Cisco Unified Enterprise Attendant Consoles Web Admin / Installation Guide

Version 3.0.1.4
April 2009

C O N T E N T S

Preface

Revised: February 20th, 2009, OL-18667-01

The following manual relates to the installation and utilisation of the **Cisco Unified Enterprise Attendant Console (CUEAC)** software product range.

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

Cisco Unified Enterprise 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 admin guide is to provide information on Cisco Unified Enterprise Attendant Console configuration.

Who Should Read this Guide

The document is intended for:-

1. Those involved in the training of Cisco Unified Enterprise 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 admin 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 Enterprise 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 Enterprise 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 Enterprise Attendant applications.
Installation Checklist and procedure for installing Cisco Unified Enterprise Attendant Admin	In order to start installing applications you must go through the checklist for successful installation. This section also provides the procedure for installing Cisco Unified Attendant Enterprise Admin and Cisco Unified Attendant Admin
Cisco Unified Enterprise Attendant Admin	This section explains in detail all the configurations that can be done through Cisco Enterprise 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.

Table 2   *Explains the writing convention used in the user guide*

Convention	Description
`screen` font	Terminal sessions and information the system displays are in screen font.
`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 has 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

Introduction

Revised: February 20th, 2009, OL-18667-01

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

Cisco Unified Enterprise 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 Enterprise 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) Ports and CTI Route Point devices within the Cisco Unified Communications Manager database.

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

- Call queue parameters,
- Operator login credentials
- Global 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
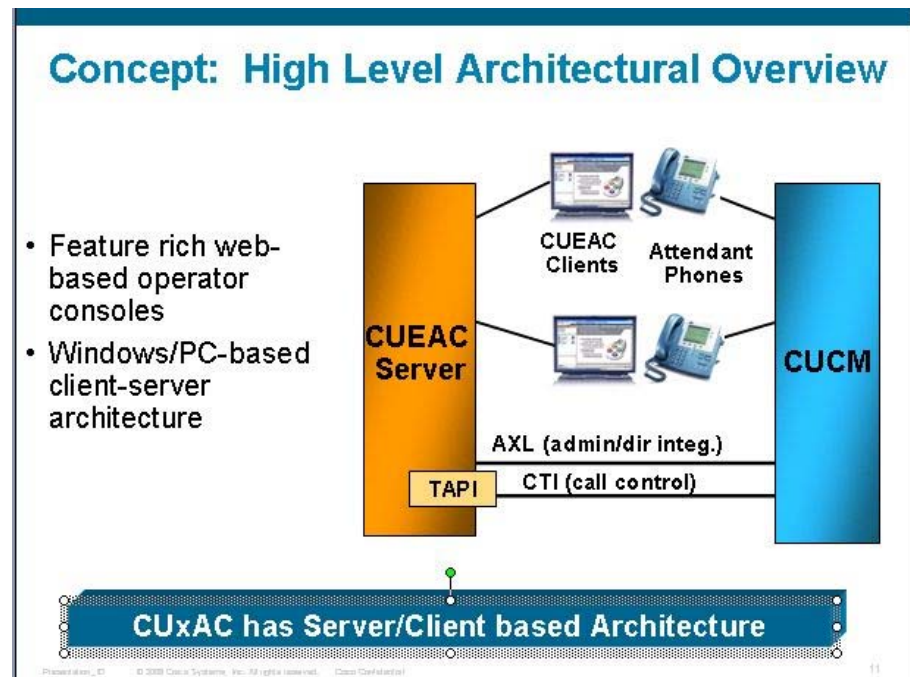
Points to Remember

Cisco Unified Enterprise 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.

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 Enterprise Attendant Server.

Accessibility for Users with Disabilities

Cisco Unified Enterprise 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 Enterprise Attendant Admin.*

Attendants also have an option to use Cisco Unified Enterprise 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 Enterprise 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

Important Information

Revised: April 14th, 2009, OL-18667-01

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

Table 2-1   displays the compatibility matrix for Cisco Unified Attendant Console with CUCM

Communication Manager	6.0	6.1	7.0	7.1
Cisco TAPI TSP	6.0.0.6	6.1 (0.10)	7.0(1.6)	7.1(1.4)
Cisco Unified Enterprise Attendant Console	3.0.0	3.0.0	3.0.0	3.0.1

Music on Hold

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

1. When an 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 Enterprise 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 Enterprise 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.

