Cisco Unified Business/Department Attendant Consoles Web Admin / Installation Guide

Version 2.0.0.10
March 2009

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: **OL-17282-01**

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

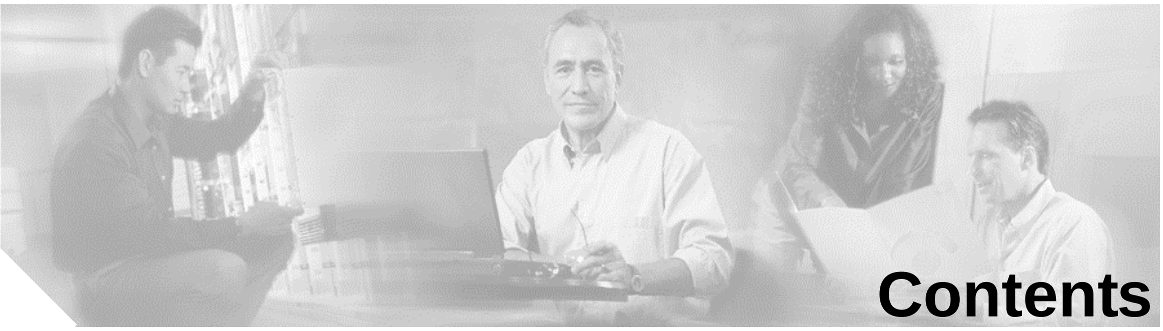
THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

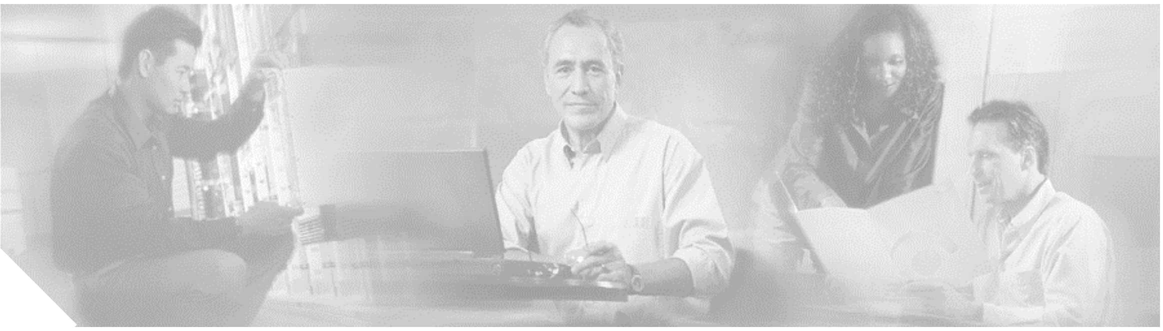
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

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 Business/Department Attendant Consoles Web Admin / Installation Guide



Contents



Preface

The following manual relates to the installation and utilisation of the **Cisco Unified Business Attendant Console (CUBAC)** and **Cisco Unified Department Attendant Console (CUDAC)** software product ranges. To make the document easier to read the name of the product ranges have been abridged to **Cisco Unified Attendant** throughtout this document.

Cisco Unified Attendant Admin provides administrator access to the configuration for Cisco Unified Attendant Console.

Cisco Unified Attendant Admin is an efficient application specially designed for configuring databases, connections to Cisco Unified Communications Manager, system and user settings. The user-friendly design of the application gives speed and flexibility to the users.

Purpose

The purpose of this user guide is to provide information on Cisco Unified Attendant Console configuration.

Who Should Read this Guide

The document is intended for,

1. Those involved in the training of Cisco Unified Attendant Admin
2. System Engineers and installers involved in the planning and provisioning of the installation and operation of Cisco Unified Enterprise Attendant Admin

How this Guide is Organized

The user guide is split into six main sections. These sections explain the functionality in a way that the users can easily get familiar with Cisco Unified Attendant Admin, perform different actions and customize it. The following table provides the organization of this guide,

Table 1: describes the sections of the user guide

Part	***Description***
Important Information	This section provides details for the compatibility of Cisco Unified Attendant applications with Cisco Unified Communications Manager.
Product Overview	This section provides a numbering test plan and gives a brief description of the Cisco Unified Attendant applications.
Installation Checklist	In order to start installing applications you must go through the checklist for successful installation.
Cisco Unified Attendant Admin	This section explains in detail all the configurations that can be done through Cisco Unified Attendant Admin.
Uninstall Attendant Cisco Unified EnterpriseAdmin	This section provides an overview on how to unistall the software successfully.

Conventions

This document uses the following conventions.

Table 2: explains the writing convention used in the user guide

Convention	***Description***
boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in braces and separated by vertical bars.
String	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in screen font.

Table 2: explains the writing convention used in the user guide

Convention	*Description*
`Boldface screen` font	Information you must enter is in boldface screen font.
`italic screen` font	Arguments for which you must supply values are in italic screen font.
→	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control-for example, the key combination ^D in a screen display means you hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Timesavers use the following conventions:

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Tips use the following conventions:

Tip Means the information contains useful tips.

Cautions use the following conventions:

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

Warnings use the following conventions:

Warning **This warning signal means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.**

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:
http://www.cisco.com/techsupport

You can access the Cisco website at this URL:
http://www.cisco.com

You can access international Cisco websites at this URL:
http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:
http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:
http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.
You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883
We appreciate your comments.

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html. If you require further assistance please contact us by sending email to export@cisco.com.

Cisco provides a free online Security Vulnerability Policy portal at this URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

1. Report security vulnerabilities in Cisco products.
2. Obtain assistance with security incidents that involve Cisco products.
3. Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:
http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:
http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release hem, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

For Emergencies only-security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

For Nonemergencies-psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:
1 877 228-7302
1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that ha been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use. If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Centre (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Reporting Security Problems in Cisco Products

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:
http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:
http://tools.cisco.com/RPF/register/register.do

Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:
http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:
Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:
http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)-An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)-Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)-Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)-You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- *The Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:
  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
  http://www.cisco.com/packet

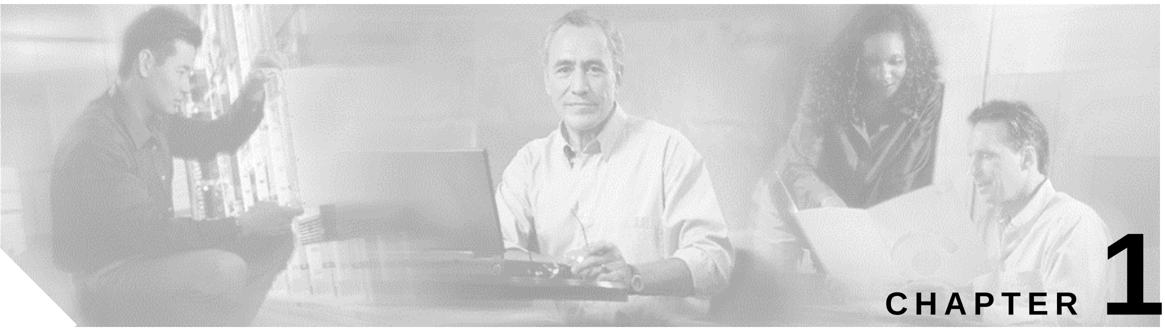
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:
  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
  http://www.cisco.com/en/US/products/index.html
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
  http://www.cisco.com/discuss/networking
- World-class networking training is available from Cisco. You can view current offerings at this URL:
  http://www.cisco.com/en/US/learning/index.html



CHAPTER 1

Introduction

Welcome to the Cisco Unified Attendant Admin User Guide. This document describes the installation and configuration procedures of the applications.

Cisco Unified Attendant Admin is the Web application that allows you to configure and manage your system and user configurations.

System configuration provides the facility to manage synchronization of devices and directory contacts with Cisco Unified Communications Manager. Cisco Unified Attendant Admin and Cisco Unified Communications Manager communicate via AXL API, using SSL, to synchronize the system devices used for queuing, servicing and parking calls. These devices are created as CTI (Computer Telephone Integration) Port and CTI Route Point devices within the Cisco Unified Communications Manager database.

User configuration allows you to manage the configuration for the Cisco Unified Attendant Console. These settings include :-

- Call queue parameters,
- Operator login credentials,
- Gobal parameters for internal/external calls access,
- Force Authorization and Client Matter Codes (FAC and CMC),
- Recall timers.

These settings are made in order to manage the call flow.

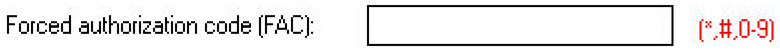
This document assumes that the reader has knowledge of,

- Cisco Unified Communications Manager
- Windows 2003/XP
- TCP/IP
- Microsoft TAPI 2.1
- Cisco Unified Communications Manager TSP

Points to Remember

Cisco Unified Attendant Admin is a set of rules that govern the way the system will operate. Each configuration is stored in a database on a Microsoft SQL Server and must be maintained to obtain optimal performance. You must note the following points,

1. Changes made through this application are not saved until you click on the **Submit** button on the page.
2. The valid range or types of characters for each field have been specified on the right-hand side of the fields in red (e.g.



Forced authorization code (FAC): (*,#,0-9)

3. Invalid input in any field will be denoted by a red colored asterisk (*).
4. Most changes to the system will be made in real-time; however, some changes will require a start and stop of Cisco Unified Attendant Server.

Accessibility for Users with Disabilities

Cisco Unified Attendant Admin provides accessibility features that make it easier for blind and visually impaired users to use the application.

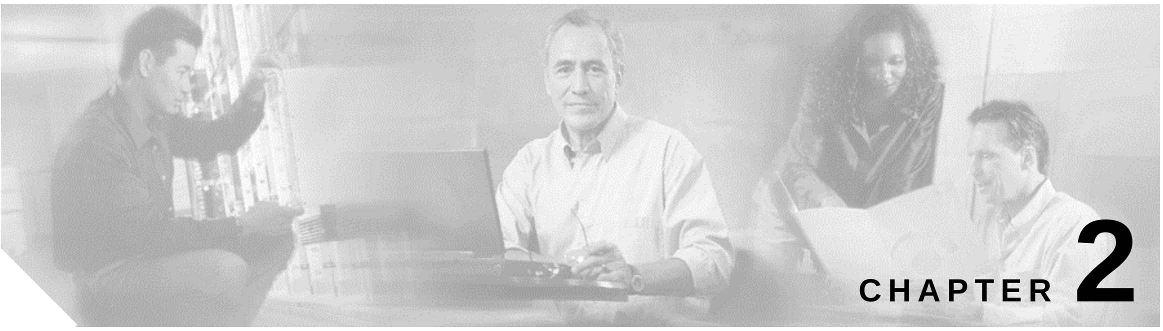
The application runs in a web browser, therefore, the configurations can be made using a mouse as well as the standard keyboard navigations supported by the web browser.

All buttons are labelled by the functionality they provide. Each icon displays a tool tip when the mouse is hovered on it, clearly defining the function of the graphic button. A list of icons along with their descriptions has also been provided in *Chapter 5 Cisco Unified Attendant Admin*.

Attendants also have an option to use Cisco Unified Business/Department Attendant Console with a screen reader plug in called JAWS. The screen reader provides the attendant with information on the status of the attendant console as well as with information about the text in the attendant console windows.

Cisco Unified Attendant Admin also comes with context-sensitive help. For every page, users can access help specific to the page they need assistance for.

For more information on Cisco Accessibility Program please contact through the following link, http://www.cisco.com/web/about/responsibility/accessibility/contact.html



CHAPTER 2

Important Information

Compatibility between Cisco Unified Attendant Console and Cisco Unified Communications Manager (CUCM)

Table 1: displays teh compatibility matrix for Cisco Unified Attendant Console with CUCM

Communications Manager	4.3	5.1	6.0	6.1	7.0
Cisco TAPI TSP	4.1(1.403)	5.1 (0.1801))	6.0.0.6	6.1 (0.10)	7.0 (1.6)
Cisco Unified Attendant Console	1.1.0	1.1.0	1.1.0	1.1.0	2.0.0

Music on Hold

Cisco Unified Attendant Console supports Music on Hold (MoH) from Cisco Unified Communications Manager in the following areas,

1. When on Operator holds a call
2. During a blind transfer
3. During a re-established transfer

A music source must be selected on the relevant Service Queue devices to enable this functionality. The use of music in both the transferring and hold scenarios is controlled via settings on Cisco Unified Attendant Admin.

TAPI Resilience

Cisco Unified Communications Manager allows a TSP client to communicate with a primary and backup CTI (Computer Telephone Integration) Manager to receive CTI information. This allows Cisco Unified Attendant Server and clients to carry on functioning if a CUCM failover occurs.

The backup CTI Manager should be the Cisco Unified Communications Manager to which the phones fail over.

Busy Lamp Field

The number of devices that are monitored by Cisco Unified Attendant Console's Busy Lamp Field may have an effect on the performance of the Attendant Console.

Call Park

The Attendant Console Call Park functionality is additional to the standard Cisco Unified Communications Manager call park and directed call park functions. Operators are able to see their available Park devices and choose whether to use a specific device or allow the system to select a device for them to park a call on.

Cisco Unified Presence Server

The Cisco Unified Attendant Console can display information extracted from Cisco Unified Presence Server (CUPs) from CUCM version 6.x onwards. The integration is managed via the Cisco Unified Business\Department Attendant CUPS Plug-in directly to the Cisco Unified Attendant Web Admin.

Changes to the CUPS Plug-in service will be managed in real-time. The CUPS Plug-in service will not be required to stop and restart for the changes to take affect.

The Attendant Console information is collected from the Cisco Unified Attendant Web Admin.

Do Not Disturb Support

The Cisco Unified Attendant Console supports the Do Not Disturb (DND) functionality available from CUCM version 6.x onwards. Do not disturb is a device feature that when enabled, will block access to the device when calls are made to it. The first release of this feature will support Cisco's *ringer off* implementation of the DND feature.

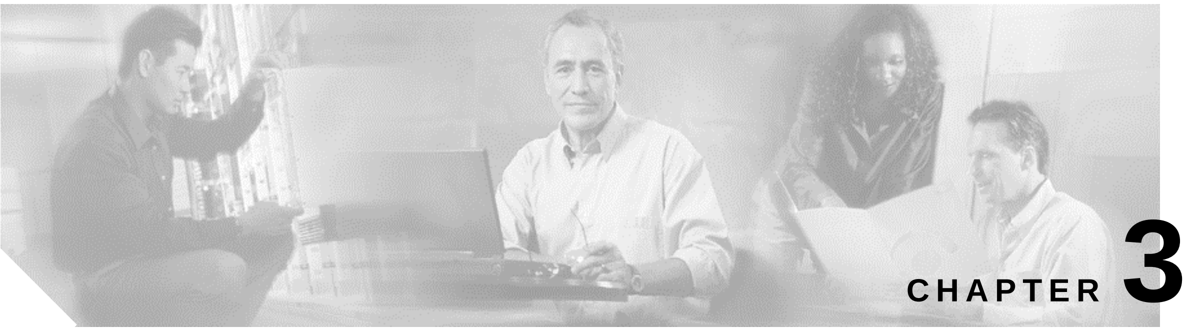
This provides the ability to display the DND status for a contact with an active BLF device, and allow the attendant operator to enable\disable the DND status for a contact with an active BLF device.

DTMF Digit Dialling

The Cisco Unified Attendant Console version 2.0 has been enhanced with the introduction of an improved method of DTMF digit dialling (Dual Tone Multi Frequency or Touchtone) so that an 'all in one' process has been adopted to increase the time of Operator dialling.

Other items to remember

1. Cisco Unified Attendant Server and Cisco Unified Attendant Console should not be installed on a machine that will act as Cisco Unified Communications Manager.
2. Headset operation is supported.



CHAPTER 3

Product Overview

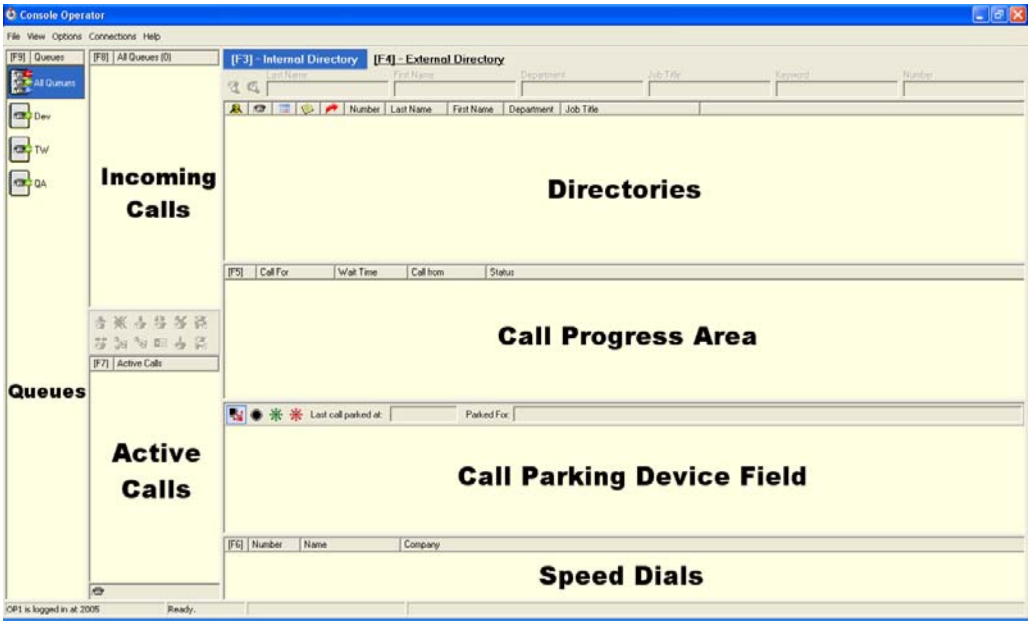
Cisco Unified Attendant Admin is the configuration tool for the Cisco Unified Attendant Console applications. It allows communication with the Cisco Unified Communications Manager to create the required system devices, and communicates with the Attendant Server to configure the system parameters. The Cisco Unified Communications Manager integration uses the AXL (Avvid XML Layer) protocol, and requires some initial configuration on Cisco Unified Communications Manager itself to create a User Profile that allows communication via AXL protocol.

The following application is configured through Cisco Unified Attendant Server,

Cisco Unified Attendant Console

This is a screen-based operator console that has been developed to work exclusively on Cisco Unified Communications Manager. The traditional functions of a telephone switchboard have been re-created as a Windows application. It is visually more appealing, easier to operate and more user friendly

.



The following devices are used to manage call routing and functionality,

Queue DDI

A Queue DDI (Direct Dial In) is the DN that is dialed to route calls into a call queue. Each configured DDI will be created on CCM as a CTI Route Point, and any call that is intended for this queue must be directed to this port, either directly or through translation.

CT Gateway Devices

The primary purpose of the CT gateway is to queue calls awaiting distribution to Cisco Unified Attendant Console. CT Gateway devices are CTI Ports that are created by the Admin application when synchronized with Cisco Unified Communications Manager.

Service Queues

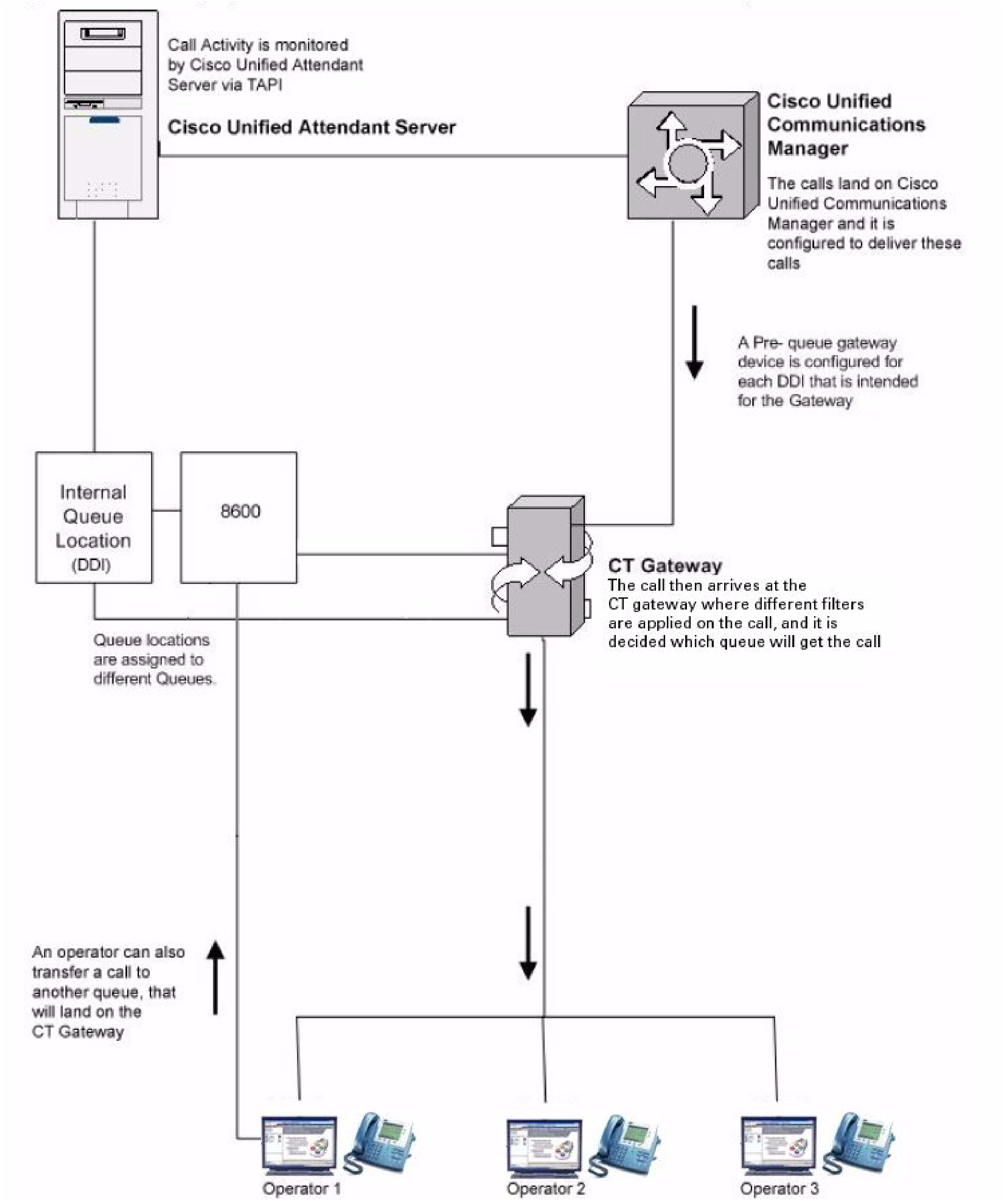
The Service Queue is a range of devices (CTI Ports) that are used manage calls after they leave the operator’s handset, for example when transferring or holding calls.

Park Devices

Another range of CTI Ports that are used exclusively for when the attendant’s wish to park a call. They can either select the preferred Park port of allow the system to select the port for them. A parked call can then be picked up by anyone on the system by dialling the Park port number. As these Park Devices are exclusive to the console attendants they are situated on the CUBAC/ CUDAC Server and will require an additional range of DN’s.

Call Flow

The following diagram shows how calls flow through Cisco Unified Attendant Console and how they are controlled by Cisco Unified Attendant Server and Cisco Unified Communications Manager.


Call Activity is monitored by Cisco Unified Attendant Server via TAPI
Cisco Unified Attendant Server
Cisco Unified Communications Manager
The calls land on Cisco Unified Communications Manager and it is configured to deliver these calls
A Pre- queue gateway device is configured for each DDI that is intended for the Gateway
Internal Queue Location (DDI)
8600
CT Gateway
The call then arrives at the CT gateway where different filters are applied on the call, and it is decided which queue will get the call
Queue locations are assigned to different Queues.
An operator can also transfer a call to another queue, that will land on the CT Gateway
Operator 1
Operator 2
Operator 3

Numbering Plan for Test Install

In order to use the system devices, that are, Service Queues, CT Gateway and Park Devices for call handling you can use the following numbering for a test install. Take a printout for the following table and fill in your own number plan in the *Directory Number* field.

Table 1: shows a numbering plan for a test installt

Device Type	**Directory Number (Example)**	**Directory Number**
Queue DDI	8100	
Queue DDI	8101	
CT Gateway	8000	
CT Gateway	8001	
CT Gateway	8002	
CT Gateway	8003	
CT Gateway	8004	
Service Queue	8400	
Service Queue	8401	
Service Queue	8402	
Service Queue	8403	
Service Queue	8404	
Park	8600	
Park	8601	
Park	8602	
Park	8603	
Park	8604	

Performance Information

Performance of Cisco Unified Attendant applications can be measured in several ways,

1. Number of Operators
2. Number of Contacts Supported
3. Number of Console Queues
4. BHCC - Busy Hours Call Completions

Table 2: shows the performance of CUBAC and CUDAC

Performance Item	Maximum (per Cisco Unified Attendant Server)	
	Department Attendant	Business Attendant
Number of Attendant Consoles	10	2
Number of Contacts Supported	750	500
Number of Console Queues	5	6
BHCC	1000	500

Hardware / Software Requirements

The information provided below gives details of the minimum hardware/software required to run Cisco Unified Attendant applications.

Applies To	PC Specification
Cisco Unified Attendant Server	**Pentium 4 2.2 GHz** 2 GB RAM 72 GB Hard Drive CD-ROM/DVD-Rom Network Card SVGA (1024x768) display card with correct drivers Windows 2003 Server SP2 running Windows English Regional Settings. .Net Framework 2.0 SP1* MS SQL Server 2005 (Express) * Internet Information Service (IIS) 6.0 (or later).* *** Note:** The Attendant Console Server installation will install these applications automatically. If MS SQL Express 2005 is installed manually, it must be installed as the **Default instance** for the Attendant Console to function. Cisco Unified Attendant applications will not work with a **Named instance** of SQLExpress. ** **Note**: IIS is installed seperately to the Attendant Console Server Installation the ASP.NET component must beenabled and installed. This is done via the ***Add/Remove Windows Component > Applications Server*** and ***Details***.

The Server should be connected to the network via the TCP/IP protocol.

You will require appropriate Operating System Licenses.

Note

Cisco Unified Attendant Server is not supported within a 64 bit Operating System.

Cisco Unified Enterprise Attendant Server is not supported on the Cisco MCS (Media Convergence Server) Operating System.

2. The minimum specification required by Cisco Unified Attendant Console is as follows,

Applies To	PC Specification
Cisco Unified Attendant Console	Pentium 4 Entry Level Specification 1 GB RAM 1GB available Hard Drive space CD-ROM/DVD-ROM Network Card Connected to Network via TCP/IP SVGA (1024x768) display card Windows Small Fonts *17 Monitor highly recommended* Windows 2000 Professional / XP Professional / Vista Professional (32 bit) SoundBlaster compatible sound card and speakers are recommended for the Console Operator.

3. Backups – As with all systems, we advise that backup facilities are provided to ensure application and data integrity, should an unforeseen circumstance arise.

Examples:

CD Writer

Tape streamer. DLT, DAT, Travan etc

Zip / Jaz drive or other type of Magneto Optical drive

If possible, choose a solution that gives a one step disaster recovery. This is a solution that has the ability to restore the complete contents of a hard drive from a bootable floppy disk and the restore media.

4. Server Redundancy – It is strongly recommended that the PC Server should be a redundant system with the following redundancy methods. This is at the discretion of the customer

Multiple hot-swap power supplies

Hot-swap Hard Drive arrays

UPS / power conditioners

RAID

5. Security Considerations

There are many different AntiVirus products that are supported on a CUxAC system server. Typically, the most commonly used products are McAfee VirusScan, Norton AntiVirus or Trend OfficeScan.
This is not a definitive list. Any AntiVirus program can be used on the CUxAC Server, as long as it is configured as below:-
Folder/File Exclusions
It is important that the AntiVirus product supports "Exclusions". This is the ability for the user to specify specific files and/or folders that will NOT be scanned by the AntiVirus program.
The following exclusions should be set when using AntiVirus on a CUxAC Server

File Location	Use
\\DBData	This folder is where the System Configuration Databases are located
\\Program Files\Cisco\Logging	This is where all the system log files are stored.
\\Temp\Cisco\Trace	This is where the Cisco TSP Trace files are located

Note - The "File Locations" and "File Names" may be changed by your System Administrator.

The files in the above table are constantly being written to and updated during standard operation of the CUxAC system.
Due to this, these files are permanently being accessed - an AntiVirus "Scan on access" policy for these files will mean that the files are constantly being scanned for Viruses. This will in turn slow down the operation of the Server. Therefore, excluding these files from being continuously scanned will allow the Server to function as expected.

6. The following table outlines the network requirements for running Cisco Unified Attendant applications.

Applies To	Network Specification
All Network Types	The network will need to support/run TCP/IP.
	Cisco Unified Attendant Admin application will need to run under an Administrator profile. (Local Administrator is acceptable)
Microsoft Windows Network	If the network uses DHCP then the PC Server will need a static IP address allocated to it.

Product Feature Table

The following table displays a break down by feature of the following products.

- Cisco Attendant Console (CAC). (EOL (End of Lifed) April 2009).
- Cisco Unified Deparment Attendant Console (CUDAC)
- Cisco Unified Business Attendant Console (CUBAC)
- Cisco Unified Enterprise Attendant Console (CUEAC)

The symbols denote the level of support within the product :-
● = Supported, ◗ = Partial Support, ○ = Unsupported

Feature	**Version**			
	CAC	**CUDAC**	**CUBAC**	**CUEAC**
Installation	Browser	Web & Wizard	Web & Wizard	Web & Wizard
Configuration	CUCM	Browser	Browser	Browser
Support	Cisco TAC	Cisco TAC 3rd tier - Arc	Cisco TAC 3rd tier - Arc	Cisco TAC 3rd tier - Arc
Queue Features				
Queues supported	Hunt Groups	● 1	● 3	● >50
Configurable queue names and priority	○	○	●	●
Show all calls in all queues option	○	○	●	●
Queue salutations	○	○	○	●
Show & pick calls from each Queue	●	●	●	●
Queue wait time overflow	●	○	○	●
Queue limit overflow (no of calls)	●	●	●	●
Operator overflow (no operators)	○	●	●	●
Queue overflow destinations supported	○	●	●	●
Overflow options	●	●	●	●
Service options				
Emergency mode switch	○	○	●	●
Emergency mode destination	○	○	●	●
Night service switch	●	○	●	●
Night service hours/timing	●	○	●	●

Feature	Version			
	CAC	CUDAC	CUBAC	CUEAC
Night service destination	●	○	●	●
Directory features				
Directory size supported	100k	750	500	100k
Search fields	2	3	4	6
Mobile number support	○	●	●	●
Internal directory support	●	●	●	●
External directory support	○	◗	◗	◗
Speed dials	●	●	●	●
Alternative number search (hotkey)	○	●	●	●
Alternate Contacts search	○	○	○	●
Directory to XML phones	○	○	○	○
Cross tab searching	○	○	○	●
Notes against person	○	●	●	●
Presence / Status features				
Busy Lamp Fields / Phone Status supported	Yes	750	500	7000
Presence integration with CUPS	○	◗	◗	●
Telephony features				
Transfer Reversion (Call Recall)	○	●	●	●
Hold Recall	○	●	●	●
Call toggle	●	●	●	●
Camp on	○	○	○	●

Feature	**Version**			
	CAC	**CUDAC**	**CUBAC**	**CUEAC**
Call hold with notes	○	○	○	●
Undirected Call park (finds first slot)	●	●	●	●
Directed Call Park (to specific Park location)	●	●	●	●
Call Hold	◗	●	●	●
Park recall	◗	●	●	●
Transfer	●	●	●	●
Conference	●	●	●	●
System features				
No of Clients	●	2	6	25
Keyboard driven	●	●	●	●
System logging	○	◗	◗	●
Cisco Unified CallManager Supported				
CallManager Supported	4.3, 5.1, 6.0, 6.1, 7.0	4.3, 5.1, 6.0, 6.1, 7.0	4.3, 5.1, 6.0, 6.1, 7.0	6.0, 6.1, 7.0
Localisation and accessibility				
Languages supported*	20	1* (15 in 2009)	1* (15 in 2009	1**
Accessibility support (with JAWS Script)	○	●	●	●

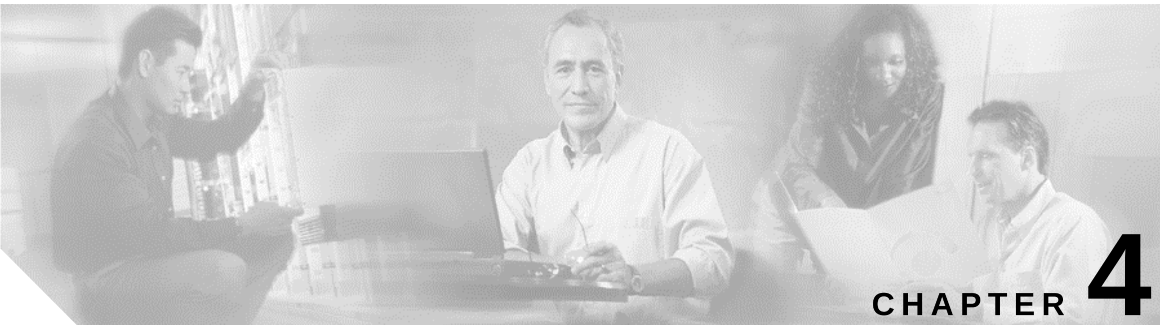
Legend: ● = Supported, ◗ = Partial Support, ○ = Unsupported

* The localisation languages supported are dependant on the software release version. In the case of CUDAC and CUBAC, thirteen languages are supported in software version 1.1.1.25, although the new version 2.0.0.11 which has only been available since October 2008 only supports English, with further languages to be supported in future releases. Please check with your reseller if localisation is required.

** The initial CUEAC (version 3.0.0.2) release supports English. This will be expanded to the 15 core languages within later versions scheduled for 2009 and 2010.

Core Languages

The 15 core languages that are supported are: English, French, Italian, German, Spanish, Portugese, Chinese (simpl), Chinese (trad.), Japanese, Korean, Arabic, Dutch, Swedish, Russian & Danish



CHAPTER 4

Installation of Cisco Unified Attendant Applications

This section describes in detail the installation procedures for the following applications,

1. Cisco Unified Attendant Server
2. Cisco Unified Attendant Console

In order to install Cisco Unified Attendant Applications, you must configure an End User profile on the Cisco Unified Communications Manager. All other configuration on the Cisco Unified Communications Manager will be handled by the Attendant Admin. Please refer to the following installation checklist for step-by-step installation sequence.

Please note that installation via Terminal Services/Remote Desktop is NOT supported. Only a local installation or VNC connection is supported.

Installation Overview

This overview is designed to guide you through the installation process for Cisco Unified Attendant Console in an easy to follow step-by-step sequence. A certain amount of preparation is required to ensure that a quick setup is achieved.

Installation and Configuration Overview

Step 1 Preparation

Formulate numbering plan for test install. Refer to *Table 1, page 24* for required Directory Numbers.

Prepare a Windows 2003 Service Pack 2 server with Internet Information Services (IIS) installed.

Step 2 Cisco Unified Communications Manager Configuration

Create partition and Calling Search Space or add to existing ones as required. (Note: All CTI devices created for the Attendant Console, as well as operators extensions need to be able to receive and make calls to a full range of destinations.)

For CUCM 4.3 see Appendix A *"Creating the Attendant Applications End User for CallManager 4.3" on page 97*.
For CUCM 5.x/6.x see Appendix B *"Creating the Attendant Application End User for CallManager 5.x/6.x/7.x" on page 101*

Create an End User

Create a User Group

Assign roles to User Group

Assign End User to User Group

Assign End User to CCM Super User Group

Step 3 Install and Configure Cisco Unified Attendant Admin

Install Cisco Unified Attendant Admin.
See *"Installing Cisco Unified Attendant Server" on page 37*.

