



Cisco Unified Attendant Console Standard - Installation and Configuration Guide

Version 12.0.2
December 4, 2017

Cisco Systems, Inc.
www.cisco.com

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

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

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

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

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

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

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

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

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

Cisco Unified Attendant Console Standard - Installation and Configuration Guide
© 2017 Cisco Systems, Inc. All rights reserved.



About This Guide i

Who Should Read This Guide	i
How This Guide is Organized	i
Document Conventions	ii
Obtaining Documentation and Submitting Service Requests	iii

CHAPTER 1

Introduction to Cisco Unified Attendant Console Standard 1-1

Accessibility for Users with Disabilities	2
Cisco Unified Attendant Console Standard User Interface	1-2
Accessing Help on the Application	1-3

CHAPTER 2

Installing Cisco Unified Attendant Console Standard 2-1

PC Hardware and Software Requirements	2-1
Operating System Support	2-1
Virtual Desktop Support	2-2
Jabber Support	2-2
Network Requirements	2-2
Round Trip Time	2-3
Virus Scan Exclusions	2-3
Windows Folder Permissions	2-3
Scalability	2-4
Directory Synchronization	2-4
Presence	2-4
Cisco Unified Communications Manager Compatibility	2-4
Shared Lines	2-5
Configuring Cisco Unified Communications Manager	2-6
Creating an Access Control Group	2-6
Assigning Roles to a User Group or Access Control Group	2-7
Creating and Assigning an Application User	2-8
Assigning Devices to Application User to Enable Operator Log In and Directory Contact BLF	2-8
End User Account Required For Presence	2-9
Installing or Upgrading Cisco Unified Attendant Console Standard	2-9
Licensing Cisco Unified Attendant Console Standard	2-11
Activating Evaluation Software	2-12

Activating Purchased and Upgraded Software 2-13
 Relicensing Software 2-15

CHAPTER 3

Starting Cisco Unified Attendant Console Standard 3-1
 Starting Cisco Unified Attendant Console Standard 3-2
 Accessing Cisco Unified Attendant Console Standard When There Are No Valid Devices 3-4
 Signing Out 3-4
 Logging In to Hunt groups 3-5
 Logging Out of Hunt groups 3-5
 Exiting Cisco Unified Attendant Console Standard 3-5

CHAPTER 4

Configuring Cisco Unified Attendant Console Standard 4-1
 Preventing Access To Options Tabs 4-2
 Making Options Tabs Accessible 4-2
 Setting Operator Details 4-3
 Using Single Sign-on 4-3
 Configuring Presence Server 4-4
 Modifying Presence Server Connection Details 4-4
 Configuring Multi-Domain Presence Server 4-5
 Configuring Single Domain Presence Server 4-6
 Connecting to a Different Cisco Unified Communications Manager 4-6
 Setting the Operator Voicemail Prefix 4-7
 Configuring Alerts 4-7
 Managing Sign In Devices 4-8
 Manually Adding Sign In Devices 4-9
 Importing Sign In Devices 4-9
 Deleting Sign In Devices 4-10

CHAPTER 5

Directories 5-1
 Contact Matching 5-2
 Directory Synchronization 5-3
 Synchronizing From a CSV Source File 5-4
 Configuring Synchronization 5-4
 Application Dial Rules 5-5
 Directory Filtering 5-5
 Creating Directory Filters 5-6
 Directory Field Mappings 5-7

Destination Fields	5-7
Source Fields	5-7
Setting Directory Field Mappings	5-8
BLF Rules	5-8
Adding BLF Rules	5-9
Editing BLF Rules	5-10
Test All Rules	5-10
Deleting BLF Rules	5-11
Reordering BLF Rules	5-11
Directory Groups	5-12
Creating Directory Groups	5-12
Deleting Directory Groups	5-12
Renaming Directory Groups	5-13
Importing Contacts Into Directory Groups	5-13
Manually Adding Contacts To Directory Groups	5-14
Deleting Contacts From Directory Groups	5-15
Editing Contacts In Directory Groups and the Corporate Directory	5-16
Exporting Contacts From Directory Groups	5-16
Viewing and Using Directories	5-18
Changing the Directory Tab Order	5-19
Changing the Directory View	5-20
Changing what data columns are displayed and column order	5-20
Changing contact order	5-20
Searching For Contacts	5-21
Search Preferences	5-21
Viewing Contact Information	5-22
Contact Notes	5-23
Adding Contact Notes	5-23
Editing Contact Notes	5-23
Deleting Contact Notes	5-23

CHAPTER 6**Keyboard Shortcuts** 6-1

Defining and Editing Keyboard Shortcuts	6-2
Removing Keyboard Shortcuts	6-3
Resetting Shortcuts to their Default Values	6-3

APPENDIX A**Application Log Configuration and Collection** A-1

Access the Logging Menu	A-1
Configuring Logging	A-1

Log Collection A-2

APPENDIX B

Import/Export File Formats B-1

XML File Format B-1

CSV File Formats B-2

CSV Files for Synchronization B-2

CSV Files for Directory Import and Export B-3

CSV Files for Importing Sign In Devices B-3

APPENDIX C

Phones Supported by Cisco Unified Attendant Console Standard C-1

APPENDIX D

Troubleshooting Guide D-1

CUCM Upgrade Version Must Match Installed Version D-1

APPENDIX E

Using a Cisco Unified Communications Manager TFTP server for all non-TAPI functions E-1

New Installation Instructions E-1

Modifying an Existing Installation E-2

INDEX



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
Chapter 1, “Introduction to Cisco Unified Attendant Console Standard”	Introduction to Cisco Unified Attendant Console Standard
Chapter 2, “Installing Cisco Unified Attendant Console Standard”	Preparing Cisco Unified Communications Manager and installing Cisco Unified Attendant Console Standard
Chapter 3, “Starting Cisco Unified Attendant Console Standard”	Starting Cisco Unified Attendant Console Standard and configuring operator details
Chapter 4, “Configuring Cisco Unified Attendant Console Standard”	Configuring Cisco Unified Attendant Console Standard, including managing sign in devices
Chapter 5, “Directories”	Using and controlling directories
Chapter 6, “Keyboard Shortcuts”	Setting up keyboard shortcuts
Appendix A, “Application Log Configuration and Collection”	Configuring application logging
Appendix B, “Import/Export File Formats”	Formats of import and export files
Appendix C, “Phones Supported by Cisco Unified Attendant Console Standard”	List of supported Cisco phones

Section	Contains
Appendix D, “Troubleshooting Guide”	Instructions for solving notable problems with Cisco Unified Attendant Console Standard.
Appendix E, “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.

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.
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic</i> 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.
<code>courier font</code>	Terminal sessions and information the system displays appear in <code>courier</code> font.



Note

Means *reader take note*.



Tip

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



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



Timesaver

Means *the described action saves time*. You can save time by doing what is described in the paragraph.



Warning

Means *reader be warned*. In this situation, you might do something that could result in bodily injury.

Obtaining Documentation and Submitting Service Requests

For information on obtaining additional documentation and submitting service requests, 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 details of the supported versions, see [Cisco Unified Communications Manager Compatibility, page 2-4](#). Cisco Unified Attendant Console Standard supports up to 5000 contacts on a single instance.