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 Enterprise Attendant Console can display information extracted from Cisco Unified Presence Server (CUPs) from CUCM version 6.x onwards. Cisco Unified Presence is a standards-based platform that collects information about a user's availability and communications capabilities to provide unified user presence status and facilitate presence-enabled communications for Cisco Unified Communications and critical business applications. With this scalable and easy-to-manage solution, Cisco Unified Presence delivers a consistent presence-enabled communications experience across Cisco Unified Communications applications everywhere, every time, independent of user device, application, or workspace location. In addition, Cisco Unified Presence gives customers and partners the flexibility to presence-enable and streamline business communications by interoperating with critical business applications through open interfaces.

The integration is managed via the Cisco Unified Attendant CUPS Plug-in directly to the Cisco Unified Enterprise 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 Enterprise Attendant Web Admin.

Other items to remember

1. Cisco Unified Enterprise Attendant Server and Cisco Unified Enterprise Attendant Console should not be installed on a machine that will act as Cisco Unified Communications Manager.

2. Headset operation is supported.

# Product Overview

Revised: March 4th, 2009, OL-18667-01

Cisco Unified Enterprise Attendant Admin is the configuration tool for the Cisco Unified Enterprise 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 Enterprise 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.

Figure 3-1   displays the default layout of the Cisco Unified Enterprise Attendant Console
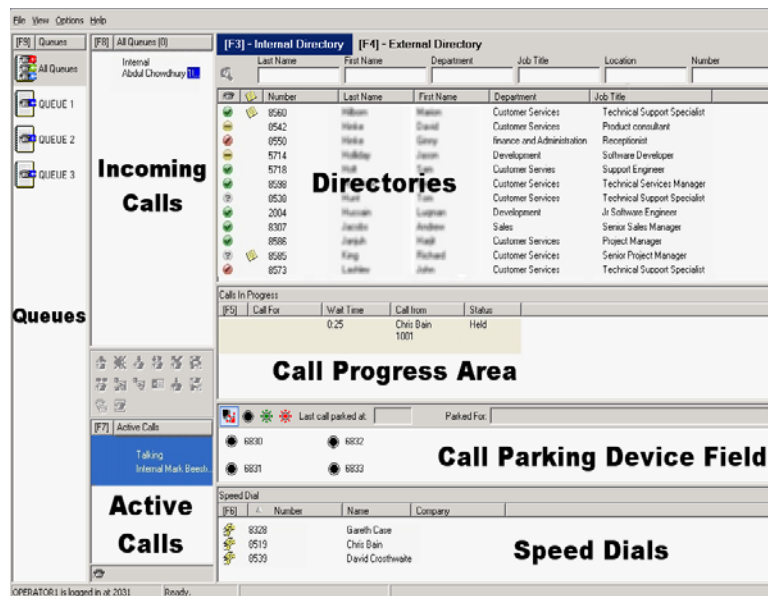
The following devices are used to manage call routing and functionality,