Check Cisco Unified Communications Manager connectivity.
See *"CUCM Connectivity" on page 58.*

Configure CT Gateway, Service and Park devices.
See *"System Configuration" on page 68.*

Synchronize with CCM. Adds all required CTI devices to CCM, and adds them to the End User profile for CTI control.
See "Synchronizing with CUCM" on page 71.

Configure Directory Synchronization if required.
See *"LDAP Directory Connectivity (for CUCM 4.3 only)" on page 62* and *"Directory Synchronization" on page 77.*

Configure Cisco Unified Attendant Console User Settings.
See *"User Configuration" on page 79.*

General Settings,
Access Numbers

FAC and CMC Settings

Recall Timers
Working Days

Queue Management
General (Name, DDI, Priority)
Emergency destination
Overflow destinations
Night Service destination

Operator management

Operator login names and passwords

Step 4 Install Cisco TSP on Cisco Unified Attendant Server

Browse to Communications Manager configuration and select *Application > Plugins.* See *"Installing the TAPI TSP" on page 109*

Select Cisco Telephony Service Provider and run the install following the onscreen instructions.

After rebooting the Server configure the TSP.

Install Cisco TAPI Wave Driver (instructions are in the TSP readme file). See *"Installing the TAPI TSP" on page 109*

Reboot the server.

Step 5 Test TAPI

Use Phone1.exe from Julmar.com to test that,
a) all Associated devices appear in the line list, and b) that a CTI Ports can be monitored and a call made to a nearby handset.

Step 6 Install Cisco Unified Attendant Console.

See *"Installing Cisco Unified Attendant Console Client" on page 44*

Installing Cisco Unified Attendant Server

Note When installing the software you will need to have administration rights

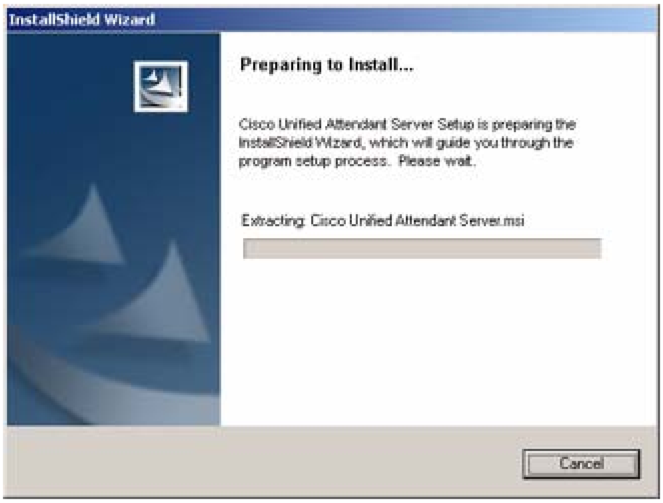
Prior to installing the Cisco Unified Enterprise Attendant Console software, it has to be downloaded. For information related to the download and registration of the software, refer to *Appendix D - Downloading, Updating and Registering Software* on page 105 of this manual.

1. Browse to the directory where the downloaded installation files are saved.

The following steps are followed in order to install the application, The following steps are followed in order to install the application,

1. The first stage of installation will be to install any required 3rd party applications, including MS SQL Server 2005 Express IE 6.0 and MS Dotnet if they are not already installed. The default user name for the SQL connection will be **sa** and the default password will be **Z1ppyf0rever**. The first window appears displaying a progress bar while the setup prepares the system for installation.

Figure 1: displays the screen that is shown while the setup prepares for installation



InstallShield Wizard

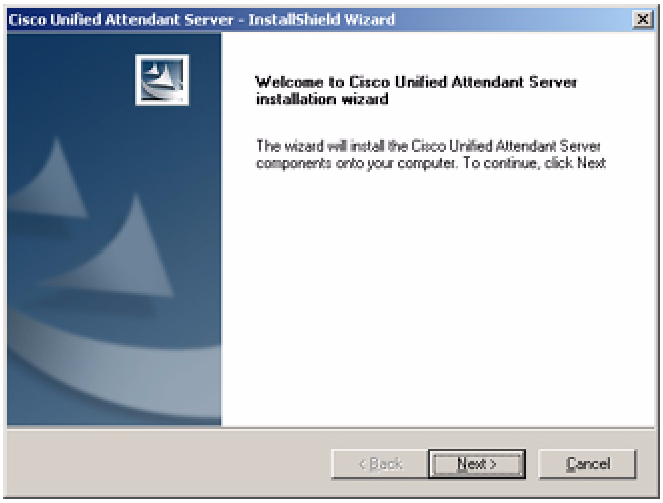
Preparing to Install...

Cisco Unified Attendant Server Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.

Extracting: Cisco Unified Attendant Server.msi

2. The next screen displays a welcome note and instructions on installing. Click **Next**.

Figure 2: displays the welcome screen for the



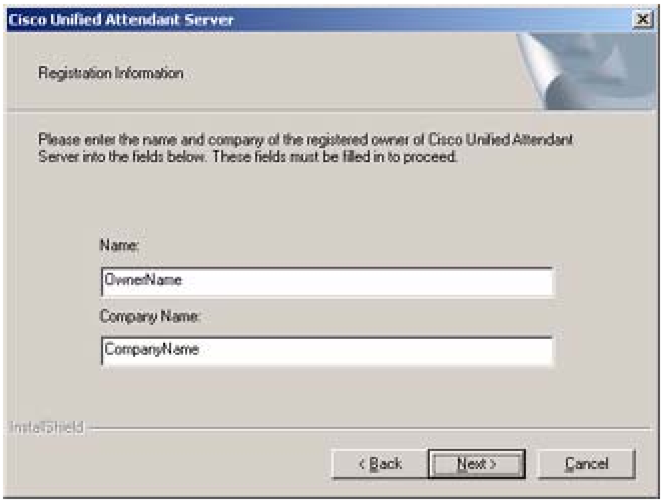
Cisco Unified Attendant Server - InstallShield Wizard

Welcome to Cisco Unified Attendant Server installation wizard

The wizard will install the Cisco Unified Attendant Server components onto your computer. To continue, click Next

3. The next window contains registration information. In the *Name* text box, type the name of the license holder, and type the company name into the *Company* text box. Click the **Next** button to proceed.

Figure 3: displays the Registration Information screen of the install



Cisco Unified Attendant Server

Registration Information

Please enter the name and company of the registered owner of Cisco Unified Attendant Server into the fields below. These fields must be filled in to proceed.

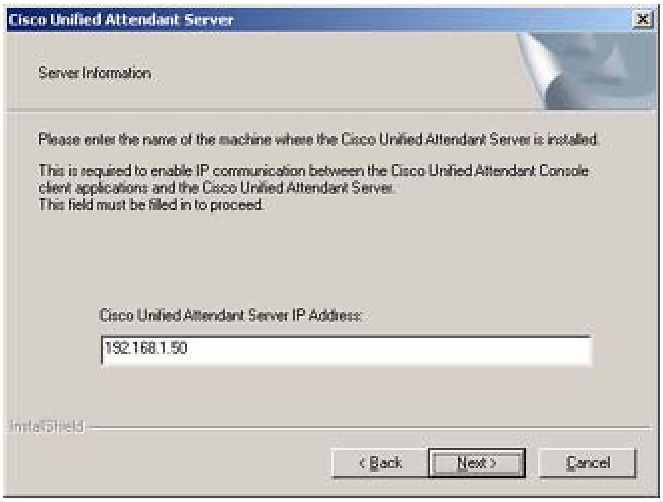
Name: OwnerName

Company Name: CompanyName

4. In this window, it is necessary to type the Machine Name or IP Address of the machine onto which the Server application is being installed. Click **Next**.

Note If you are unsure of the machine name, it is possible to find out through *Control Panel >Network*. This must be done on the machine that runs Cisco Unified Attendant Server.

Figure 4: displays the Server Information screen for the installation



Cisco Unified Attendant Server

Server Information

Please enter the name of the machine where the Cisco Unified Attendant Server is installed.

This is required to enable IP communication between the Cisco Unified Attendant Console client applications and the Cisco Unified Attendant Server.
This field must be filled in to proceed.

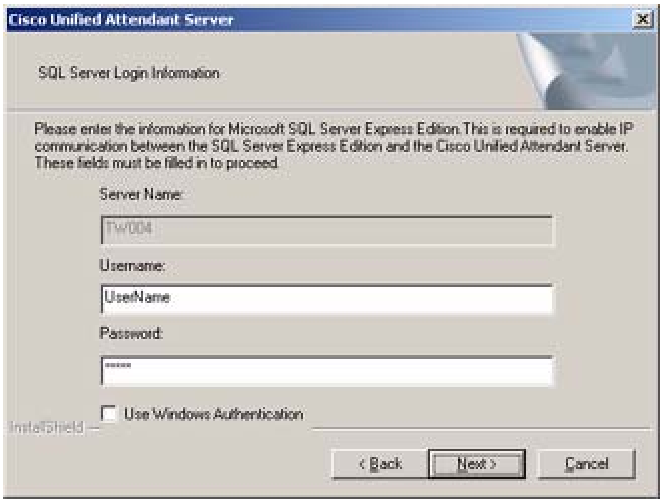
Cisco Unified Attendant Server IP Address: 192.168.1.50

5. If you already have MS SQL Server 2005 Express Edition, the screen below will be displayed. Enter the *Server Name*, *Username* and *Password* to connect to MS SQL Server Express 2005 Edition. Click **Next**.

Note If MS SQL Server is not installed on your machine, it will be installed automatically by Cisco Unified Attendant Server Installation. Please refer to Step 1.

Note Previous versions of CUBAC/CUDAC installed MS SQL Server with a default *Username* and *Password* of **sa** and **cisco**. With the release of version 2.0 the password was changed to impliment a more secure password structure.

Figure 5: displays the Server Login Information screen for installation



Cisco Unified Attendant Server

SQL Server Login Information

Please enter the information for Microsoft SQL Server Express Edition. This is required to enable IP communication between the SQL Server Express Edition and the Cisco Unified Attendant Server. These fields must be filled in to proceed.

Server Name: TW004

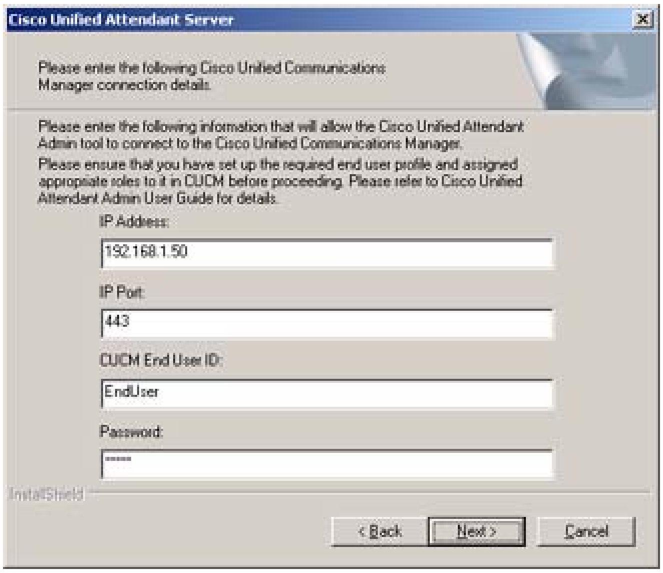
Username: UserName

Password: *****

□ Use Windows Authentication

6. In order to connect to Cisco Unified Communications Manager, you must enter the IP address and port. You must also specify the *Cisco Unified Communications Manager End User ID* and its password. Make sure the end user that you specify in this screen exists in the system. This can be done through Cisco Unified Communications Manager administration. The creation of an end user has been explained in the appendices at the end of the document. Click **Next**.

Figure 6: displays the CUCM information screen



Cisco Unified Attendant Server

Please enter the following Cisco Unified Communications Manager connection details.

Please enter the following information that will allow the Cisco Unified Attendant Admin tool to connect to the Cisco Unified Communications Manager.

Please ensure that you have set up the required end user profile and assigned appropriate roles to it in CUCM before proceeding. Please refer to Cisco Unified Attendant Admin User Guide for details.

IP Address: 192.168.1.50

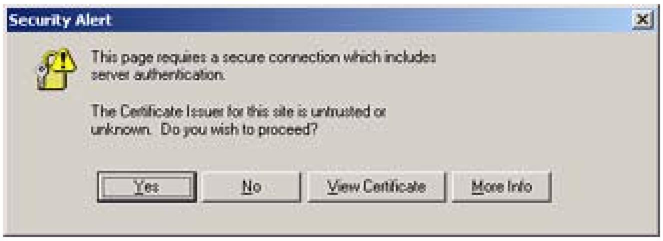
IP Port: 443

CUCM End User ID: EndUser

Password: *****

7. When you enter the username and password to connect to Cisco Unified Communications Manager in the previous window, two security alerts will be displayed. Click **Yes** on both the alerts to proceed.

Figure 7: displays the confirmation to access CUCM



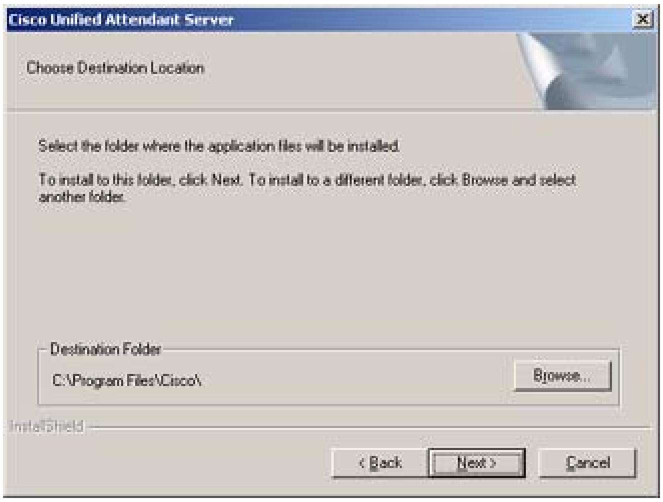
Security Alert

This page requires a secure connection which includes server authentication.

The Certificate Issuer for this site is untrusted or unknown. Do you wish to proceed?

8. The next window is for selecting the directory into which you wish to install the application. The default location is C:\Program Files\Cisco. By using the Browse button, you can select a different path and directory. Click the **Next** button.

Figure 8: displays the screen to specify location for the files to be installed to



Cisco Unified Attendant Server

Choose Destination Location

Select the folder where the application files will be installed.

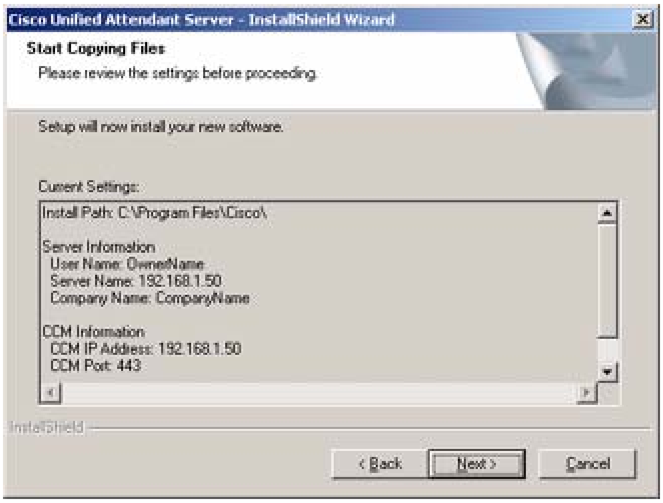
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files\Cisco\

9. In the next window, the summary for the current settings specified will be displayed. Click **Next** to proceed with installation or click Back to edit the settings made on the previous screens.

Figure 9: displays the summary for the configuration made



Cisco Unified Attendant Server - InstallShield Wizard

Start Copying Files

Please review the settings before proceeding.

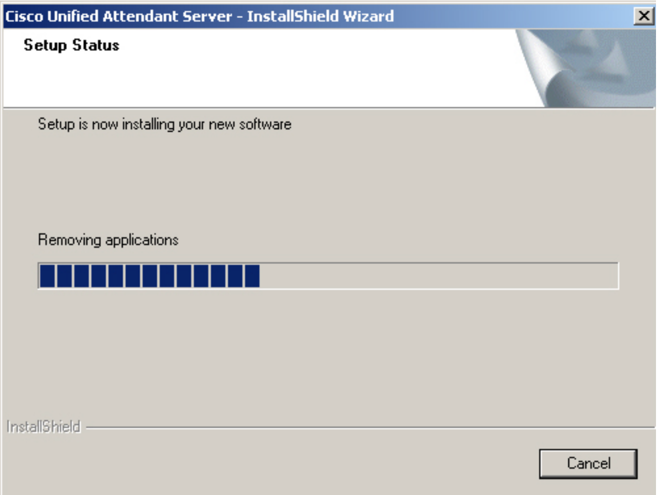
Setup will now install your new software.

Current Settings:

```
Install Path: C:\Program Files\Cisco\

Server Information
  User Name: OwnerName
  Server Name: 192.168.1.50
  Company Name: CompanyName

CCM Information
  CCM IP Address: 192.168.1.50
  CCM Port: 443
```

10. The next screen will display the progress bar for the installation.

Figure 10: displays the progress foe i



Cisco Unified Attendant Server - InstallShield Wizard

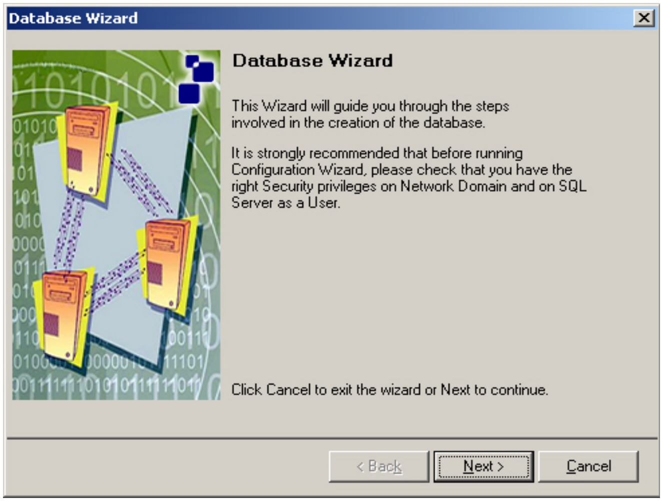
Setup Status

Setup is now installing your new software

Removing applications

11. Once the application has been installed, the *Database Wizard* will create and configure the databases for the application. Click **Next**.

Figure 11: displays the Database Wizard welcome screen



Database Wizard

Database Wizard

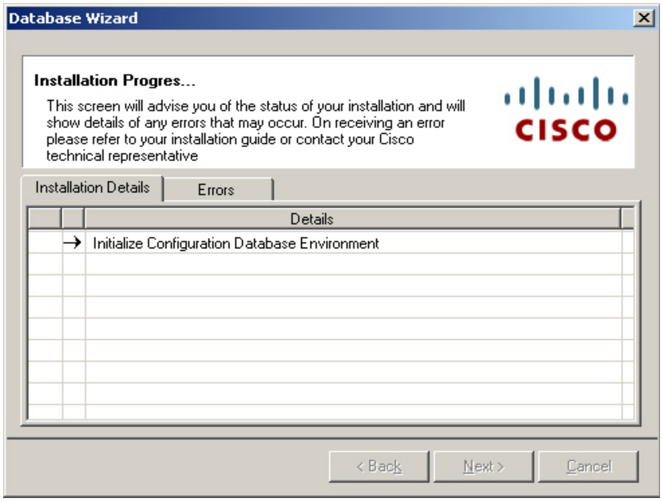
This Wizard will guide you through the steps involved in the creation of the database.

It is strongly recommended that before running Configuration Wizard, please check that you have the right Security privileges on Network Domain and on SQL Server as a User.

Click Cancel to exit the wizard or Next to continue.

12. In the next window, the status of database installation will be displayed. Once the installation is complete, click **Finish**.

Figure 12: displays the installation progress of the databases



Database Wizard

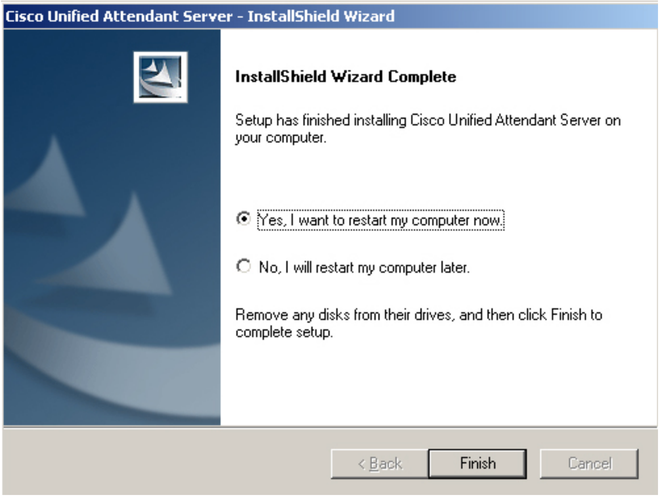
Installation Progres...

This screen will advise you of the status of your installation and will show details of any errors that may occur. On receiving an error please refer to your installation guide or contact your Cisco technical representative

→ Initialize Configuration Database Environment

13. The application has now been installed successfully. It is recommended that you restart your computer.

Figure 13: displays the screen once the installation is complete



Cisco Unified Attendant Server - InstallShield Wizard

InstallShield Wizard Complete

Setup has finished installing Cisco Unified Attendant Server on your computer.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

Note After the restart and before using the software, the Cisco TSP and Cisco TAPI Wave driver have to be installed and configured. This is covered in Appendix C “TAPI Configuration” on page 101

Installing Cisco Unified Attendant Console Client

Note When installing the software you will need to have administration rights.

Prior to installing the Cisco Unified Enterprise Attendant Console Client software, it has to be downloaded. For information related to the download and registration of the software, refer to *Appendix D - Downloading, Updating and Registering Software* on page 105 of this manual.

1. Browse to the directory where the downloaded installation files are saved.

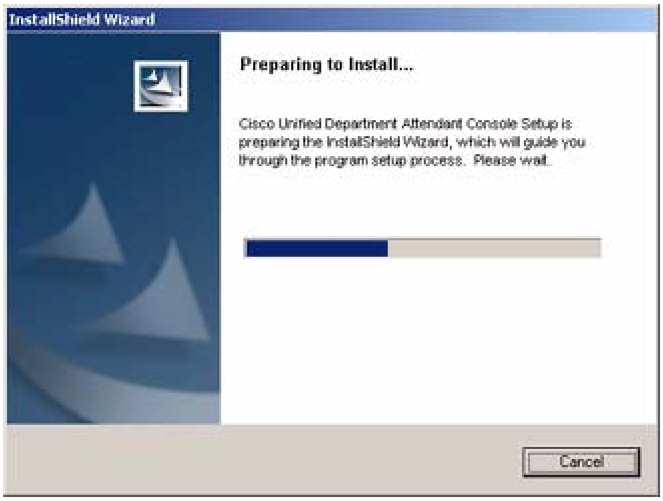
The following steps are followed in order to install the application.

The installation instructions provided below describe the procedure to install Cisco Unified Department Attendant Console. Please note that installation for Cisco Unified Business Attendant Console follows the same procedure.

1. The first window appears displaying a message that Cisco Unified Attendant Console Installation Wizard is preparing to install. The progress bar on the screen shows the status of the setup and also shows the names of the files being extracted. Once the installation

wizard is ready to install the application, a new screen will be displayed that will guide you through the setup process for Cisco Unified Attendant Console.

Figure 14: displays the first install screen



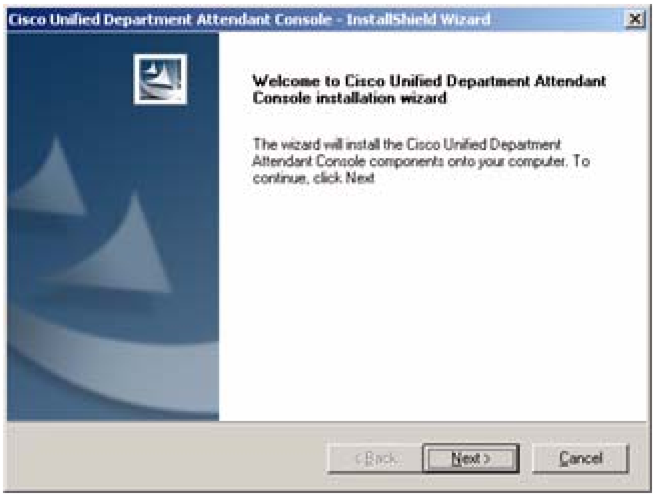
InstallShield Wizard

Preparing to Install...

Cisco Unified Department Attendant Console Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.

2. The new window that is displayed after the *Preparing to Install* window, shows a welcome note. This screen specifies that Cisco Unified Attendant Console and its components will be installed on your computer. To continue, click **Next**. If you wish to exit from the setup at this point, click **Cancel**.

Figure 15: displays the welcome screen to installation



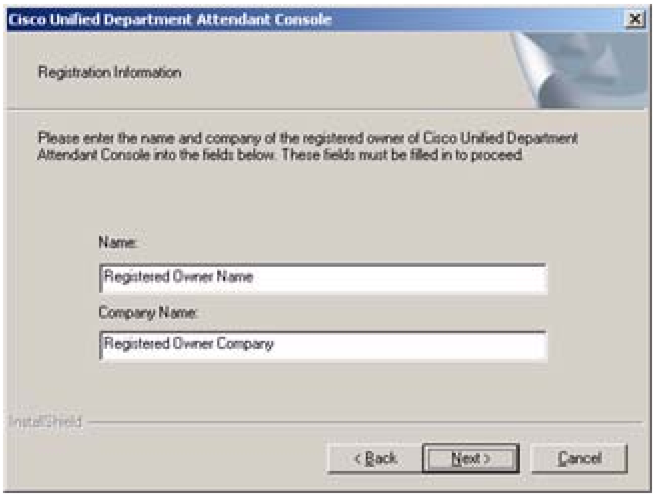
Cisco Unified Department Attendant Console - InstallShield Wizard

Welcome to Cisco Unified Department Attendant Console installation wizard

The wizard will install the Cisco Unified Department Attendant Console components onto your computer. To continue, click Next

3. The next window contains the registration information. In the *Name* text box, type the name of the registered owner of Cisco Unified Attendant Console, and type the owner's company name into the *Company* text box. Click the **Next** button to proceed.

Figure 16: displays the screen for Registration Information



Cisco Unified Department Attendant Console

Registration Information

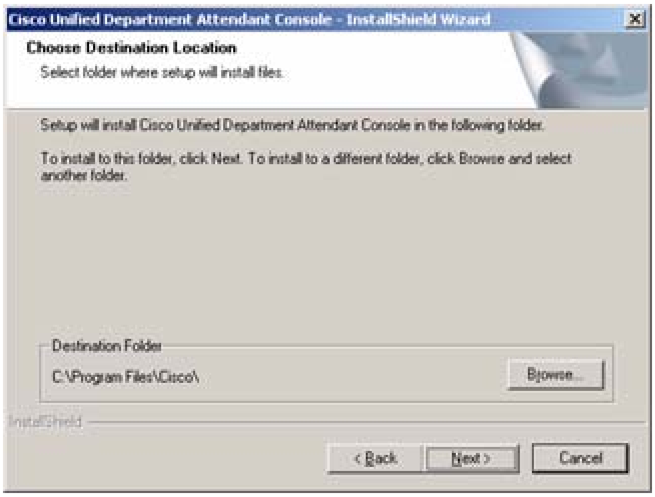
Please enter the name and company of the registered owner of Cisco Unified Department Attendant Console into the fields below. These fields must be filled in to proceed.

Name:
Registered Owner Name

Company Name:
Registered Owner Company

4. In the next window, select the folder where you wish to install the application. It is recommended to use the default destination folder specified on the screen. The default destination folder is created on the following path:
   C:\Program Files\Cisco\
   If you wish to install the application to a different location, use the Browse button to select a different location. Click **Next** to proceed.

Figure 17: displays the screen used to select a location where the application must be installed



Cisco Unified Department Attendant Console - InstallShield Wizard

Choose Destination Location
Select folder where setup will install files.

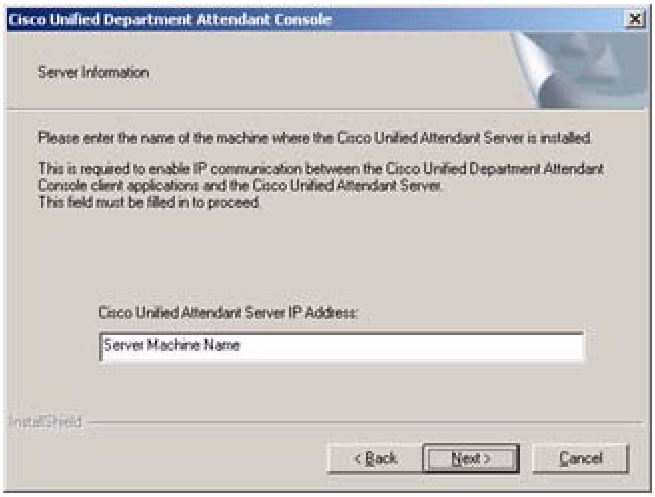
Setup will install Cisco Unified Department Attendant Console in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder
C:\Program Files\Cisco\

5. In the next window, enter the *IP Address* of the machine running Cisco Unified Attendant Server. This is required in order to enable communication between Cisco Unified Attendant Console and Cisco Unified Attendant Server.
   Note: If the IP address for Cisco Unified Attendant Server is entered incorrectly, Attendant Console will not be able to connect to the server and will therefore not function.

Figure 18: displays the screen for Server Information



Cisco Unified Department Attendant Console

Server Information

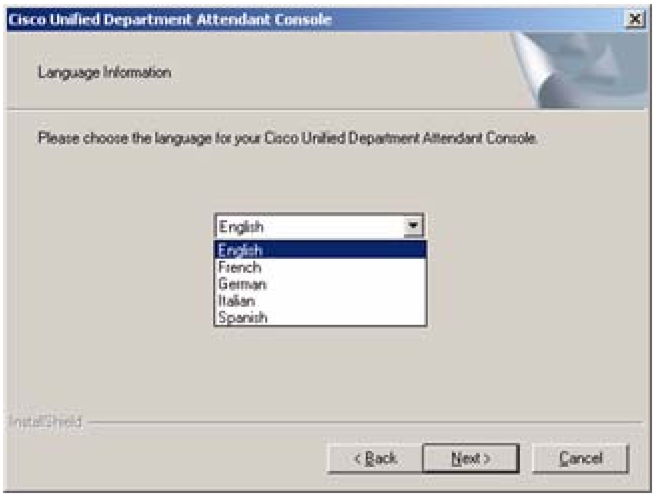
Please enter the name of the machine where the Cisco Unified Attendant Server is installed.

This is required to enable IP communication between the Cisco Unified Department Attendant Console client applications and the Cisco Unified Attendant Server.
This field must be filled in to proceed.

Cisco Unified Attendant Server IP Address: Server Machine Name

6. In the next window, you must select the language in which you want to install the application. Click **Next** to continue.

Figure 19: displays the screen used to select the language for the application



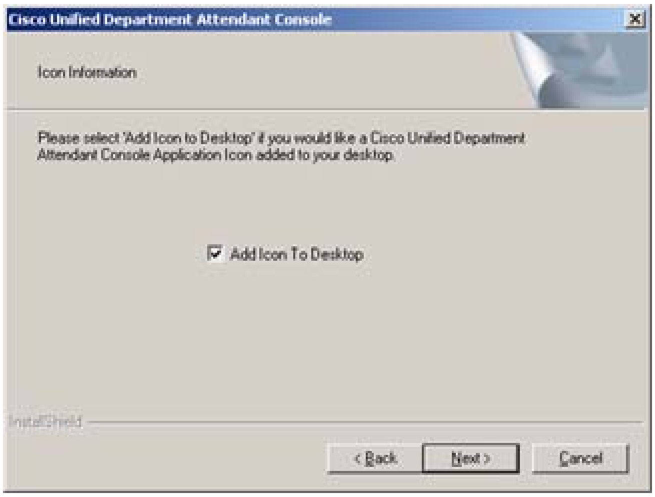
Cisco Unified Department Attendant Console

Language Information

Please choose the language for your Cisco Unified Department Attendant Console.

7. In the next window, select the check box to add an icon for Cisco Unified Attendant Console on the desktop. Click **Next** to proceed.

Figure 20: displays the screen that asks to add an icon to desktop



Cisco Unified Department Attendant Console

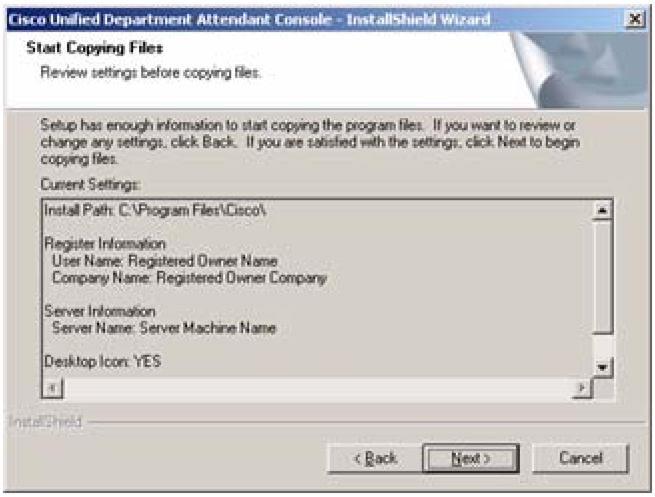
Icon Information

Please select 'Add Icon to Desktop' if you would like a Cisco Unified Department Attendant Console Application Icon added to your desktop.

☑ Add Icon To Desktop

8. In the next window, the installation wizard displays the summary of the information you have entered so far. You can review these settings on this screen and click **Back** if you wish to edit some information. If you are satisfied with the settings, click **Next** to allow the setup to start copying the files.

Figure 21: displays the screen that shows the summary for the setup



Cisco Unified Department Attendant Console - InstallShield Wizard

Start Copying Files

Review settings before copying files.