Cisco Unified Attendant Console Standard enables you to do the following:

- Control calls on your local IP Phone, XMPP client (such as Jabber), or Cisco IP Communicator
- Make, answer and end calls
- Hold and resume calls
- Blind/consult transfer calls to directory contacts or voicemail, or any other valid number
- Direct transfers
- Join calls
- Set Call Forward and Do Not Disturb on the operator phone
- Park calls
- Create and manage conference calls
- Import custom directories of contacts not in your Cisco Unified Communications Manager directory
- Create custom directories (directory groups) and export them to share with other operators
- Synchronize Cisco Unified Attendant Console Standard's corporate (main) directory with a CUCM or CSV file source directory
- During synchronization with your source directory:
 - Map the fields from your source directory to the ones in the corporate directory
 - Filter contacts, so that only certain ones are added to the corporate directory
 - Modify contact numbers using BLF rules
- See the line state and presence of each contact
- View call history
- Specify the devices used to sign in to the application
- Log in to a hunt group when you sign in to the application
- Use Jabber presence integration in a single sign-on (SSO) environment

Online help on the application is available. For how to display the help, see [Accessing Help on the Application, page 1-3](#).

Accessibility for Users with Disabilities

The Cisco Unified Attendant Console Standard user interface and controls are described in [Cisco Unified Attendant Console Standard User Interface, page 1-2](#).

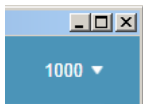
Cisco Unified Attendant Console Standard incorporates the following features to make it easier for blind and visually impaired people to use it:


- 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 [Chapter 6, “Keyboard Shortcuts”](#).
- You can set the size of call and directory text in the interface.
- A tooltip is displayed for each graphical interface control when you point to it

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

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

Component	Function
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 in to 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 <i>any</i> line on the console phone, including the call status and duration, and controls for frequently used actions, such as transferring or ending the call.

Component	Function
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	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. This pane is not displayed by default; use View > Show Call History to display it.
Directory pane	<p>Displays the synchronized directory, directory groups and search results. Contact information includes line state, presence and any notes. Includes the following controls:</p> <ul style="list-style-type: none">  – Search box for finding contacts by last name, first name, department and number. Search Preferences – Click to configure how searches are conducted. + – Click to create a new directory group. <p>For more information on the Directory pane, see Viewing and Using Directories, page 5-18.</p>

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 Help on the Application

You can display help about Cisco Unified Attendant Console Standard by doing one of the following:

- In the main menu, choose **Help > Cisco Unified Attendant Console Standard Help**.
- Press **F1**.

The Help contains the following to make it easy to find what you need to know:

- Text search tool
- Index
- Contents list.



Installing Cisco Unified Attendant Console Standard

To install Cisco Unified Attendant Console Standard you must do the following:

1. Ensure that the PC running it satisfies the minimum hardware and software requirements. These are described below.
2. Within Cisco Unified Communications Manager, create an Application User with associated phones. 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, as described in [End User Account Required For Presence, page 2-9](#). For more information about SSO, see [Starting Cisco Unified Attendant Console Standard, page 3-2](#).
3. Install the Cisco Unified Attendant Console Standard software. For instructions, see [Installing or Upgrading Cisco Unified Attendant Console Standard, page 2-9](#).

PC Hardware and Software Requirements

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

- 2.4 GHz Core 2 Duo
- 4 GB RAM
- 10 GB available hard drive space
- 100 Mbps network card, connected to the same network as Cisco Unified Communications Manager using TCP/IP
- Monitor with a minimum resolution of 1440x900
- Keyboard with 10-key number pad
- Headset (recommended)

Operating System Support

Cisco Unified Attendant Console Standard is supported under the following operating systems:

- Windows 7 with SP1
- Windows 8.1 Update 1, v. 6.3.9600 or later

- Earlier builds will need the update ([KB2919355](#)) applied prior to installing Cisco Unified Attendant Console
- Windows 10 (Desktop Mode)

For a summary of the operating systems and Cisco Unified Communications Manager versions compatible with Cisco Unified Attendant Console Standard, see the table on [page 2-5](#).

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

- Microsoft Visual C++ 2010 Redistributable
- Microsoft Visual C++ 2015 Redistributable
- Microsoft .NET Framework 4.6.1

**Note**

During the installation of Microsoft Visual C++ 2010 and C++ 2015 Redistributable, the system may require a reboot. After the reboot, the installation will continue automatically.

Virtual Desktop Support

Cisco Unified Attendant Console Standard is not supported in any virtualized desktop environment such as Citrix, Horizon or VMware Workstations.

Jabber Support

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

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. It should be installed on a Microsoft Windows computer that has been configured according to your company's operating systems hardening guidelines, and with the following network requirements considered.

The computer running Cisco Unified Attendant Console Standard must provide TCP/IPv4 and must be able to access the Cisco Unified Communications Manager and the Cisco Unified IM&P Server/Cisco WebEx Server. By default, these use the following two-way TCP ports:

- Cisco Unified Communications Manager – Port 443
- Cisco Unified IM&P Server – Port 5222
- Cisco WebEx Server - Port 5222
- TSP – Port 2748

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**

Don't forget to consider the default dynamic port range appropriate to your computer's operating system when defining its firewall settings, 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 your anti-virus software, add the following folders to your virus scan exclusions:

- *\Program Files\Cisco\Cisco Unified Attendant Console Standard* (under 32-bit operating systems)
- *\Program Files (x86)\Cisco\Cisco Unified Attendant Console Standard* (under 64-bit operating systems)
- *\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
 - Modify
 - Read & execute
 - List folder contents
 - Read
 - Write
 - Special permissions
- *\ProgramData\CUACS*
 - Modify
 - Read & execute
 - List folder contents
 - Read
 - Write
 - Special permissions

Scalability

Cisco Unified Attendant Console Standard supports up to 5000 contacts on a single instance. You can associate up to 5000 lines (not phones) with the Application User that connects Cisco Unified Attendant Console Standard to the Cisco Unified Communications Manager; any more than that and system performance may become degraded.

Directory Synchronization

Although the recommended maximum Cisco Unified Attendant Console Standard directory size is 5000 contacts, there is no theoretical limit to the number that can be stored. However, if many users (say 500) with large directories (say 50000 contacts) simultaneously try to synchronize with Cisco Unified Communications Manager it would struggle to cope.

**Note**

Cisco Unified Communications Manager's User and CTI (TSP client) resources are perfectly adequate to support this many concurrent Cisco Unified Attendant Console Standard users.

If you do have many concurrent Cisco Unified Attendant Console Standard users who are synchronizing more than the recommended maximum number of contacts, we recommend that these users:

- Configure Cisco Unified Attendant Console Standard to sync the directory infrequently; for example, once a day when they launch the application
- Stagger the times at which they synchronize or launch the application.

Presence

Cisco Unified Attendant Console Standard uses its user's personal Jabber credentials to enable presence indicators in its directory. So long as hundreds of users are not sharing the same Jabber credentials, the load on the presence server will be distributed, and there will be no problems with presence.

Cisco Unified Communications Manager Compatibility

Cisco Unified Attendant Console Standard is compatible with the Cisco Unified Communications Manager versions shown in the table on [page 2-5](#).

**Note**

The 32-bit version of TSP is required when running Cisco Unified Attendant Console under a 32-bit operating system. The 64-bit version of TSP is required when running Cisco Unified Attendant Console under a 64-bit operating system.

**Note**

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

- a. In your web browser, under **Tools**, choose **Internet Options**.
- b. In the dialog box, select the **Advanced** tab.
- c. Under **Security**, deselect (uncheck) **Check for publisher's certificate revocation**.
- d. Under **Security**, deselect (uncheck) **Check for server certificate revocation**.
- e. Click **OK**.

