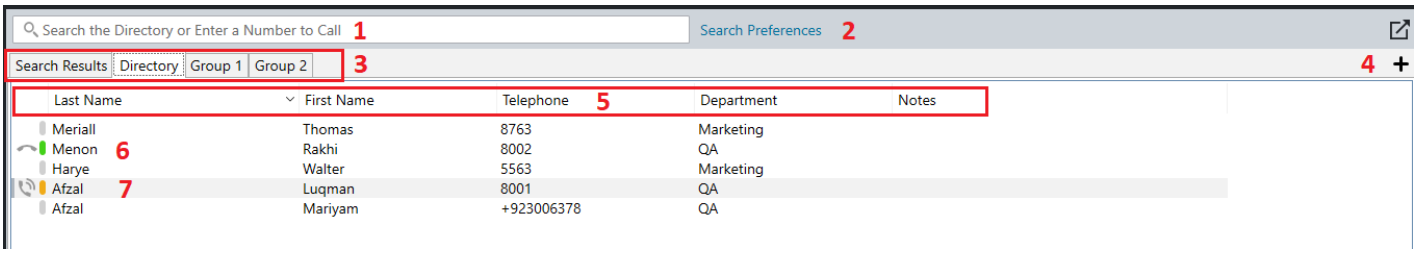
c. Select the **Directory Group** to export.

d. Click **Export Contacts**.

The export progress is displayed.

Viewing and Using Directories

The bottom part of the interface consists of the directories and their associated controls. For example:



1. Search – type details of the contact to search for.
2. Search Preferences – define which contact information to search.
3. Directory tabs – select the directory to display. Includes both corporate directory and directory groups. Drag the tabs to change their order; see Changing the Directory Tab Order.
4. Create a new directory group.
5. Column headings – identify the data and enable you to change what columns are displayed, the column order, and the contact sort order. These are described below.
6. Phone state – the state of the contact's phone, such as Ringing, On hook, and Do not disturb.

Note If a contact DN includes spaces (for example, +44 123 456), the phone line state will not be shown. However, a call can be made to this contact successfully.

7. Presence state – this mimics a Jabber or CUPC client, where a symbol indicates the real-time status of the contact, such as Available, Do not disturb, and Away. All other contacts have their subscriptions opened only when displayed in the Directory pane.

The following information can be displayed for each contact (columns displayed by default are shown in **bold**):

- **Last Name** - always displayed
- **First Name**
- **Telephone** - always displayed
- **Department**
- **Notes**
- Middle Name
- Email
- Directory URI
- Mobile
- Home Phone
- Manager
- User Field 1
- User Field 2
- Location

For more information on how to change what columns of information are displayed, see Changing the Directory View.

If the contact was imported or manually entered into Cisco Unified Attendant Console Standard you can also edit the contact information.

Changing the Directory Tab Order

Each directory is identified by a tab, which you click to display that directory. When you first start the application, the default directory tabs are displayed in a default order. You can change the order of the default directory tabs - and any new ones you create - by dragging them to the left or right and dropping them in the required position. If you drag a tab to the left and drop it on another tab, it replaces that tab, which then moves to the right one position. If you drag a tab to the right and drop it on another tab, it replaces that tab, which then moves to the left one position. For example, if you have tabs 1, 2 3 and 4 in that order, and you drag tab 4 and then drop it on tab 1, the tabs become ordered 4, 1, 2, 3. If you then drag tab 1 and drop it on tab 3, the order changes to 4, 2, 3, 1.

Note You cannot move the **Search Results** tab.

The positions of the tabs are stored when you log out or exit the application, and the tabs are displayed in the saved order when you next use it.

Changing the Directory View

You can change:

- which data columns are displayed,
- the order of the columns, from left to right,
- the contact order according to the data in any of the columns.

Changing what data columns are displayed and column order

You can display any of the columns of information for each contact, so long as your selection includes **Last Name** and **Telephone**.

To select which columns to display and their order:

Step 1 Right-click any column heading. A menu appears, listing the default columns, with a tick preceding each column displayed.

Step 2 To hide a selected (ticked) default column or display an un-ticked column, click the item in the menu.

Step 3 To control non-default columns or change the order in which all columns are displayed, click **More**. A dialog box appears listing the possible columns. Displayed columns have a tick in their check box.

Step 4 Use this dialog box to add or remove columns from the display, and to change the order in which the columns are displayed in the following ways:

- To show a column in the directory pane, click the corresponding check box to select it.
- To remove a column from the directory pane, click the corresponding check box to clear it (you cannot remove **Last Name** or **Telephone**).
- To move a column in the directory pane, select it (not the check box), and click **Move Up** (to move the displayed column to the left) and **Move Down** (to move the displayed column to the right).