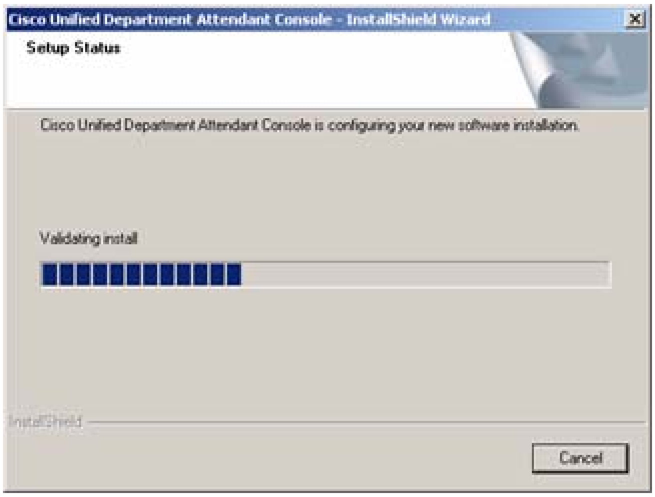
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
Install Path: C:\Program Files\Cisco\

Register Information
  User Name: Registered Owner Name
  Company Name: Registered Owner Company

Server Information
  Server Name: Server Machine Name

Desktop Icon: YES
```

9. In the next window, a progress bar is displayed that shows the status of the installation configurations and the files being copied. If you wish to exit the setup at this point, click **Cancel**.

Figure 22: displays the progress bar for the software configuration



Cisco Unified Department Attendant Console - InstallShield Wizard

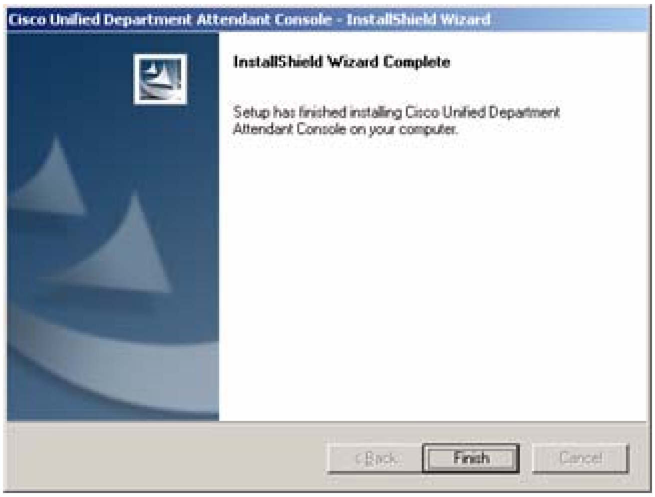
Setup Status

Cisco Unified Department Attendant Console is configuring your new software installation.

Validating install

10. The final window displays the confirmation that Cisco Unified Attendant Console has been installed successfully. Click the **Finish** button.

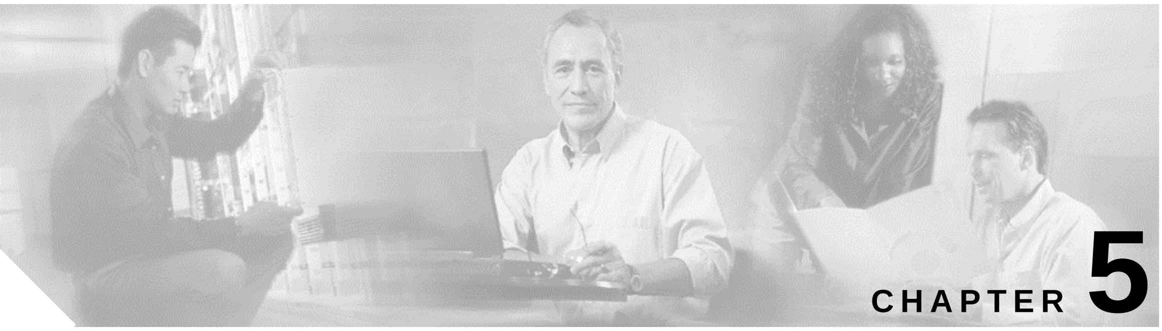
Figure 23: displays the screen notifying that the installation is complete



Cisco Unified Department Attendant Console - InstallShield Wizard

InstallShield Wizard Complete

Setup has finished installing Cisco Unified Department Attendant Console on your computer.



Cisco Unified Attendant Admin

This section will guide you through configuration for Cisco Unified Attendant Console. Cisco Unified Attendant Admin allows you to create and manage the Attendant Console system.

System configuration provides the facility to manage synchronization of devices and queues with Cisco Unified Communications Manager. Cisco Unified Attendant Console and Cisco Unified Communications Manager communicate via AXL API, using SSL, to synchronize the system devices used for queuing, servicing and parking calls. These devices are created as CTI Port and CTI Route Point devices within the Cisco Unified Communications Manager database.

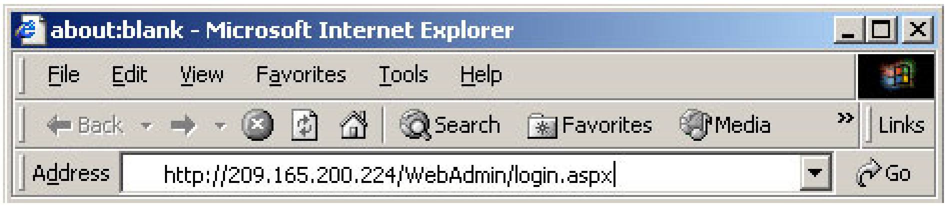
User configuration allows you to make configurations for the Cisco Unified Attendant Console. These settings are configured in order to make global configurations for internal/external calls access, Force Authorization and Client Matter Codes and Recall timers. These settings are made in order to manage the call flow.

In order to get started, an initial URL will be used to access Cisco Unified Attendant Admin web session. This URL will be in the following format:

http://<<*ip address of Unified Attendant Server*>>/webadmin/login.aspx

The URL, as provided by the network administrator will be entered in the address bar of the web browser, as shown in the following image:

Figure 1: displays URL entered in the Internet Explorer address bar



http://209.165.200.224/WebAdmin/login.aspx

You must login to Cisco Unified Attendant Admin in order to configure settings for Cisco Unified Attendant Console.

The following icons may be used while configuring the Cisco Unified Attendant Console,

Table 1: provides the description for the icons used in the user guide

Icon	Description
💾	Submit
🔐	Reset Password
☑	Test Connection
🔧	Repair Database
▶	Start Server
⏹	Stop Server
ℹ	Information Icon: Used to view runtime information for a service.
🔄	Refresh
⇄	Synchronize with CUCM

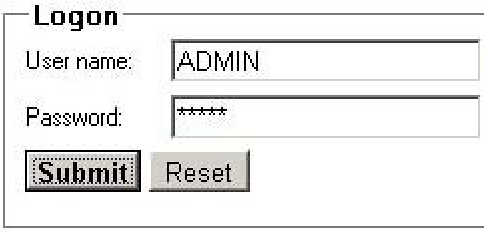
Administrator Login

Cisco Unified Attendant Admin has an authentication mode for users. It is accessible only to the Administrator for making new configurations for Cisco Unified Attendant Console or updating them. Most of the settings configured using Cisco Unified Attendant Admin will be made in real-time, however, some changes may require Cisco Unified Attendant Server to be restarted. The default user name is **ADMIN** and the default password is **CISCO**.

To log on to Cisco Unified Attendant Admin,

1. Enter the URL specified by your network administrator to access Cisco Unified Attendant Admin.
2. The **Logon** page will open.
3. Enter *User name*.
4. Enter *Password*.
5. Click **Submit**.

Figure 2: displays the login page for the application



User name: ADMIN

Password: *****

The following table gives a brief description for the fields mentioned in the form displayed above,

Table 2: provides the description for the fields of the login page

Field	Example	Description
User name	ADMIN	This field specifies the user name to log in with. The user name is ADMIN by default.
Password	*****	The number used by the operator to log in.

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

Home Page

Following a successful log in, you will be shown the home page that displays the main menus for configuring the application. The following areas can be accessed and configured,

Table 3: provides the details for different types of configurations available

Configuration Menu	Description
Engineering	This section provides connectivity and support management facilities.
System Configuration	This section provides the administrator with facilities to manage synchronization of devices and queues with Cisco Unified Communications Manager.
User Configuration	This section provides the administrator with facilities to manage Cisco Unified Attendant Console configuration.
Help	Provides help information and also includes a section for licensing the applications.

These configurations are explained in detail in the following sections.

Engineering

The Engineering section provides connectivity and support management facilities. It allows administrators to:

- Manage administrator access
- Manage the database environment
- Manage connections to the Cisco Unified Communications Manager
- Manage CUPS Connectivity (for CUCM 6.0 onwards)
- Manage Cisco Unified Attendant services
- Manage LDAP Directory Connectivity (for CUCM 4.3 only)
- Enable\disable logging

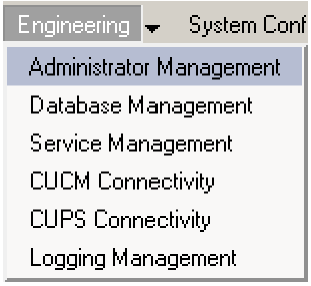
Administrator Management

This section allows you to change or reset the password used for logging into the Web Admin application.

To change password,

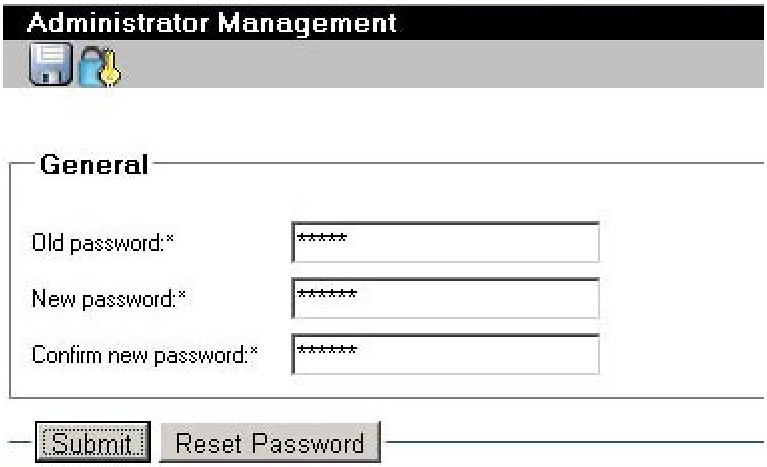
1. Go to *Engineering > Administrator Management*.

Figure 3: displays the menu option for Administrator Management



2. Enter *Old Password*.
3. Enter *New Password*.
4. Re-enter new password in the *Confirm New Password* field.
5. Click **Submit** to save changes.

Figure 4: displays the Administrator Management page



Administrator Management

General

Old password:* *****

New password:* ******

Confirm new password:* ******

The following table gives a brief description for the fields mentioned in the form displayed,

Table 4: provides the description for the fields mentioned on the Administrator Management page

Field	Example	Description
Old password	*****	The existing password for the ADMIN user name.
New Password	*****	The new password you wish to switch to.
Confirm new password	*****	The new password has to be re-entered in this field in order to confirm you did not mistype in the *New Password* field.

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

Database Management

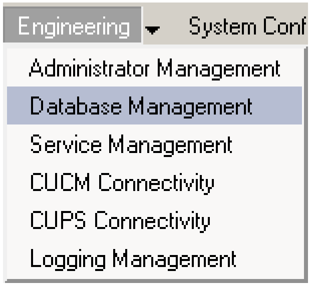
This web page allows configuration for database connectivity details. You can test and repair the databases as well.

Configuration and logging databases will be created at the time of installation. Only the connectivity details can be modified through this page.

To manage database,

1. Go to *Engineering* > *Database Management*.

Figure 5: displays the Database Management menu option



2. In the Server field, specify the name of the machine where the SQL Server is installed.
3. Check the *SQL authentication* checkbox in case *User name* and *Password* are required to access the database.
4. Enter *User Name*.
5. Enter *Password*.

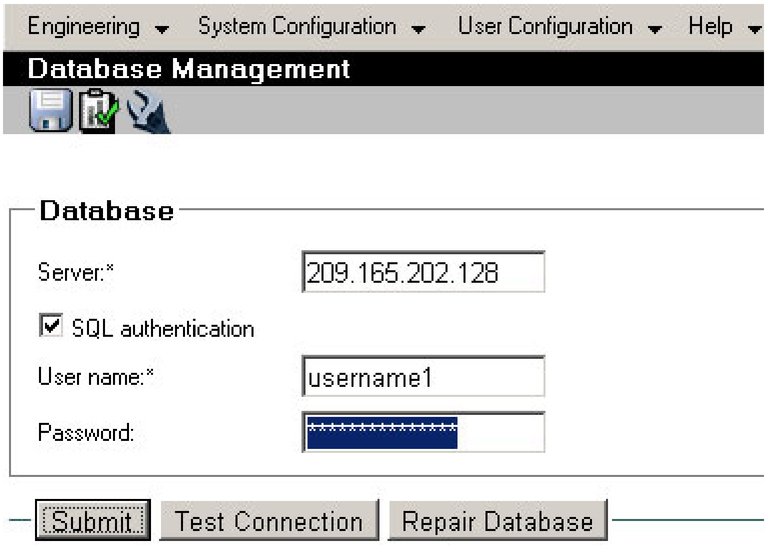
6. To save changes, click **Submit**. You will be prompted that Cisco Unified Attendant Server must be restarted for the changes to take affect. If you select the option, Cisco Unified Attendant Admin can restart server automatically.

7. To test the database, click **Test Connection**.

8. To repair database, click **Repair Database**. You will be prompted that Cisco Unified Attendant Server must be stopped before repairing the database. If you select the option, Cisco Unified Attendant Admin can stop the server and repair the database. The server service will need to be manually restarted.

The following image shows the configurations you can set using the above-mentioned procedure.

Figure 6: displays the Database Management page



Server:* 209.165.202.128

☑ SQL authentication

User name:* username1

Password: ***************

The following table gives a brief description for the fields mentioned in the form displayed above,

Table 5: provides description for the fields mentioned in the Database Management page

Field	Example	Description

Table 5: provides description for the fields mentioned in the Database Management page

Server	209.165.202.128	In this field you specify the IP Address of the machine where MS SQL Server 2005 is installed.
SQL Authentication		This checkbox must be selected if you require SQL Authentication to connect to the SQL Server.
User name	username1	You must enter the user name used to connect to SQL Server. If MS SQL Server was installed through *Cisco Unified Attendant Server Installation Wizard*, the user name would be **sa**.
Password	*****	You must enter the password used to connect to SQL Server. If MS SQL Server was installed through *Cisco Unified Attendant Server Installation Wizard*, the user name would be **sa**.

Note

Changes to the database configuration will require a stop and restart of Cisco Unified Attendant Server.

Service Management

The *Service Management* web page allows you to start or stop the following servers,

1. Cisco Unified Attendant Server
2. Cisco Unified Attendant LDAP Plug-in

The following controls are available,

Table 6: provides the description for server controls

Control	Icon	Description
Start Server	▶	This button allows you to start the server.
Stop Server	■	This button allows you to stop the server.
Information	ⓘ	This button allows you to view runtime information for the service. The information is displayed in a separate pop-up window.

Table 6: provides the description for server controls

Refresh	↻	The **Refresh** button and the icon shown on the left allow you to see the current status of the server.

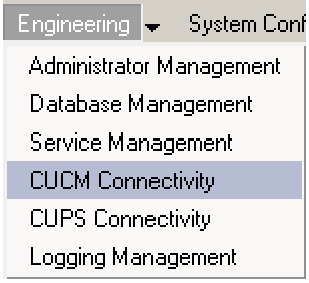
CUCM Connectivity

CUCM Connectivity is essential to allow system devices to be configured automatically on the Cisco Unified Communications Manager. This section allows the connection details to be managed and tested, initially using the details entered during the installation process.

To manage connectivity details,

1. Go to *Engineering* > *CUCM Connectivity.*

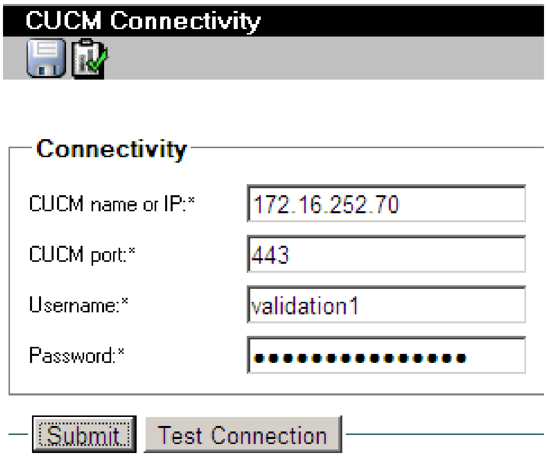
Figure 7: displays the menu option for CUCM Connectivity



2. Enter *CUCM name*. This is the IP Address of the Cisco Unified Communications Manager Publisher.
3. Enter *CUCM Port* number. This should be left as 443 by default.
4. Enter *User name* and *Password* of the End User profile that is used to connect to Cisco Unified Communications Manager.
5. To save, click **Submit**.
6. To test, click Test Connection.

The following image shows the configurations you can set using the above-mentioned procedure.

Figure 8: displays the CUCM Connectivity page



CUCM Connectivity

Connectivity

CUCM name or IP:* 172.16.252.70

CUCM port:* 443

Username:* validation1

Password:* ●●●●●●●●●●●●●●●

Table 7: provides description for the fields on the CUCM Connectivity page

Field	Example	Description
CUCM name or IP	209.165.201.0	In this field you specify the IP Address of the machine where CUCM is installed.
CUCM port	443	In this field you specify the CUCM port you wish to connect to. This is set to **443** by default.
Username	username1	You must enter the end user id used to connect to CUCM. The end user is created through CUCM administration. This is has been explained in the appendices at the end of the guide.
Password	*****	You must enter the password used to connect to CUCM.

Warning

1. **The Username and Password provided here are case-sensitive. Please make sure you enter the information in these fields in proper case.**
2. **The information provided in the Username and Password fields must not belong to an application user, for example CCMAdministrator.**

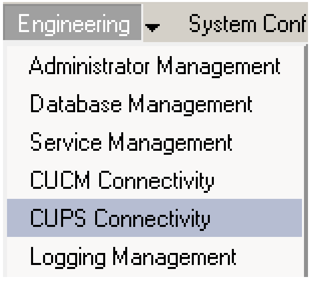
CUPS Connectivity

CUPS Connectivity details are used to configure the Cisco Unified Business/Department Attendant CUPs Plug-in with the Cisco Unified Presence Server, which is available with CUCM 6.0 upwards.

To manage connectivity details,

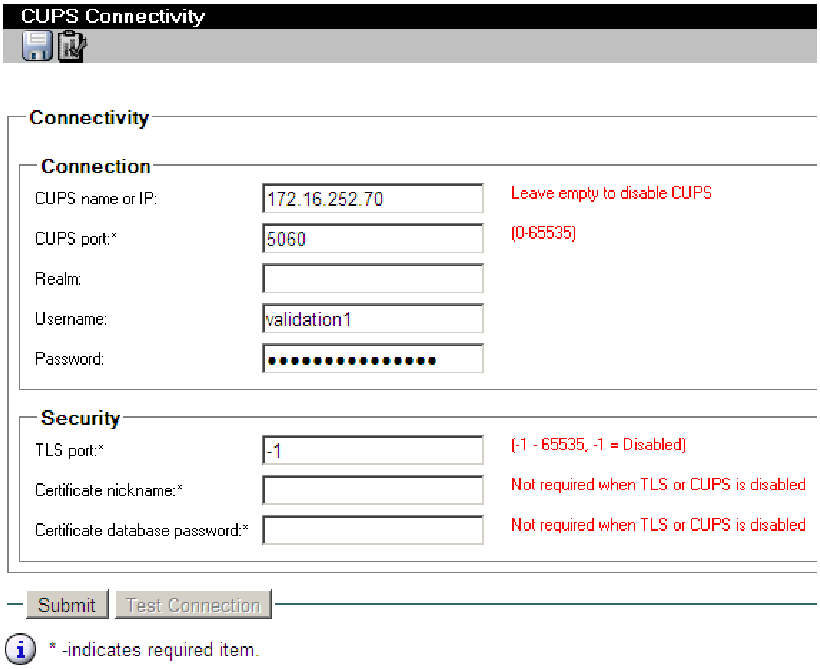
1. Go to *Engineering > CUPS Connectivity.*

Figure 7: displays the menu option for CUPS Connectivity



2. Enter *CUPS name or IP.* This is the IP Address of the Cisco Unified Presence server.
3. Enter *CUPS Port* number.
4. Enter *Realm*. The realm is used to authenicate the SIP communication. If this is left blank then the IP address of the Cisco Unified Presence Server will be used.
5. Enter *User name* and *Password* of the End User profile that is used to connect to Cisco Unified Presence Server.
6. Enter the *CUPs TLS* (Transport Layer Security) Port. By default this is set to -1 indicating that TLS is switched off. To enable TLS, specify the correct Port number (Normally either 5061 or 5062).
7. Enter *Certificate nickname* and the *Certificate Database password* if TLS has been enabled.

Figure 8: displays the CUPs Connectivity page



CUPS Connectivity

Connectivity

Connection

CUPS name or IP: 172.16.252.70 Leave empty to disable CUPS

CUPS port:* 5060 (0-65535)

Realm:

Username: validation1

Password: ●●●●●●●●●●●●●●●

Security

TLS port:* -1 (-1 - 65535, -1 = Disabled)

Certificate nickname:* Not required when TLS or CUPS is disabled

Certificate database password:* Not required when TLS or CUPS is disabled

* -indicates required item.

8. To save, click **Submit**.

9. To test, click Test Connection.

Table 8: provides description for the fields on the CUCM Connectivity page

Field	Example	Description
CUPS name or IP	209.165.201.0	In this field you specify the IP Address of the machine where CUPS is installed.
CUPS port	5060	In this field you specify the CUPS port you wish to connect to. This is set to **5060** by default.(When not using TLS)
Realm		The realm is used to authenicate the SIP communication. If this is left blank then the IP address of the Cisco Unified Presence Server will be used.
Username	username1	You must enter the end user id used to connect to CUPS.
Password	*****	You must enter the password used to connect to CUPS.
TLS Port	-1	Transport Layer Security Port. By default this is set to -1 indicating that TLS is switched off. To enable TLS, specify the correct Port number (Normally either 5061 or 5062).
Certificate nickname	nickname1	Transport Layer Security certificate nickname is used to identify the correct certificate in the certificate database
Cerificate database password	******	Transport Layer Security certificate password will validate the user name above to provide access to the database.

Warning

1. **The Username and Password provided here are case-sensitive. Please make sure you enter the information in these fields in proper case.**
2. **The information provided in the Username and Password fields must not belong to an application user, for example CCMAdministrator.**

Note

IMPORTANT - The Cisco Unified Attendant CUPs Plug-in has to be added to the firewall information on the CallManager. *See section* “Configuring Access for the Cisco Unified Attendant CUPS Plug-In” on page 106

LDAP Directory Connectivity (for CUCM 4.3 only)

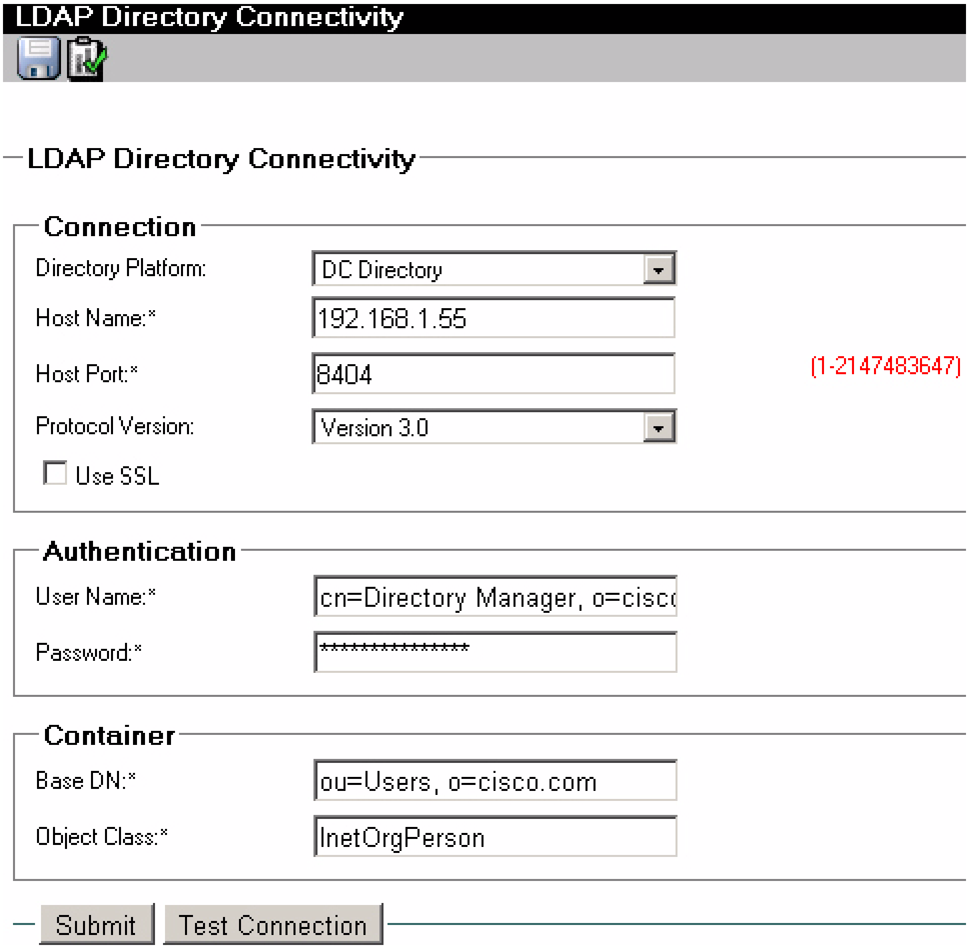
The *LDAP Directory Connectivity* allows you to specify the directory platform you wish to use for downloading contacts. The application supports the following directory platforms:

- iPlanet/Netscape directory
- Microsoft Active Directory
- DC Directory

The *LDAP Directory Connectivity* page is divided into the following sections:

- Connection
- Authentication
- Container

Figure 9: displays the LDAP Directory Connectivity page



LDAP Directory Connectivity

LDAP Directory Connectivity

Connection

Directory Platform:	DC Directory ▾	
Host Name:*	192.168.1.55	
Host Port:*	8404	(1-2147483647)
Protocol Version:	Version 3.0 ▾	

□ Use SSL

Authentication

User Name:*	cn=Directory Manager, o=cisco
Password:*	****************

Container

Base DN:*	ou=Users, o=cisco.com
Object Class:*	InetOrgPerson

The following table gives brief description for the fields you can configure:

Table 9: provides description of the fields displayed on LDAP Directory Connectivity page

Field	Example	Description
Connection: This section is used to select the Directory Platform to be used.		
Directory Platform	DC Directory	This list is used to choose the directory platform LDAP must connect to.
Host Name	192.168.1.55	This field is used to specify the Directory Host. Once the Directory platform is selected, the directory host is specified by default. However, you may edit the host if required.
Host Port	8404	This field is used to specify the Directory Port. Once the Directory platform is selected, the directory port is specified by default. However, you may edit the host if required.
Protocol Version	Version 3.0	This list is used to specify the Protocol Version. The latest protocol version is selected by default. However, you may select a different protocol version if required.s
Use SSL		This checkbox is used in order to specify whether you wish to use SSL for connectivity or not.
Authentication: This section is used to specify authentication information to access the selected directory.		