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 Enterprise 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 to manage calls after they leave the operator's handset, for example when transferring or holding calls.
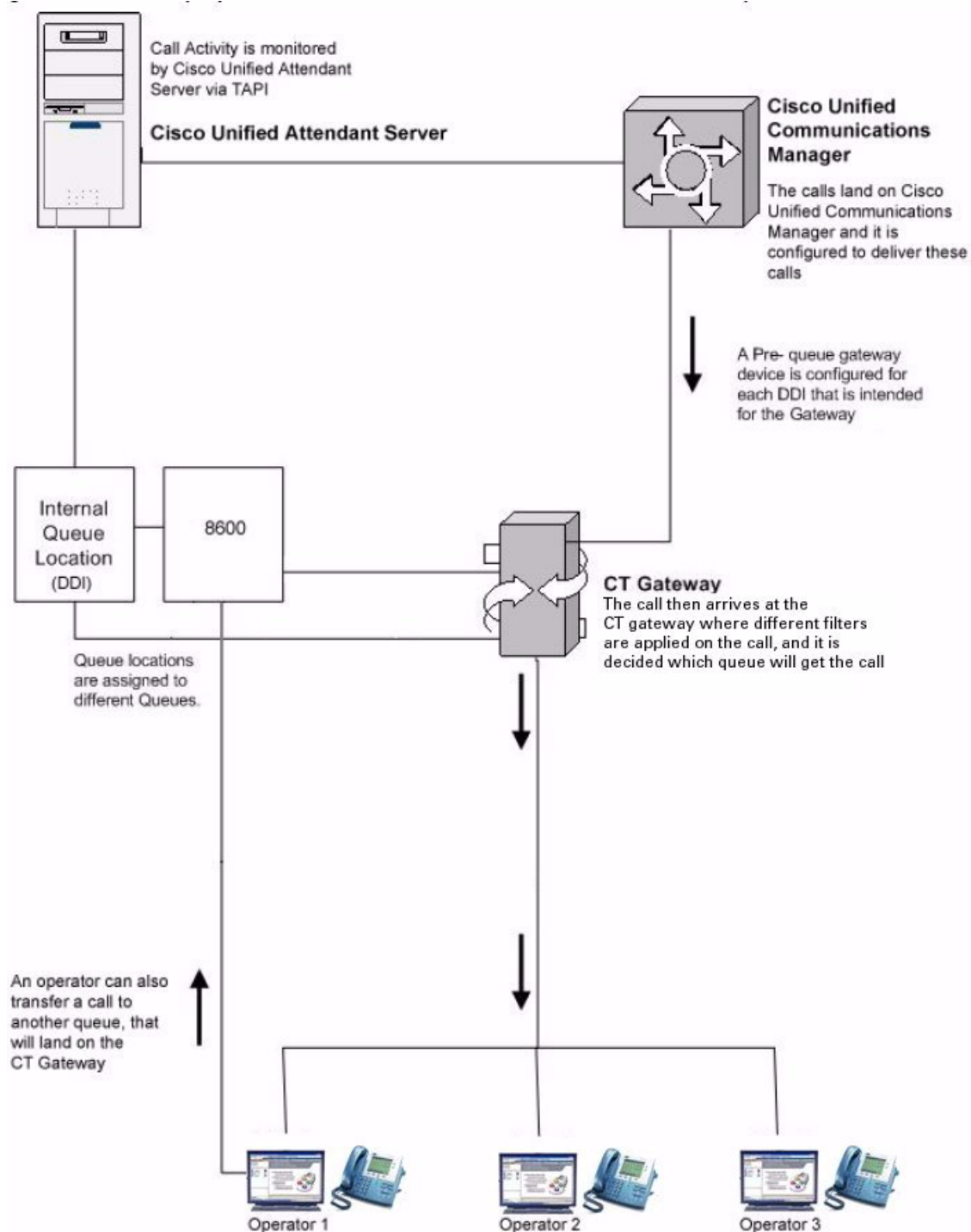
Park Devices

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 Cisco Unified Attendent Server and will require an additional range of DN's.

Call Flow

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

Figure 3-2   ***displays the Call flow from CUCM to the Cisco Unified Enterprise Attendent Console***

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

Queue locations are assigned to different Queues.

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

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 3-1   *shows a numbering plan for a test install*

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 Enterprise 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 3-2   *shows the performance of Cisco Unified Enterprise Attendant Console*

Performance Item	Maximum numbers with Cisco Unified Enterprise Attendant Console
Number of Attendant Consoles	25
Number of Contacts Supported	100k

Table 3-2   *shows the performance of Cisco Unified Enterprise Attendant Console*

Performance Item	Maximum numbers with Cisco Unified Enterprise Attendant Console
Number of Console Queues	50
BHCC	6000

Hardware / Software Requirements

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

Table 3-3   *minimum specification required by Cisco Unified Enterprise Attendant Server*

Applies To	PC Specification
Cisco Unified Enterprise 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 3.5**
	MS SQL Server 2005 (Express) * (See "SQL Consideration and Scalability" on page 3-7 for further information)
	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 and the ASP.NET component must be enabled 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 Enterprise Attendant Server is not supported within a 64 bit Operating System.