Note You can also change the order of the columns in the Directory pane by using your mouse to select a column heading; you can then drag it to another place in the table.

Step 5 Click **Save**.

The contact information in the Directory pane changes accordingly.

Changing contact order

When the data is first displayed it appears in its default order, as copied from the Call Manager. You can change the alphanumeric sort order of the directory table rows by clicking the following column headings – the entire table will be sorted according to the data in that column.

- **Last Name**
- **First Name**
- **Telephone**
- **Department**

The small arrowheads in the column heading row show the direction in which the column is sorted: an up-arrow for ascending (normal alphanumeric) order, a down-arrow for descending (reverse) order, and both arrows for default order. Repeatedly clicking the column heading toggles through these sort modes.

The sort column and sort order are remembered by the application when you log off or exit, and are re-applied when you log in again.

Searching For Contacts

You can search for contacts in any open directory (the corporate directory and any directory groups you are displaying). Details of matching contacts are shown under the **Search Results** directory tab.

You can search on any of the contact data fields, but no more than five at any time. The fewer fields you configure, the better will be the search speed. For more information on how to configure the searchable fields, see Search Preferences.

You do not need to specify which field you want to search: the string you type in the Search field is matched against all of them. So, for example, if you have a *Sales* department, and a staff member with the last name *Saunders*, searching for the characters *Sa*, will display all the matching last names (and first names) and list everyone in Sales.

If you type a string containing one or more spaces, all the individual "words" in the string and the entire string are searched for. For example, if you search for *Del Toro*, each directory field is searched for *Del* AND for *Toro* AND for *Del Toro*.

Searching begins as soon as you start typing; and the more characters you type, the fewer contacts will match. Matching occurs even with the accented equivalents of unaccented letters; for example: typing *o* will match with *ö*, *ô* and any other accented equivalents in the contact data. When the contact you require is displayed, select it, and then use the controls interface to communicate with that contact.

Search Preferences

The Search Preferences enable you control which fields are searched, and which contacts are displayed.

You can choose from one to five **Searchable Fields** from the following **Available Fields** (default searchable fields shown in **bold**):

- **First Name**
- **Last Name**
- **Telephone Number**
- **Department**
- **Email**
- Middle Name
- Directory URI
- Mobile
- Note
- Home Phone
- Manager

- User Field 1
- User Field 2
- Location

Use the Left-arrow and Right-arrow buttons to move the field selected in either list to the other.

You can also limit which contacts are displayed in the search results using these **Filters**:

- **Has Telephone** – Display only those contacts with a telephone number assigned. All other contacts are filtered out (excluded) from the search results.
- **Has Emails** – Display only those contacts with an email address assigned. All other contacts are filtered out (excluded) from the search results.

Setting Search Preferences

To set the search preferences, do the following:

Step 1 Click **Search Preferences**. The **Search Preferences** dialog box appears.

Step 2 Select **Searchable Fields** and **Available Fields**, as required, moving them between the lists by clicking Left-arrow and Right-arrow as required to define the searchable fields.

Step 3 Select the required filters.

Step 4 Click **Save**.

Step 5 In the confirmation message, click **OK**.

Viewing Contact Information

The directory display contains basic information about each contact. You can view more information about a selected contact by viewing their contact details. How you view contact details depends on whether the contact is in the corporate directory or a directory group.

To view a contact's details, do the following:

Step 1 Display the directory containing the contact.

Step 2 Right-click the contact.

Step 3 Click **View/Edit Contact**.

The **Contact** dialog box is displayed.

If you are viewing the details of a contact in a directory group, you can also edit the details. For more information, see Editing Contacts In Directory Groups and the Corporate Directory.

Step 4 When you have finished viewing the information, click **Cancel**.

Contact Notes

You can add notes to any contact record in the main directory, the search results, or any directory group. The notes are text containing additional information about the contact. Notes are stored in the database and are available whenever you sign in. If you delete a contact - for example by applying BLF rules - any contact notes are also deleted. If you export a contact, their notes are also exported, and if you import a contact with notes, they are visible in the application.

Adding Contact Notes

To add contact notes:

Step 1 Select the contact to add notes to.

Step 2 Do one of the following:

- Right-click the contact, and then choose **Add/Edit Note**.
- Choose **Edit > Contacts > Add/Edit Note**.

The **Edit Note** dialog box appears.

Note You can configure a keyboard shortcut to do this. For instructions, see Keyboard Shortcuts.

Step 3 In the text box, type the notes and then either click **Save** or tab to the control and press **Enter** to add the notes to the contact.