User Name	cn=Directory Manager, o=cisco.com	This field is used to specify the user name to access the directory.
Password	******	This field is used to enter the password for authentication.
Container: This section is used to specify the location of the data and the object type required for LDAP directory synchronization.		
Base DN	ou=Users, o=cisco.com	In this field you must enter the Base Distinguished Name for the container that holds the desired records. This is so as the records that we want to retrieve are within a specific container that is on a particular domain.

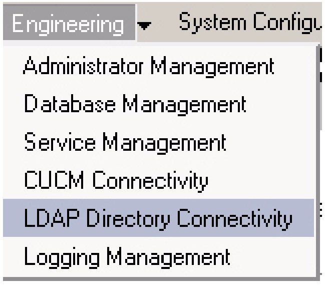
Table 9: provides description of the fields displayed on LDAP Directory Connectivity page

Object Class	inetOrgPerson	In this field you must enter the type of record that you want to import from the LDAP Directory. Once the directory platform is selected, the object class is specified by default. However, you may edit the object class if required.

To manage LDAP directory connectivity,

1. Go to *Engineering > LDAP Directory Connectivity.*

Figure 10: displays the LDAP Directory Connectivity menu



2. Enter *Connection* details.
3. Enter *Authentication* details.
4. Enter *Container* details.
5. Click **Test Connection** to verify the information entered is accurate.
6. Click **Submit** to save.

The following protocol versions are recommended for the following Directory Platforms:

Table 10: displays the list of recommended protocol versions for each directory platform

Directory Platform	Protocol Version
DC Directory	Version 3.0
Microsoft Active Directory	Version 3.0
iPlanet/Netscape Directory	Version 2.0 or Version 3.0

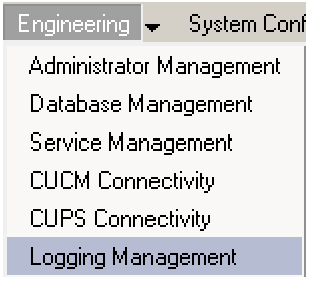
Logging Management

The *Logging Management* page allows real-time logging to be enabled or disabled for Cisco Unified Attendant Server and Cisco Unified Attendant LDAP Plug-in.

To manage logging,

1. Go to *Engineering > Logging Management*.

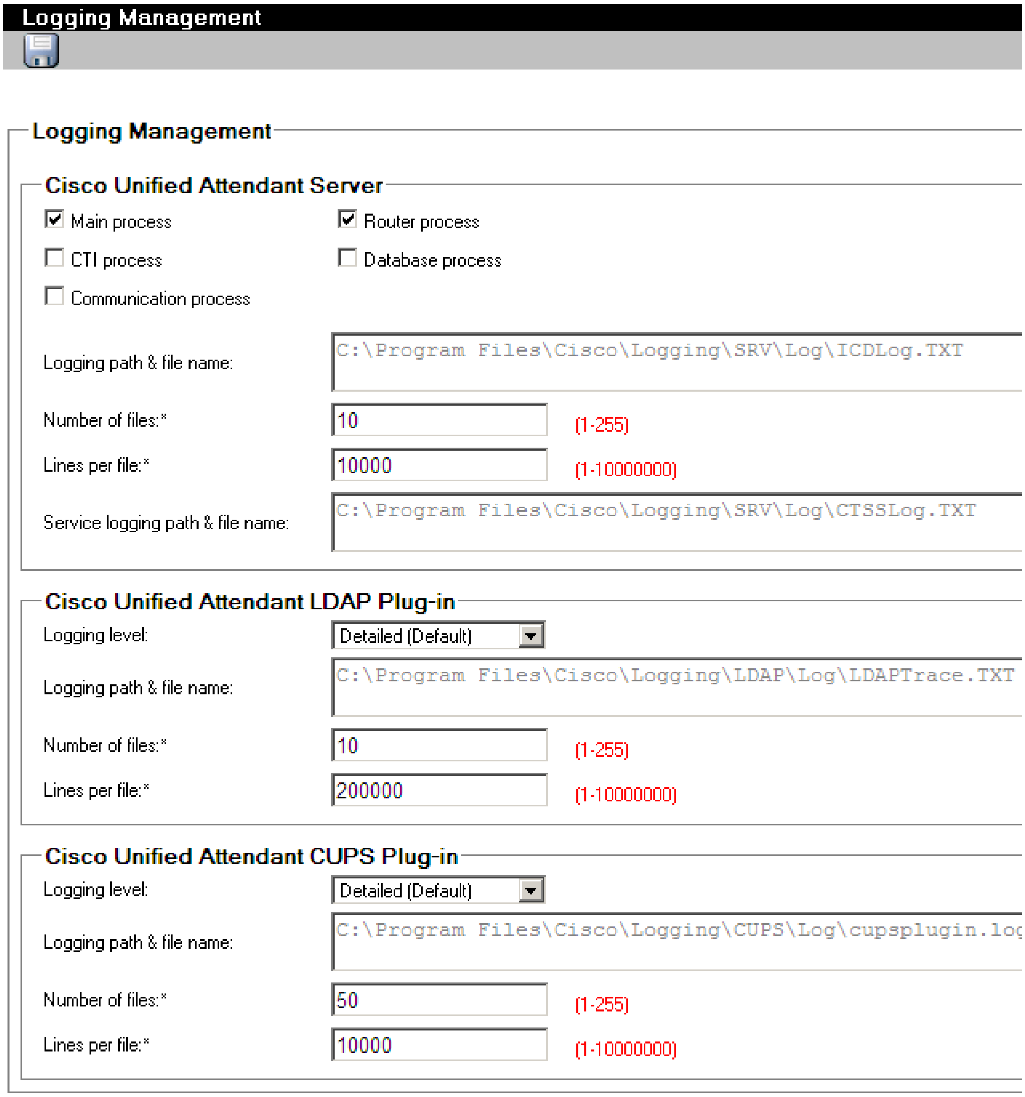
Figure 11: displays the menu option for Logging Management



2. Enter Cisco Unified Attendant Server Logging Management details.
3. Enter Cisco Unified Attendant LDAP Plug-in Logging Management details.
4. Click **Submit** to save changes.

The following image shows the configurations you can set using the above-mentioned procedure.

Figure 12: displays the Logging Management page



Logging Management

Logging Management

Cisco Unified Attendant Server

☑ Main process ☑ Router process

□ CTI process □ Database process

□ Communication process

Logging path & file name: C:\Program Files\Cisco\Logging\SRV\Log\ICDLog.TXT

Number of files:* 10 (1-255)

Lines per file:* 10000 (1-10000000)

Service logging path & file name: C:\Program Files\Cisco\Logging\SRV\Log\CTSSLog.TXT

Cisco Unified Attendant LDAP Plug-in

Logging level: Detailed (Default)

Logging path & file name: C:\Program Files\Cisco\Logging\LDAP\Log\LDAPTrace.TXT

Number of files:* 10 (1-255)

Lines per file:* 200000 (1-10000000)

Cisco Unified Attendant CUPS Plug-in

Logging level: Detailed (Default)

Logging path & file name: C:\Program Files\Cisco\Logging\CUPS\Log\cupsplugin.lo

Number of files:* 50 (1-255)

Lines per file:* 10000 (1-10000000)

The following table gives a brief description for the fields mentioned in the form displayed above,

Table 11: provides the description for the fields on the Logging Management page

Field	Example	Description
Logging Management		
Cisco Unified Attendant Server		
Main process		This checkbox is checked to log the main process.
CTI process		This checkbox is checked to log the CTI process.
Communication process		This checkbox is checked to log the communication process.
Router process		This checkbox is checked to log the router process.
Database process		This checkbox is checked to log the database process.
Logging path & file name	C:\Program Files\Cisco\Attendant LDAP Plug-in\Log\log.txt	In this field you specify the location where the log file must be saved. Include the name of the log file in the path so that the file is created by the name specified.
Number of files	200	In this field you specify the number of log files that can be created in the logging folder.
Lines per file	10000	In this field you specify the number of lines each log file can contain.
Service logging path & file name	C:\Program Files\Cisco\Attendant Server\Log\ICD1.TXT	In this field you specify the location and name for the file that stores the logs for the service.
Cisco Unified Attendant LDAP Plug-in		
Logging level	Detailed (default)	This can be set from Detailed, Advanced, Minimum, Full.
Logging path & file name	C:\Program Files\Cisco\Attendant Server\Log\ICD.TXT	In this field you specify the location where the log file must be saved. Include the name of the log file in the path so that the file is created by the name specified.

Table 11: provides the description for the fields on the Logging Management page

Number of files	200	In this field you specify the number of log files that can be created in the logging folder.
Lines per file	10000	In this field you specify the number of lines each log file can contain.
Cisco Unified Attendant CUPS Plug-in		
Logging level	Detailed (default)	This can be set from Detailed, Advanced, Minimum, Full.
Logging path & file name	C:\Program Files\Cisco\Attendant Server\Log\CUPS.TXT	In this field you specify the location where the log file must be saved. Include the name of the log file in the path so that the file is created by the name specified.
Number of files	200	In this field you specify the number of log files that can be created in the logging folder.
Lines per file	10000	In this field you specify the number of lines each log file can contain.

Cisco Unified Attendant Server Logging

Runtime logging for Cisco Unified Attendant Server maintains logs for each event that is fired by Cisco Unified Attendant Server. The logs can be maintained for the following areas,

1. Main Process
2. Router Process
3. CTI Process
4. Database Process
5. Communication Process

By default Main and Router processes will be activated at installation. You should only need to amend these settings if requested as part os a Support Case investigation.

To manage logging for Cisco Unified Attendant Server,

1. You must select the areas for which the log is to be maintained. In order to keep the log file up to a manageable size, it is recommended that you should keep only the required areas selected.
2. You must specify the *Logging path* and *file name* where the log must be created.
3. Specify the number of log files that must be created in the *Number of files* field.
4. Specify the number of lines each log file can contain in the *Lines per file* field.
5. Enter *Service logging path* and *file name* to maintain log of the services for Cisco Unified Attendant Server.

Cisco Unified Attendant LDAP Plug-in Logging

Cisco Unified Attendant Admin has the ability to keep records of all the events and processes through the process of logging. It is structured to enable and support you to check LDAP Plug-in's performance and activity, determine functionality loss and the configuration issues.

To manage logging for Cisco Unified Attendant LDAP Plug-in,

1. Select the *Logging Level* for LDAP Plug-in. Cisco Unified Attendant Admin provides the following options:
   a. Detailed
   b. Advanced
   c. Minimum
   d. Full
2. Specify the *Logging path* and *file name* where the log must be created.
3. Specify the number of log files that must be created in the *Number of files* field.
4. Specify the number of lines each log file can contain in the *Lines per file* field.

Cisco Unified Attendant CUPS Plug-in Logging

Cisco Unified Attendant Admin has the ability to keep records of all the events and processes through the process of logging. It is structured to enable and support you to check CUPS Plug-in's performance and activity, determine functionality loss and the configuration issues.

To manage logging for Cisco Unified Attendant CUPS Plug-in,

1. Select the *Logging Level* for CUPS Plug-in. Cisco Unified Attendant Admin provides the following options:
   a. Detailed
   b. Advanced
   c. Minimum
   d. Full
2. Specify the *Logging path* and *file name* where the log must be created.
3. Specify the number of log files that must be created in the *Number of files* field.
4. Specify the number of lines each log file can contain in the *Lines per file* field.

System Configuration

This section provides facilities to manage synchronization of devices and queues with Cisco Unified Communications Manager. The following configurations are available under this menu,

1. System Device Management
1. Attendant Console Device Management
2. CUCM Synchronization
3. Directory Filtering
4. Directory Synchronization

System Device Management

This web page allows device ranges to be configured and synchronized with Cisco Unified Communciations Server.

To add devices,

1. Go to *Engineering* > *System Device Management*.

2. Select a *Template Device*. All device properties of the selected device will be mapped onto new devices being created.
3. Enter a device range for each of the following:
   a. CT Gateway Devices
   b. Service Devices
   c. Park Devices

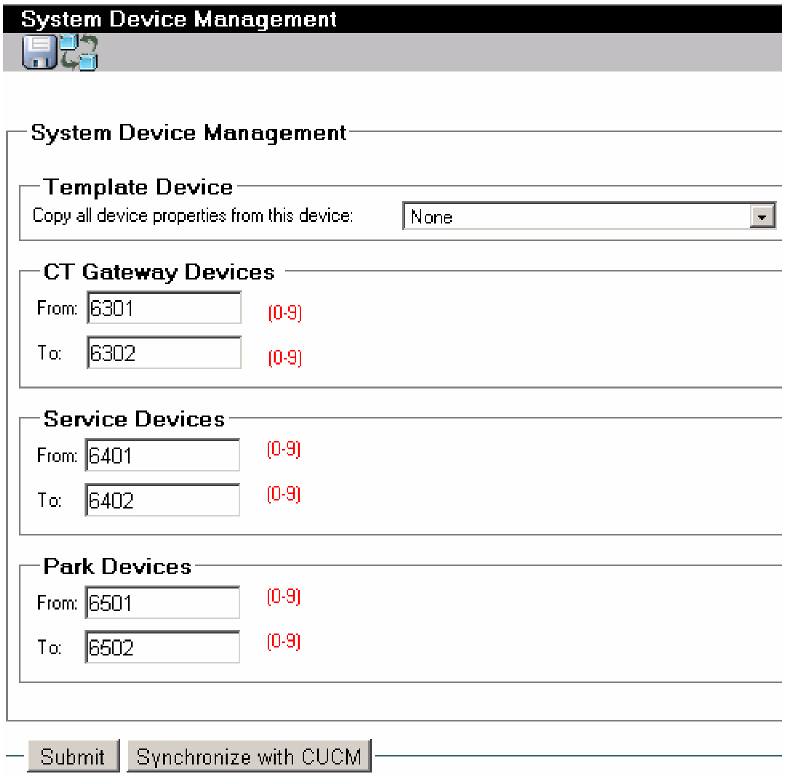
Note

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

4. Click **Submit** to save changes.
5. Clicking **Synchronize with CUCM** will redirect to *Synchronizing with CUCM* page within Cisco Unified Attendant Admin application.

The following image shows the configurations you can set using the above-mentioned procedure.

Figure 13: displays the Device Management page



System Device Management

System Device Management

Template Device

Copy all device properties from this device: None

CT Gateway Devices

From: 6301 (0-9)

To: 6302 (0-9)

Service Devices

From: 6401 (0-9)

To: 6402 (0-9)

Park Devices

From: 6501 (0-9)

To: 6502 (0-9)

The following table gives a brief description for the fields mentioned in the form displayed above,

Table 12: provides description for the fields on the System Device Management page

Field	Example	Description
Template Device		
Copy all device properties from this device		From this dropdown list you can select the device you want to copy the properties from, including Partition, Calling Search Space amongst others.
CT Gateway Devices		
From	6301	Specify the starting number for the range of devices to be configured.
To	6302	Specify the last number in the range of devices to be configured.
Service Devices		
From	6401	Specify the starting number for the range of devices to be configured.
To	6402	Specify the last number in the range of devices to be configured.
Park Devices		
From	6501	Specify the starting number for the range of devices to be configured.
To	6502	Specify the last number in the range of devices to be configured.

Attendant Console Device Management

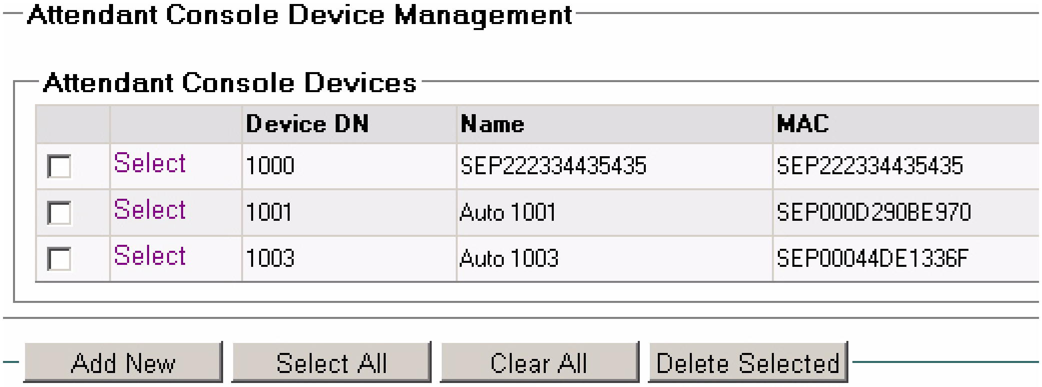
When operators log into Cisco Unified Attendant Console application, the Extension number that is entered during login is the Primary Number for a device. It is possible that the same extension number might be configured as a primary number for another device on a different partition. In order to differentiate between the two devices configured on the same extension number, the MAC address can be used to identify each device. A MAC address is a unique identifier for each physical device.

Using Attendant Console Device Management page, you can select a device to be associated to a particular directory number.

To select a device against a directory number,

1. Go to *System Configuration > Attendant Console Device Management*. A table will be displayed showing the Attendant Console Devices.

Figure 14: displays the Attendant Console Devices



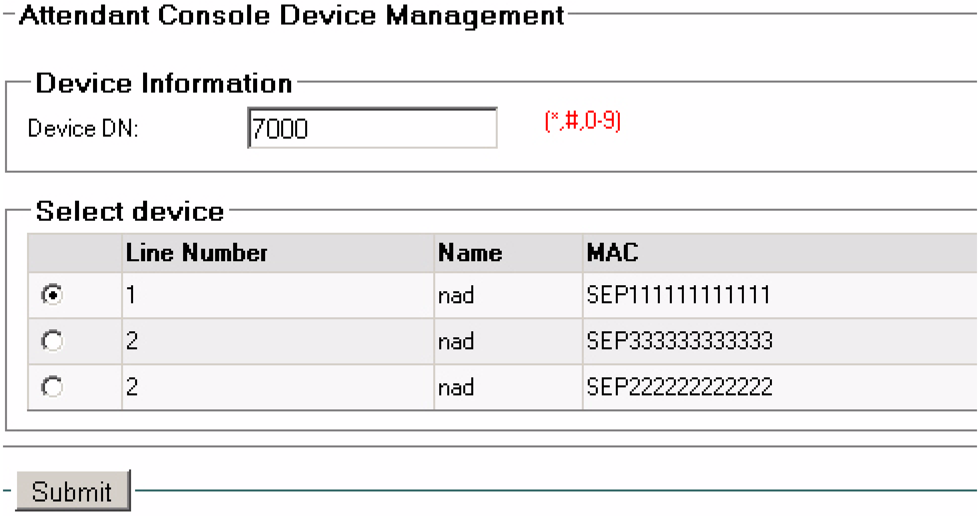
Attendant Console Device Management

Attendant Console Devices

		Device DN	Name	MAC
□	Select	1000	SEP222334435435	SEP222334435435
□	Select	1001	Auto 1001	SEP000D290BE970
□	Select	1003	Auto 1003	SEP00044DE1336F

2. Click **Add New** to add a new device against a directory number.

Figure 15: displays the list of devices configured on the specified directory number



Attendant Console Device Management

Device Information

Device DN: 7000 (*,#,0-9)

Select device

	Line Number	Name	MAC
●	1	nad	SEP111111111111
○	2	nad	SEP333333333333
○	2	nad	SEP222222222222

3. Enter the *Device DN*. A list of devices will be displayed in the **Select device** area.
4. Using the radio button, select the device that must be used to log into Cisco Unified Attendant Console application with the specified Device Directory Number.
5. Click **Submit**.

Please note that a new device can only be added if the chosen device is not in use at that time. Similarly a selected device cannot be deleted if the device is in use.

Synchronizing with CUCM

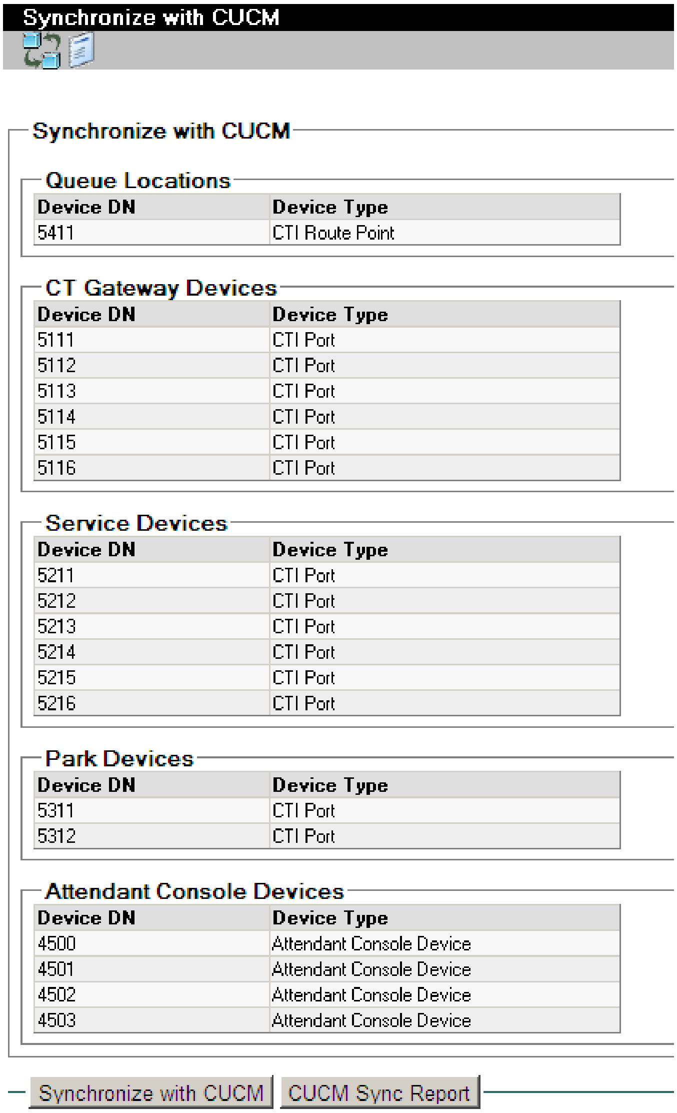
This web page is used to synchronize device configurations with Cisco Unified Communications Manager via AXL API. It will create the devices that have been configured if they don't already exist and assign them to the End User profile. The following devices will be displayed on this page,

1. Queue Locations
2. CT Gateway Devices
3. Service Devices
4. Park Devices

5. Attendant Console Devices

To synchronize the above-mentioned devices with Cisco Unified Communciation Manager, click **Synchronize with CUCM**. Cisco Unified Attendant Admin will automatically synchronize the devices with CUCM for you. You will not have to login to the CUCM administration.

Figure 16: displays the devices that will be synchronized with CUCM



Synchronize with CUCM

Synchronize with CUCM

Queue Locations

Device DN	Device Type
5411	CTI Route Point

CT Gateway Devices

Device DN	Device Type
5111	CTI Port
5112	CTI Port
5113	CTI Port
5114	CTI Port
5115	CTI Port
5116	CTI Port

Service Devices

Device DN	Device Type
5211	CTI Port
5212	CTI Port
5213	CTI Port
5214	CTI Port
5215	CTI Port
5216	CTI Port

Park Devices

Device DN	Device Type
5311	CTI Port
5312	CTI Port

Attendant Console Devices

Device DN	Device Type
4500	Attendant Console Device
4501	Attendant Console Device
4502	Attendant Console Device
4503	Attendant Console Device

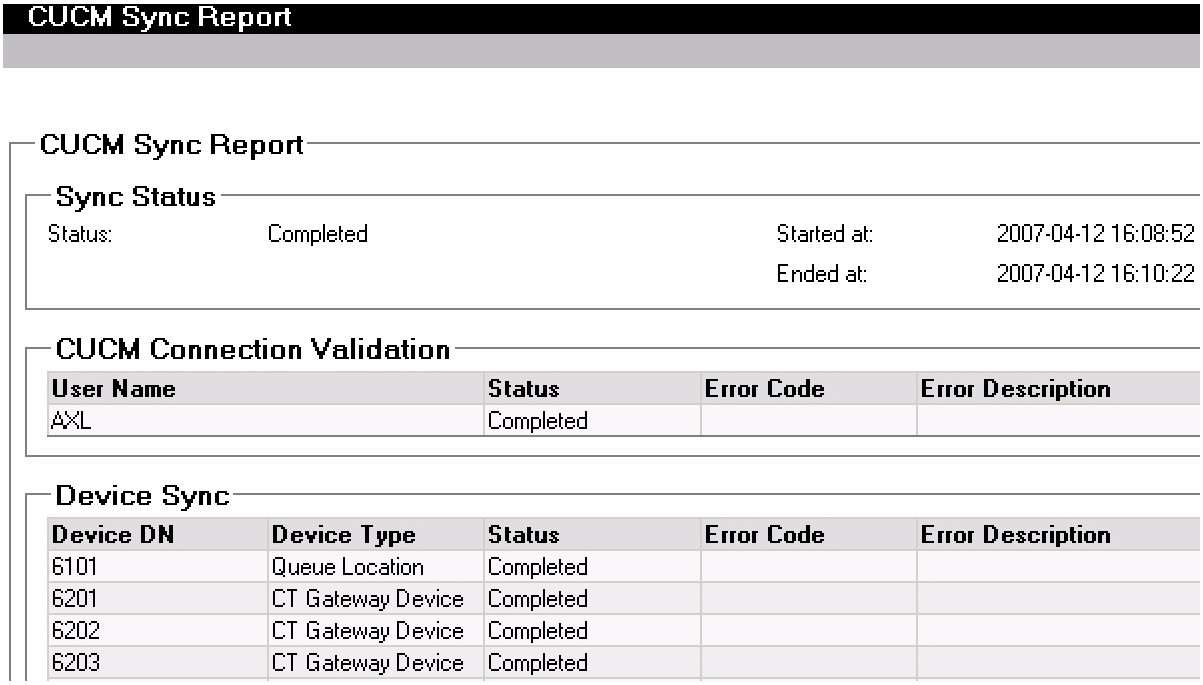
The following table gives a brief description for the fields mentioned in the form displayed above,

Table 13: provides description for the fields shown on the Synchronize with CUCM page

Field	Example	Description
Device DN	2000	This field specifies the directory number of each configured device.
Device Type	CTI Route Point	This field specifies the type of device.

Once the synchronization has been initiated, you can click on **CUCM Sync Report** to view the status of synchronization. This will confirm that all devices have been created and assigned to the End User Profile. When you click on the button the following window appears,

Figure 17: displays the CUCM Sync Report generated after the CUCM synchronization



CUCM Sync Report

CUCM Sync Report

Sync Status

Status:	Completed	Started at:	2007-04-12 16:08:52
		Ended at:	2007-04-12 16:10:22

CUCM Connection Validation

User Name	Status	Error Code	Error Description
AXL	Completed		

Device Sync

Device DN	Device Type	Status	Error Code	Error Description
6101	Queue Location	Completed		
6201	CT Gateway Device	Completed		
6202	CT Gateway Device	Completed		
6203	CT Gateway Device	Completed		

The following table explains the fields shown in the image above,

Table 14: provides description for the fields mentioned on the CUCM Sync Report

Field	Example	Description
Sync Status		
Status	Completed	This field specfies whether the synchronization was successful or not. The following statuses can be viewed, **In Progress** - This is displayed when the synchronization is taking place. **Completed** - This is displayed when synchronization is completed without any error. **Error** - This is displayed when synchronization process encounters an error.
Started At	2007-04-12 16:08:52	This field specifies the date and time when CUCM synchronization started.

Table 14: provides description for the fields mentioned on the CUCM Sync Report

Ended At	2007-04-12 16:08:52	This field specifies the date and time when CUCM synchronization ended.
CUCM Connection Validation		
User Name	username1	This specifies the CUCM end user profile ID.
Status	Completed	This specifies whether the CUCM Connection established or not.
Error Code	9400	This field specifies the code of the error that has been encountered. The error codes have been explained in detail in the next table.
Error Description	HTTP/1.1 503 Service Unavailable	This field gives a brief description of the error that has been encountered.
Device Sync		
Device DN	6101	This field specifies the number of the device being synchronized.
Device Type	Queue Location	This field specifies the type of device being synchronized.
Status	Completed	This field specifies the status of the device synchronization.
Error Code	9550	This field specifies the error code in case an error encountered synchronizing a device.
Error Description	HTTP/1.1 403 Access to the requested resource has been denied	This field specifies the description of the error.

The table below gives a list of error codes and description that may be encountered during CUCM synchronization.

Table 15: provides error codes that may be displayed in the CUCM Sync Report

Error Code	Error Description
AXL Errors	
Less than 5000	These are errors that directly correspond to DBL Exception error codes.
5000	Unknown Error—An unknown error occurred while processing the request. This can be due to a problem on the server, but can also be caused by errors in the request.

Table 15: provides error codes that may be displayed in the CUCM Sync Report