The operating system and Cisco Unified Communications Manager (CUCM) version compatibility is summarized below:

CUCM Version	Windows 7 SP1	Windows 8.1 Update 1	Windows 10 (Desktop Mode)
10.0(1)	Supported	Not supported	Not supported
10.5(1)	Supported	Supported	Not supported
10.5(2)	Supported	Supported	Supported (10.5.2.14900-16 or later)
11.0(x)	Supported	Supported	Supported (11.0.1.22900-14 or later)
11.5(1.13032-4) or later	Supported	Supported	Supported
12.0(1)	Supported	Supported	Supported

Shared Lines

Shared lines are used when you:

- Have multiple phones but want one phone number
- Share call-handling with co-workers
- Handle calls on behalf of someone else, such as a manager

Shared lines in the user's controlled phone are supported but with several caveats:

The user will only see full activity against the specific device they're logged into the application against. Other devices with the same DN will not show calls in the Call Control area. Furthermore, if for example Device A and Device B both have DN 1000, and a CUACS user logs in using Device A, 1000 will appear in their call control area. They will accurately see all call control for Device A. Any call activity that occurs on Device B will not be shown. Finally, call activity on non-user devices with the same DN as the user's device will cause changes in the BLF of the user's line.

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

When logged into an Extension Mobility device, the Extension Mobility DN will be searchable at the login screen and the device Extension Mobility is logged in will be selectable. If Extension Mobility is not logged in before the application is started, the Extension Mobility DN will not be selectable.

Cisco Unified Attendant Console Standard supports both shared lines and extension mobility, so long as the device is associated with the Application User. You can associate up to 5000 lines (not phones) with the Application User; any more than that and you may experience performance degradation.

All contacts sharing the same telephone number display the BLF status of the device that is the primary line *unless* none of the contacts is the primary line (for example, if the primary line becomes unregistered from Cisco Unified Communications Manager), in which case the device names are sorted in ascending order and the contacts display the BLF status of the *next* device in this list. If the primary device goes out of service but is still registered with Cisco Unified Communications Manager, no BLF status is displayed until the primary device comes back into service.

**Note**

For BLF status to work correctly with shared lines, you must ensure that all user roles described in [Assigning Roles to a User Group or Access Control Group, page 2-7](#) are assigned.

If you intend to have multiple operators using Cisco Unified Attendant Console Standard to answer calls into a single destination (for example, an office's main phone number), rather than relying on Shared Lines for call distribution you should 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.

Configuring Cisco Unified Communications Manager

Cisco Unified Attendant Console Standard must be able to communicate with the Cisco Unified Communications Manager, which it does using Cisco Unified Communications Manager TSP. Consequently, before you install Cisco Unified Attendant Console Standard you must first perform the following steps:

1. [Creating an Access Control Group, page 2-6](#).
2. [Assigning Roles to a User Group or Access Control Group, page 2-7](#).
3. [Creating and Assigning an Application User, page 2-8](#).
4. [End User Account Required For Presence, page 2-9](#).

Creating an Access Control Group

Access Control Groups define the roles and permissions available to the Application Users who are members of that group.

To create an Access Control Group, do the following:

-
- Step 1** Use your internet browser to access Cisco Unified CM Administration, and then log in.
 - Step 2** In the main menu, choose **User Management > User Settings > Access Control Group**.
 - Step 3** Click **Add New** to create a new Access Control Group.
 - Step 4** Type a **Name** for the new Access Control Group.
 - Step 5** Click **Save** to save the Access Control Group.
 - Step 6** Assign roles to the user group, as described in [Assigning Roles to a User Group or Access Control Group, page 2-7](#).
-

Assigning Roles to a User Group or Access Control Group

Roles define what the members (Application Users) of a User Group or Access Control Group can do.

To add the roles to a User Group or Access Control Group required to enable Cisco Unified Attendant Console Standard to work properly, do the following:

-
- Step 1** On the **Find and List User Groups** page, **Find** the User Group/Access Control Group you just created.
 - Step 2** In the **Search Results**, click **Roles** for the User Group/Access Control Group.
 - Step 3** Click **Assign Role to Group**.
The roles that can be assigned are listed.
 - Step 4** 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**
 - Step 5** If you are using phone models 69xx, 7931, 7965, 88xx, 89xx and 99xx, you must also select:
 - **Standard CTI Allow Control of Phones supporting Connected Xfer and conf**
 - **Standard CTI Allow Control of Phones supporting Rollover Mode**
 - Step 6** Click **Add Selected** to assign the roles.
 - Step 7** Click **Save**.
-

Creating and Assigning an Application User

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

- One operator requires a single Application User with all required devices assigned to it.
- Multiple operators using the same devices require a single Application User with all devices required by all operators assigned to it.
- Multiple operators using different devices require multiple Application Users, each with the required devices assigned to it. Operators requiring identical devices can use a single Application User.
- You can associate up to 5000 lines (not phones) with the Application User.

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

-
- Step 1** Use your internet browser to access Cisco Unified CM Administration, and then log in.
 - Step 2** In the main menu, choose **User Management > Application User**.
 - Step 3** Click **Add New**.
 - Step 4** Enter information in the following fields:
 - **User ID** (a name of your choice)
 - **Password**
 - **Confirm Password** (this must match the Password)
 - Step 5** Scroll down to the **Permissions Information** section and click **Add to Access Control Group**.
 - Step 6** Click **Save** to save the Application User.
-

Assigning Devices to Application User to Enable Operator Log In and Directory Contact BLF

Several Cisco Unified Attendant Console Standard devices need to be associated with (controlled by) a Cisco Unified CM Application User account for authentication purposes:

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

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

-
- Step 1** Use your internet browser to access Cisco Unified CM Administration, and then log in.
- Step 2** In the main menu, choose **User Management > Application User**.
- Step 3** Find and then select your Application User.
The **Application User Configuration** page appears.
- Step 4** Under **Device Information**, select the relevant **Available Devices** and then add them to the **Controlled Devices** list. To add many devices you will probably find it easier to click **Find more Phones**, and then find, select and **Add** the devices using the dialog box displayed.
- Step 5** Click **Save**.
-

End User Account Required For Presence

The presence facility within Cisco Unified Attendant Console Standard requires that each Attendant has an End User Account with Presence enabled, so that Cisco Unified Attendant Console Standard can communicate with the Cisco Unified IM&P Server/Cisco WebEx Server. The Presence User ID is used to obtain the presence information for a contact.

In most cases the Attendants will already have an End User Account on the Cisco Unified Communication Manager/Cisco WebEx Server. If they do not, ask your telephony system manager to set them up for you.

Installing or Upgrading Cisco Unified Attendant Console Standard

These instructions apply to both installing Cisco Unified Attendant Console Standard from scratch and manually upgrading your installation. When you upgrade your software the installation Wizard offers you details of your current installation, which you can accept or change, as required. You do not need to uninstall the old version before installing the new software; the following settings and configuration from the previous installation are retained:

- Database
- Log file settings
- Debug log files

However, if you manually upgrade from one major version to another (from version n.x to version n+1.x), the current licensing information is deleted (irrespective of its state) and the application reverts to running as evaluation software for 10 days. During this period, you will need to relicense the application for the new version, following the instructions in [Licensing Cisco Unified Attendant Console Standard, page 2-11](#).

Cisco Unified Attendant Console Standard requires .NET framework 4.0 to run. If .NET framework 4.0 has not been supplied or configured before installation, the installation wizard installs and configures it for you.

**Note**

To be able to install the software you must have administrator rights.

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

- Step 1** Check that your Cisco Unified Communications Manager is compatible with this version of Cisco Unified Attendant Console Standard, as described in [Cisco Unified Communications Manager Compatibility, page 2-4](#).
- Step 2** Ensure that your Application User has all the required roles assigned, as described in [Assigning Roles to a User Group or Access Control Group, page 2-7](#).
- Step 3** Browse to the installation location and run *CUACS_Setup.exe*.
The installation wizard appears.
- Step 4** In the Welcome page, click **Next**.
- Step 5** In the **Cisco Unified Communications Manager Connection Details** page, type the following:
- The **Cisco Unified Communications Manager Host Name**, Fully Qualified Domain Name (FQDN) or IP address
 - The **Cisco Unified Communications Manager Application User ID** to use
 - The **Password** that corresponds with the Cisco Unified Communications Manager User ID.
- and then click **Next**.