Note You must enter some text for you to be able to save it. When adding/editing a note, the changes will only occur for the directory group contact against which you make the changes. That is, the changes will not copy from the duplicate to the original or the other way around.

The notes appear in the contact's **Notes** column.

Editing Contact Notes

You can edit existing contact notes. To do so, follow the procedure of adding notes, but instead edit the existing notes. For more information, see Adding Contact Notes.

Deleting Contact Notes

To delete existing contact notes:

Step 1 Select a contact with notes to delete.

Step 2 Do one of the following:

- Right-click the contact, and then choose **Delete Note**.
- Choose **Edit > Contacts > Delete Note**.

Note

- These menu options are disabled if there are no notes to delete.
- You can configure a keyboard shortcut to do this. For instructions, see Keyboard Shortcuts.

The notes are deleted from the contact **Notes** column.

Call Tags

Contact Matching and Caller ID Pass-through

Within the application **Call Control** panel, **Call Tags** are presented for any call residing on a line associated with the login device. The **Name** presented in a call tag is the result of a series of comparative and selective background tasks.

In instances where multiple matches exist from a variety of sources, including manually created directory contacts, synchronized directory contacts, and Caller ID Pass-through from Cisco Unified Communications Manager the software prioritizes matches by source, presenting the highest-ranking name in the **Call Tag**. Ranked from highest to lowest:

1. **Contact Matching** - manually created directory contacts
2. **Contact Matching** - synchronized directory contacts
3. **Caller ID Pass-through** - provided by Cisco Unified Communications Manager via Cisco TSP Plug-in
4. **Private Caller** - there are no contact matches and the Caller ID pass-through indicates the name is blocked.
5. **Unknown Caller** - there are no contact matches, and no caller ID pass-through data exists.

When displaying inbound or outbound calls Cisco Unified Attendant Console Standard displays the name of the matching contact, which is determined in the following way:

- If the caller is a manually created (speed dial) contact in the database, the name from there is displayed.
- If the caller is not manually created, but their name is synchronized in the database, that is displayed.
- If there is no caller name in the database, it is retrieved from Cisco Unified Communications Manager.

If **Unknown Caller** is displayed, the caller name has not been found. If **Private Caller** is displayed, the caller is blocked.

Keyboard Shortcuts

Keyboard shortcuts enable you to quickly do things in the interface without needing to use the mouse or menus. The application comes configured with the following keyboard shortcuts.

Action	Shortcut
Dial	Ctrl+D
Answer	Ctrl+A
End Call	Ctrl+H
Hold Call	Ctrl+L
Transfer Call (Blind transfer)	Ctrl+X
Consult Transfer (speak to destination before transfer)	Ctrl+T
Direct Transfer	Ctrl+R
Join Call	Ctrl+J
Park Call	Ctrl+P
Start Conference	Ctrl+N
Transfer to Voicemail	Ctrl+O
Sign out of application	Ctrl+S
Login/ Logout of Hunt Groups	Ctrl+I
Open Help	F1
Outbound Dialing Override	Ctrl+Enter

In addition, you can define shortcuts for the following actions:

- Dial (Mobile)
- Dial (Home)
- Transfer (Mobile)
- Transfer (Home)
- Consult Transfer (Mobile)
- Consult Transfer (Home)
- Conference (Mobile)
- Conference (Home)
- Resume Call
- Retrieve Park Call
- Email
- Options
- Import contacts
- Export contacts
- Exit
- Keyboard Shortcut Options
- Add Contact
- Delete Selected Contact
- Add Directory Group / Speed Dial
- Edit Selected Directory Group / Speed Dial
- Delete Selected Directory Group / Speed Dial
- View/Edit Contact
- Open Parked Calls Pane
- Open Call History Pane
- Revert to Default Layout
- Open About Box
- Add/Edit Note
- Delete Note
- Show/Hide Directory Columns

Note

- You cannot use the same keyboard shortcut for more than one action.
- When defining shortcuts using the **Alt** key, be mindful of the standard Windows behavior that uses **Alt** to activate the menu of the application currently open on the screen in order to quickly open menu items by holding **Alt** and pressing the underlined letter of each item. For example, if you set a shortcut for **Alt+F** to **Delete Note**, instead of performing the action you defined for that shortcut, pressing **Alt+F** opens the menu item **File**.

Note

- Users are unable to configure or use the shortcut **Ctrl+Shift+A** against any action while Cisco IP Communicator is running. To configure the shortcut, exit the Cisco IP Communicator application and try again.
- When parking a call, if the call is not picked up, it will be recalled after a defined period. However, on phone model 8851, the recall does not show up on the console but on the phone itself. Press the resume button on the phone to make the recall show up on the console.