5002	Unknown Request Error—This error occurs if the user agent submits a request that is unknown to the API.
5003	Invalid Value Exception—This error occurs if an invalid value is detected in the XML request.
5004	AXL Unavailable Exception—This error occurs if the AXL service is too busy to handle the request at that time. The request should be sent again at a later time.
5005	Unexpected Node Exception—This error occurs if the server encounters an unexpected element. For example, if the server expects the next node to be <*name*>, but encounters <*protocol*>, then this error is returned. These errors are always caused by malformed requests that do not adhere to the latest AXL Schema.
-239	Duplicate value in a UNIQUE INDEX column - This error occurs if the device being synchronized already exists in CUCM.
9000	Exception in AXL component - This error occurs if the device being synchronized already exists in CUCM.
9200	Device already created - This error occurs if the device being synchronized already exists in CUCM.
9300	Template device not found - This error occurs if the template device that you have selected to copy all device properties from does not exist.
9400	HTTP/1.1 503 Service Unavailable - This error is encountered when the CUCM limit for input through AXL exceeds.
9500	HTTP/1.1 401 Unauthorized - This error occurs due to problems in user authentification.
9550	HTTP/1.1 403 Access to the requested resource has been denied - This error occurs when access to a device is denied.
9600	CallManager OS not recognized - This error occurs when access to CUCM is denied.
9650	CallManager Version not detected - This error occurs when access to CUCM is denied.
9700	Socket error - This error occurs due to network problems.
9750	Connection refused - This error occurs due to network problems.
9755	Read Timeout - This error occurs due to network problems.
10000	Connection timeout - This error occurs due to network problems.

Table 15: provides error codes that may be displayed in the CUCM Sync Report

9900	An unknown error occured - This is an unknown error.

Directory Filtering (for Cisco Unified Department Attendant Console only)

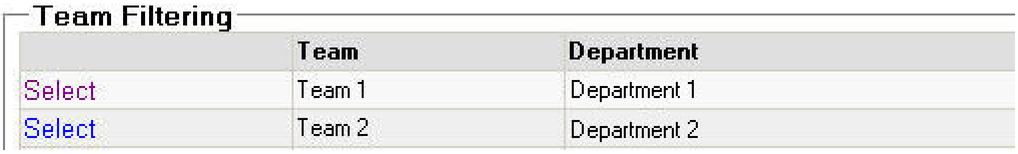
This section provides a list of teams and the departments they belong to. The Directory Filtering web page allows you to filter the teams in order to facilitate synchronization of contact details from Cisco Unified Attendant Console database with Cisco Unified Communications Manager via AXL API. You can select a team and view or edit the following information,

1. **Team:** This field displays the name of the team. This information cannot be changed.
2. **Department:** This field specifies the name of the department. You can update the department name through this page.
3. **Maximum Imported Records:** This field is used to specify the maximum number of contacts that can be imported for a particular team through LDAP.

Please note that this feature is only available for Cisco Unified Department Attendant Console.

1. Choose System *Configuration* > *Directory Filtering*.
2. In the *Team Filtering* section, select a team that you wish to modify.

Figure 18: displays a grid displaying the teams and their departments

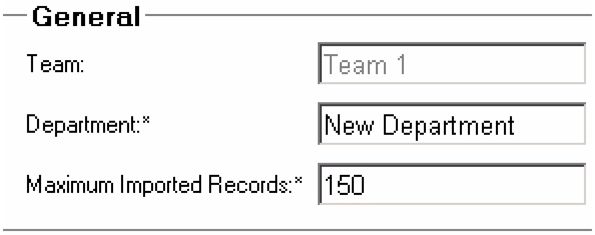


Team Filtering

	Team	Department
Select	Team 1	Department 1
Select	Team 2	Department 2

3. Edit the information for the selected team.

Figure 19: displays the information that can be edited



General

Team:	Team 1
Department:*	New Department
Maximum Imported Records:*	150

The department name that you enter in the *Department* field shown above, can be searched on exact match as well as pattern match basis. If you enter an exact name (for example, **New Department**) in the field, the contacts will be synchronized for the particular department name entered.

The pattern match is based on wildcard. The following symbols are used to support wildcard,

Table 16: provides the list of symbols that may be use for wildcard

Symbol	Description
?	Used to match any single character.
–	
*****	Used to match zero or more characters.
%	

If you enter a pattern in the *Department* field (for example, ***Department?**), the contacts will be synchronized for all the departments that have names following the pattern entered in the field (in this case, **New Department1**, **Sales Department 3**).

4. Once you have configured directory synchronization, click 💾 **Submit** would save the changes.

Directory Synchronization

The *Directory Synchronization* web page provides the ability to synchronize the contact details for the Cisco Unified Attendant Console database with Cisco Unified Communications Manager via AXL API. The page has been divided into following sections,

1. **Directory Import:** In order to enable directory import, you must check the *Enable contact synchronization* checkbox. *Auto Synchronization* and *Schedule Settings* fields will remain disabled if you do not select the *Enable contact synchronization* option.
2. **LDAP System Configuration:** This section allows you to *Enable External LDAP Integration*. This checkbox is checked when you wish to synchronize with CUCM using an external LDAP instead of CUCM's LDAP.
   a. **DC Directory**. Standard Supported fields are:- Department, First_Name, Last_Name and INTL. With External LDAP turned on:- Email, Fax, Mobile, Title and Initials are available.
   b. **Microsoft Active Directory**. Standard Supported fields are:- Department, First_Name, Last_Name and INTL. With External LDAP turned on:- Email, Title, Company, Home Phone, Mobile, Initials and Fax are available.
   c. **iPlanet/Netscape Directory**. Standard Supported fields are:- Department, First_Name, Last_Name and INTL. With External LDAP turned on:- Email, Initials and Fax are available.
4. **Auto Synchronization:** You can set preferences for automatic synchronization. The following options are available to do so,
   a. **On start-up:** If this checkbox is checked then the synchronization is started when Cisco Unified Attendant Server starts.
   b. **On reconnect:** If this checkbox is selected then the synchronization will start when Cisco Unified Attendant Server reconnects with the LDAP plug-in following a loss of connection.
4. **Schedule Settings:** This section requires information on the scheduling of synchronization. You must enter the following information,
   a. **Type:** This is an option list. The synchronization will take place on the basis of the type selected. It has the following options,
      i. None
      ii. Hourly

iii. Daily
iv. Weekly
v. Monthly

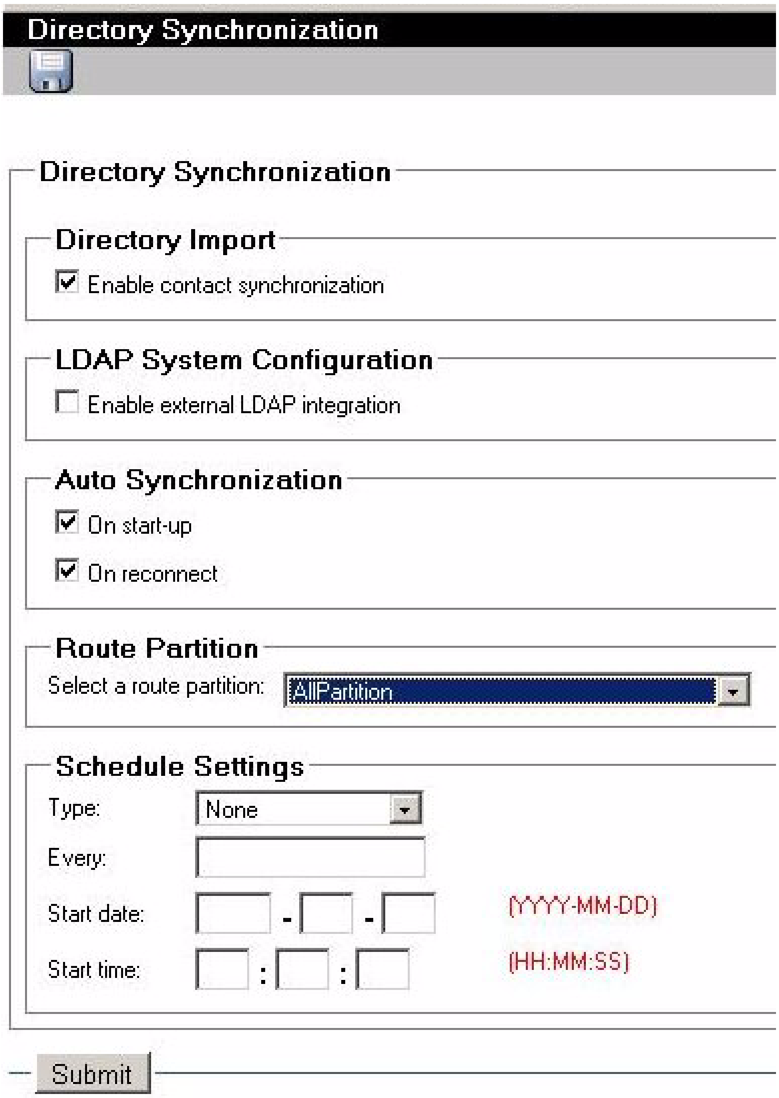
b. **Every [(Number)(Type)]:** The caption for this option changes with the selection of the *Type*. For example, Every 2 **Week(s)** or Every 1 **Day(s)**.
c. **Start date:** This field is used to specify a date to start the synchronization.
d. **Start time:** This field is used to specify the time to start the synchronization.

To configure directory synchronization for Cisco Unified Business Attendant Console,

1. Go to *System Configuration > Directory Synchronization*.
2. Enter specifications for the above-mentioned sections.
3. Once you have configured directory synchronization, click **Submit** would save the changes.

The following image shows the configurations you can set using the above-mentioned procedure.

Figure 20: displays the settings for Directory Synchronization



Directory Synchronization

Directory Synchronization

Directory Import

☑ Enable contact synchronization

LDAP System Configuration

☐ Enable external LDAP integration

Auto Synchronization

☑ On start-up

☑ On reconnect

Route Partition

Select a route partition: AllPartition

Schedule Settings

Type: None

Every:

Start date: - - (YYYY-MM-DD)

Start time: : : (HH:MM:SS)

Submit

To configure directory synchronization for Cisco Unified Department Attendant Console,

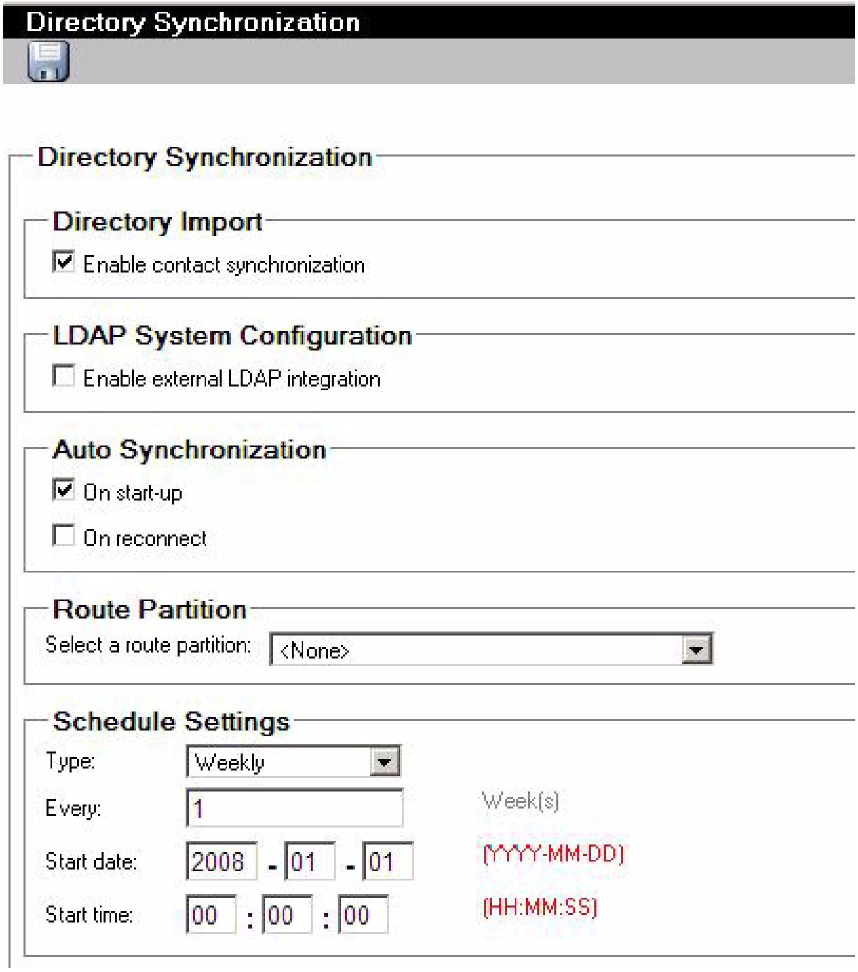
1. Go to *System Configuration > Directory Synchronization*.

2. Enter specifications for the following,
   a. Directory Import
   b. LDAP System Configuration
   c. Auto Synchronization
   d. Route Partition
   e. Schedule Settings

6. Once you have configured directory synchronization, click **Submit** would save the changes.

The following image shows the configurations you can set using the above-mentioned procedure.

Figure 21: displays the Directory Synchronization page for Cisco Unified Department Attendant Console



Directory Synchronization

Directory Synchronization

Directory Import

☑ Enable contact synchronization

LDAP System Configuration

☐ Enable external LDAP integration

Auto Synchronization

☑ On start-up

☐ On reconnect

Route Partition

Select a route partition: <None>

Schedule Settings

Type: Weekly

Every: 1 Week(s)

Start date: 2008 - 01 - 01 (YYYY-MM-DD)

Start time: 00 : 00 : 00 (HH:MM:SS)

User Configuration

The *User Configuration* section provides administrators with facilities to manage Cisco Unified Attendant Console configuration. These include,

- General settings for Cisco Unified Attendant Console
- Queue Management
- Operator Management

General Properties

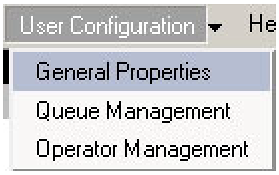
This web page manages the global configuration for Cisco Unified Attendant Console. It has been divided into four sections,

1. **Internal/External Access:** These settings allow Cisco Unified Attendant Console to distinguish between internal and external calls. They also ensure that the correct digit is used that allows you to access an external line. The fields required here are**,**
   a. **Minimum internal device digit length:** This text box requires you to enter the minimum number of digits being used for an internal device.
   b. **Maximum internal device digit length:** This text box requires you to enter the maximum number of digits being used for an internal device. **Note** The default setting for this is 4 digits. If your Internal Extension Numbers exceed this it will require changing to accommodate this.
   c. **External access number:** This field specifies the access number when making a call to an external number.
   d. **External international access number:** This is the number that is to be dialled when making a call to an international external number.
   e. **External area code:** This field represents the Country Code for where the CUCM is located. When a call is dialled out by the system and the number string is determined to be in a standard international format i.e +44 (0) 208 8241000, the Area code set here will determine if the call is dialled as an international call or a domestic call. In this example an Area Code of 44 would result in a domestic call being dialled.
2. **Default FAC and CMC Settings:** If Forced Authorization (FAC) and/or Client Matter Codes (CMC) are configured in CUCM then these may be needed for any Attendant calls or transfers to be made. The codes entered here are generic and will be used in certain situations that require the system to place these calls or transfers. An example would be a blind transfer where the final outbound call is made from a Service Queue CTI port. If a call or transfer is made which results in the call being made from the operator’s handset externally, then the operator will be presented with a CFAC or CMC dialog box, requiring them to manually enter the code from their application.
3. **Recall Timers:** This area is used for setting the time duration for the recall activity of the calls. You can update three types of timers for the calls. These are as follows,
   a. **Hold recall:** This is the maximum time limit a call can be put on hold by an operator.
   b. **Transfer recall:** When an operator transfers a call, and if the call is not received within the time period specified in the *Transfer recall* field, it will come back to the same operator who had transferred the call.
   c. **Park recall:** When an operator parks a call, and if the call is not received within the time period specified in the *Park recall* field, it will come back to the same operator who had parked the call.
4. **Working Days (for Cisco Unified Business Attendant Console only):** This section allows you to set specific days and hours when the Attendant Console queues will be active. You must specify the following fields,
   a. The checkboxes provided allow you to select the days the queues are active.
   b. You must also enter the *Working hours from time* and *Working hours to time* in order to specify the time period that the queues will be active during these working days.

To configure General Properties,

1. Go to *User Configuration* > *General Properties*.

   Figure 22: displays menu option for General Properties

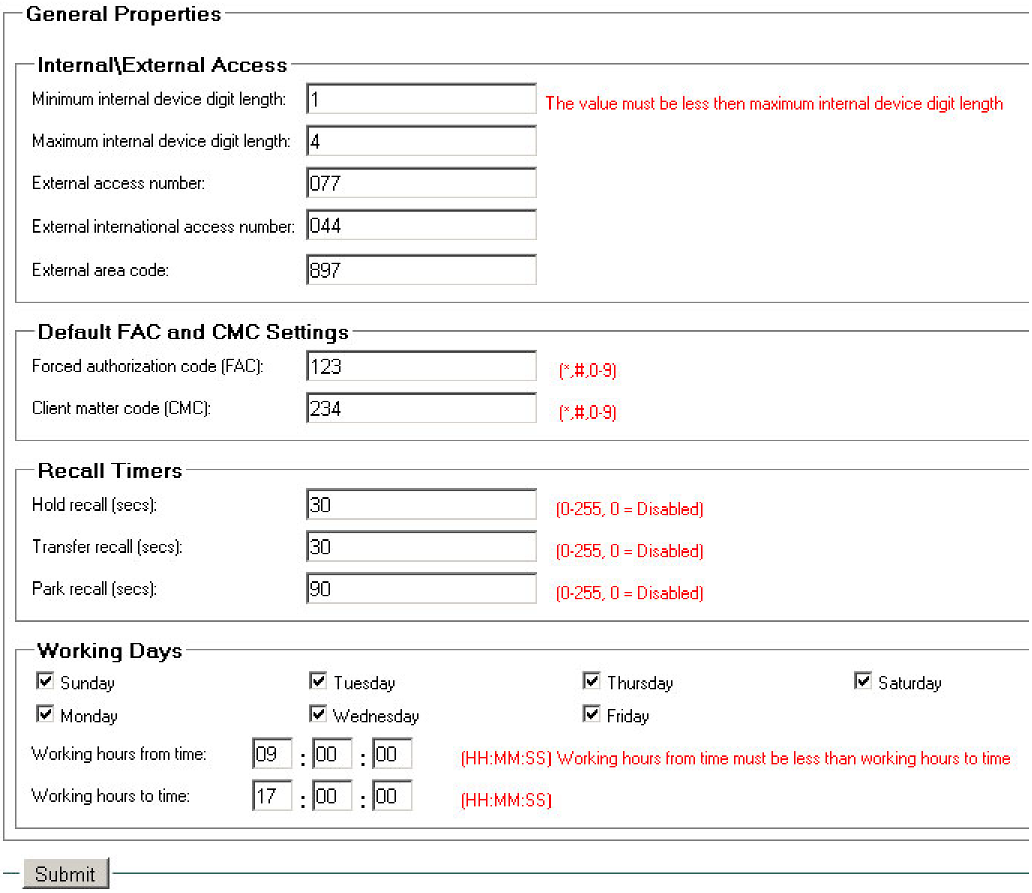


2. Enter specifications for the above-mentioned sections.

3. Once you have configured the general properties, click **Submit** to save the changes.

The following image shows the *General Properties* page for Cisco Unified Business Attendant Console. The *Working Days* section is available here. Users with the license for Cisco Unified Department Attendant Console will not be provided with the *Working Days* section.

Figure 23: displays the setting made on the General Properties page



General Properties

Internal\External Access

Minimum internal device digit length: 1 The value must be less then maximum internal device digit length

Maximum internal device digit length: 4

External access number: 077

External international access number: 044

External area code: 897

Default FAC and CMC Settings

Forced authorization code (FAC): 123 (*,#,0-9)

Client matter code (CMC): 234 (*,#,0-9)

Recall Timers

Hold recall (secs): 30 (0-255, 0 = Disabled)

Transfer recall (secs): 30 (0-255, 0 = Disabled)

Park recall (secs): 90 (0-255, 0 = Disabled)

Working Days

☑ Sunday ☑ Tuesday ☑ Thursday ☑ Saturday

☑ Monday ☑ Wednesday ☑ Friday

Working hours from time: 09 : 00 : 00 (HH:MM:SS) Working hours from time must be less than working hours to time

Working hours to time: 17 : 00 : 00 (HH:MM:SS)

Queue Management

The *Queue Management* web page allows you to manage the configuration for existing queues. The configuration is divided into four sections,

1. **General:** This section allows you to configure the general attributes of a queue. The following fields can be edited in this section,

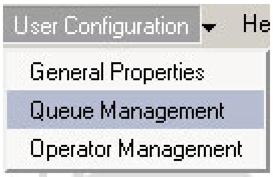
   a. **Name (for Cisco Unified Business Attendant Console):** This field specifies the name of the queue.
   b. **Team (for Cisco Unified Department Attendant Console):** This field specifies the name of the team.
   c. **DDI:** This is the number that is dialled internally to reach the respective queue session. External calls must be routed to this DN to reach the queue.
   d. **Priority (for Cisco Unified Business Attendant Console):** You can assign a priority number to a queue that determines which queue must be given priority when calls are being routed.

2. **Emergency (for Cisco Unified Business Attendant Console):** The *Emergency number* field allows you to specify a number in case the calls need to be forwarded to another number in the event of sudden need.
3. **Overflow:** In case the number of calls waiting exceeds the number of calls that are allowed to wait in a queue, an overflow occurs. This section allows you to manage such overflow by configuring the following fields,
   a. **Overflow number:** In case of an overflow the exceeding number of calls will be transferred to the number specified in this field.
   b. **Maximum calls:** This field allows you to set the total number of calls that can wait in a Queue at any given time.
   c. **No operator overflow:** If there is no operator logged in to thie selected queue, an incoming call will be immediately routed to the *Overflow number* if this checkbox is selected.
4. **Night Service (for Cisco Unified Business Attendant Console):** This section allows you to specify a *Night service number.* The calls made on the days and time specified for night service, are routed to this number.

To manage queues,

1. Go to *User Configuration* > *Queue Management*.

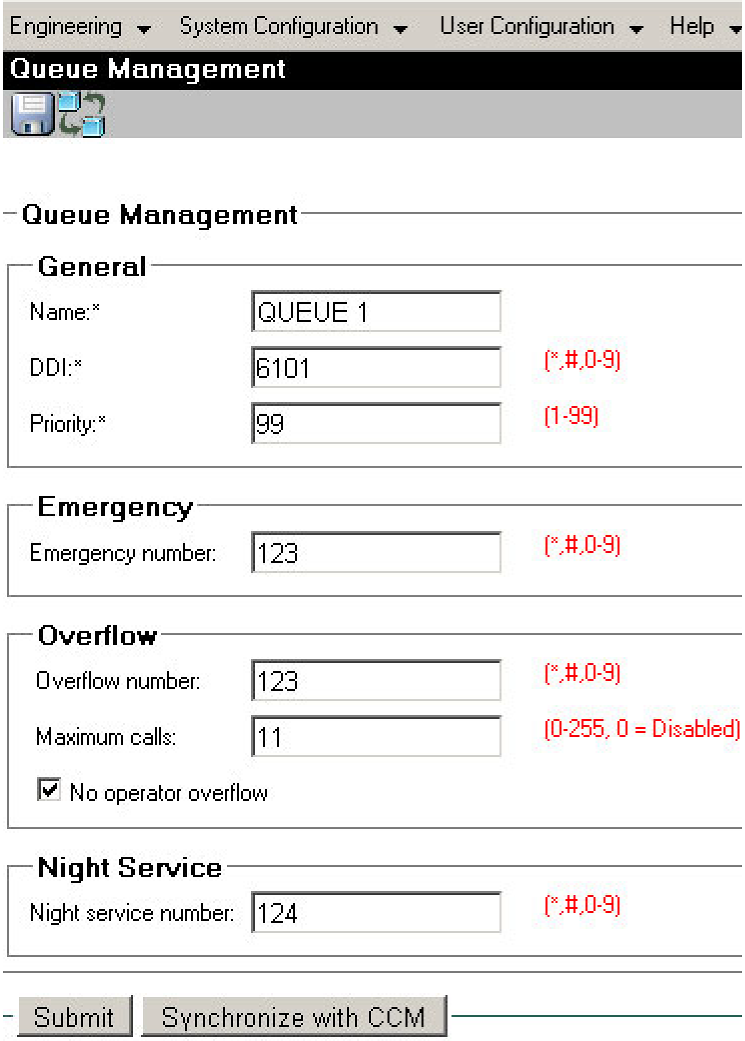
Figure 24: displays the menu option for Queue Management



2. Select the queue profile that needs to be modified. Once the queue is selected, the form will be automatically loaded with the queue configuration.
3. Edit the specifications for the above-mentioned sections.
4. Once you have modified the configuration, click **Submit** to save the changes.
5. Click **Synchronize with CUCM** will redirect to *Synchronizing with CUCM* page.

The following image shows the *Queue Management* page used to configure Cisco Unified Business Attendant Console.

Figure 25: displays the Queue Management page for Cisco Unified Business Attendant Console



Queue Management

General

Name:* QUEUE 1

DDI:* 6101 (*,#,0-9)

Priority:* 99 (1-99)

Emergency

Emergency number: 123 (*,#,0-9)

Overflow

Overflow number: 123 (*,#,0-9)

Maximum calls: 11 (0-255, 0 = Disabled)

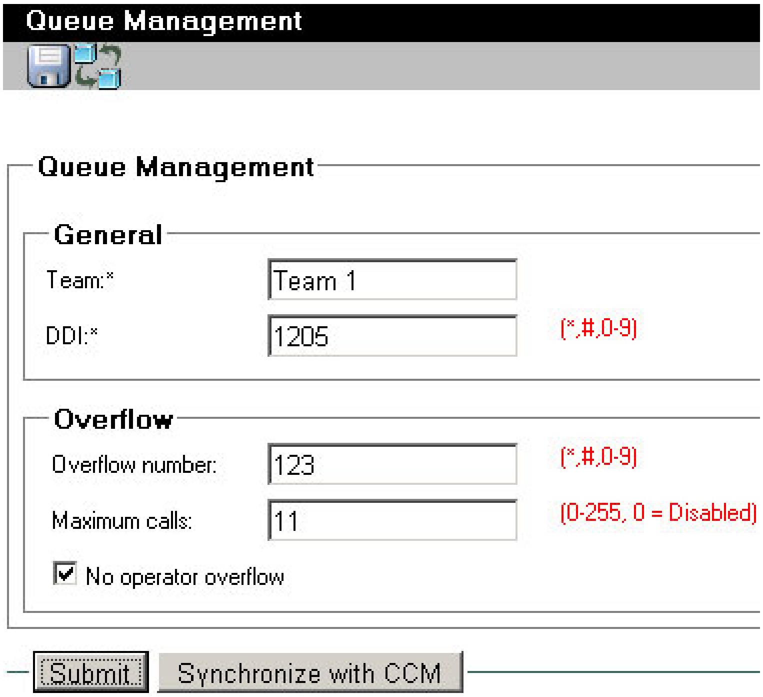
☑ No operator overflow

Night Service

Night service number: 124 (*,#,0-9)

If you have a license for Cisco Unified Department Attendant Console you will only be able to configure the fields shown in the following image,

Figure 26: displays the Queue Management page for Cisco Unified Department Attendant Console



Queue Management

Queue Management

General

Team:* Team 1

DDI:* 1205 (*,#,0-9)

Overflow

Overflow number: 123 (*,#,0-9)

Maximum calls: 11 (0-255, 0 = Disabled)

☑ No operator overflow

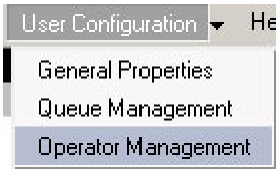
Operator Management

The *Operator Management* web page allows you to manage the configuration for the operator profile.

To manage operators,