If you are manually upgrading your Cisco Unified Attendant Console Standard software, this page will contain your current details.

**Note**

The following:

- Port 443 is used by default. You can change the Cisco Unified Communications Manager configuration after you have installed Cisco Unified Attendant Console Standard. For instructions, see [Connecting to a Different Cisco Unified Communications Manager, page 4-6](#).
 - Connecting to the Cisco Unified Communications Manager also populates the Primary CTI Manager. 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, refer to [Appendix E, "Using a Cisco Unified Communications Manager TFTP server for all non-TAPI functions"](#) for configuration instructions.
-

- Step 6** In the two **Security Alert** messages, click **Yes**.

**Note**

During installation the Cisco Unified Communications Manager TSP appropriate to the Cisco Unified Communications Manager you intend to use is downloaded and installed.

- Step 7** In the **Language Information** page, select the language you want to use, and then click **Next**.

If you are manually upgrading your Cisco Unified Attendant Console Standard software, this page will contain your current details.

Step 8 In the **Cisco Unified Presence Server Connection Information** page, type the following:

- The **Server Address** or URL required for hosted presence.
- The **Domain** containing the server
- The **Cisco Unified Presence User Name** to use
- The **Cisco Unified Presence Password** appropriate to the User Name

and then click **Next**.

If you are manually upgrading your Cisco Unified Attendant Console Standard software, this page will contain your current details.

**Note**

The following:

- 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, page 4-4](#).
- The Presence credentials are stored in the configuration file using AES-256 encryption.

Step 9 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 10 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 11 In the **InstallShield Wizard Complete** page, select **Yes, I want to restart my computer now**, and then click **Finish**.

If you have manually upgraded from one major version to another you will now need to relicense the application for the new version, following the instructions in the next section.

Licensing Cisco Unified Attendant Console Standard

This section describes how to license your Cisco Unified Attendant Console Standard software when:

- Installing Cisco Unified Attendant Console Standard on a system that does not have any version of Cisco Unified Attendant Console installed on it.
- Upgrading from either:
 - Cisco Unified Attendant Console Department Edition to Cisco Unified Attendant Console Standard.
 - One major version of Cisco Unified Attendant Console Standard to another; when you do this the application reverts to running as evaluation software. *You do not need to relicense Cisco Unified Attendant Console Standard for minor version upgrades.*

This section contains the following topics:

- [Activating Evaluation Software](#)
- [Activating Purchased and Upgraded Software, page 2-13](#)
- [Relicensing Software, page 2-15](#)

Activating Evaluation Software

You can use downloaded software for 10 days before you must license it. Licensing the software enables you to activate the software for 60 more days of evaluation. If you do not activate the download, you will be unable to use it after the tenth day.

To activate the evaluation software, do the following:

- Step 1** As a local administrator, sign in to each instance of Cisco Unified Attendant Console Standard that you want to license and activate, and do the following:
- Choose **Help > About Cisco Unified Attendant Console Standard**.
An information box appears. If the application is already licensed, its *Registration Code* is shown in this box.
 - In the information box, click **Register**.
 - Note the **Machine Code**. This is the registration code for that instance.



Tip

Keep these codes safe, as you require them to activate the 60 evaluation period *and* to license purchased software.

- Step 2** Use your internet browser to go the [Cisco Unified Attendant Console Downloads and Licensing](#) website.
- Step 3** Enter your **User Name** and **Password**, and then click **Log In**.
- Step 4** In the navigation bar, click **ACTIVATE EVALUATION SOFTWARE**.
- Step 5** Select your **Reseller**, then select your **Customer**, and then select your **Customer Site**.



Note

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

- Step 6** Select the **Version** and the **Product** that you have installed, and then click **Next**.
- Step 7** Enter the **Registration Codes** collected in [Step 1](#), and then click **Next**.



Note

Click **+** to create new fields for additional codes.

- Step 8** Enter any additional email addresses to receive the registration file, and then click **Submit**.
If the registration codes are valid, 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 can hold licensing information for multiple instances, but each license needs to be individually applied.
- Step 9** Open the email and save the RGF file to a location that can be browsed by Cisco Unified Attendant Console Standard.
- Step 10** In Cisco Unified Attendant Console Standard, do one of the following:

- In the main menu, choose **Help > About Cisco Unified Attendant Console Standard**.
- Use the keyboard shortcut you have defined, as described in [Defining and Editing Keyboard Shortcuts](#), page 6-2.

Step 11 In the message box, click **Register**.

Step 12 In the License dialog box, either:

- a. Select **File Registration**.
- b. Type the name of or browse to the RGF file.
- c. Click **Validate**.

or – if you know details of the license for the specific instance you are licensing

- a. Select **Key Registration**.
 - b. Type an activation key **Serial Number**, which is included with the license in the RGF file.
 - c. Type the corresponding **Registration Code**.
 - d. Click **Register**.
-

Activating Purchased and Upgraded Software

You can purchase the Cisco Unified Attendant Console Standard software at any time in the evaluation period, giving you unlimited use. When you purchase the software, Cisco provides you with a 27-digit license activation code (LAC) for each instance of the application you have purchased. After activating the software, you cannot revert to the trial version.



Note

If you have purchased *à la carte* upgrade licenses, or requested UCSS upgrade licenses through the Cisco Product Upgrade Tool, you must ensure that the previous version's 27-digit LACs are activated *before* activating the upgrade LACs. If you do not do this the upgrade activation will fail.

If you have an upgrade agreement, you can manually upgrade any Cisco Unified Attendant Console Department Edition (version 8.x or 9.x) installations to Cisco Unified Attendant Console Standard. However, you must activate the Cisco Unified Attendant Console Department Edition LACs before you can activate the upgrade LACs.

When you upgrade using UCSS licenses you can convert Cisco Unified Attendant Console Department Edition license instances into the same number of Cisco Unified Attendant Console Standard instances. You can upgrade either:

- All the Cisco Unified Attendant Console Department Edition seats into Cisco Unified Attendant Console Standard at once.
- Some of the Cisco Unified Attendant Console Department Edition seats and then upgrade the remainder later.

For example, if you had a Cisco Unified Attendant Console Department Edition LAC with 10 seats, you can either activate all 10 LAC codes at once to obtain 10 Cisco Unified Attendant Console Standard licenses, or you can, say, obtain 5 Cisco Unified Attendant Console Standard UCSS Upgrade licenses today and the remainder later.

**Note**

If you had 10 Cisco Unified Attendant Console Department licenses, and upgraded 5 of these to Cisco Unified Attendant Console Standard version 10, you can upgrade the 5 remaining licenses to Cisco Unified Attendant Console Standard version 11 using your old Cisco Unified Attendant Console Department Registration Code or LAC.

If you have UCSS, you can convert each version 10 license you have to a version 11 license by supplying either the Registration Code or LAC for that license.

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


-
- Step 1** Use your internet browser to go 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 PURCHASED SOFTWARE**.
- Step 4** Select your **Reseller**, then select your **Customer**, and then select your **Customer Site**.

**Note**

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

-
- Step 5** Select the **Version** and the **Product** (CUAC Standard) that you have installed, and then click **Next**.
- Step 6** Enter a unique **Registration Code** (one of the machine codes collected on [page 2-12](#)) and **License Activation Code** pair for each instance, and then click **Next**.

**Note**

Click  to create new fields for any additional pairs of codes.