Defining and Editing Keyboard Shortcuts

To define or edit a keyboard shortcut, do the following:

Step 1 Do either of the following:

- In the main menu, choose **Edit > Keyboard Shortcuts**.

or

a. In the main menu, choose **File > Options**. The **Options** window appears.

b. Click the **Keyboard Shortcuts** tab.

Step 2 Select the **Action** to define. This can be an action that already has a shortcut.

Step 3 Click **Set Shortcut**.

Step 4 Type the shortcut you require. For example, to set an action to Ctrl+Y or Ctrl+Shift+Y, simply type **Ctrl+Y** or **Ctrl+Shift+Y** (press and hold the Ctrl key or the Ctrl and Shift key, and then press the Y key).

Step 5 Click **Apply**.

Removing Keyboard Shortcuts

To remove a keyboard shortcut, do the following:

Step 1 Access the **Keyboard Shortcuts** page; see Defining and Editing Keyboard Shortcuts.

Step 2 Select the action from which to remove the keyboard shortcut.

Step 3 Click **Clear Shortcut**.

Step 4 Click **Apply**.

Resetting Shortcuts to their Default Values

To reset keyboard shortcuts to their default values, do the following:

Step 1 Access the **Keyboard Shortcuts** page; see Defining and Editing Keyboard Shortcuts.

Step 2 Do one of the following, as appropriate:

- To reset all keyboard shortcuts to their default values, click **Reset All Shortcuts to Default**.
- To reset a single keyboard shortcut to its default value:

a. Select the action to reset.

b. Click **Reset Shortcut**.

Step 3 Click **Apply**.

Uninstalling Cisco Unified Attendant Console Standard

To uninstall Cisco Unified Attendant Console Standard, do the following:

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

Step 2 From the list, select Cisco Unified Attendant Console Standard, and then click **Remove**. The Wizard prepares to (un)install the console application.

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

Step 4 You are asked *Do you want to delete the application database?* (Application database contains configuration and local directory contacts.)

- Selecting **Yes** allows you to delete all unneeded personal information for security and privacy reasons.
- Selecting **No** allows you to retain the application database. This is preferred if intending to reinstall Cisco Unified Attendant Console Standard.

Step 5 When prompted that the uninstallation is complete, select *Yes, I want to restart my computer now*. and click **Finish**.

Note All Cisco Unified Attendant Console Standard application logs are deleted as part of the uninstallation process.

Application Log Configuration and Collection

Note Access to the functions described in this section may be restricted by your system administrator, and you may need a password to access the necessary Options tab. For more information, see Preventing Access To Options Tabs.

Cisco Unified Attendant Console Standard can keep a log of all events that occur within the application. This information can be used to gauge the application's configuration and performance, and to help troubleshoot any errors. You can control which application subsystems are monitored, which events are logged, and the size and number of the log files.

Access the Logging Menu

Step 1 In the main menu, choose **File > Options**. The **Options** window appears.

Note You can configure a keyboard shortcut to do this. For instructions, see Keyboard Shortcuts.

Step 2 Click the **Logging** tab to configure logging.

Configuring Logging

From the **Options > Logging** tab, adjust the following values as required:

- **Number of Files**: Type the maximum number of log files to be retained. Once the threshold is met, the application will begin overwriting the log files starting with the oldest.

  The default value is 10.

- **Max File Size (In MBs)**: Type the maximum file size, in MBs. Once the threshold is met, the log file will close, and a new log file is opened.

  The default value is 20.

- **Logging Level**: Select the logging level that fits your logging needs.
  - Debug is the most verbose, with each subsequent level moving down in verbosity until Fatal, which is the least verbose.
  - Custom, allows you to set a different logging level for the individual modules of the application. Each line in the application log files notes the module it belongs to (for example, a line marked ViewModel would be affected by the ViewModel module setting). A custom level of logging is not suitable for general use.
  - The default and recommended value is **Debug**.

Log Collection

Step 1 From the **Options** > **Logging** tab, select **Collect Logs**.

Step 2 You are prompted to browse to a folder, where the application logs can be saved to. After making your selection, click **OK**.

- The Windows User account must have write-permissions to the specified folder.

Step 3 Once the log collection completes an alert indicating the success of the compressed log file creation and the file path will appear. Click **OK** to dismiss the alert.

- The output will be stored in a .zip file containing all the log files and a log configuration file.

Note The collection file also includes audit logs which are stored in the same location as the user logs. For more information, see Application Audit Logging.