1. Select *User Configuration > Operator Management*.

Figure 27: displays the menu option for Operator Management

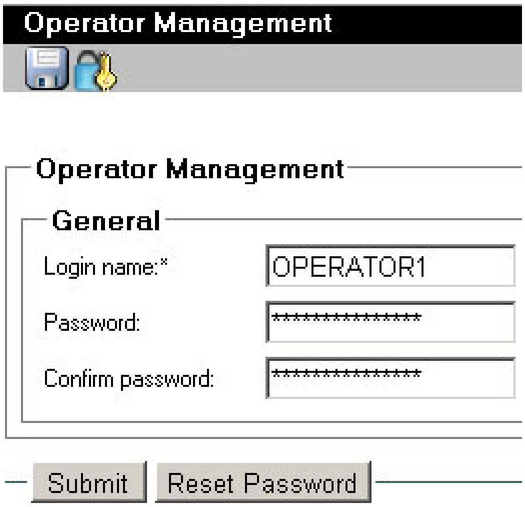


2. Select the operator profile that needs to be modified. Once an operator profile is selected, the form will be automatically loaded with the operators profile information.
3. Edit *Login name*.
4. Edit *Team* name (for Cisco Unified Department Attendant Console only).
5. Change *Password*.
6. Re-enter password to confirm in the *Confirm password* field.
7. Click 💾 **Submit** to save changes.

8. Click 🔒 **Reset password** to reset the user password to be the same as the operator's login name.

The following image shows the *Operator Management* page used to configure Cisco Unified Business Attendant Console.

Figure 28: displays Operator Management page for CUBAC



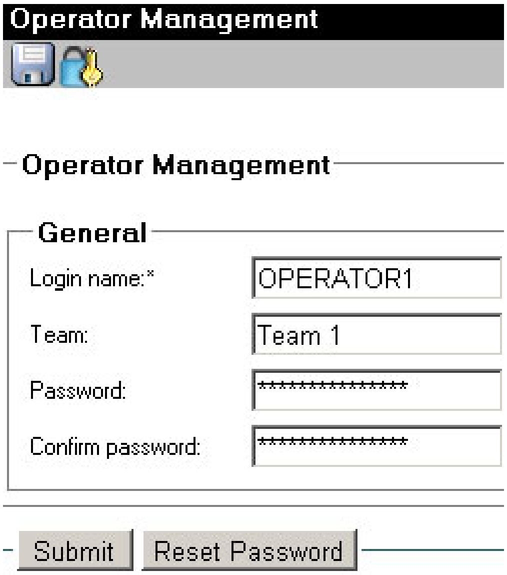
Login name:* OPERATOR1

Password: ****************

Confirm password: ****************

If you have a license for Cisco Unified Department Attendant Console you will be able to configure the fields shown in the following image,

Figure 29: displays Operator Management page for CUDAC

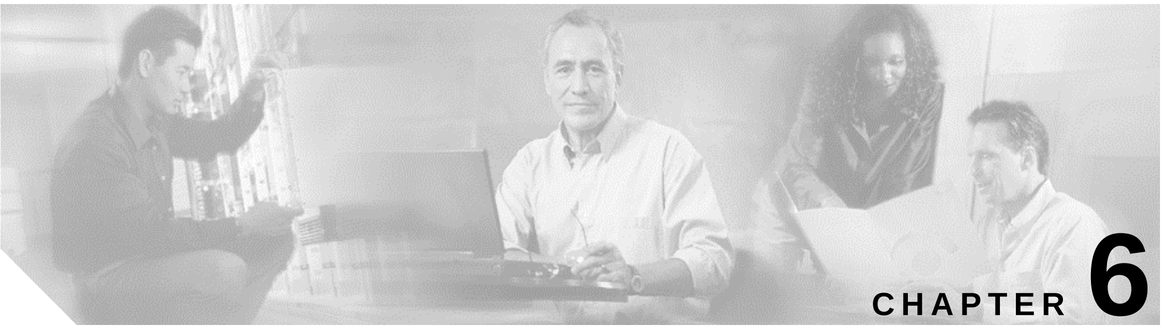


Login name:* OPERATOR1

Team: Team 1

Password: ****************

Confirm password: ****************



CHAPTER 6

Uninstalling the Application and its Components

This section describes in detail how to uninstall the following,

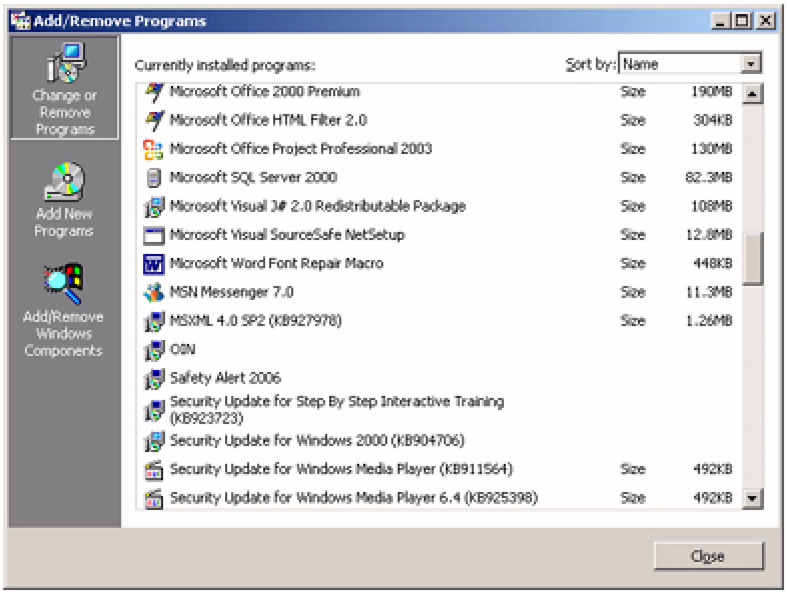
1. Cisco Unified Attendant Server
2. SQL Server 2005
3. BDE
4. .Net Framework

Uninstalling Cisco Unified Attendant Server

The following steps are followed in order to uninstall the application,

1. Go to *Start* > *Settings* > *Control Panel* > *Add/Remove Programs*.

Figure 1: displays the Add/Remove Programs window



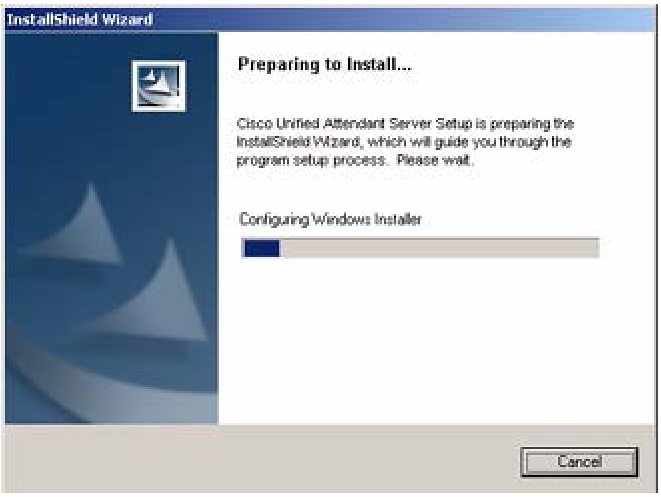
Currently installed programs:

Sort by: Name

Microsoft Office 2000 Premium	Size	190MB
Microsoft Office HTML Filter 2.0	Size	304KB
Microsoft Office Project Professional 2003	Size	130MB
Microsoft SQL Server 2000	Size	82.3MB
Microsoft Visual J# 2.0 Redistributable Package	Size	108MB
Microsoft Visual SourceSafe NetSetup	Size	12.8MB
Microsoft Word Font Repair Macro	Size	448KB
MSN Messenger 7.0	Size	11.3MB
MSXML 4.0 SP2 (KB927978)	Size	1.26MB
OIN		
Safety Alert 2006		
Security Update for Step By Step Interactive Training (KB923723)		
Security Update for Windows 2000 (KB904706)		
Security Update for Windows Media Player (KB911564)	Size	492KB
Security Update for Windows Media Player 6.4 (KB925398)	Size	492KB

2. Select Cisco Unified Attendant Server from the list of Programs. Click **Remove**.
3. The next window that is displayed will show the status of the wizard while the files are being prepared to uninstall the application.

Figure 2: displays the Preparing to Install screen



InstallShield Wizard

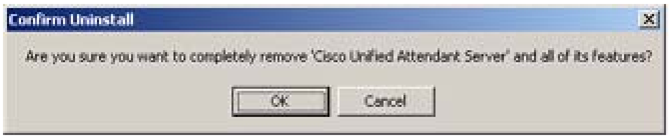
Preparing to Install...

Cisco Unified Attendant Server Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.

Configuring Windows Installer

4. The following message box will appear confirming whether you want to remove Cisco Unified Attendant Server from your machine or not. Click **OK** to continue.

Figure 3: displays the message box that asks you if you want to remove the application from the system

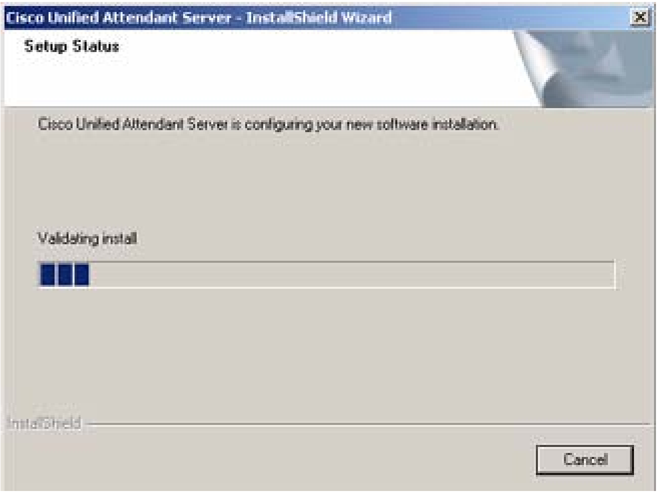


Confirm Uninstall

Are you sure you want to completely remove 'Cisco Unified Attendant Server' and all of its features?

5. The next window displays the progress of the un-installation.

Figure 4: displays the un-installation progress of the application



Cisco Unified Attendant Server - InstallShield Wizard

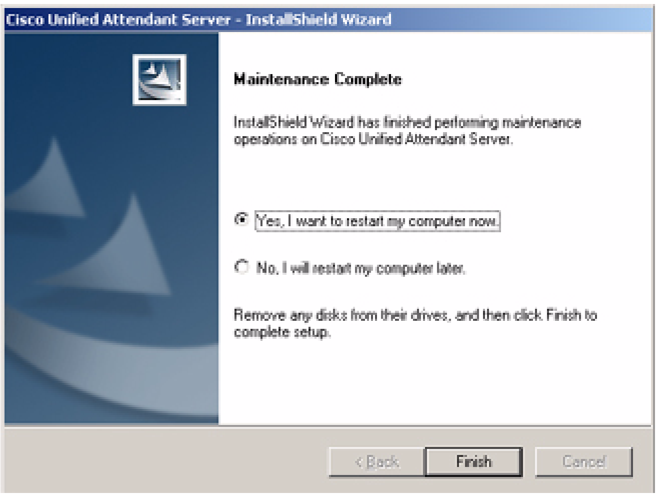
Setup Status

Cisco Unified Attendant Server is configuring your new software installation.

Validating install

6. Once the files have been uninstalled successfully, the next window will ask whether you wish to restart the computer now or later. It is recommended that you restart the machine. Click **Finish**.

Figure 5: displays the options for restarting the machine



Cisco Unified Attendant Server - InstallShield Wizard

Maintenance Complete

InstallShield Wizard has finished performing maintenance operations on Cisco Unified Attendant Server.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

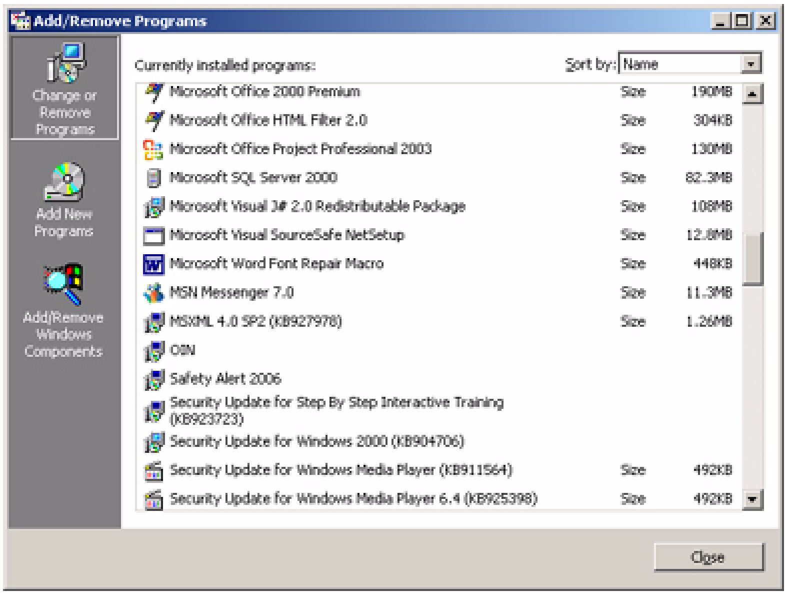
Uninstalling MS SQL Server

Once you have uninstalled the application, you are required to remove all the third-party components installed with the application. Therefore we uninstall MS SQL Server as well.

To uninstall the SQL Server,

1. Go to *Start* > *Settings* > *Control Panel* > *Add/Remove Programs*.

Figure 6: displays the Add/Remove Programs window



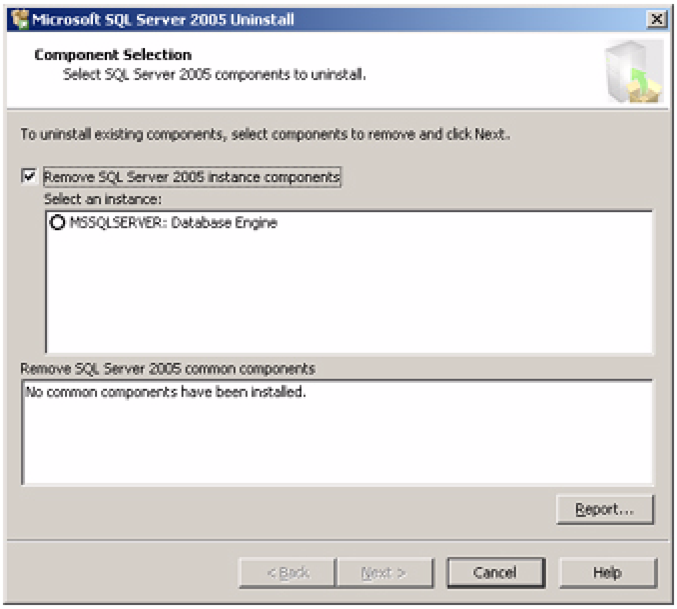
Add/Remove Programs

Currently installed programs: Sort by: Name

Microsoft Office 2000 Premium	Size	190MB
Microsoft Office HTML Filter 2.0	Size	304KB
Microsoft Office Project Professional 2003	Size	130MB
Microsoft SQL Server 2000	Size	82.3MB
Microsoft Visual J# 2.0 Redistributable Package	Size	108MB
Microsoft Visual SourceSafe NetSetup	Size	12.8MB
Microsoft Word Font Repair Macro	Size	448KB
MSN Messenger 7.0	Size	11.3MB
MSXML 4.0 SP2 (KB927978)	Size	1.26MB
OIN		
Safety Alert 2006		
Security Update for Step By Step Interactive Training (KB923723)		
Security Update for Windows 2000 (KB904706)		
Security Update for Windows Media Player (KB911564)	Size	492KB
Security Update for Windows Media Player 6.4 (KB925398)	Size	492KB

2. Select Microsoft SQL Server from the list of Programs. Click **Remove**.
3. The next window will display the list of server instances. Select the instance that you wish to be removed.

Figure 7: displays the server instance to be removed



Microsoft SQL Server 2005 Uninstall

Component Selection
Select SQL Server 2005 components to uninstall.

To uninstall existing components, select components to remove and click Next.

☑ Remove SQL Server 2005 instance components

Select an instance:

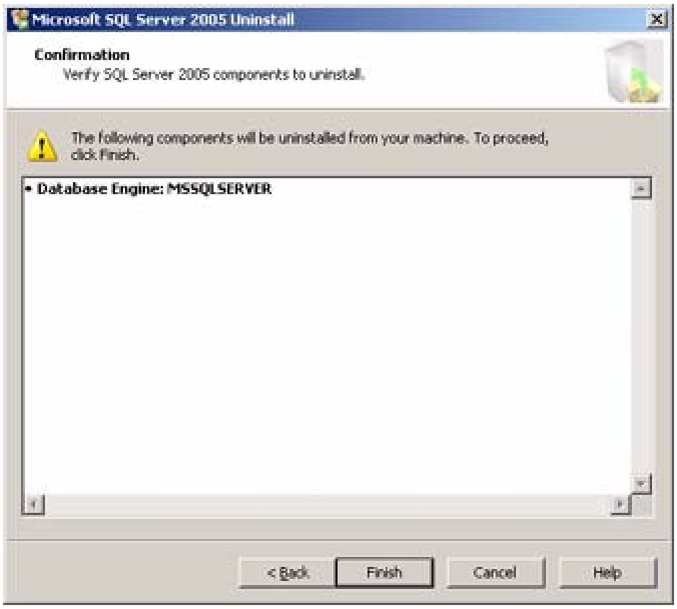
○ MSSQLSERVER: Database Engine

Remove SQL Server 2005 common components

No common components have been installed.

4. The next window will display a summary of the components that will be removed. Click the **Finish** button to proceed. Click **Back** in case you wish to change any of the information.

Figure 8: displays the summary screen for the components that need to be uninstalled



Microsoft SQL Server 2005 Uninstall

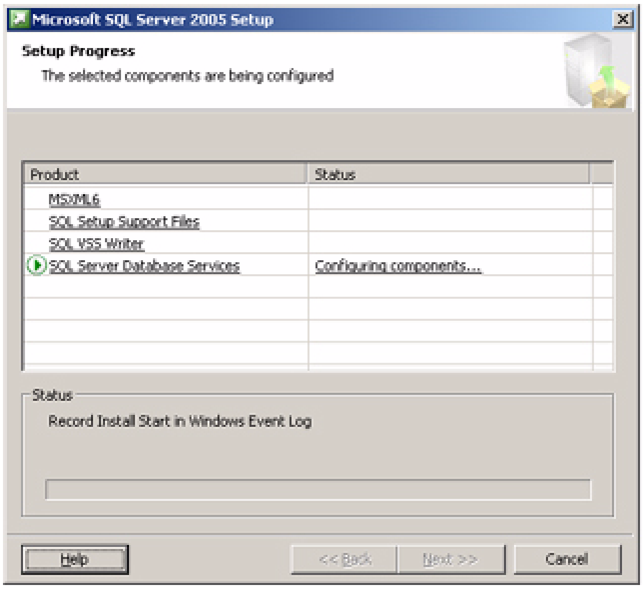
Confirmation
Verify SQL Server 2005 components to uninstall.

The following components will be uninstalled from your machine. To proceed, click Finish.

- **Database Engine: MSSQLSERVER**

5. In the next window, the status will be displayed for the components removal. Click **Finish** once all the components have been removed.

Figure 9: displays the setup progress



Microsoft SQL Server 2005 Setup

Setup Progress

The selected components are being configured

Product	Status
MSXML6	
SQL Setup Support Files	
SQL VSS Writer	
SQL Server Database Services	Configuring components...

Status

Record Install Start in Windows Event Log

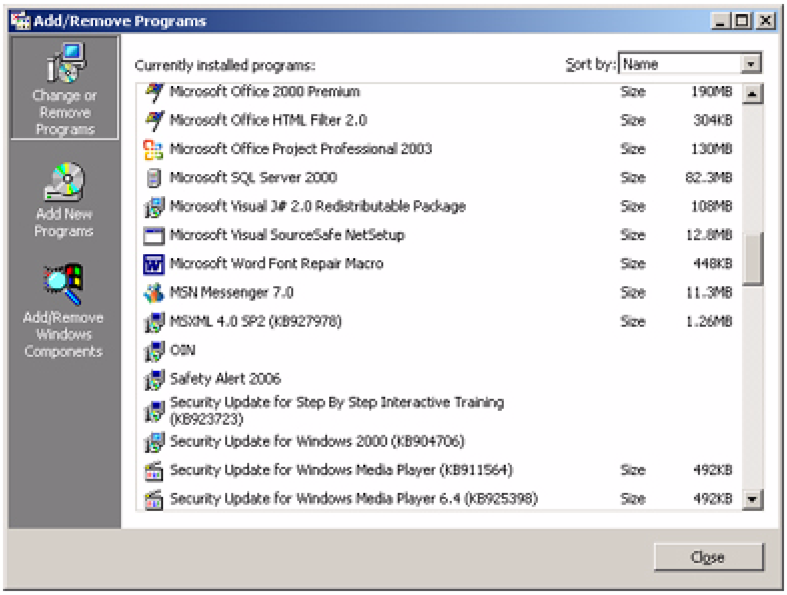
6. Once you have uninstalled MS SQL Server, you must delete the databases on the following location,
C:\DBdata\

Uninstalling BDE Utility

The following steps are followed in order to uninstall BDE Utility,

1. Go to *Start* > *Settings* > *Control Panel* > *Add/Remove Programs*.

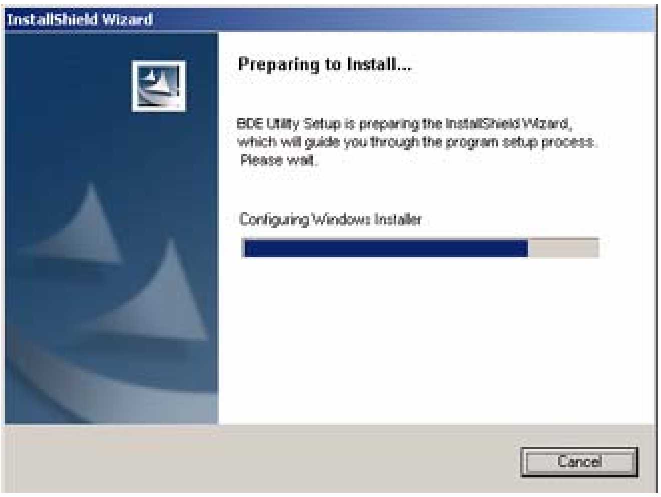
Figure 10: displays the Add/Remove Programs window


Add/Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Currently installed programs:
Sort by: Name
Close

Microsoft Office 2000 Premium	Size	190MB
Microsoft Office HTML Filter 2.0	Size	304KB
Microsoft Office Project Professional 2003	Size	130MB
Microsoft SQL Server 2000	Size	82.3MB
Microsoft Visual J# 2.0 Redistributable Package	Size	108MB
Microsoft Visual SourceSafe NetSetup	Size	12.8MB
Microsoft Word Font Repair Macro	Size	448KB
MSN Messenger 7.0	Size	11.3MB
MSXML 4.0 SP2 (KB927978)	Size	1.26MB
OIN		
Safety Alert 2006		
Security Update for Step By Step Interactive Training (KB923723)		
Security Update for Windows 2000 (KB904706)		
Security Update for Windows Media Player (KB911564)	Size	492KB
Security Update for Windows Media Player 6.4 (KB925398)	Size	492KB

2. Select BDE Utility from the list of Programs. Click **Remove**.
3. The next window that is displayed will show the status of the wizard while the files are being prepared to uninstall BDE.

Figure 11: displays the Preparing to Install screen



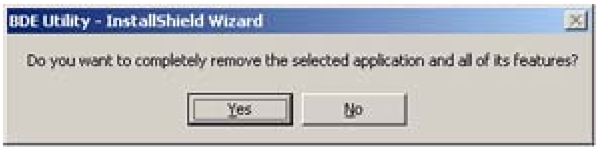
Preparing to Install...

BDE Utility Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.

Configuring Windows Installer

4. The next message box will confirm whether you wish to remove BDE or not. Click **OK** to continue.

Figure 12: displays the message box to confirm whether all features of the BDE Utility need to removed or not

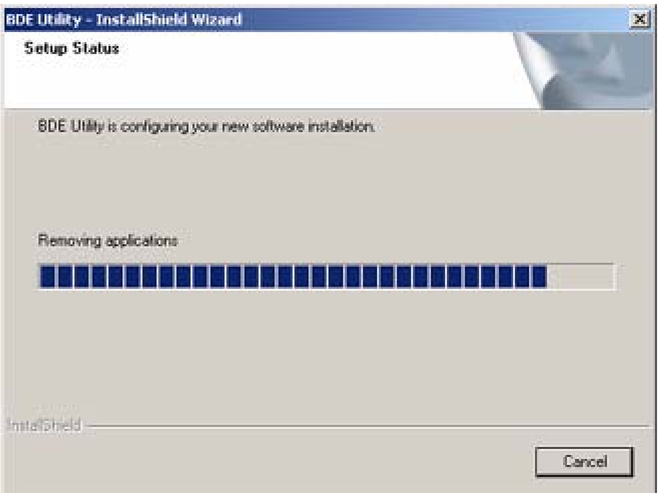


BDE Utility - InstallShield Wizard

Do you want to completely remove the selected application and all of its features?

5. The next window will display the setup status and the progress for the features removed.

Figure 13: displays the setup status for the uninstallation of the application



BDE Utility - InstallShield Wizard

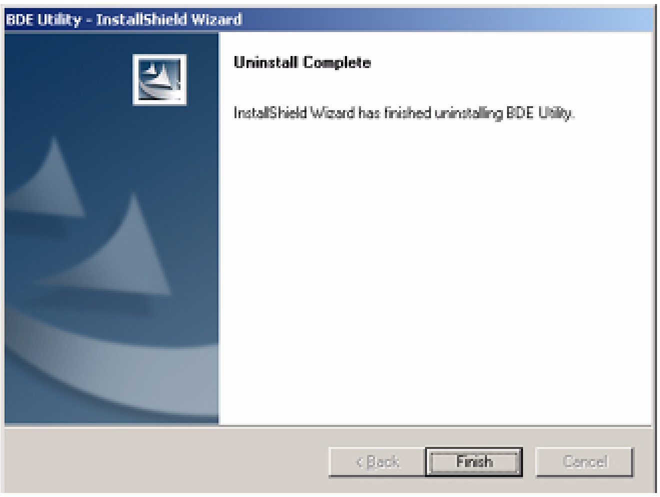
Setup Status

BDE Utility is configuring your new software installation.

Removing applications

6. Once the BDE Utility has been removed the following screen will appear.

Figure 14: displays the screen that shows that the removal of BDE Utility is complete



BDE Utility - InstallShield Wizard

Uninstall Complete

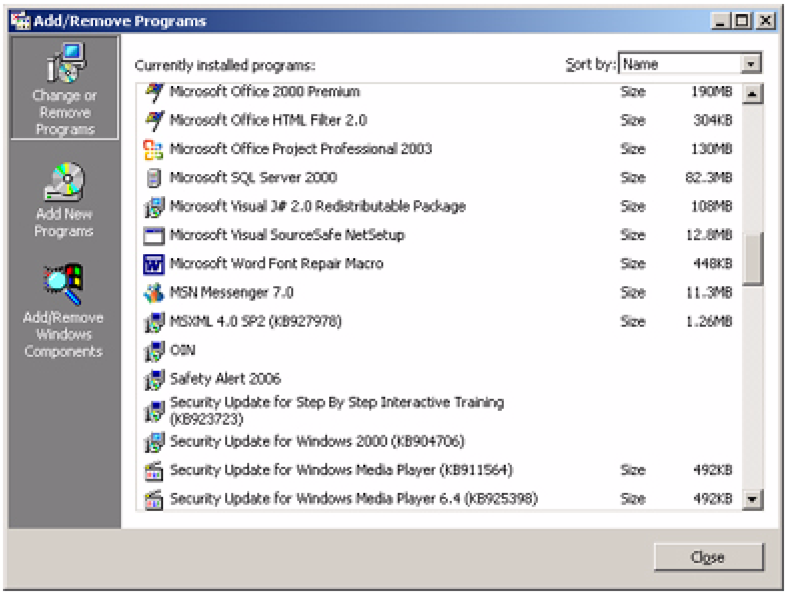
InstallShield Wizard has finished uninstalling BDE Utility.

Uninstalling .NET Framework

The following steps are followed in order to uninstall .NET Framework,

1. Go to *Start* > *Settings* > *Control Panel* > *Add/Remove Programs*.

Figure 15: displays the Add/Remove Programs window

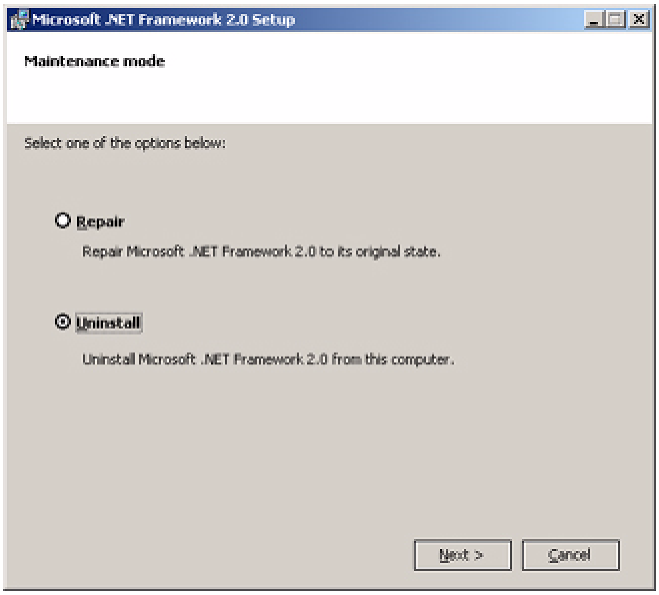


Currently installed programs:

Microsoft Office 2000 Premium	Size	190MB
Microsoft Office HTML Filter 2.0	Size	304KB
Microsoft Office Project Professional 2003	Size	130MB
Microsoft SQL Server 2000	Size	82.3MB
Microsoft Visual J# 2.0 Redistributable Package	Size	108MB
Microsoft Visual SourceSafe NetSetup	Size	12.8MB
Microsoft Word Font Repair Macro	Size	448KB
MSN Messenger 7.0	Size	11.3MB
MSXML 4.0 SP2 (KB927978)	Size	1.26MB
OIN		
Safety Alert 2006		
Security Update for Step By Step Interactive Training (KB923723)		
Security Update for Windows 2000 (KB904706)		
Security Update for Windows Media Player (KB911564)	Size	492KB
Security Update for Windows Media Player 6.4 (KB925398)	Size	492KB

2. Select Microsoft .NET Framework 2.0 from the list of Programs. Click **Remove**.
3. The next window provides you with the option to either repair the installed files or uninstall .NET Framework.

Figure 16: displays the option to either repair or uninstall .NET Framework



Maintenance mode

Select one of the options below:

○ Repair

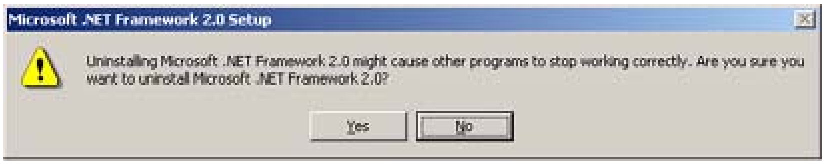
Repair Microsoft .NET Framework 2.0 to its original state.

● Uninstall

Uninstall Microsoft .NET Framework 2.0 from this computer.

4. The next message box will appear confirming if you would like to remove .NET Framework. Click **OK**.

Figure 17: displays the message box to confirm whether you wish to remove .NET Framework or not

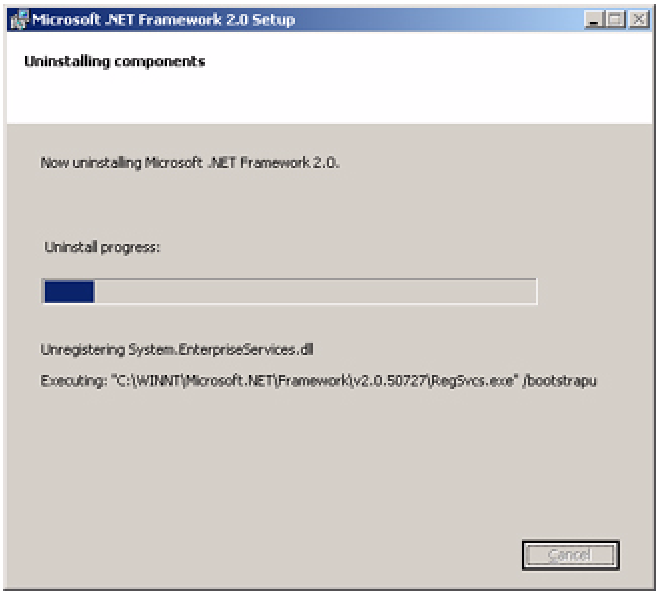


Microsoft .NET Framework 2.0 Setup

Uninstalling Microsoft .NET Framework 2.0 might cause other programs to stop working correctly. Are you sure you want to uninstall Microsoft .NET Framework 2.0?

5. The next window will display the setup progress of the components being removed.

Figure 18: displays the setup progress for the uninstallation of .NET Framework



Microsoft .NET Framework 2.0 Setup

Uninstalling components

Now uninstalling Microsoft .NET Framework 2.0.

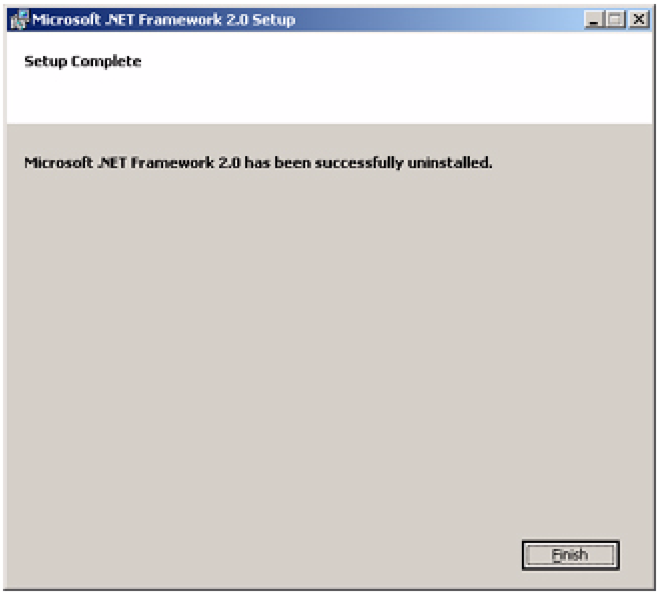
Uninstall progress:

Unregistering System.EnterpriseServices.dll

Executing: "C:\WINNT\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe" /bootstrapu

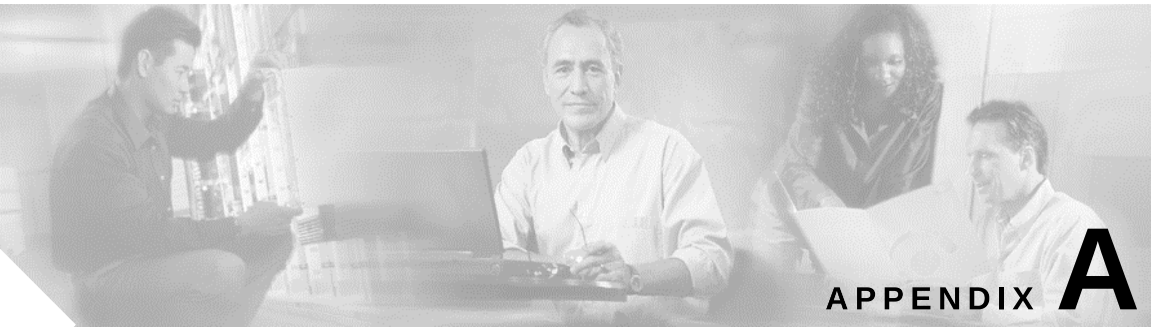
6. The next window will display that the components have been uninstalled successfully.Click **Finish**.

Figure 19: displays the message that the .NET Framework components have been removed successfully



Setup Complete

Microsoft .NET Framework 2.0 has been successfully uninstalled.



APPENDIX A

Creating the Attendant Applications End User for CallManager 4.3

An **End User** is required within CallManager to allow Cisco Unified Attendant applications to communicate with the CallManager via TSP. This user is created in order to,

- Access AXL API
- All CTI related functionalities

The end user profile that is created here is later used to connect to CCM through Cisco Unified Attendant Admin. This end user profile provides you enough roles and privileges to modify or synchronize information. These roles have been explained in the following sections.

Creation of a user involves the following steps,

1. Setting up an End User
2. Creating a User Group with the correct *roles* associated
3. Associating the user with the user group.
4.

These steps have been explained in detail in the following sections.

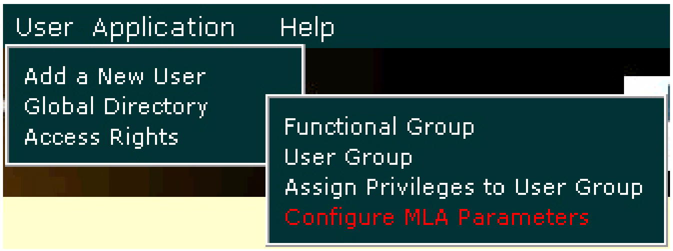
Note If you are using Active Directory to Synchronize with the CallManager, the End User profile must exist in AD.

Assigning Access Rights

In order to assign access rights required to create new End User, you must log into Cisco Unified CallManager 4.3. Enable MultiLevelAdmin as instructed below,

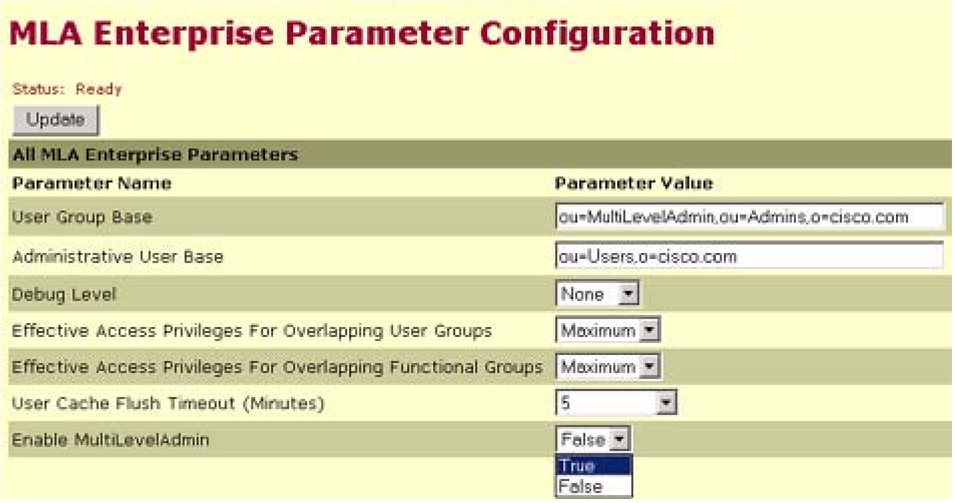
1. Go to *User > Access Rights > Configure MLA Parameters*.

Figure 1: displays the menu to configure Access Rights option



2. From the *Enable MultiLevelAdmin* dropdown list, select *True*.

Figure 2: displays the configuration for MLA



MLA Enterprise Parameter Configuration

Status: Ready

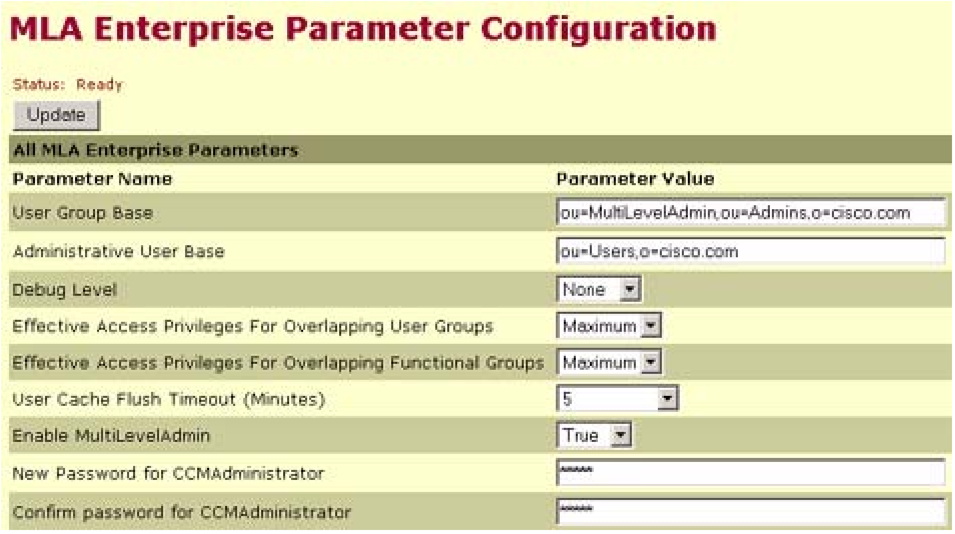
Update

All MLA Enterprise Parameters

Parameter Name	Parameter Value
User Group Base	ou=MultiLevelAdmin,ou=Admins,o=cisco.com
Administrative User Base	ou=Users,o=cisco.com
Debug Level	None
Effective Access Privileges For Overlapping User Groups	Maximum
Effective Access Privileges For Overlapping Functional Groups	Maximum
User Cache Flush Timeout (Minutes)	5
Enable MultiLevelAdmin	False True False

Two new fields, *New password for CCMAdministrator* and *Confirm password for CCMAdministrator*, will appear on the same page, as shown in the image below,

Figure 3: displays the new fields to set new CCM Administrator password



MLA Enterprise Parameter Configuration

Status: Ready

Update

All MLA Enterprise Parameters

Parameter Name	Parameter Value
User Group Base	ou=MultiLevelAdmin,ou=Admins,o=cisco.com
Administrative User Base	ou=Users,o=cisco.com
Debug Level	None
Effective Access Privileges For Overlapping User Groups	Maximum
Effective Access Privileges For Overlapping Functional Groups	Maximum
User Cache Flush Timeout (Minutes)	5
Enable MultiLevelAdmin	True
New Password for CCMAdministrator	******
Confirm password for CCMAdministrator	******

3. Enter password in *New password for CCMAdministrator* field.
4. Re-enter to confirm the password in *Confirm password for CCMAdministrator* field.
5. Click **Update**.

Once the password has been set, you must restart Cisco Unified CallManager and log in with CCMAdministrator login using the new password set in the procedure mentioned above.

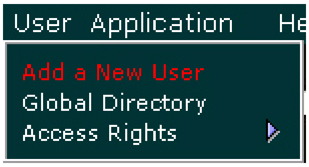
Setting Up an End User

Once you have logged in as CCMAdministrator, you must follow these steps,

From CUCM Administration,

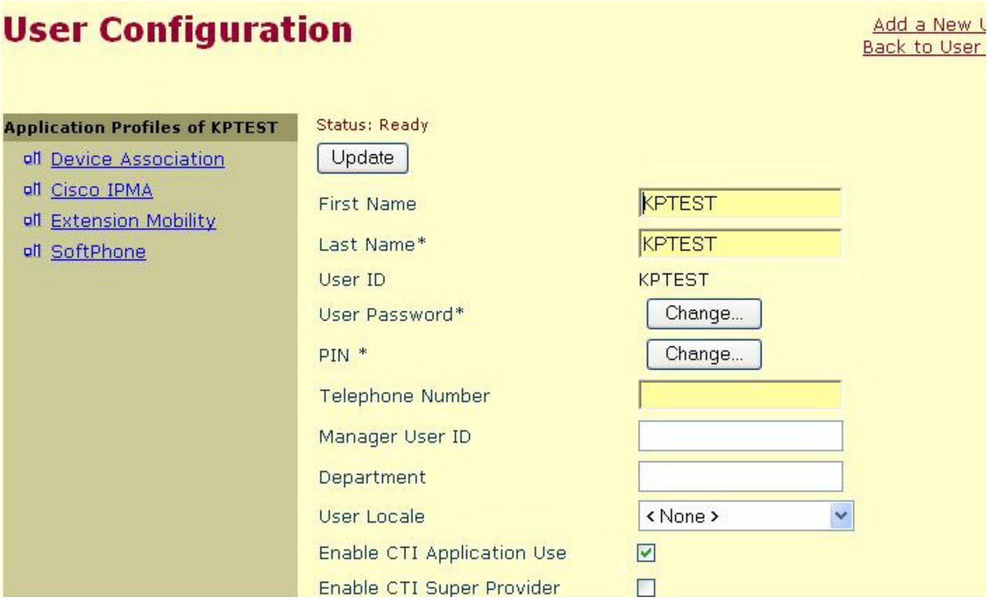
1. Choose *User > Add a New User.*

Figure 4: displays the menu used to create a new user



2. Enter information in the following fields. Please note that the fields mentioned below are mandatory.
   a. Last Name
   b. User ID
   c. User Password
   d. Confirm Password
   e. PIN
   f. Confirm PIN
   g. Enable CTI Application Use

Figure 5: displays the user configuration for End User



Status: Ready

First Name	KPTEST
Last Name*	KPTEST
User ID	KPTEST
User Password*	Change...
PIN *	Change...
Telephone Number	
Manager User ID	
Department	
User Locale	< None >
Enable CTI Application Use	☑
Enable CTI Super Provider	□

3. Click **Insert**.

Assigning the End User to SuperUserGroup

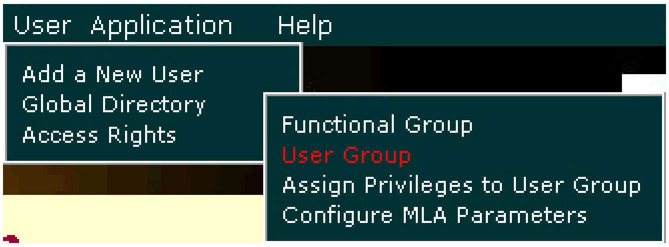
The SuperUserGroup represents a named user group that always has full access permission to all named roles. You cannot delete this user group. You can only make additions and deletions of users to this group.

After you have added the user to the newly created group, you must also add this user to the SuperUserGroup.

To add the user to SuperUserGroup,

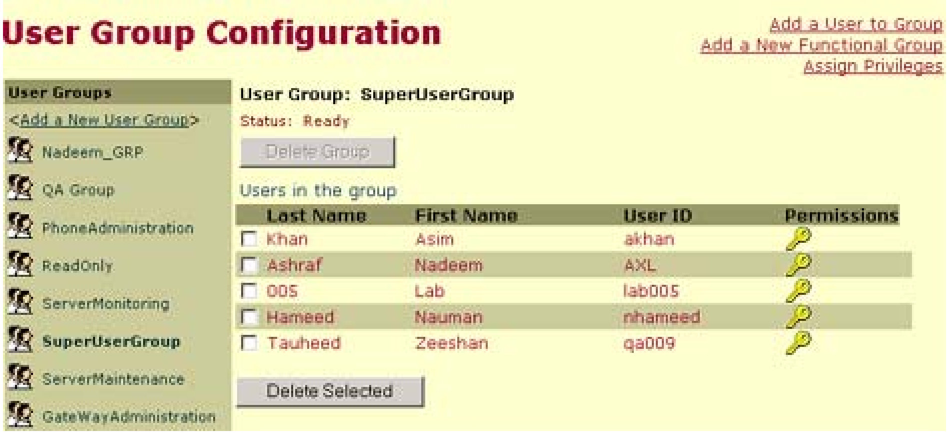
1. Choose *User* > *Access Rights* > *User Group*.

Figure 6: displays the menu for User Group



2. On the *User Group Configuration* page, select **SuperUserGroup** from the User Groups list.

Figure 7: displays the User Group Configuration page for SuperUserGroup



User Group Configuration

User Group: SuperUserGroup

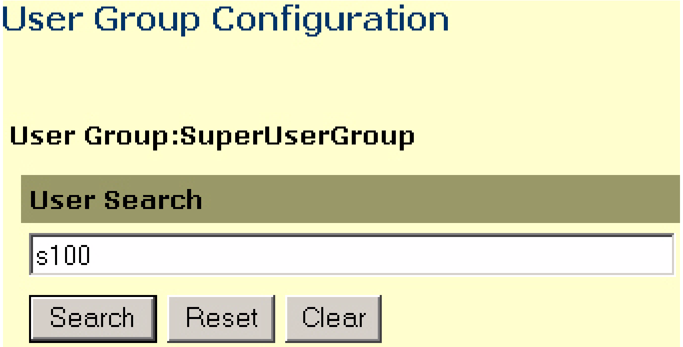
Status: Ready

Users in the group

	Last Name	First Name	User ID	Permissions
□	Khan	Asim	akhan	🔑
□	Ashraf	Nadeem	AXL	🔑
□	005	Lab	lab005	🔑
□	Hameed	Nauman	nhameed	🔑
□	Tauheed	Zeeshan	qa009	🔑

3. Click **Add a User to Group**.
4. On the next page search for the user you created in the previous section

Figure 8: displays the search option to find the newly created user



User Group Configuration

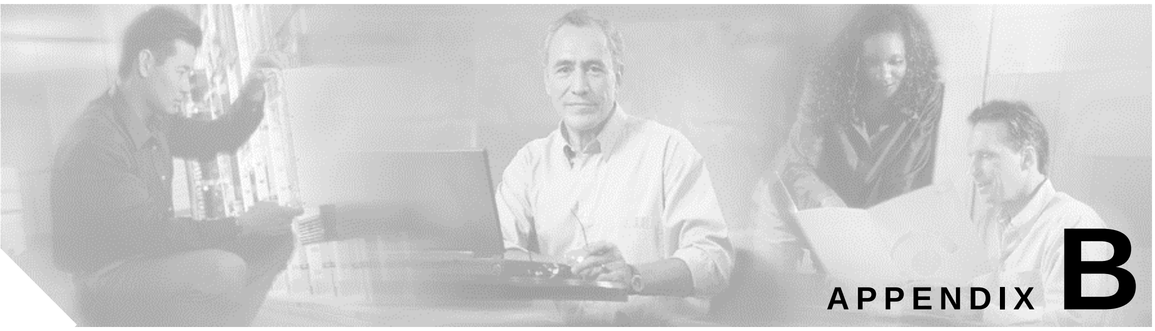
User Group:SuperUserGroup

User Search

s100

5. From the Search Result, select the user and click **Add Selected**.