✎

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

Table 3-4   minimum specification required by Cisco Unified Enterprise Attendant Console Client is as follows,

Applies To	PC Specification
Cisco Unified Enterprise 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
	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.

Table 3-5   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 Enterprise 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.**

SQL Considerations and Scalability

CUEAC installs SQL 2005 Express by default as part of its standard installation process. The performance limitation that SQL Server 2005 Express possesses is that it can access only a single CPU and 1 GB of RAM with a maximum database size of 4Gb.

In sites where one or more of the following are expected;-

- A large number of operators – more than 10,

- A high call volume – greater than 500 calls per operator per day,

- A Large Directory – greater than 10,000 contacts;

The use of SQL Server 2005 Standard or Enterprise should be strongly considered. Where a system out grows the SQL2005 Express deployment, or issues are experienced that are related to the use of SQL 2005 Express, the Standard or Enterprise versions of SQL 2005 can be used to upgrade the existing implementation with minimal effort.

Note   For future versions of CUEAC to benefit from some features, SQL 2005 express will not be an option and SQL 2005 Standard or Enterprise will be required.

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

Table 3-6   Product Feature table

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	● 5	● 3	● <=50
Configurable queue names and priority	○	○	●	●
Show all calls in all queues option	○	○	●	●
Queue salutations	○	○	○	●
Show & pick calls from each Queue	●	●	●	●

Table 3-6   Product Feature table

Feature	Version			
	CAC	CUDAC	CUBAC	CUEAC
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	●	○	●	●
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)	○	●	●	●

Cisco Unified Enterprise Attendant Consoles Web Admin / Installation Guide

Table 3-6   Product Feature table

Feature	Version			
	CAC	**CUDAC**	**CUBAC**	**CUEAC**
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	○	○	○	●
Call hold with notes	○	○	○	●
Undirected Call park (finds first slot)	●	●	●	●
Directed Call Park (to specific Park location)	●	●	●	●
Call Hold	◗	●	●	●
Park recall	◗	●	●	●
Transfer	●	●	●	●
Conference	●	●	●	●

Table 3-6   Product Feature table

Feature	Version			
	CAC	**CUDAC**	**CUBAC**	**CUEAC**
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, 7.1
Localisation and accessibility				
Languages supported*	20	15*	15*	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

Installation Checklist and Procedure for Cisco Unified Enterprise Attendant Admin

Revised: April 20th, 2009, OL-18667-01

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

1. Cisco Unified Attendant Server

2. Cisco Unified Enterprise 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.

Note 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 Enterprise 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.

Table 4-1   Installation and Configuration overview

Step 1 Preperation	
Formulate numbering plan for test install. Refer to "shows a numbering plan for a test install" on page 3 - 4 for required Directory Numbers.	
Prepare a Windows 2003 Service Pack 2 server with Internet Information Services (IIS) installed and ASP.NET.	

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 6.x/7.x see *"Creating the Attendant Application End User for CallManager 6.x" on page A - 1* or *"Creating the Attendant Application End User for CallManager 7.x" on page B - 1*	
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 Enterprise Attendant Admin

Install Cisco Unified Enterprise Attendant Admin. See *"Installing Cisco Unified Attendant Server" on page 4 - 4*	
Check Cisco Unified Communications Manager connectivity. See *"CUCM Connectivity" on page 5 - 9*.	
Configure CT Gateway, Service and Park devices. See *"System Configuration" on page 5 - 18*.	
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 5 - 21*.	
Configure Directory Synchronization if required. *"Directory Synchronization" on page 5 - 26*.	

Step 3 Install and Configure Cisco Unified Enterprise Attendant Admin

Configure Cisco Unified Enterprise Attendant Console User Settings. See *"User Configuration" on page 5 - 30*	
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

Run the CiscoTSP.exe. As part of the install this file is extracted from the CUCM to the desktop. If you require to manually collect the file go to Communication Manager configuration and select *Application > Plugins.* See *"Installing the TAPI TSP" on page C - 1*	
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 C - 1*	
Reboot the server.	