Application Audit Logging

Application Audit Logs record any configuration changes to the application made by a user or that occurred as a result of user actions. Audit logs conform to RFC 5424 and are stored in the same location where user logs are stored.

The following information is logged as part of the audit logs:

- User Login/Logout process along with the user extension and Windows username information,
- Hunt Group Login/Logout information,
- AXL Test Connection success/failure information,
- License validation and expiry information,
- Operator Logged in Device information,
  - In Service
  - Out of Service
  - Do Not Disturb
  - Forwarding
- Contact Synchronization Start and Finish Events,
- Any other configuration changes are logged as a standard message.

Disabling Audit Logging

Audit logging is enabled by default. To disable it, do the following:

Step 1 Navigate to the %AppData%\Roaming\CUACSLogging folder.

Step 2 Open the log4net.config file in the notepad.

Step 3 Locate the following lines:

<logger name="AuditLog">

<level value="INFO" />

<appender-ref ref="AuditAppender" />

</logger>

Step 4 Change *<level value="**INFO**" />* to *<level value="**OFF**" />*.

Step 5 Restart the application.

Import/Export File Formats

Cisco Unified Attendant Console Standard can handle contact directory files in XML and CSV formats.

It can also import login devices from CSV files. For more information, see CSV Files for Importing Sign In Devices.

XML File Format

XML files that you import into Cisco Unified Attendant Console Standard must have the following format:

```
<SpeedDialUsers>
      <G n="Sample Group">
            <E>
                  <N>Jim Kathirine</N>
                  <T>25421</T>
                  <M>Jim@cisco.com</M>
                  <D>Jim@cisco.com</D>
                  <O>This is a sample entry</O>
                  <P>00443454332</P>
                  <H>0044556634</H>
                  <S>Reading</S>
                  <A>IT</A>
                  <R>Jason Rumsey</R>
                  <U>Software Engineer</U>
                  <V>Management</V>
            </E>
      </G>
</SpeedDialUsers>
```

Tags

- <SpeedDialUsers> = the file contains XML data for import into Cisco Unified Attendant Console Standard.
- <G> = Directory group name
- <E> = Individual contact
- <N> = Name
- <T> = Telephone number
- <M> = Email address
- <D> = Directory URI
- <O> = Note
- <P> = Mobile
- <H> = Home phone number
- <S> = Site
- <A> = Department
- <R> = Manager
- <U> = UserField1
- <V> = UserField2

CSV File Formats

Cisco Unified Attendant Console Standard handles two types of comma-separated value (CSV) files:

- CSV Files for Synchronization
- CSV Files for Directory Import and Export

These files differ in the number of data fields they contain in each contact record.

All CSV files used by Cisco Unified Attendant Console Standard must have the following format:

- Each contact is on a single line.
- Empty comma-separated values are valid.
- Lines starting with # or ; are comments and are ignored. Empty and blank lines are also ignored.

CSV Files for Synchronization

In a CSV file for synchronization, the data for each contact must be in the following order:

```
Sync ID, Last Name, First Name, Telephone Number, Department, User Field 1, User
Field 2, Site, Building, Directory URI.
```

A unique Sync ID must be presented for every contact record in the CSV file. Suggestions for composing a unique Sync ID include:

- Recommended: copy values from another column whose content is unique (for example, Directory URI).
- Generate a unique value composed of numbers and letters (for example, *sync0001*, *sep00001*). This is easily achieved in Microsoft Excel using the default increment feature, or via an array of formulas.

The following is a sample CSV file:

```
#       * Copyright (c) 2021 by Cisco Inc.
#       * All rights reserved.
#
# Here is a sample CSV File for Synchronization - used to sync contacts to the
‘Directory’ tab.
#
# Requirements:
# A unique Sync ID must be presented for every contact record in the CSV file.
#
# Suggestions for composing a unique Sync ID include:
#       * Copy values from another column whose content is unique (for example
Directory URI).
#       * Generate a unique value composed of numbers and letters (for example
sync0001, sep00001, etc.). This is easily achieved in Microsoft Excel using the
default increment feature, or via an array of formulas.
#
# Comma separated entries, one line per user in the directory.
#
# The values should be in the following format:
# # Sync ID, Last Name, First Name, Telephone number, Department, User Field 1,
User Field 2, Site, Building, Directory URI
#
# Empty values are legal (no department etc.), with the exception of SyncID.
#
# Lines starting with '#' or ';' are treated as comments # and ignored. Empty or
blank lines are ignored as well


C0001,Kathirine,Jim,25421,Marketing,,,,,Jim@cisco.com
C0002,Martha,Bryan,87952,Support,,,,,martha@cisco.com
C0003,Luce,Richard,2548,Marketing,,,,,luce@cisco.com
C0004,Meriall,Thomas,8763,Marketing,,,,,meriall@cisco.com
C0005,Harye,Walter,5563,Marketing,,,,,harye@cisco.com
```

CSV Files for Directory Import and Export

Both main directory and speed dial contacts can be exported and imported through CSV files.