The user will be added to the SuperUserGroup successfully.



APPENDIX B

Creating the Attendant Application End User for CallManager 5.x/6.x/7.x

An **End User** is required within CUCM to allow Cisco Unified Attendant applications to communicate with the CallManager via TSP. This user is created in order to,

- Access AXL API
- All CTI related functionalities

The end user profile that is created here is later used to connect to CCM through Cisco Unified Attendant Admin. This end user profile provides you enough roles and privileges to modify or synchronize information. These roles have been explained in the following sections.

Creation of a user involves the following steps,

1. Setting up an End User
2. Creating a User Group with the correct *roles* associated
3. Associating the user with the user group.

These steps have been explained in detail in the following sections.

Note If you are using Active Directory to Synchronize with the CallManager, the End User profile must exist in AD.

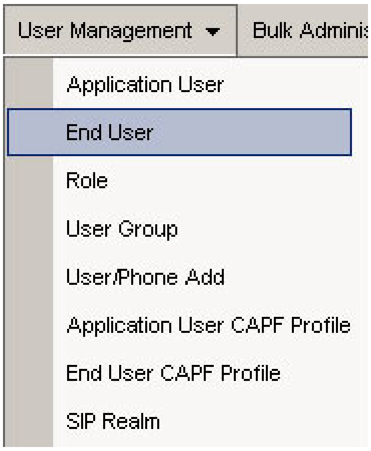
Setting Up an End User

To set up a new End User, you must follow these steps,

From CUCM Administration,

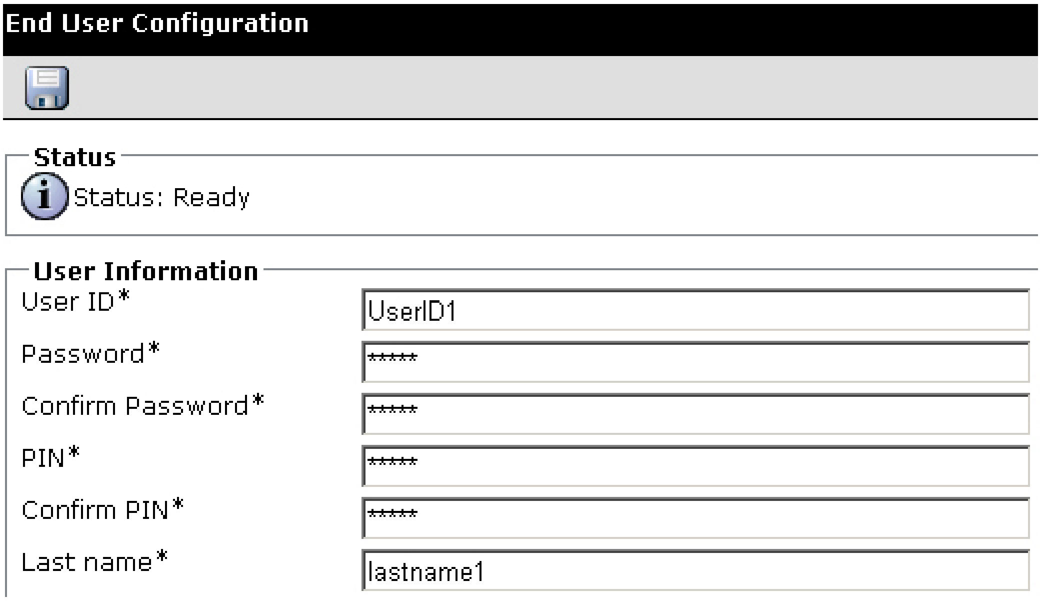
1. Choose *User Management > End User.*

Figure 1: displays menu option for End User configuration



2. Click the ✚ button to add a new user.
3. Enter information in the following fields. Please note that the fields mentioned below are mandatory.
   a. User ID
   b. Password
   c. Confirm Password
   d. PIN
   e. Confirm PIN
   f. Last Name

Figure 2: displays the End User Configuration page



End User Configuration

Status

Status: Ready

User Information

User ID*	UserID1
Password*	*****
Confirm Password*	*****
PIN*	*****
Confirm PIN*	*****
Last name*	lastname1

4. Click 💾 **Save** to save the settings for newly created user.

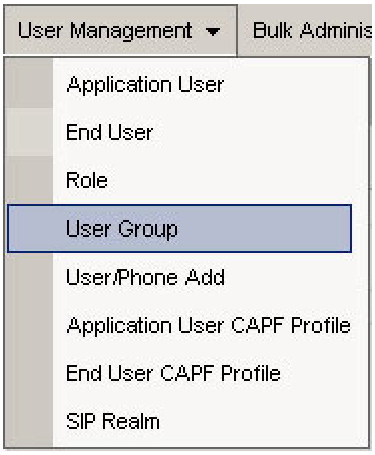
Creating a User Group

Once the user is created, in order to associate it with a group, a new group must also be configured. The User Group will then have Roles assigned to it which govern what can be done using this profile.

To create a new user group,

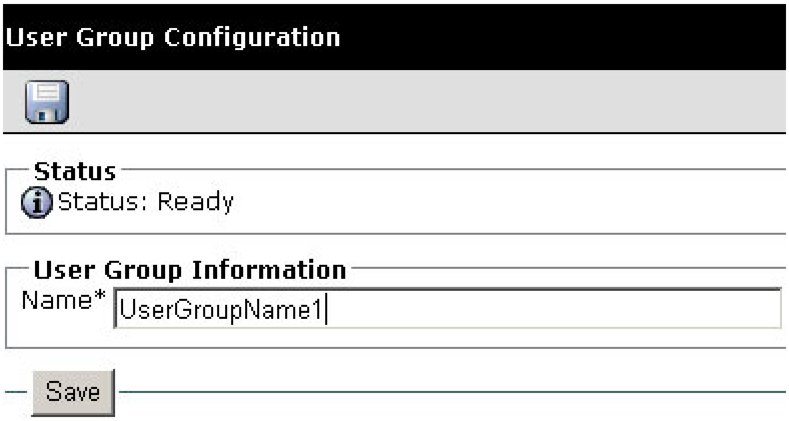
1. Choose *User Management* > *User Groups*.

Figure 3: displays the menu option for User Group



2. Click the ➕ button to add a new user group.
3. Enter *Name* for the new user group.

Figure 4: displays the User Group Configuration page



User Group Configuration

Status

Status: Ready

User Group Information

Name* UserGroupName1

Save

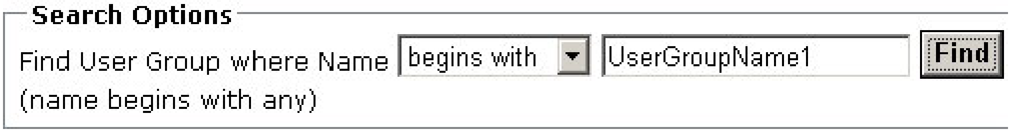
4. Click 💾 **Save** to save the settings for newly created user group.

Assigning Roles and User to the User Group

To assign roles to the newly created user group,

1. Choose *Back To Find/List* > *Go* or *User Management* > *User Groups*.
2. On *Find and List User Groups* page, search for the user group you created.

Figure 5: displays the field you may use to search a user group



Search Options

Find User Group where Name [begins with ▾] [UserGroupName1] [Find]

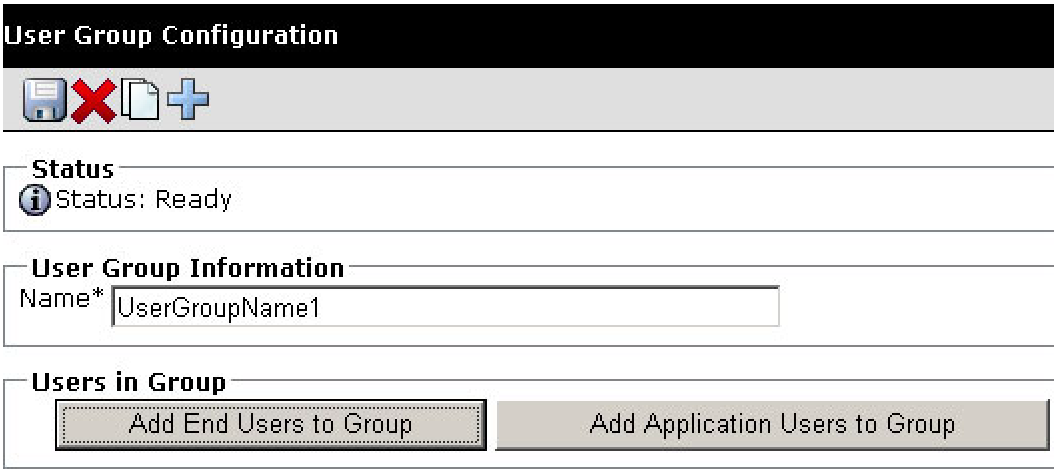
(name begins with any)

3. In the *Search Results*, click on the *Roles* link ⓘ for the user group.
4. Click **Assign Role to Group** to find and list roles for assignment.
5. Select the roles that need to be assigned to this group. The following checkboxes must be selected,
   a. *Standard CTI Allow Car Park Monitoring*
   b. *Standard CTI Allow Calling Number Modification*
   c. *Standard CTI Allow Control of All Devices*
   d. *Standard CTI Allow Reception of SRTP Key Material*
   e. *Standard CTI Enabled*
6. Click **Add Selected** to assign roles.
7. Click **Save**.

To add the End User to the User Group,

1. Choose *User Management > User Groups*.
2. Click the newly created User Group.
3. Click **Add End Users to the Group** to find and list the users.

Figure 6: displays the User Group Configuration page



User Group Configuration

Status

ⓘ Status: Ready

User Group Information

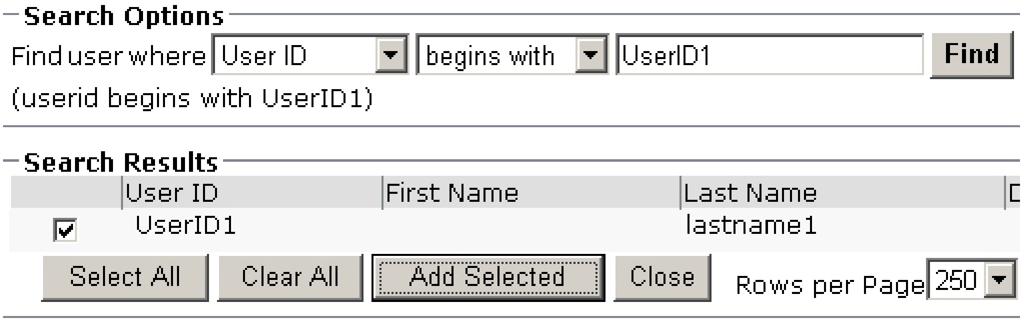
Name* [UserGroupName1]

Users in Group

[Add End Users to Group] [Add Application Users to Group]

4. Select the newly created End user from the list and click **Add Selected** to successfully add the user to the group.

Figure 7: displays the search field you may use to search for a User ID



Search Options

Find user where User ID ▾ begins with ▾ UserID1

(userid begins with UserID1)

Search Results

	User ID	First Name	Last Name	D
☑	UserID1		lastname1	

Rows per Page 250 ▾

Adding End User to Standard CCM Super Users group

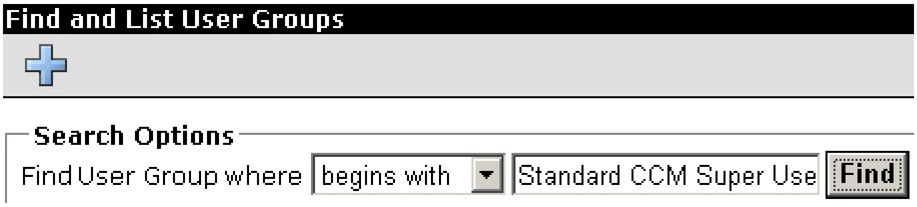
The standard CCM Super Users user group represents a named user group that always has full access permission to all named roles. You cannot delete this user group. You can only make additions and deletions of users to this group.

After you have added the user to the newly created group, you must also add this user to the Standard CCM Super User group.

To add the user to Standard Super CCM User,

1. Choose *User Management > User Groups*.
2. Find **Standard Super CCM User** using the search field.

Figure 8: displays the search option you may use to find and list user group



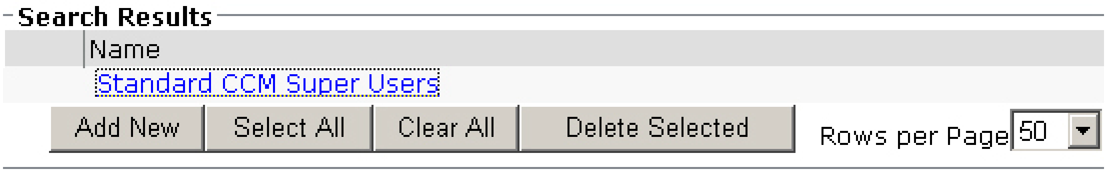
Find and List User Groups

Search Options

Find User Group where begins with ▾ Standard CCM Super Use

3. In the Search Results, Click *Standard Super CCM Users*.

Figure 9: displays the search result for the user group



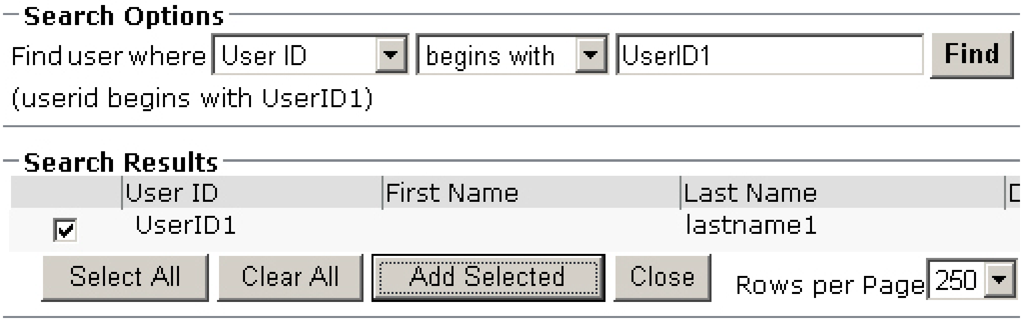
Search Results

	Name
	Standard CCM Super Users

Rows per Page 50 ▾

4. Click **Add End Users to the Group** to find and list the users.
5. Select the newly created End user from the list and click **Add Selected** to successfully add the user to this group.

Figure 10: displays the selected search result that is to be added to the user group



Search Options

Find user where User ID ▼ begins with ▼ UserID1 Find

(userid begins with UserID1)

Search Results

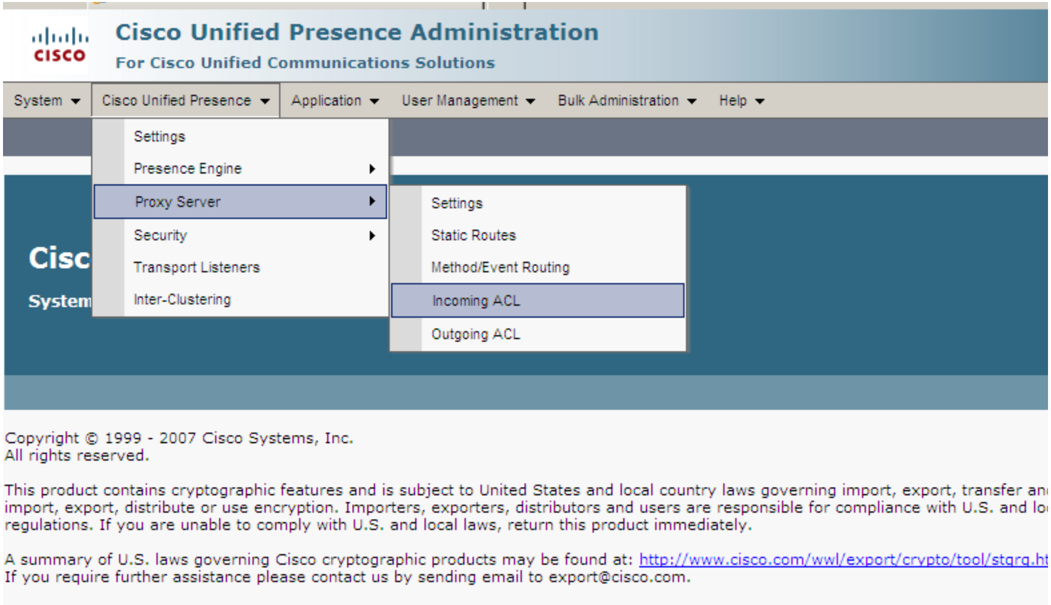
	User ID	First Name	Last Name	D
☑	UserID1		lastname1	

Configuring Access for the Cisco Unified Attendant CUPS Plug-In

It is important that the Cisco Unified Attendant CUPs Plug-in Address is added to the firewall information on the CallManager.

To do this go to Cisco Unified Presence menu, and select Proxy Server and Incoming ACL (access control list)

Figure 11: displays accessing the Cisco Unified Presence Proxy Server, Incoming ACL menu.



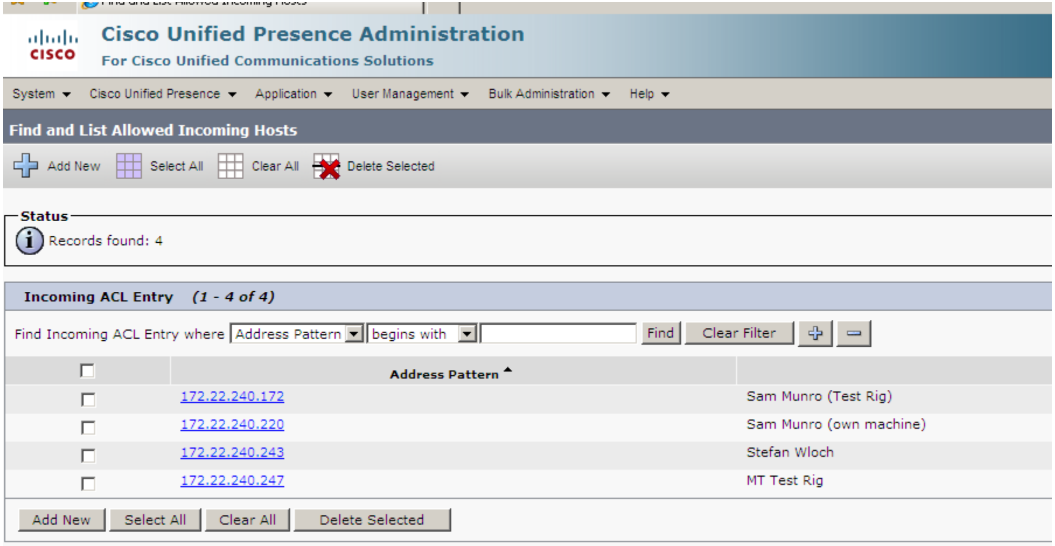
Copyright © 1999 - 2007 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer an import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and lo regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.ht
If you require further assistance please contact us by sending email to export@cisco.com.

The page ***Find and List Allowed Incoming Hosts*** will be displayed.

Figure 12; Displays Find and List Allowed Incoming Hosts page



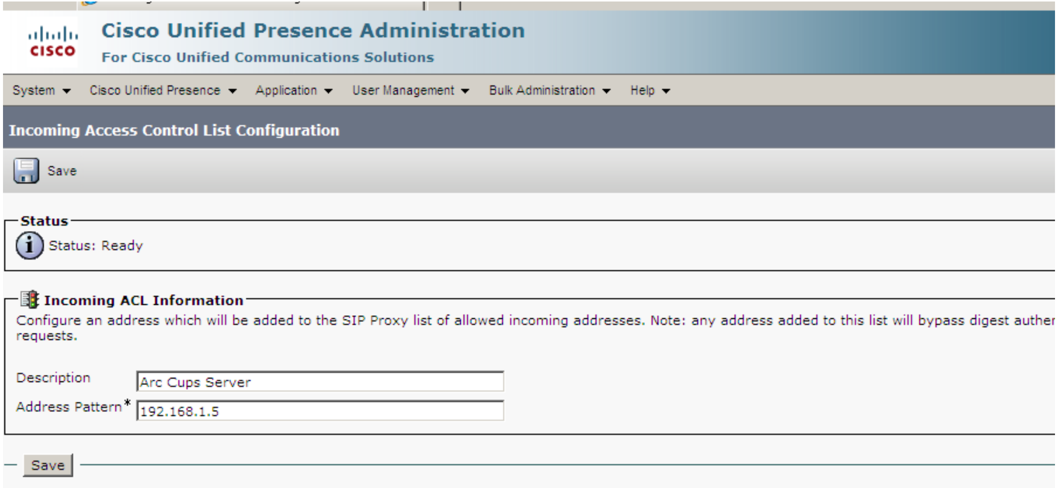
Records found: 4

Find Incoming ACL Entry where Address Pattern begins with

□	Address Pattern	
□	172.22.240.172	Sam Munro (Test Rig)
□	172.22.240.220	Sam Munro (own machine)
□	172.22.240.243	Stefan Wloch
□	172.22.240.247	MT Test Rig

Click on **Add New** and enter the **Description** and **Address Pattern**.

Figure 13: displays Incoming Access Control List Configuration page


Cisco Unified Presence Administration
For Cisco Unified Communications Solutions
System
Cisco Unified Presence
Application
User Management
Bulk Administration
Help
Incoming Access Control List Configuration
Save
Status
Incoming ACL Information
Save

Status: Ready

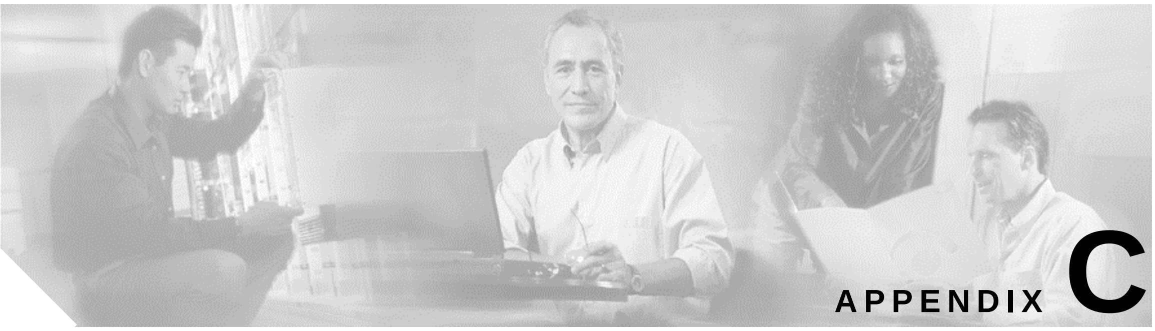
Configure an address which will be added to the SIP Proxy list of allowed incoming addresses. Note: any address added to this list will bypass digest auther requests.

Description: Arc Cups Server

Address Pattern*: 192.168.1.5

Click on **Save**.

Confirm the address and description have been added.



APPENDIX C

TAPI Configuration

You must install Cisco Telephony Service Provider (TSP) on the machine that will run the Cisco Unified Attendant Server. This allows the Server to communicate with CUCM's CTI Manager service to allow call control on all devices associated to the End User profile created for the Server.

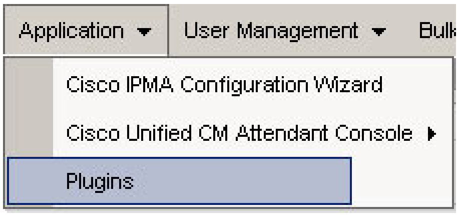
Installing the TAPI TSP

To install the Cisco TSP you must follow the steps mentioned below.

The installation of the Cisco Unified Attendant Console will download the TSP installation file to the Desktop of the server machine. To download manually follow steps 1-4 below.
On the Server machine browse to CUCM Administration,

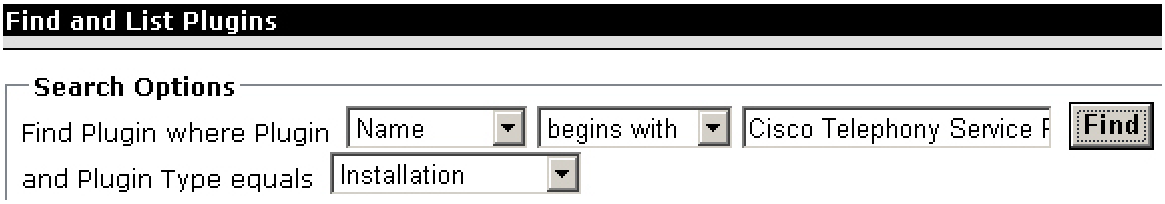
1. Select *Application > Plugins*.

Figure 1: displays the menu option for plugins


Application
User Management
Bulk
Cisco IPMA Configuration Wizard
Cisco Unified CM Attendant Console
Plugins

2. Find Cisco Telephony Service Provider using the search field.

Figure 2: displays the search option to find and list the required plugin


Find and List Plugins

Search Options

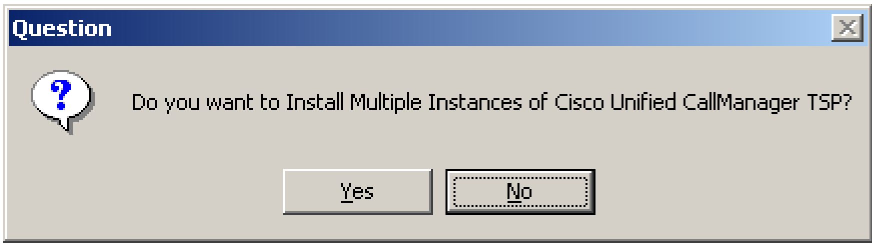
Find Plugin where Plugin: Name, begins with, Cisco Telephony Service F

and Plugin Type equals: Installation

3. In the Search Results, click Download on the Cisco Telephony Service Provider line.

4. Save **CiscoTSP.exe** on your desktop.
5. Double Click the **CiscoTSP.exe** icon on the desktop and follow the on screen instructions to complete the install.
6. During the installation, you will be asked if you want to install multiple instances of TSP. Click **No**.

Figure 3: displays the message box confirming whether multiple instances for TSP are to be installed or not



Question

Do you want to Install Multiple Instances of Cisco Unified CallManager TSP?

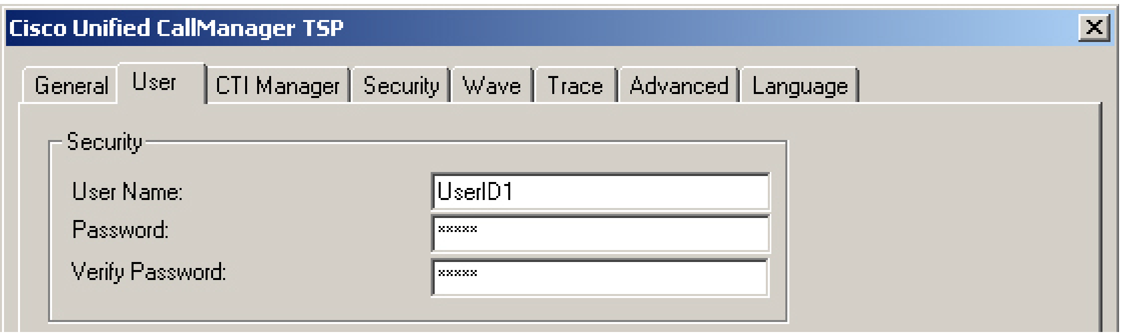
7. After a successful installation the setup will prompt you to restart the system. You must restart the machine for the changes to take effect.

Configuring the TAPI TSP

To configure TSP,

1. Go to *Start* > *Settings* > *Control Panel* > *Phone and Modem Options*.
2. Select *Advanced* tab.
3. Select CiscoTSP001.tsp.
4. Click **Configure**.
5. Enter the End User ID of the user that was created for the CallManager earlier in the *User Name* field.
6. Enter the password of the user in the *Password* field.

Figure 4: displays the End User ID information to be entered in the fields



Cisco Unified CallManager TSP

Security

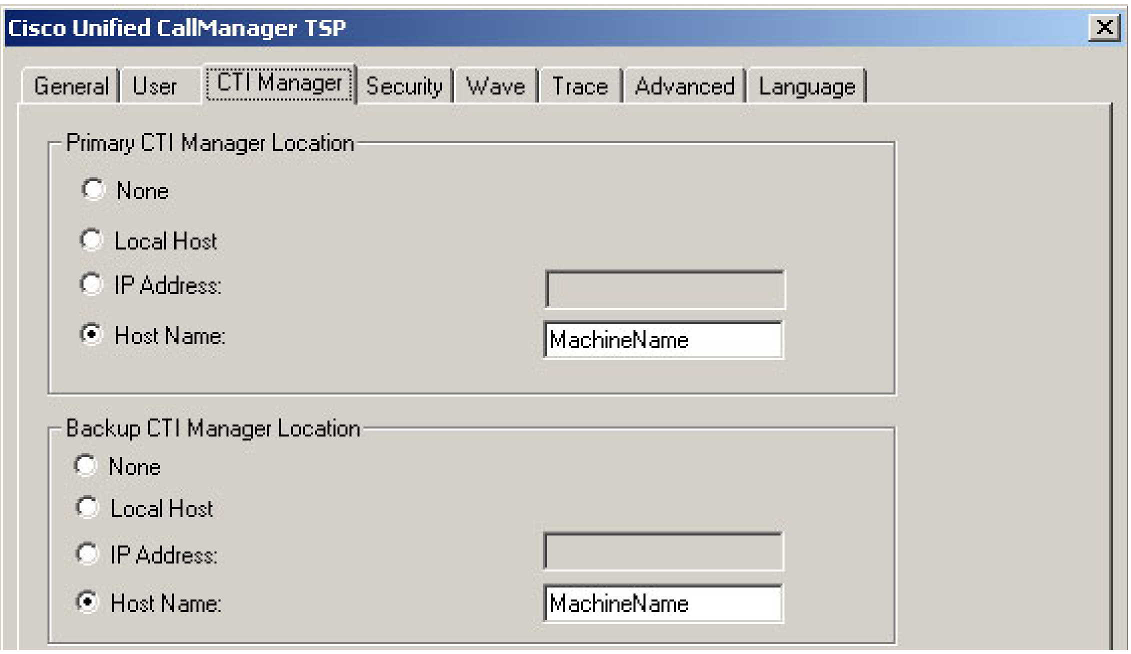
User Name: UserID1

Password: *****

Verify Password: *****

7. Select the *CTI Manager* tab,

Figure 5: displays the CTI Manager information to be entered for the TAPI configuration



Cisco Unified CallManager TSP

Primary CTI Manager Location

○ None

○ Local Host

○ IP Address:

● Host Name: MachineName

Backup CTI Manager Location

○ None

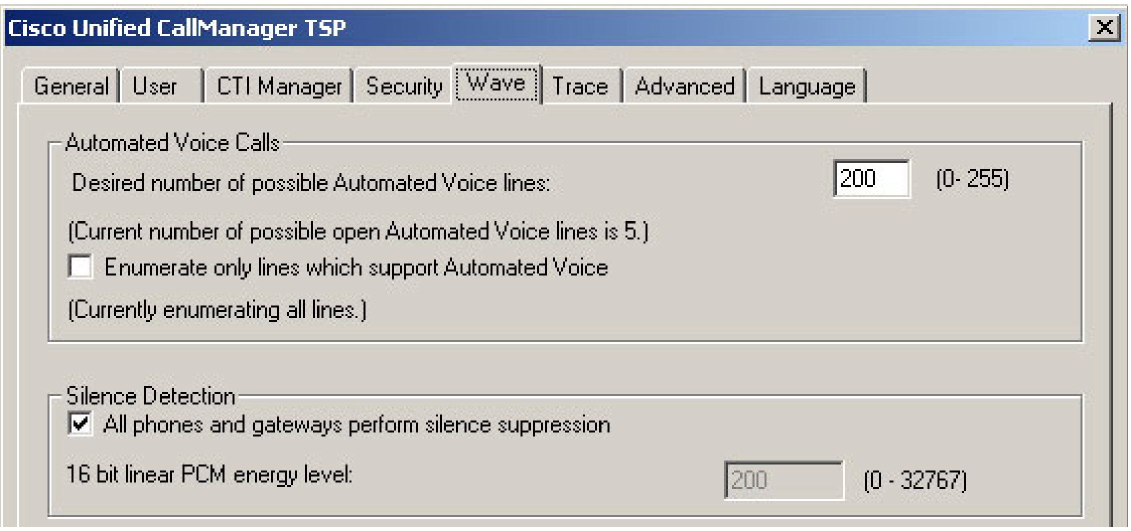
○ Local Host

○ IP Address:

● Host Name: MachineName

8. Enter the *Name* or *IP Address* of the CTI Manager that you require to obtain your TAPI information from. A second CTI Manager can be used for resilience if required and available. **Note** CTI Manager is a service that runs on each of the CUCM Nodes within a cluster. It is recommended that the primary CTI Manager points to the publisher CUCM and the backup on one of those subscriptions.
9. Select the *Wave* tab.
10. Enter the number of desired *Voice Lines*. You must enter a value that will allow all of your CTI Ports being monitored by this TSP in this field. You may want to add a higher figure at this point for future expansion of ports. After completing the TSP configuration you will need to install the *Cisco TAPI WAVE* driver. The instructions on how to do this are included on the Cisco TSP readme file. You will also need to uninstall and reinstall this driver every time you change the figure here.

Figure 6: displays the Wave configuration for TAPI



Cisco Unified CallManager TSP

Automated Voice Calls

Desired number of possible Automated Voice lines: 200 (0- 255)

(Current number of possible open Automated Voice lines is 5.)

□ Enumerate only lines which support Automated Voice

(Currently enumerating all lines.)

Silence Detection

☑ All phones and gateways perform silence suppression

16 bit linear PCM energy level: 200 (0 - 32767)

11. Click **OK**.

12. Select *Advanced* tab.
13. In the Provider Open Completed Timeout (secs) field enter 300.
14. Click **OK**.
15. Reboot the machine.
16. Install the Cisco Tapi Wave driver, using instructions in the Cisco TSP readme file located in C:\Program Files\Cisco\ciscotsp.txt
17. Reboot the server.
    TAPI has now been successfully installed.

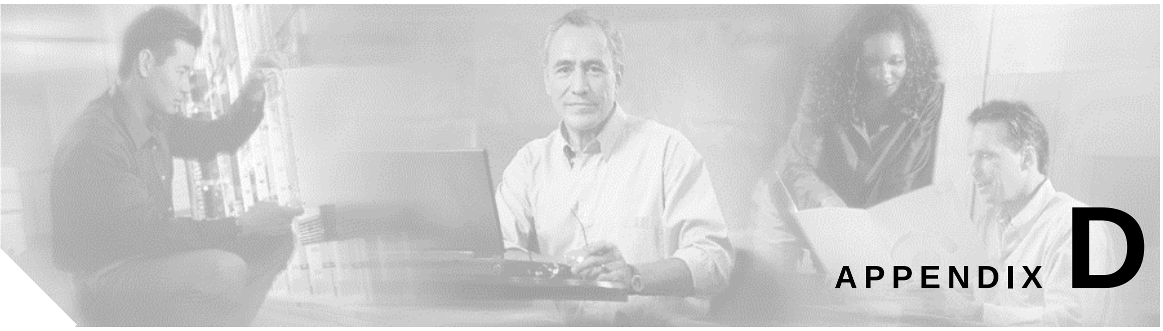
Installing the Cisco TAPI Wave driver

The following instructions are also in the Cisco TSP readme file located in C:\Program Files\Cisco\ciscotsp.txt and relate to installation on a Windows 2003 Server.

1. From Control Panel execute the *Add Hardware* utility. Click the **Next** button.
2. Select **Yes, I have already connected the hardware** Radio button. Click **Next**.
3. Select **Add a new Hardware device** from the list. Click the **Next** button.
4. Select **Install the hardware that I manually select from a list** radio button. Click the **Next** button.
5. Select **Sound, video and game controller** when prompted for hardware type. Click the **Next** button.
6. Click the **Have Disk** button when prompted to **Select a Device Driver**. Click the **Browse** button on the **Install from Disk** window. Browse to ***C:\Program Files\Cisco\Wave Drivers*** and select the file **OEMSETUP**.
7. Click **Open** to install the Cisco Wave Driver and select **OK**.
8. Highlight the **Cisco TAPI Wave Driver** in Select a Device Driver window and select **Next**. Select **Next** in **Start Hardware Installation** window.
9. If Prompted for **Digital signature Not Found** click on **Continue Anyway** button.

When prompted for **Install from disk 1** for file ***avaudio32.dll***, choose **Browse** button and select path *C:\Program Files\Cisco\Wave Drivers* and click **Open** to install the ***avaudio32.dll***.

1. You will be prompted to reboot the server. Do so.
2. TAPI has now been successfully installed.



Downloading, Updating and Registering Software

The following Appendix outlines the process of downloading, updating and licensing the Cisco Unified Attendant Applications. This is done via the Solutions + website.

Updating from an Earlier Version of Cisco Unified Attendant Applications

The Cisco Attendant Console Applications are designed in such a way that to upgrade from an earlier version of the software, you simply run the installation processes as outlined in Chapter 4 of this manual.

As with any software upgrade, it is worth taking a backup prior to the install, incase there is a failure of any sort. In the case of the Cisco Attendant Console Applications it is recommended that you back up the Cisco Folder, backup of DBs and within the Registry the backup of Arcsolutions folder.

Accessing the Solutions + Website

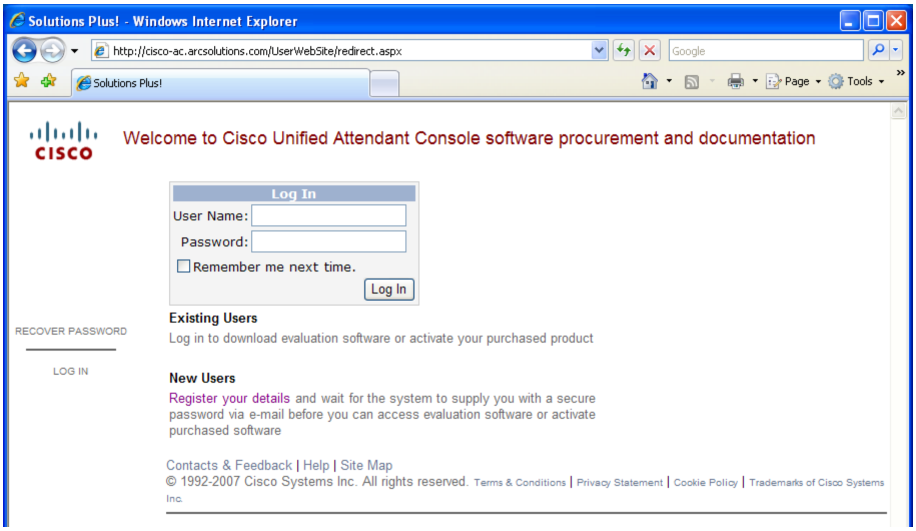
To download or register a version of the Cisco Unified Business/Department Administration Console you will need to have a valid account on the Solutions + Website.

Go the website http://cisco-ac.arcsolutions.com

Note The User Name and Password are NOT your CCO (Cisco Connection Online) ID and Password!

Enter your *User Name* and *Password* to **Log In** to the web site.

Figure 1 Solutions + Log In screen


Solutions Plus! - Windows Internet Explorer
http://cisco-ac.arcsolutions.com/UserWebSite/redirect.aspx
Google
Solutions Plus!
Page
Tools
CISCO
RECOVER PASSWORD
LOG IN

Welcome to Cisco Unified Attendant Console software procurement and documentation

Log In

User Name:

Password:

□ Remember me next time.

Log In

Existing Users

Log in to download evaluation software or activate your purchased product

New Users

Register your details and wait for the system to supply you with a secure password via e-mail before you can access evaluation software or activate purchased software

Contacts & Feedback | Help | Site Map

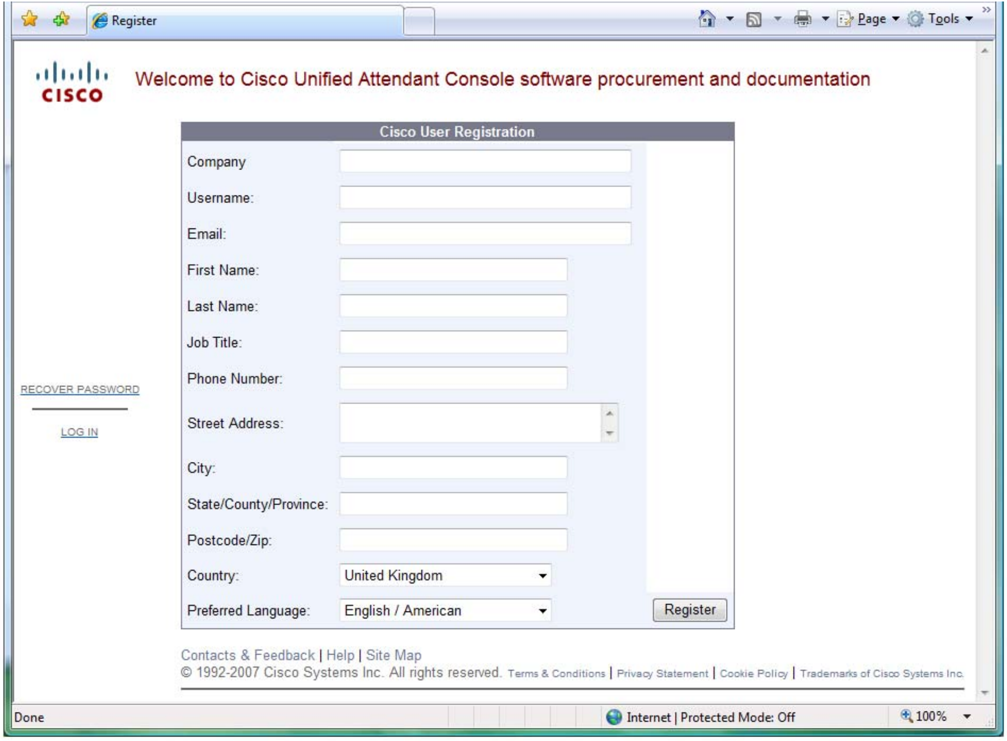
© 1992-2007 Cisco Systems Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems Inc.

Creating an Account

To create an account you will have to click on the link to *Register your details*. This will take you through a series of questions.

When these questions have been answered, click on *Register* to complete.

Figure 1 Cisco User Registration



Welcome to Cisco Unified Attendant Console software procurement and documentation

Cisco User Registration

Company

Username:

Email:

First Name:

Last Name:

Job Title:

Phone Number:

Street Address:

City:

State/County/Province:

Postcode/Zip:

Country: United Kingdom

Preferred Language: English / American

Register

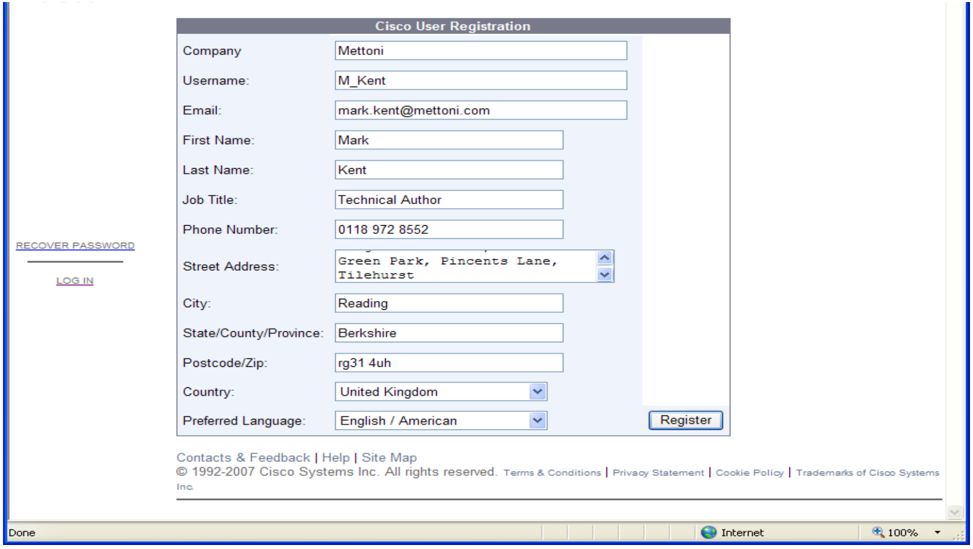
Contacts & Feedback | Help | Site Map

© 1992-2007 Cisco Systems Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems Inc.

After you have clicked on *Register* you will be prompted to confirm your **Reseller** from a drop down selection. Alternatively if your Reseller is not in the drop down selection you can *Add New Reseller.*

Click on *Submit* to complete the registration of this account..

Figure 2 Confirming your Reseller



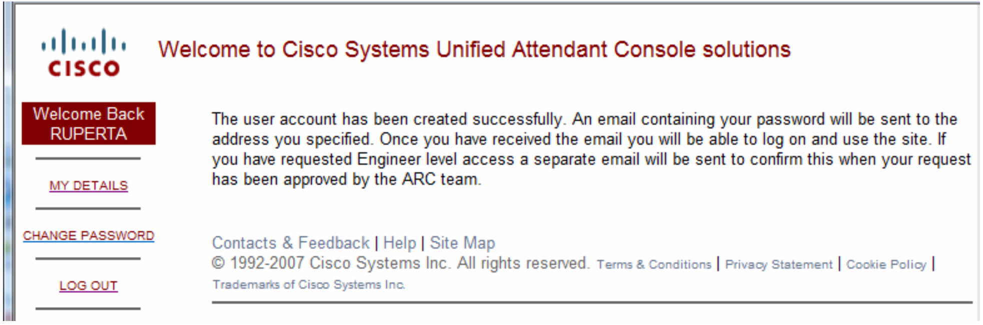
Cisco User Registration

Company	Mettoni
Username:	M_Kent
Email:	mark.kent@mettoni.com
First Name:	Mark
Last Name:	Kent
Job Title:	Technical Author
Phone Number:	0118 972 8552
Street Address:	Green Park, Pincents Lane, Tilehurst
City:	Reading
State/County/Province:	Berkshire
Postcode/Zip:	rg31 4uh
Country:	United Kingdom
Preferred Language:	English / American

Contacts & Feedback | Help | Site Map