-
- Step 7** If all the License Activation Codes are UCSS codes for Cisco Unified Attendant Console Standard, enter details of the previously used Cisco Unified Attendant Console Department Edition Registration Code and License Activation Code pairs that you wish to upgrade to Cisco Unified Attendant Console Standard.
- Step 8** In the License Request Confirmation page, optionally enter an additional e-mail address and click **Submit**. If you want to change the codes you entered in [Step 6](#) before proceeding, click **Back**.
- A registration (RGF) file is e-mailed to you, and license request confirmation information is displayed in the web page.
- Step 9** Open the email and save the registration file to a location that can be browsed by Cisco Unified Attendant Console Standard.
- Step 10** In Cisco Unified Attendant Console Standard, do one of the following:
- In the main menu, choose **Help > About Cisco Unified Attendant Console Standard**.
 - Use the keyboard shortcut you have defined, as described in [Defining and Editing Keyboard Shortcuts](#), [page 6-2](#).
- Step 11** In the message box, click **Register**.
- Step 12** In the License dialog box, either:
- a. Select **File Registration**.
 - b. Type the name of or browse to the RGF file.
 - c. Click **Validate**.

or – if you know details of the license for the specific instance you are licensing

- a. Select **Key Registration**.
 - b. Type an activation key **Serial Number**, which is included with the license in the RGF file.
 - c. Type the corresponding **Registration Code**.
 - d. Click **Register**.
-

Relicensing Software

If you do any of the following you must re-license the software with a new registration code:

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

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



Starting Cisco Unified Attendant Console Standard

Cisco Single Sign On (SSO) is a facility to help users who run multiple Cisco Unified Communications applications in a work session: once a user has signed in to any one of the applications they do not need to sign in to any of the others.



Note

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

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

How you start Cisco Unified Attendant Console Standard depends on whether your working environment has SSO configured, and whether you have configured Cisco Unified Attendant Console Standard to use it. SSO runs for a configurable length of time; if this expires while you are using Cisco Unified Attendant Console Standard you are prompted to refresh your log in so that you can continue working.

- For more information about SSO, including how to configure the Cisco Unified Communications Manager to use it, see the relevant Cisco documentation.
- For more information about configuring Cisco Unified Attendant Console Standard to run in the SSO environment, see [Using Single Sign-on, page 4-3](#).

If Cisco Unified Attendant Console Standard is configured to use SSO, and if you launch it before any other Cisco Unified Communications application you are presented with a web page asking for your SSO End User Username and Password. Once you have entered this information, you will not need to sign in to any other Cisco Unified Communications application during that work session. If you are working in an SSO environment, and Cisco Unified Attendant Console Standard is configured to use it, you *will not* be able to start it without being authenticated through this web page.

In an SSO environment, the End User accessed through the web page login provides the Presence information; so an End User does not need to be set up in Cisco Unified Attendant Console Standard. Outside the SSO environment, Cisco Unified Attendant Console Standard uses the End User credentials configured under **File > Options > Configuration** to provide Presence information.

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 If one of the following is true:

- You are working in a non-SSO environment
- You are working in an SSO environment but have not yet configured Cisco Unified Attendant Console Standard to use it (how to configure the application is described in [Using Single Sign-on, page 4-3](#))
- 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 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. 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, page 4-8](#)). 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 in to Cisco Unified Attendant Console Standard. For more information, see [Assigning Devices to Application User to Enable Operator Log In and Directory Contact BLF, page 2-8](#).

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, as described in [Accessing Cisco Unified Attendant Console Standard When There Are No Valid Devices, page 3-4](#).

- 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**

The following:

- 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.
- You can also log in or out of hunt groups as described in [Logging In to Hunt groups, page 3-5](#) and [Logging Out of Hunt groups, page 3-5](#).

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, who will create a valid device following the procedure in [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 in to the console.

While the application is running, you can change the attendant console operator directory number (DN), as described in [Setting Operator Details, page 4-3](#).

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 completely clear the Device List - so that the application can be used.

To access Cisco Unified Attendant Console Standard when no valid device is available in the Device List, the system administrator should 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.

Add one or more new devices, as described in [Manually Adding Sign In Devices, page 4-9](#), or clear all the devices from the list.

- When an Options Password *has* been set, the Options window appears, with the *Options Password* tab displayed.
 - a. Make the Device List tab accessible as described in [Making Options Tabs Accessible, page 4-2](#).
 - b. Add one or more new devices, as described in [Manually Adding Sign In Devices, page 4-9](#), or clear all the devices from the list.

Step 3 Close the Options window.

The Sign In screen appears and the operator can use a new device to sign in.

Signing Out

To sign out from your current 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, and the application continues to run and any synchronization currently in progress continues. When you sign out you are automatically logged out of any hunt groups to which you belong.

To resume using the application, sign in as before.

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 (as described on [page 3-3](#)), 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**.
- Use the **Ctrl+I** keyboard shortcut.

Also, 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, as described in [Defining and Editing Keyboard Shortcuts](#), [page 6-2](#).
- 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

Enabling password protection is described in [Preventing Access To Options Tabs, page 4-2](#); disabling it is described in [Making Options Tabs Accessible, page 4-2](#).

This chapter also describes the following configuration procedures:

- [“Setting Operator Details” on page 4-3](#)
- [“Using Single Sign-on” on page 4-3](#)
- [“Configuring Presence Server” on page 4-4](#)
- [“Connecting to a Different Cisco Unified Communications Manager” on page 4-6](#)
- [“Setting the Operator Voicemail Prefix” on page 4-7](#)
- [“Configuring Alerts” on page 4-7](#)
- [“Managing Sign In Devices” on page 4-8](#)

For details of configuring synchronization with Cisco Unified Communications Manager, see [Configuring Synchronization, page 5-4](#).

For details of moving, stretching and hiding parts of the interface, see the Cisco Unified Attendant Console Standard online Help.

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 on [page 4-1](#).

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 *Configuration* tab, as described in [Connecting to a Different Cisco Unified Communications Manager, page 4-6](#)).
 - 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 on [page 4-1](#) 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 *Configuration* tab, as described in [Connecting to a Different Cisco Unified Communications Manager, page 4-6](#)).
 - 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 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 [Chapter 6, “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 (see [“Managing Sign In Devices” on page 4-8](#)), the same restrictions as on the sign in extension apply, but the list is not displayed when you start typing.

Step 4 Click **Apply**.

Using Single Sign-on

If you are running Cisco Unified Attendant Console Standard in a Single Sign On environment, you have the option of using Single Sign On or not using it. When you install Cisco Unified Attendant Console Standard it is configured not to use Single Sign On, even if it is available. Consequently, when you start the application for the first time after installation, you are *not* prompted for Single Sign On credentials.

To use Cisco Unified Attendant Console Standard with 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 [Chapter 6, “Keyboard Shortcuts”](#).

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

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



Note The following:

- 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 [Chapter 6, “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 an 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” on page 4-5](#)
 - [“Configuring Single Domain Presence Server” on page 4-6](#)
 - **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.
-

Connecting to a Different Cisco Unified Communications Manager



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, page 4-2](#).

Once Cisco Unified Attendant Console Standard is installed, you can connect to a Cisco Unified Communications Manager different from the one you specified during installation, and so use a different source directory. However, the new Cisco Unified Communications Manager must be the same major revision as the one specified during installation; you cannot upgrade to a later revision using this method.

To connect to a different Cisco Unified Communications Manager, 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 [Chapter 6, “Keyboard Shortcuts”](#).

Step 2 Click the **Configuration** tab.

Step 3 Under **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 Password** that corresponds with the Username.

**Note**

The Cisco Unified Communications Manager credentials are stored in the configuration file using AES-256 encryption.

Step 4 Click **Apply**.

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

Step 5 Exit and then restart Cisco Unified Attendant Console Standard for the change 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, page 4-2](#).

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 [Chapter 6, “Keyboard Shortcuts”](#).