This feature has multiple benefits:

- users can make back-ups of a contact's complete data - both modifiable and non-modifiable,
- users moving from different products with extensive contact data not retained in the parent source database can use this option to migrate data,
- modifiable fields, like custom notes, can be shared and synchronized between multiple users,
- editing contacts in bulk is more efficient.

Note When updating existing contacts via CSV, it is imperative to retain the ContactID and SyncID values presented in the export. Otherwise, new contact entries will be created for each unmatched row. For more information about the possible scenarios in which duplication may occur, see Importing Contacts Into Directory Groups.

In a CSV file for directory import or export, the data for each contact must be in the following order:

```
Last Name, First Name, Telephone Number, Note, Group Name, Email, Directory URI,
Middle Name, Mobile, Home Phone, Site, Department, Manager, User Field 1, User
Field 2, ContactID, SyncID
```

ContactID and SyncID are populated during directory export.

- These fields should be left blank for new contact rows.
- Values generated during directory export must be retained in subsequent imports/updates.

For example:

```
#       * Copyright (c) 2021 by Cisco Inc.
#       * All rights reserved.
#
# Here is a sample import/update and export CSV file.
#
# Requirements:
# Comma separated entries, one line per user in the directory
#
# The values should be in the following format:
#
# Last Name, First Name, Telephone Number, Note, Group Name, Email, Directory URI,
Middle Name, Mobile, Home Phone, Site, Department, Manager, User Field 1, User
Field 2, ContactID, SyncID
#
# Importing New Contacts - Empty values are legal (no email etc.) for all fields
# Updating Existing Contacts - Empty values are legal (no email etc.) for all
fields except ContactID and SyncID
#
# If a Group Name is specified in the CSV file, it will take precedence over the
Directory Group selected at the Import screen


Kathirine,Jim,25421,This is a sample entry.,Sample Group
1,Jim@cisco.com,Jim@cisco.com,Maid, 00443454332,0044556634,Reading,IT,Martin
Taylor,Support Engineer,Senior,, Martha,Bryan,87952,This is a sample entry.,Sample
Group 1,martha@cisco.com,martha@cisco.com,Aryan,
00443454335,0044556635,Reading,IT,Martin Taylor,Support Engineer,Junior,,
Luce,Richard,2548,This is a sample entry.,Sample Group
2,luce@cisco.com,luce@cisco.com,Tace,
00443454339,0044556636,Reading,R&D,Jason Rumsey,Software Engineer,Management,,
Meriall,Thomas,8763,This is a sample entry.,Sample Group
2,meriall@cisco.com,meriall@cisco.com,Kate,
```

```
00443454331,0044556637,Reading,R&D,Jason Rumsey,Software Engineer,Junior,,
Harye,Walter,5563,This is a sample entry.,Sample Group
2,harye@cisco.com,harye@cisco.com,Heather, 00443454333,0044556638,Reading,R&D,Jason
Rumsey,Software Engineer,Senior,,
```

CSV Files for Importing Sign In Devices

You can import devices that operators use to log into Cisco Unified Attendant Console Standard. For more information, see Importing Sign In Devices.

These CSV files have the data for each device in the following format:

```
Device name, Extension, Line number
```

For example:

```
#       * Copyright (c) 2021 by Cisco Inc.
#       * All rights reserved.
#
# Here is a sample device list file. It should contain
# comma separated entries, one line per device in the device list.
# The values should in the following format:
#
# DeviceName,Extension,LineNumber #
# Empty values are not allowed (no DeviceName etc.)
#
# Lines starting with '#' or ';' are treated as comments
# and ignored. Empty or blank lines are ignored as well.


SEP2893FE130280,5868,1
SEP2893FEA2D22A,5873,1
SEP000C299DA714,5870,1
SEP88AE1DB0F66C,5869,1
SEP00141C48DDD9,5859,1
SEP00141C48DDD9,5870,2
```

Note Any devices in the file that lack one or more of the fields Device name, Extension, or Line number are considered non-Cisco devices and will not be imported.

Phones Supported by Cisco Unified Attendant Console Standard

Cisco Unified Attendant Console Standard user and end-point device support. See Shared Lines and Extension Mobility for details regarding shared lines and extension mobility.