© 1992-2007 Cisco Systems Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems Inc.

A confirmation screen will appear and you will then be sent an email containing your password which will enable you to access the website.

Figure 3 Completing the Account creation



Welcome to Cisco Systems Unified Attendant Console solutions

The user account has been created successfully. An email containing your password will be sent to the address you specified. Once you have received the email you will be able to log on and use the site. If you have requested Engineer level access a separate email will be sent to confirm this when your request has been approved by the ARC team.

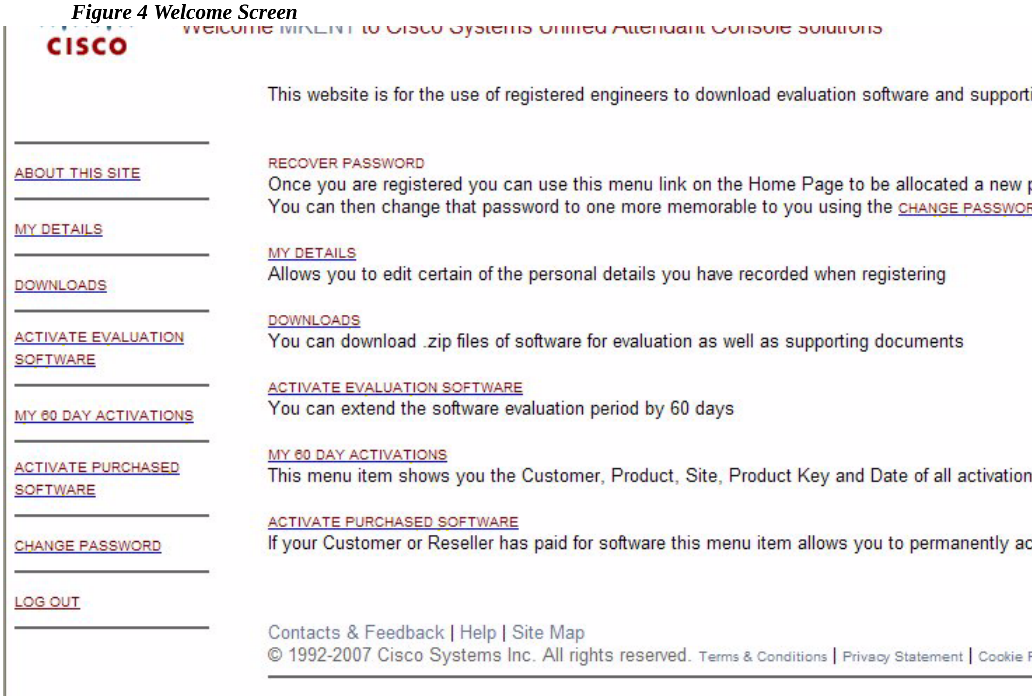
Contacts & Feedback | Help | Site Map
© 1992-2007 Cisco Systems Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems Inc.

Logging into the site

When you log into the account, the initial Welcome screen provides the following options:-

- **About this Site** - Is a link back to this Welcome page when you are in other screens.
- **My Details** - Selecting this will display a page with the information that was requested when you registered the account.
- **Downloads** - Selecting this will display a page with the facility to download the software and other supporting documentation if required.
- **Activate Evaluation Software** - After the inital 5 days the software requires registration. This Evaluation license lasts for 60 days.
- **My 60 Day Evaluations** - Displays all information related to activated software including Customer Name, Product, Site, Product Key and Date.
- **Activate Purchased Software** - Selecting this will provide a screen where you are required to enter the registration details to confirm the purchase and activate the full product license.

Figure 4 Welcome Screen



Welcome MRENT to Cisco Systems Unified Attendant Console solutions

This website is for the use of registered engineers to download evaluation software and supporti

RECOVER PASSWORD
Once you are registered you can use this menu link on the Home Page to be allocated a new p
You can then change that password to one more memorable to you using the CHANGE PASSWOR

MY DETAILS
Allows you to edit certain of the personal details you have recorded when registering

DOWNLOADS
You can download .zip files of software for evaluation as well as supporting documents

ACTIVATE EVALUATION SOFTWARE
You can extend the software evaluation period by 60 days

MY 60 DAY ACTIVATIONS
This menu item shows you the Customer, Product, Site, Product Key and Date of all activation

ACTIVATE PURCHASED SOFTWARE
If your Customer or Reseller has paid for software this menu item allows you to permanently ac

Contacts & Feedback | Help | Site Map
© 1992-2007 Cisco Systems Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie P

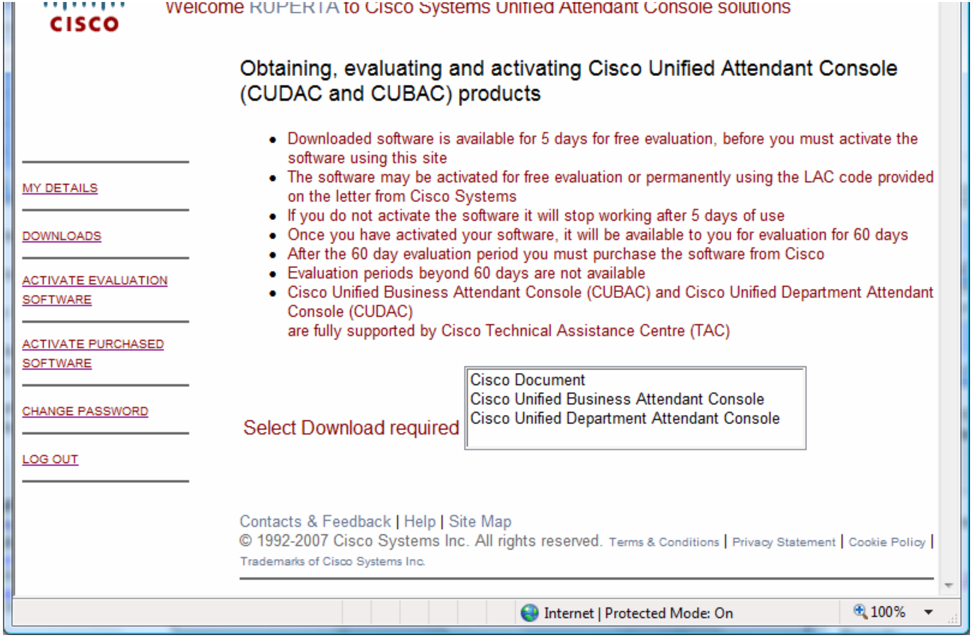
My Details

My details screen provides a summary of the information that was entered when the account was registered. There is facility to *Edit* the **User Details**, but the **User Name** and **Email Address** is read only.

Downloads

Selecting **Downloads** from the right hand menu will present you with information regarding the available downloads, and any criteria or constraints that may impact on the use of the software.

Figure 5 Download Screen



Welcome RUPERTA to Cisco Systems Unified Attendant Console solutions

Obtaining, evaluating and activating Cisco Unified Attendant Console (CUDAC and CUBAC) products

- Downloaded software is available for 5 days for free evaluation, before you must activate the software using this site
- The software may be activated for free evaluation or permanently using the LAC code provided on the letter from Cisco Systems
- If you do not activate the software it will stop working after 5 days of use
- Once you have activated your software, it will be available to you for evaluation for 60 days
- After the 60 day evaluation period you must purchase the software from Cisco
- Evaluation periods beyond 60 days are not available
- Cisco Unified Business Attendant Console (CUBAC) and Cisco Unified Department Attendant Console (CUDAC) are fully supported by Cisco Technical Assistance Centre (TAC)

Select Download required

Cisco Document
Cisco Unified Business Attendant Console
Cisco Unified Department Attendant Console

© 1992-2007 Cisco Systems Inc. All rights reserved.

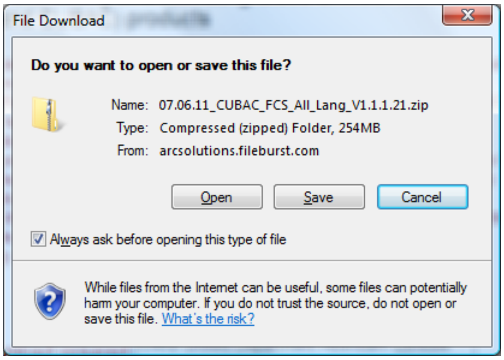
CISCO
MY DETAILS
DOWNLOADS
ACTIVATE EVALUATION SOFTWARE
ACTIVATE PURCHASED SOFTWARE
CHANGE PASSWORD
LOG OUT
Contacts & Feedback | Help | Site Map
Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems Inc.
Internet | Protected Mode: On
100%

When the software required is selected the screen will display the file format and the size of the download.

Click on *Download* to continue.

You will be prompted to *Open* or *Save* the Download. Saving the file to a local area is recommended

Figure 6 File Download prompt to either Open or Save



Do you want to open or save this file?

Name: 07.06.11_CUBAC_FCS_All_Lang_V1.1.1.21.zip
Type: Compressed (zipped) Folder, 254MB
From: arcsolutions.fileburst.com

☑ Always ask before opening this type of file

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Note

The download for CUBAC and CUDAC are around 250mb. The contents include SQL database, explorer, installs, languages and the CUxAC software.

When the software has been downloaded, continue with the installation process described in Section 4 Installation of Cisco Unified Attendant Applications of this manual.

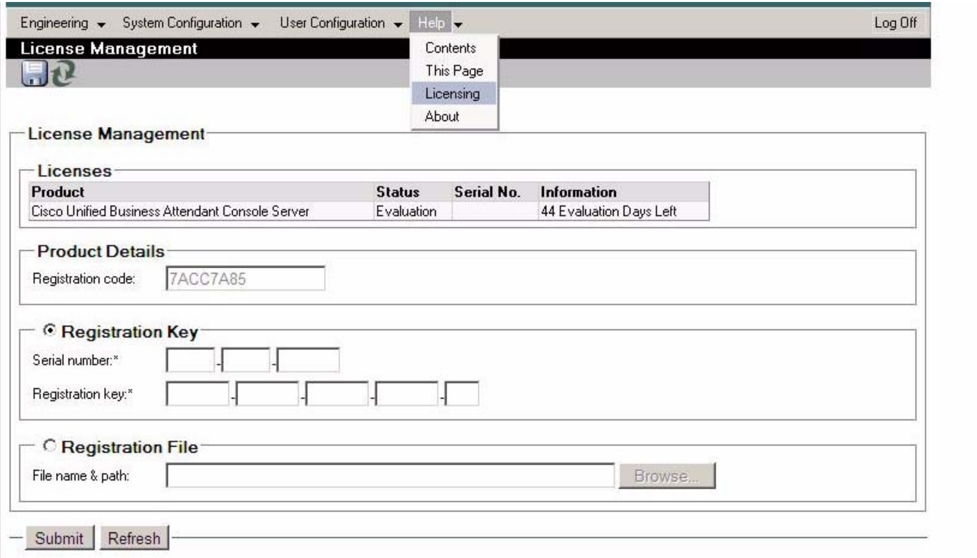
To Activate the 60 day Evaluation Software

Initially the download can be used for 5 days. After that period the software must be registered with Cisco to extend it to a 60 day evaluation copy.

You will require:-

- To enter the Reseller, Customer and Site Details. This is done across a drill down method across three screens.
- Registration code from an installed CUBAC/CUDAC software. This information is obtained from the *Help* menu within the Cisco Unified Business/Department Attendant Console Web Admin.

Figure 7 License Management screen within CUBAC/CUDAC software



License Management

License Management

Licenses

Product	Status	Serial No.	Information
Cisco Unified Business Attendant Console Server	Evaluation		44 Evaluation Days Left

Product Details

Registration code: 7ACC7A85

● Registration Key

Serial number:* ___-___-___

Registration key:* ___-___-___-___-___

○ Registration File

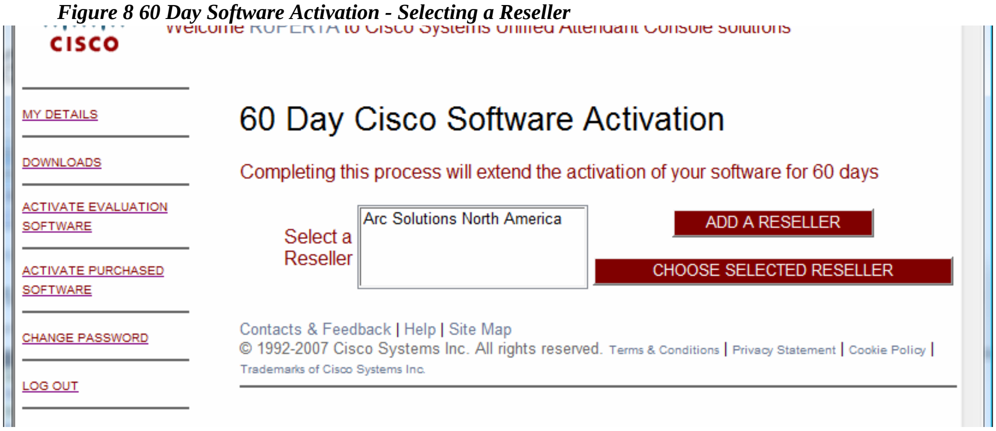
File name & path:

Log into the account, and select *Activate Evaluation Software*. You will be prompted to select your *Reseller.*

Note

If your Reseller is not available there is facility to add a Reseller.

Figure 8 60 Day Software Activation - Selecting a Reseller


CISCO
MY DETAILS
DOWNLOADS
ACTIVATE EVALUATION SOFTWARE
ACTIVATE PURCHASED SOFTWARE
CHANGE PASSWORD
LOG OUT
ADD A RESELLER
CHOOSE SELECTED RESELLER
Contacts & Feedback | Help | Site Map

Welcome RUPERTA to Cisco Systems Unified Attendant Console solutions

60 Day Cisco Software Activation

Completing this process will extend the activation of your software for 60 days

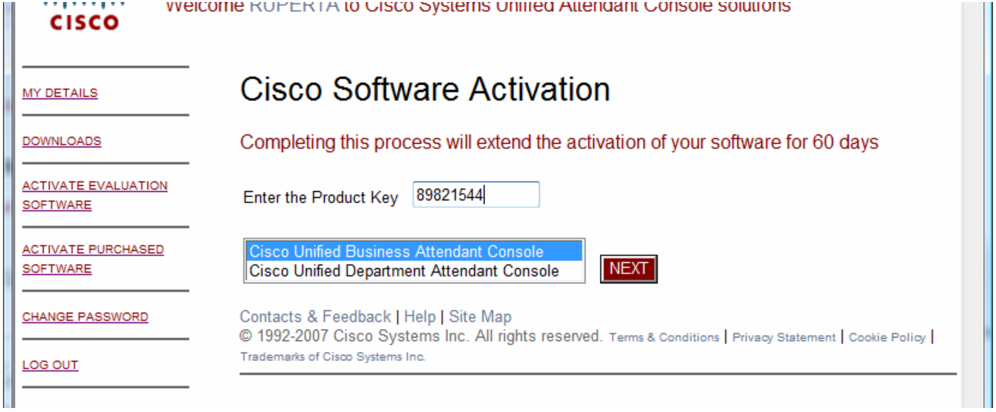
Select a Reseller: Arc Solutions North America

© 1992-2007 Cisco Systems Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems Inc.

When you have completed the *Reseller*, *Customer* and *Site Details* you will be prompted to enter the *Product Key* from an installed CUDAC/CUBAC software. This information is obtained from the *Help>Licensing* menu within the Cisco Unified Business/Department Attendant Console Web Admin.

Note Within the Cisco Unified Business/Department Attendant Console Web Admin the Product Key is refered to as Registration Code within the *Help>Licensing* menu.

Figure 9 60 Day Software Activation - Software Activation (Product Key)



Welcome RUPERTA to Cisco Systems Unified Attendant Console solutions

Cisco Software Activation

Completing this process will extend the activation of your software for 60 days

Enter the Product Key 89821544

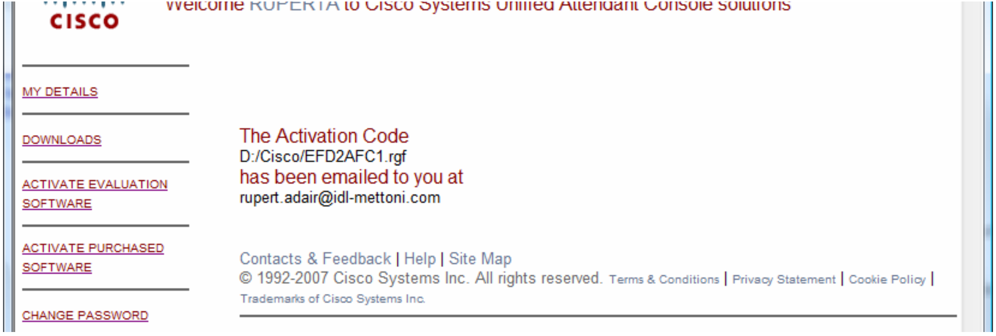
Cisco Unified Business Attendant Console
Cisco Unified Department Attendant Console

Contacts & Feedback | Help | Site Map
© 1992-2007 Cisco Systems Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy |
Trademarks of Cisco Systems Inc.

Select the Product that you have installed.

When you click **Next**. an Activation Code will be emailed out to the registered email address, and a confirmation screen will confirm this.

Figure 10 60 Day Software Activation - Confirmation screen

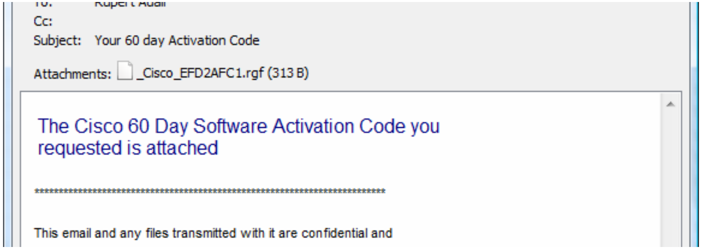


Welcome RUPERTA to Cisco Systems Unified Attendant Console solutions

The Activation Code
D:/Cisco/EFD2AFC1.rgf
has been emailed to you at
rupert.adair@idl-mettoni.com

Contacts & Feedback | Help | Site Map
© 1992-2007 Cisco Systems Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy |
Trademarks of Cisco Systems Inc.

Figure 11 The confirmation email with the activation code



To: Rupert Adair
Cc:
Subject: Your 60 day Activation Code
Attachments: _Cisco_EFD2AFC1.rgf (313 B)

The Cisco 60 Day Software Activation Code you requested is attached

****

This email and any files transmitted with it are confidential and

Save the Activation code to a location where it can be browsed to from the CUBAC/CUDAC Web Admin server.

Return to the CUBAC/CUDAC Web Admin Server and bring up the License Management screen (Help > Licensing)

Figure 12 License Management screen

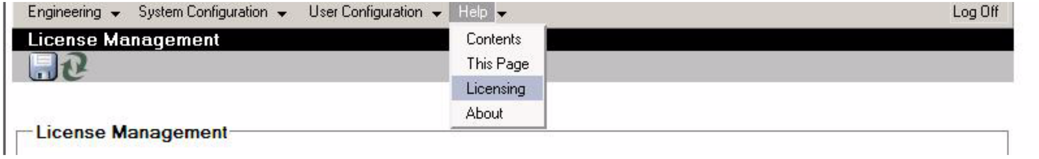
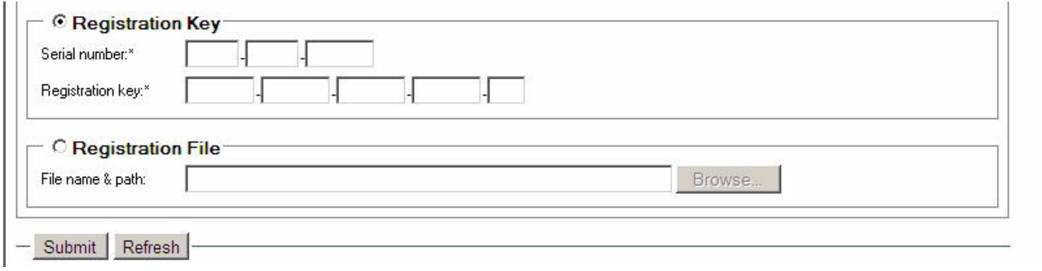


Figure 13 License Management screen - Registration File



Use **Browse** to locate the Registration File. When the file has been found, Click on **Submit** to complete the process

Note

The Registration Key section is not usually required. Its inclusion on this page is to cater for existing customers that do not have physical access to the server and are required to enter the registration numbers manually.

This is done by opening the Registration file with Notepad and entering the two respective codes into the *Serial Number* and *Registration Key.*

Activate Purchased Software

The Activation of the purchased software is done in a similar way to the 60 evaluation except there are several considerations to be made:

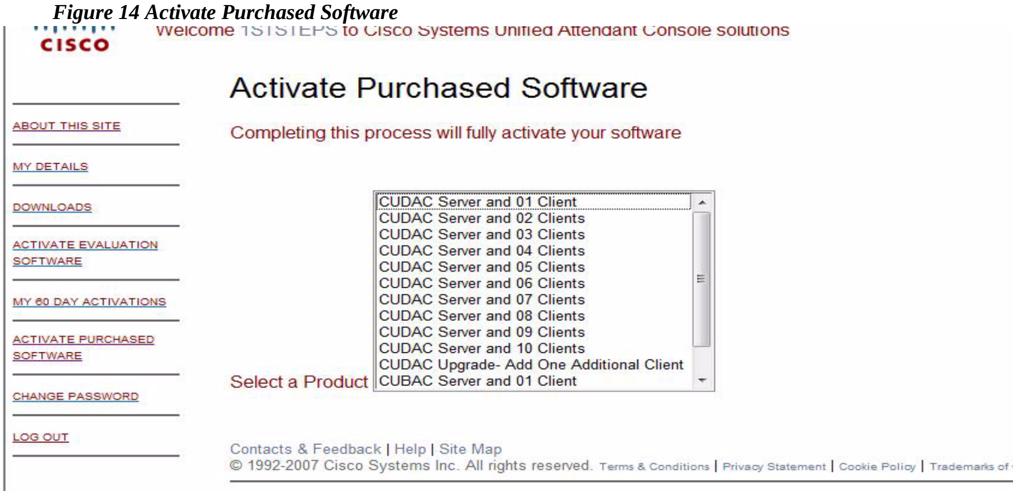
- This activation is permanent and you can not revert back to a trial version.
- It can be completed at any point within either the 5 day free evaluation, or the 60 day activated evaluation period.
- Requires 27 digit LAC (entitlement code) provided by Cisco on purchase of software.

Note

ONE LAC per system, regardless of number of client licenses ordered

Log into the account, and select *Activate Purchased Software*. You will be prompted to select your *Reseller*, *Customer* and *Site Details* you will be prompted to select the version of software and LAC number that you are activating.

Figure 14 Activate Purchased Software


cisco
ABOUT THIS SITE
MY DETAILS
DOWNLOADS
ACTIVATE EVALUATION SOFTWARE
MY 60 DAY ACTIVATIONS
ACTIVATE PURCHASED SOFTWARE
CHANGE PASSWORD
LOG OUT
Contacts & Feedback | Help | Site Map
Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of

Welcome 1STSTEPS to Cisco Systems Unified Attendant Console solutions

Activate Purchased Software

Completing this process will fully activate your software

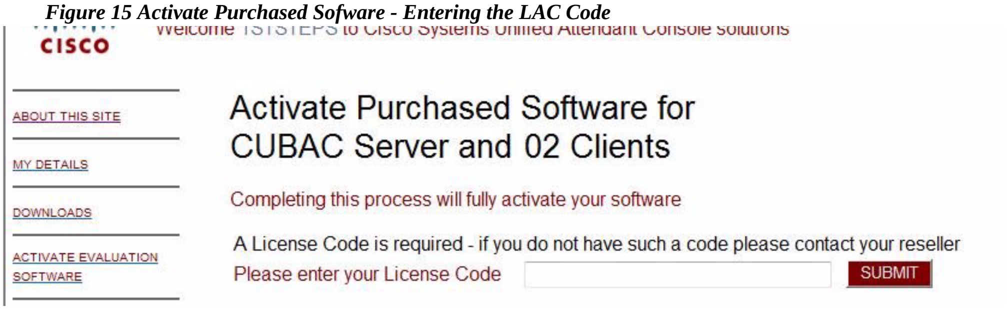
Select a Product

- CUDAC Server and 01 Client
- CUDAC Server and 02 Clients
- CUDAC Server and 03 Clients
- CUDAC Server and 04 Clients
- CUDAC Server and 05 Clients
- CUDAC Server and 06 Clients
- CUDAC Server and 07 Clients
- CUDAC Server and 08 Clients
- CUDAC Server and 09 Clients
- CUDAC Server and 10 Clients
- CUDAC Upgrade- Add One Additional Client
- CUBAC Server and 01 Client

© 1992-2007 Cisco Systems Inc. All rights reserved.

The License Code (LAC) is obtained from the reseller when the product is purchased.

Figure 15 Activate Purchased Sofware - Entering the LAC Code



Welcome 1STSTEPS to Cisco Systems Unified Attendant Console solutions

Activate Purchased Software for CUBAC Server and 02 Clients

Completing this process will fully activate your software

A License Code is required - if you do not have such a code please contact your reseller

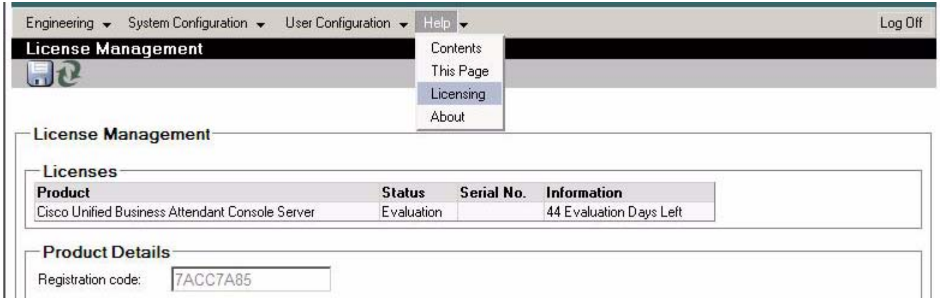
Please enter your License Code

When you click **Submit,** another screen will appear and you will be prompted to enter the *Product Key.* This information is obtained from the *Help>Licensing* menu within the Cisco Unified Business/Department Attendant Console Web Admin.

Note

Within the Cisco Unified Business/Department Attendant Console Web Admin the Product Key is refered to as Registration code within the *Help>Licensing* menu.

Figure 16 License Management screen within CUBAC/CUDAC software



License Management

License Management

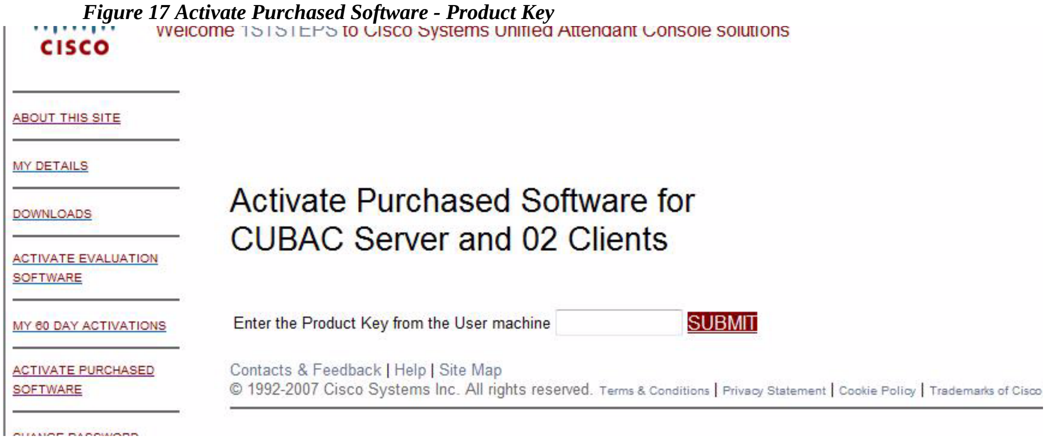
Licenses

Product	Status	Serial No.	Information
Cisco Unified Business Attendant Console Server	Evaluation		44 Evaluation Days Left

Product Details

Registration code: 7ACC7A85

Figure 17 Activate Purchased Software - Product Key



Welcome 1STSTEPS to Cisco Systems Unified Attendant Console solutions

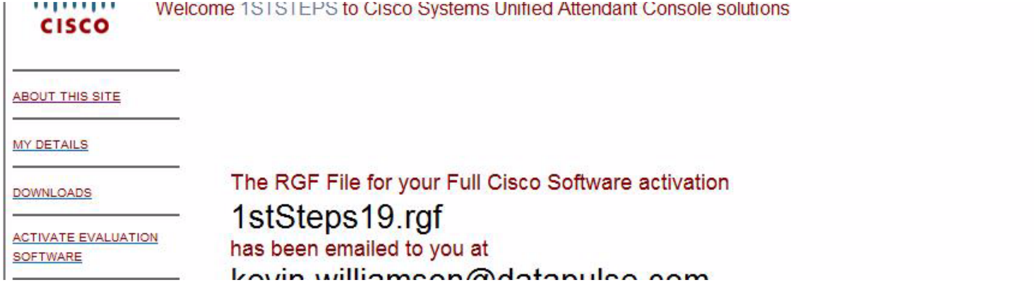
Activate Purchased Software for CUBAC Server and 02 Clients

Enter the Product Key from the User machine

cisco
ABOUT THIS SITE
MY DETAILS
DOWNLOADS
ACTIVATE EVALUATION SOFTWARE
MY 60 DAY ACTIVATIONS
ACTIVATE PURCHASED SOFTWARE
SUBMIT
Contacts & Feedback | Help | Site Map
© 1992-2007 Cisco Systems Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco

When you click **Submit**. The Activation Code will be emailed out to the registered email address, and a confirmation screen will confirm this.

Figure 18 Software Activation - Confirmation screen



Welcome 1STSTEPS to Cisco Systems Unified Attendant Console solutions

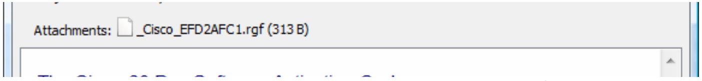
The RGF File for your Full Cisco Software activation

1stSteps19.rgf

has been emailed to you at

kevin.williamson@datapulse.com

Figure 19 The confirmation email with the activation code



Attachments: _Cisco_EFD2AFC1.rgf (313 B)

Save the Activation code to a location where it can be browsed to from the CUBAC/CUDAC Web Admin server.

Return to the CUBAC/CUDAC Web Admin Server and bring up the License Management screen (*Help > Licensing*)

Figure 20 License Management screen

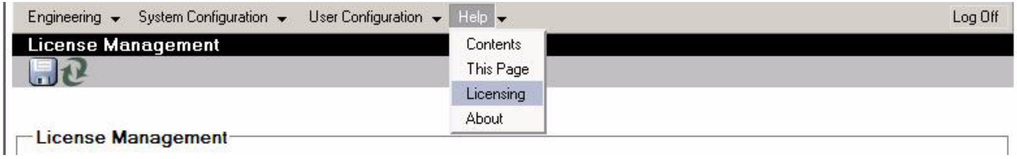
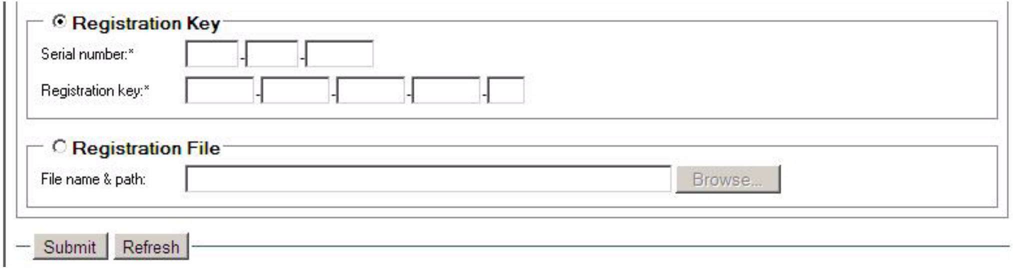


Figure 21 License Management screen - Registration File



● Registration Key

Serial number:* ___ - ___ - ___

Registration key:* ___ - ___ - ___ - ___ - ___

○ Registration File

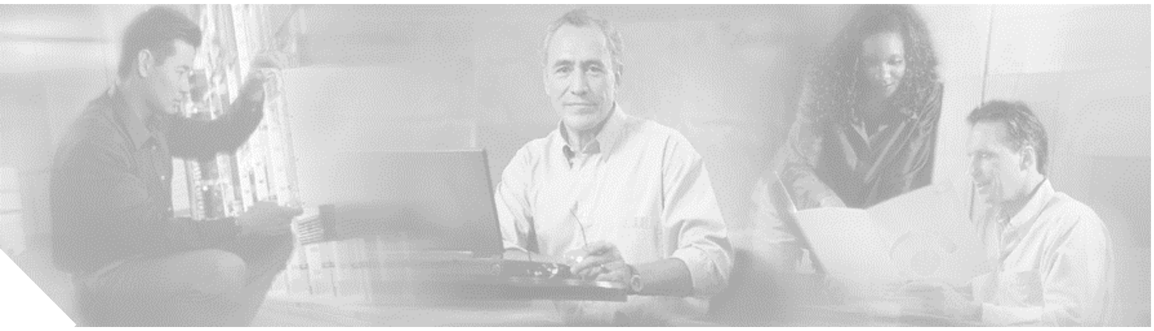
File name & path: ___

Use **Browse** to locate the Registration File. When the file has been found, Click on **Submit** to complete the process

Note

The **Registration Key** section is not usually required. Its inclusion on this page is to cater for existing customers that do not have physical access to the server and are required to enter the registration numbers manually.

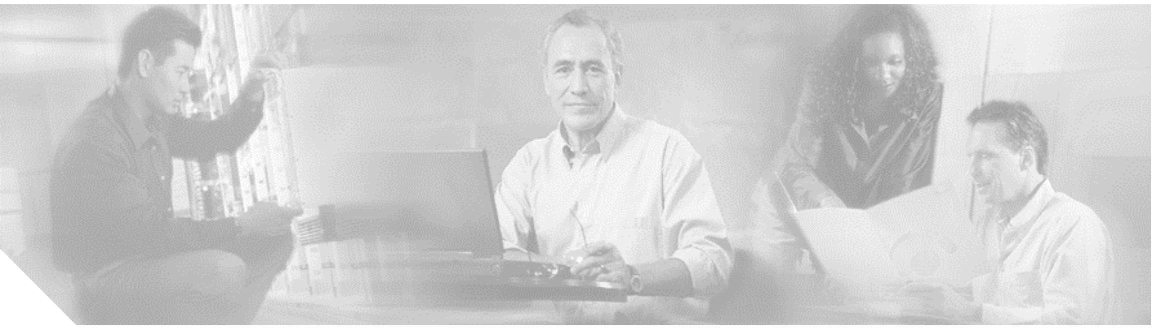
This is done by opening the Registration file with Notepad and entering the two respective codes into the *Serial Number* and *Registration Key.*



Glossary

AXL API	The AVVID XML Layer (AXL) Application Programming Interface (API) provides a mechanism for inserting, retrieving, updating, and removing data from the database using an eXtensible Markup Language (XML) Simple Object Access Protocol (SOAP) interface. This allows a programmer to access Cisco Unified Communications Manager data using XML and receive the data in XML form, instead of using a binary library or DLL.
Call Parking Devices	Virtual devices where calls can be held temporarily and picked from any other call centre extension.
CMC	Client Matter Code (CMC) is used to provide extra call logging facilities within the Communications Manager. This is used to log calls from different destinations. The user has to enter their CMC Code before their external consult transfer can proceed. The call detail records are updated with the CMC code along with the call information. This can then be used later on to charge calls to different cost centres.
CTI Port	The Computer Telephony Integration (CTI) port is actually a virtual device that allows you to create a virtual line. A CTI port must be added for each active voice line intended to be used on a Cisco IP SoftPhone.
CTI Route Point	A computer telephony integration (CTI) route point designates a virtual device that can receive multiple, simultaneous calls for application-controlled redirection.

FAC	Forced Authorization Code (FAC) is used to provide security in the Communications Manager for dialling "Route Patterns". Traditionally, this is used to block calls to external numbers. For example, often in call centres, only some callers are allowed to make external consult transfers to certain numbers. In order to enforce security, these callers are provided with a Forced Authorization Code. The concept of FAC is that if the user makes such an external call transfer that is protected by a FAC, the user must enter the FAC before the call can continue. If an incorrect FAC is entered, or if no FAC is entered, the call fails.
Night Service	This facility allows you to take the queue out of operation at certain times of the day. During this time, calls are routed to some other destination. For example, if you close down the 'Accounts service' queue every day at 7pm, beyond that time calls can be routed to a destination - device or another queue.
SSL	Short for Secure Sockets Layer, a protocol used for transmitting private data through the Internet.



Index