Step 2 Click the **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 [Chapter 6, “Keyboard Shortcuts”](#).

Step 2 Click the **Alerts** tab.

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

- Select the **Taskbar** check box if you want the application icon in the Windows taskbar to flash when that event occurs.
- Select the **Pop to Front** check box 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 in to 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, page 4-2](#).

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, page 4-2](#).

You can import sign in devices from a CSV file with the format described in [CSV Files for Importing Sign In Devices, page B-3](#).

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, page 4-2](#).

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 and write access. However, if the file does not include a unique identifier (Primary Key) for each contact, it needs to be on the machine running Cisco Unified Attendant Console Standard.

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, page 5-3](#).

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, page 5-13](#).
- Contacts you enter yourself. For more information, see [Manually Adding Contacts To Directory Groups, page 5-14](#).

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.



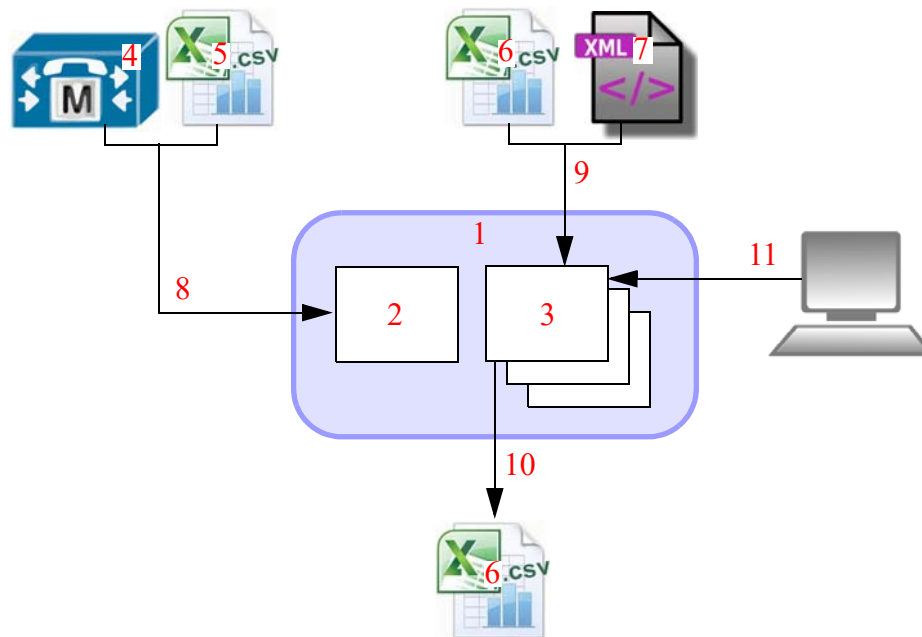
Note

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

You cannot amend contact records in the corporate directory. By contrast, directory groups are *not* updated by synchronization; and you *can* amend the contact details they contain.

For more information, see “[Directory Groups](#)” on [page 5-12](#).

The relationships between directories and external information is summarized below.



Legend

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, page B-2](#).
6. CSV file for importing and exporting. For details of the format, see [CSV File Formats, page B-2](#).
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.

Contact Matching

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:

1. If the caller is a manually-created (speed dial) contact in the database, the name from there is displayed.
2. If the caller is not manually created, but their name is synchronized in the database, that is displayed.
3. 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.

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, page 5-7](#).

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, page 5-5](#).

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, page 5-8](#).



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, page 5-4](#).

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, page B-2](#). The first column of the CSV file must contain a unique identifier, known as a GUID, which identifies that contact as unique. If it does not, Cisco Unified Attendant Console Standard adds a first, GUID, column.

If your CSV file does not have a GUID column, and you intend storing it in a shared location that does not have write access, then before you put it there, you should place it locally and provide read-write access so that Cisco Unified Attendant Console Standard can add the GUID column.

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, page 4-2](#).

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.



Note

You can configure a keyboard shortcut to do this. For instructions, see [Chapter 6, “Keyboard Shortcuts”](#).

- Step 2** Click the **Configuration** 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** If you do not want to specify a different Cisco Unified Communications Manager, skip this step. Otherwise, under **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 the roles described in [Assigning Roles to a User Group or Access Control Group, page 2-7](#).
 - The **Application Password** that corresponds with the Username.

- Step 5** If you do want 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.
- If you do not have a CSV source, click **Clear** to clear this field.
- To view a sample CSV file, click **View Sample**.
- Step 6** Click **Apply**.
-

Application Dial Rules

Cisco Unified Communications Manager uses Application Dial Rules to automatically strip digits from, or add digits to, dialed numbers. When a user logs into Cisco Unified Attendant Console Standard these rules are downloaded (synchronized) from Cisco Unified Communications Manager and stored locally by Cisco Unified Attendant Console Standard. When handling outbound calls, Cisco Unified Attendant Console Standard executes the local rules as required (including during transfers, conferences and diverts). If there are multiple rules, they are executed in the same priority order as defined in the Cisco Unified Communications Manager. If the login synchronization fails, dial rules cannot be applied.

During rule synchronization:

- If a rule is not stored locally, it is added to the store.
- If a rule is stored locally, it is updated as required.
- If a rule is stored locally but has been deleted from Cisco Unified Communications Manager, it is deleted from the local store.

Any changes made to Cisco Unified Communications Manager application dial rules are not updated in the local store until you exit and restart Cisco Unified Attendant Console Standard. You cannot edit application dial rules from within Cisco Unified Attendant Console Standard.



Note

- Because all outbound numbers dialed by operators are subject to dial rules, you must ensure that your Call Parking devices use numbers that do not cause a rule to be applied, otherwise you will be unable to retrieve calls parked on these extensions.
 - Before **Application Dial Rules** can be processed, CUACS will only pass through dialable characters (including: *,+, 0-9, #). Any non-dialable characters will be dropped from contact directory numbers when executing call control actions against them.
-

Directory Filtering

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

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, page 4-2](#).

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 [Chapter 6, “Keyboard Shortcuts”](#).

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

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

- 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.
- Select the contact **Field** to compare.
- Select the **Condition** to use in the comparison.
- In **Value**, type the text to compare with the Field.
- 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. How to do these is described in [Setting Directory Field Mappings, page 5-8](#).

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, page 4-2](#).

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 [Chapter 6, “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, page 4-2](#).

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 [Chapter 6, “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, page 4-2](#).

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 [Chapter 6, “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. These are described in [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**.
- Step 2** The **Options** window appears.
- Step 3** Click the **BLF Rules** tab.
- Step 4** Click **Test All Rules**.
- Step 5** In the pop-up window, enter the **Pre-Transformation Number** on which to test your rules.
- Step 6** Select the **Directory Source** (All, CUCM or CSV).
- Step 7** Click **Run Test** to see **Test Results**.
- Step 8** 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, page 4-2](#).

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 [Chapter 6, “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, page 4-2](#).

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 [Chapter 6, “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:
- Select the rule.
 - To move the rule towards the top of the list, click **Move Up**.
 - 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, page 5-12](#).

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

- Importing contacts from CSV files or XML files, as described in [Importing Contacts Into Directory Groups, page 5-13](#).
- Manually creating contacts, see [Manually Adding Contacts To Directory Groups, page 5-14](#).

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, as described in [Defining and Editing Keyboard Shortcuts, page 6-2](#).

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, as described in [Defining and Editing Keyboard Shortcuts, page 6-2](#).
-

Renaming Directory Groups

To rename a directory group, do 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, as described in [Defining and Editing Keyboard Shortcuts, page 6-2](#).

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 file 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 [Appendix B, “Import/Export File Formats”](#).



Note

The following points:

- You cannot import contacts into a directory group while the application is synchronizing to the corporate directory.