Term	Description
Full	Console user device and BLF status for directory contacts
Console User	Console user device only
BLF Status	BLF status for directory contacts only
Not Supported	Tested, but not supported
Not Tested	Not tested, therefore no formal support
^x	Reference footnote

Device Type/Phone Model	Supportability	Device Type/Phone Model	Supportability
3905	Not Supported	7960	Full
6901	Not tested	7961	Full
6911	Full	7961G-GE	Full
6921	Full	7962	Full
6941	Full	7965	Full
6945	Full	7965G	Full
6961	Full	7970	Full
7811	Full	7971	Full
7821	Full	7975	Full1
7841	Full	8811	Full
7861	Full	8841	Full
7902	Not tested	8845	Full
7905	Full	8851	Full
7906	Full	8851NR	Full
7910	Full	8861	Full
7911	Full	8865	Full
7912	Full	8865NR	Full
7915	Full	8941	Full
7916	Full	8945	Full
7920	Full	8961	Full
7921	Full	9951	Full
7925	Full	9971	Full
7925G	Full	Calling in Webex Teams (Unified CM)	Full
7925G-EX	Full	Cisco Jabber for Android	Not Supported
7926	Full	Cisco Jabber for iPad	Not Supported
7931	Full[2]	Cisco Jabber for iPhone	Not Supported
7940	Full	Cisco Jabber for Mac	Full[3]

Device Type/Phone Model	Supportability	Device Type/Phone Model	Supportability
7941	Full	Cisco Jabber for Windows	Full[3]
7941G-GE	Full	DX70	Full
7942	Full	DX80	Full
7942-G	Full	DX650	Full
7945	Full	IP Communicator	Full
7945G	Full		

1. Using this device to sign into the application requires the maximum calls setting in Cisco Unified Communications Manager to be set to a minimum of two.
2. If **Log in to hunt groups at sign in** is selected, the device will reset as part of the login process.
3. Both standard Jabber installations (locally installed on the operator computer) and VXME installations (installed in a VXME environment) are supported as console user devices and end points.

Manual Installation of TAPI Plug-in and Using a Cisco Unified Communications Manager TFTP server for all non-TAPI functions

Cisco Unified Attendant Console Standard can be configured to pass all AXL communications through a Unified Communications Manager TFTP server (not running the CCM service), while sending all TAPI communications to a node running the CCM service. This should only be a consideration for users that wish to disable Tomcat services on their CTI managers.

To manually install CISCO TSP Plug-in, skip to Step 2.

Installation Instructions

Step 1 Follow the instructions in Install or Upgrade Cisco Unified Attendant Console Standard, specifying the Cisco Unified Communications Manager TFTP Host Name, Fully Qualified Domain Name (FQDN) or IP address under Step 5.

Step 2 After the PC restarts, you will need to manually download and install the Cisco TAPI client from Cisco Unified Communications Manager.

a. Navigate to your Cisco Unified Communications Manager Administration webpage, and log in.

b. Navigate to **Application** > **Plugins**.

c. Search for and download the 64-bit Cisco TAPI Client.

d. Execute the installer, following the on-screen prompts provide the following data:

- Number of TSPs to install: **1**
- Provide the **Application User** specified for your Cisco Unified Attendant Console Standard installation.
- Provide the **CTI Manager 1** (and 2 if applicable) Host Name, Fully Qualified Domain Name (FQDN) or IP address, selecting IPv4 from the associated drop-down menu.

- Specify a **UDP Port Range**, Start 50000, End 54000.
- Select **Never Auto-Upgrade**.
- Restart the PC when prompted.

Update Cisco TSP Primary CTI Manager Address, Application User and Password

Note

- For more information on how to modify the Cisco Unified Communications Manager directory source address or user credentials, see Changing Cisco Unified Communications Manager directory source details.
- The new Cisco Unified Communications Manager address version must match the existing version.

Step 1 Launch **Cisco TSPx64 Configuration**.

Step 2 Select *CiscoTSP001.tsp*.

Step 3 Click **Configure**.

Step 4 Make the required modifications:

- **Primary CTI Manager**
  a. Select **CTI Manager** tab.
  b. Provide the new **IP Address** or **Host Name**.
- **Application User Details**
  a. Select **User** tab.
  b. Provide **User Name** and/or **Password**.

Step 5 Click **OK**, then click **OK**.

Step 6 Restart the PC.

Configuring Secure TSP

Note If Cisco Unified Communications Manager was enabled for but not properly configured for secure TSP, implementing the steps described under Configure Cisco Unified Communications Manager breaks communication between the Cisco Unified Attendant Console Standard and Cisco Unified Communications Manager.

To configure Cisco Unified Communication secure TSP, first follow the steps outlined here: Configuring Secure TSP.