- When you import from these types of file, no checks are made to see if the contact information is duplicated in any directory group, including the one that you are importing the data into.
- The format of CSV files imported/exported is different from that of CSV files used for synchronization.

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, page 5-12](#).

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

Step 1 Do one of the following:

- In the main menu, choose **File > Import Contacts**.
or
- a. In the main menu, choose **File > Options**.
- b. In the **Options** window, click the **Import/Export** tab.
or
- Right-click in any directory group, and then select **Import Contacts**.
or
- Use the keyboard shortcut you have defined, as described in [Defining and Editing Keyboard Shortcuts, page 6-2](#).

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**.

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, as described in [Defining and Editing Keyboard Shortcuts, page 6-2](#).
- The **Contact** dialog box appears.
- Step 2** Type the contact information, which is described in [Destination Fields, page 5-7](#). 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, as described in [Defining and Editing Keyboard Shortcuts, page 6-2](#).

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, as described in [Defining and Editing Keyboard Shortcuts, page 6-2](#).

The **Contact** dialog box appears.

Step 3 Edit the contact information, which is listed in [Destination Fields, page 5-7](#).



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**.

or

- a. In the main menu, choose **File > Options**.
- b. In the **Options** window, click the **Import/Export** tab.

or

- Right-click in any directory group, and then select **Export Contacts**.

or

- Use the keyboard shortcut you have defined, as described in [Defining and Editing Keyboard Shortcuts, page 6-2](#).

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

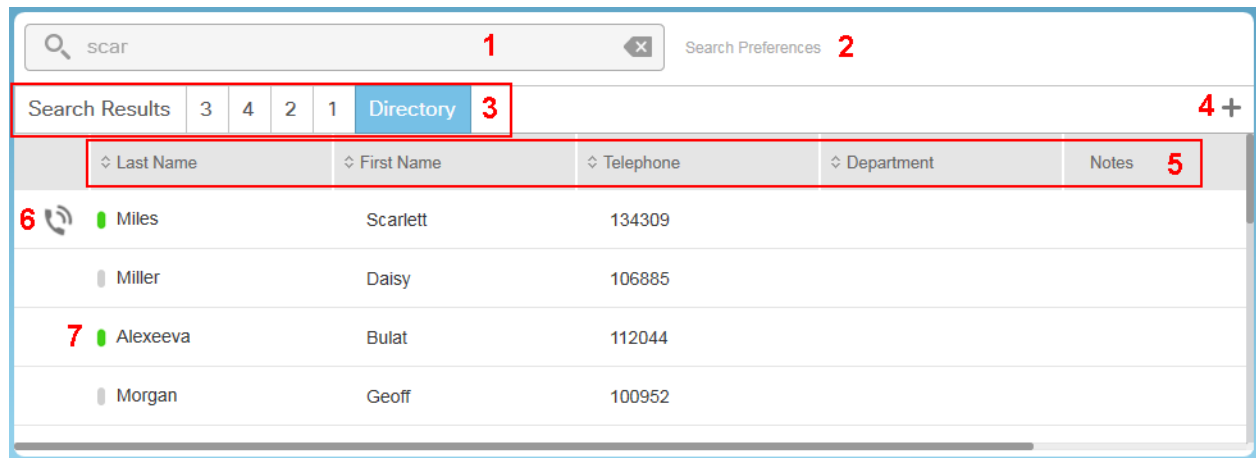
The format of CSV files imported/exported is different from that of CSV files used for synchronization.

- 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:



Legend

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, as described in [Changing the Directory Tab Order](#), page 5-19.
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

How to change what columns of information are displayed is described [Changing the Directory View, page 5-20](#).

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 the following:

- What 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. Configure the searchable fields as described in [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, as described in [Editing Contacts In Directory Groups and the Corporate Directory, page 5-16](#).
- 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**.



Note You can configure a keyboard shortcut to do this. For instructions, see [Chapter 6, “Keyboard Shortcuts”](#).

The Edit Note dialog box appears.

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 [Adding Contact Notes](#) procedure, but edit the existing 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**

The following:

- These menu options are disabled if there are no notes to delete.
 - You can configure a keyboard shortcut to do this. For instructions, see [Chapter 6, “Keyboard Shortcuts”](#).
-

Step 3 The notes are deleted from the contact **Notes** column.



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:

- 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.

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**.
 - b. The **Options** window appears.
 - c. 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, simply type **Ctrl+Y** (press and hold the **Ctrl** 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, as described in [Defining and Editing Keyboard Shortcuts, page 6-2](#).
 - 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, as described in [Defining and Editing Keyboard Shortcuts, page 6-2](#).
 - 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**.
-



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, page 4-2](#).

Cisco Unified Attendant Console Standard can keep a log of all event 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 [Chapter 6, "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.

- Logging Level - 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 of the log files and a log configuration file.



Import/Export File Formats

Cisco Unified Attendant Console Standard can handle contact directory files in the following formats:

- [XML File Format, page B-1](#)
- [CSV File Formats, page B-2](#)

It can also import login devices from CSV files, with the format described in [CSV Files for Importing Sign In Devices, page B-3](#).

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:

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

For example:

```
#      * Copyright (c) 2017 by Cisco Inc.
#      * All rights reserved.
#
# Here is a sample corporate directory file. It should contain
# comma separated entries, one line per user in the directory
# The values should in the following format:
#
# Last Name, First Name, Telephone number, Department, User Field 1, User Field 2, Site,
Building, Directory URI
#
# Empty values are legal (no department etc.)
#
# Lines starting with '#' or ';' are treated as comments
# and ignored. Empty or blank lines are ignored as well

Kathirine,Jim,25421,Marketing,,,,,Jim@cisco.com
Martha,Bryan,87952,Support,,,,,martha@cisco.com
Luce,Richard,2548,Marketing,,,,,luce@cisco.com
Meriall,Thomas,8763,Marketing,,,,,meriall@cisco.com
```

```
Harye,Walter,5563,Marketing,,,,,harye@cisco.com
```

CSV Files for Directory Import and Export

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.
```

For example:

```
#      * Copyright (c) 2017 by Cisco Inc.
#      * All rights reserved.
#
# Here is a sample import file. It should contain
# 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
#
# Empty values are legal (no email etc.)
#
# If a Group Name is specified in the CSV file, it will take precedence over the Directory Group
selected at the Import screen.
#
# Lines starting with '#' or ';' are treated as comments
# and ignored. Empty or blank lines are ignored as well

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,
```

CSV Files for Importing Sign In Devices

You can import devices that operators use to log into Cisco Unified Attendant Console Standard, as described in [Importing Sign In Devices, page 4-9](#).

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

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

For example:

```
#      * Copyright (c) 2017 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 supports the following phones:

Phone Type	Supported
3905	Not as Console and cannot support , but can transfer.
3911	
3951	
6901	Not tested
6911	Yes
6921	Yes
6941	Yes
6945	Yes
6961	Yes
7811	Yes
7821	Yes
7841	Yes
7861	Yes
7902	Not tested (Obsolete)
7905	Yes
7906	Yes
7910	Yes
7911	Yes
7912	Yes
7915	Yes
7916	Yes
7920	Yes
7921	Yes
7925	Yes
7925G	Yes

Phone Type	Supported
7925G-EX	Yes
7926	Yes
7931	Yes
7940	Yes
7941	Yes
7941G-GE	Yes
7942	Yes
7942-G	Yes
7945	Yes
7945G	Yes
7960	Yes
7961	Yes
7961G-GE	Yes ‡
7962	Yes
7965	Yes
7965G	Yes
7970	Yes
7971	Yes
7975	Yes ‡
8811	Yes
8841	Yes
8845	Yes
8851	Yes
8851NR	Yes
8861	Yes
8865	Yes
8865NR	Yes
8941	Yes
8945	Yes
8961	Yes
9951	Yes
9971	Yes
Cisco CSF	Yes
Cisco Jabber for Android	Supported for the purpose of monitoring contact BLF status.
Cisco Jabber for iPad	Supported for the purpose of monitoring contact BLF status.

Phone Type	Supported
Cisco Jabber for iPhone	Supported for the purpose of monitoring contact BLF status.
Cisco Jabber for Windows	Yes.
DX70	Yes
DX80	Yes
DX650	Yes
IP Communicator	Yes

‡ If **Log in to hunt groups at sign in** is selected, the Cisco Unified Communications Manager resets this phone type when the user logs in to the Cisco Unified Attendant Console Standard client.



Troubleshooting Guide

This appendix describes notable problems with Cisco Unified Attendant Console Standard and their solutions. It describes the following:

[CUCM Upgrade Version Must Match Installed Version.](#)

CUCM Upgrade Version Must Match Installed Version

After entering the **Call Manager Detail** in the **Options** window, you see the error message:

CUCM upgrade version must be matched with the installed version. Please check the connection details and try again.

Reason

There has been a major Cisco Unified Communications Manager (CUCM) upgrade since Cisco Unified Attendant Console Standard was installed.

Solution

Uninstall and then reinstall Cisco Unified Attendant Console Standard.

■ CUCM Upgrade Version Must Match Installed Version



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.

New Installation Instructions

- Step 1** Follow the instructions in [Chapter 2, “Installing or Upgrading 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.
1. Navigate to your Cisco Unified Communications Manager Administration webpage, and log in.
 2. Navigate to **Application > Plugins**.
 3. Search for and download the appropriate Cisco TAPI 32 or 64-bit Client
 4. 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 51019.
 - Select **Never Auto-Upgrade**.
 - Restart the PC when prompted.

Modifying an Existing Installation

- Step 1** Update the Call Manager Server Address in the Cisco Unified Attendant Console Standard, Options menu.
- a. Select **File > Options**.
 - b. Select **Configuration**.
 - c. Modify the **Call Manager Server Address** to reflect the address of the TFTP server.
 - d. Click **Apply**, close the Options window, and exit the console.
- Step 2** Modify the Cisco TSP configured Primary/Backup CTI Manager (if required).
- a. Launch Cisco TSP Configuration.
 - b. Select **Configure**, select **CTI Manager**.
 - c. Update the **Primary** (and Backup if applicable) CTI Manager Location to reflect the intended CTI Manager running the CCM service.
- Step 3** Restart the PC.



A

Access Control Group

- assigning roles to [2-7](#)
- creating [2-6](#)

accessibility for users with disabilities [1-2](#)

active call information [1-2](#)

alerts, configuring [4-7](#)

application dial rules [5-5](#)

Application User

- assigning devices to, for directory BLF [2-8](#)
- creating and assigning [2-8](#)

B

BLF rules [5-3, 5-8 to 5-12](#)

- adding [5-9](#)
- deleting [5-11](#)
- editing [5-10](#)
- reordering [5-11](#)

C

Call Control pane [1-2](#)

Call History pane [1-3](#)

Cisco Unified Attendant Console Standard

- features [1-1](#)
- installing [2-9](#)
- licensing [2-11 to 2-15](#)
- upgrading [2-9](#)

Cisco Unified Communications Manager

- compatibility [2-4](#)
- configuring [2-6 to 2-9](#)

- connecting to a different [4-6](#)

computer requirements [2-1](#)

contact information

- editing [5-16](#)
- viewing [5-22](#)

contact matching [5-2](#)

contact notes [5-23](#)

contact order [5-20](#)

contacts

- adding [5-14](#)
- searching [5-21](#)

corporate directory [5-1](#)

CSV file [5-1](#)

- formats [B-2](#)
- for synchronization [B-2](#)

CUCM, *See* Cisco Unified Communications Manager

D

device list [4-8](#)

directories [5-1 to 5-24](#)

- editing contacts [5-16](#)
- sorting [5-20](#)
- viewing and using [5-18](#)

directory

- change view [5-20](#)
- destination fields [5-7](#)
- group [5-1](#)
- search preferences [5-21](#)
- source fields [5-7](#)
- sources [5-1](#)
- synchronization [5-3 to 5-5](#)

directory field mappings [5-3, 5-7](#)

- setting [5-8](#)
- directory filters [5-3, 5-5](#)
 - creating [5-6](#)
- directory groups [5-12 to 5-17](#)
 - adding contacts manually [5-14](#)
 - creating [5-12](#)
 - deleting [5-12](#)
 - deleting contacts [5-15](#)
 - exporting contacts [5-16](#)
 - importing contacts [5-13](#)
 - renaming [5-13](#)
- Directory pane [1-3](#)
- directory tabs [5-18](#)
 - reordering [5-19](#)

E

- End User account for Presence [2-9, 3-1, 4-5](#)
- evaluation software, licensing [2-12](#)
- exiting Cisco Unified Attendant Console Standard [3-5](#)
- export contacts [5-1](#)
- exporting contacts [5-16](#)

F

- features of Cisco Unified Attendant Console Standard [1-1](#)
- file formats when importing data [B-1](#)
- filtering directories [5-5](#)
- firewall exceptions [2-2](#)

H

- hardware requirements [2-1](#)
- Help, accessing [1-3](#)
- hunt group login [3-3, 3-5](#)

I

- import/export file formats [B-1 to B-4](#)
- importing contacts [5-1, 5-13](#)
- installing Cisco Unified Attendant Console Standard [2-1 to 2-15](#)
- interface, description [1-2](#)
- introduction to Cisco Unified Attendant Console Standard [1-1 to 1-3](#)

J

- Jabber support [2-2](#)

K

- keyboard shortcuts [6-1 to 6-3](#)
 - defining and editing [6-2](#)
 - removing [6-3](#)
 - resetting to default values [6-3](#)

L

- licensing [2-11](#)
 - evaluation software [2-12](#)
 - purchased and upgraded software [2-13](#)

M

- main menu [1-2](#)

N

- network requirements [2-2](#)

O

- operating system support [2-1](#)
- operator

details, setting [4-3](#)
 voicemail prefix, setting [4-7](#)
 Options Password [4-2](#)

P

pane
 Call Control [1-2](#)
 Call History [1-3](#)
 Directory [1-3](#)
 Parked Calls [1-3](#)
 Parked Calls pane [1-3](#)
 phones supported [C-1 to C-3](#)
 phone state, directory display [5-18](#)
 Presence Server
 configuring [4-4](#)
 multi-domain, configuring [4-5](#)
 single domain, configuring [4-6](#)
 presence state, directory display [5-18](#)
 purchased and upgraded software, licensing [2-13](#)

R

requirements, hardware and software [2-1](#)

S

searching for contacts [5-21](#)
 search preferences [5-21](#)
 shared lines [2-5](#)
 sign in devices [4-9](#)
 Single Sign On [3-1](#)
 using [4-3](#)
 software
 relicensing [2-15](#)
 requirements [2-1](#)
 SSO, *See* Single Sign On
 starting Cisco Unified Attendant Console
 Standard [3-1 to 3-5](#), [4-1 to 4-10](#)

synchronization [5-1](#), [5-3](#)
 configuring [5-4](#)
 from CSV Source File [5-4](#)

T

troubleshooting [D-1](#), [E-1 to ??](#)
 TSP installation [2-10](#)

U

upgrading the software [2-9](#)
 User Group
 assigning roles to [2-7](#)
 user interface, description [1-2](#)

V

virtualized desktop support [2-2](#)

W

Windows folder permissions [2-3](#)

X

XML file format [B-1](#)