The following steps are additional steps to configure secure TSP for Cisco Unified Attendant Console Standard.

Secure TSP Configuration - Additional Role Requirements

Execute the following steps if Cisco Unified Communications Manager is configured to support Secure TSP configurations.

Step 1 Navigate to the **User Management > Application User** menu.

Step 2 Search for and select the application user leveraged for Cisco Unified Attendant Console Standard.

Step 3 Under **Permissions Information**, click **Add to Access Control Group**.

Step 4 Search for and select the **Standard CTI Secure Connection and Standard CTI Allow Reception of SRTP Key Material** roles.

Step 5 Click **Add Selected** and close the window.

Secure TSP Configuration - Cisco TSP Plugin Configuration

Execute the following steps if Cisco Unified Communications Manager is configured to support Secure TSP configurations.

Step 1 On the Cisco Unified Attendant Console Standard workstation, launch *Cisco TSPx64.exe* configuration.

Step 2 Select *CiscoTSP001.tsp* and click **Configure**.

Step 3 Click the **Security** tab and select **Secure Connection to CTI Manager**.

Step 4 Populate the remainder of the security configuration fields as required by the linked Cisco Unified Communications Manager environment.

Step 5 Click **OK** to save the changes, and then click **OK** to close the configuration pane.

Step 6 Restart the workstation.

Note If Cisco Unified Communications Manager is not enabled for secure TSP configurations, implementing the steps above breaks communication between Cisco Unified Attendant Console Standard and Cisco Unified Communications Manager.

Security Best Practices

Note Before installing Cisco Unified Attendant Console Standard, follow the security best practices listed in this chapter to ensure security of the application.

Implementing security mechanisms in the Cisco Unified Attendant Console Standard prevents identity theft of phones, data tampering, and call-signaling/media-stream tampering. Cisco Unified Attendant Console is deployed on a Microsoft Client Operating System, so it is strongly recommended you use the Microsoft Security Baseline Policy for its specific Windows operating system. To find out more about these policies, see the Windows security baselines.

The following key areas should be reviewed while configuring the system to provide better security of the application:

- Application Ports and Services: Network Requirements
- Virus Scans Exclusion: Virus Scan Exclusions
- Windows Folder Permission: Windows Folder Permissions
- Securing Application Sign-In devices: Managing Sign In Devices
- Authentication: Starting Cisco Unified Attendant Console Standard
- Application Audit Logging: Application Audit Logging
- Securing TAPI: Configuring Secure TSP
- TLS protocol setup: TLS Protocol Setup

TLS Protocol Setup

Cisco Unified Attendant Console Standard supports secure communication over TLS with Cisco Unified Communication Manager and Cisco IM & Presence. It uses TLS as a client to establish a secure channel with Cisco Unified Communication Manager and Cisco IM & Presence. It is recommended you ensure that the appropriate TLS protocol version and the secure cipher are enabled, and they match between the Cisco Unified Attendant Console Standard machine and the Cisco Unified Communication Manager and Cisco IM & Presence.

When the initial TLS handshake takes place between Cisco Unified Attendant Console Standard at the Operating System level and the Cisco Unified Communication Manager and Cisco IM & Presence, a secure cipher is decided between them and selected. Cisco Unified Attendant Console Standard has no control over the selection of the TLS protocol version and the secure cipher as it is controlled by the Cisco Unified Communication Manager and Cisco IM & Presence.

Cisco Unified Attendant Console Standard supports secure communication for the following features.

Single Sign On

Cisco Unified Attendant Console Standard uses a browser engine for the single sign on process. Ensure that the required TLS protocol version is enabled in your internet settings so that the single sign on process can take place securely with Cisco Unified Communication Manager. Do the following:

Step 1 Open Windows Control Panel.

Step 2 Go to **Network and Internet** > **Internet Options** to open the **Internet Properties** configuration window.

Step 3 On the **Advanced** tab, scroll down to **Security** and find the **Use TLS** settings.

Step 4 If not already, select the required TLS protocols.

Step 5 Click **Apply** to save the settings.

Directory Synchronization

Cisco Unified Attendant Console Standard uses TLS protocol to connect with Cisco Unified Communication Manager for directory import. The required TLS protocol version should be enabled on both the Cisco Unified Attendant Console Standard machine at Operating System level and in the Cisco Unified Communication Manager.

Presence from Cisco IM & Presence

Cisco Unified Attendant Console Standard uses TLS protocol to connect with Cisco IM & Presence to retrieve contact directory presence information. The required TLS protocol version should be enabled on both the Cisco Unified Attendant Console Standard machine at Operating System level and in the Cisco Unified IM & Presence.