Step 5 Test TAPI

Use Phone1.exe (TAPI Soft Phone) from Jul-mar.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 Enterprise Attendant Console Client" on page 4 - 11*	

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 D - 1 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,

Step 1   The initial part of the installation will install the 3rd party applications, including MS SQL Server 2005 Express, IE 6.0 and MS Dotnet 3.5 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 4-1   displays the screen that is shown while the setup prepares for installation
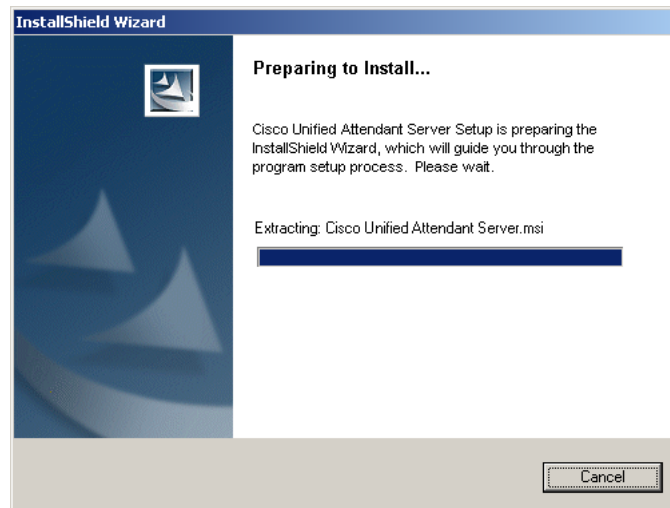
Step 2   The next screen displays a welcome note and instructions on installing. Click **Next**.

Figure 4-2   displays the welcome screen for the
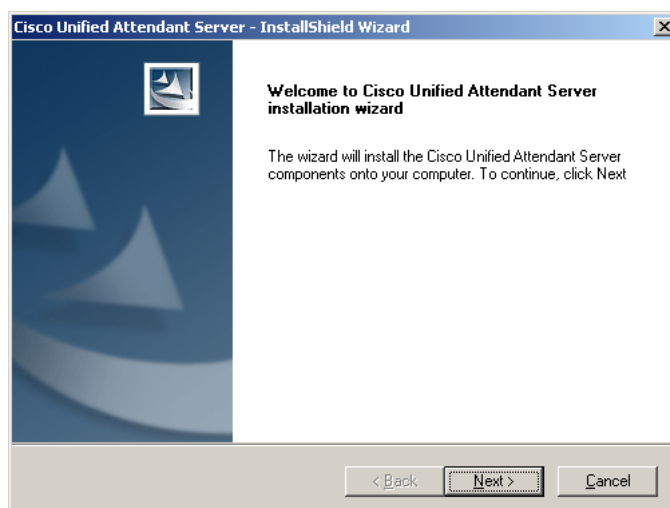
Step 3   The next window contains registration information. In the *Name* text box, type the name of the license holder, and type the company name into the *Company* text box. Click the Next button to proceed.

Figure 4-3   displays the Registration Information screen of the install
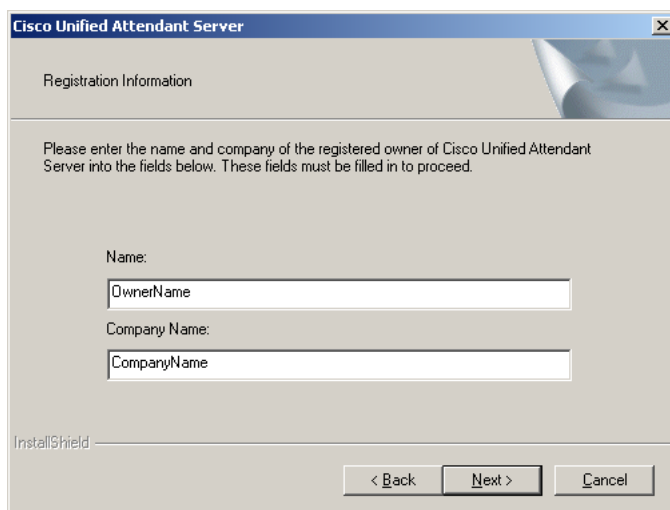
Step 4   In this window, it is necessary to type the Machine Name or IP Address of the machine onto which the Server application is being installed. Click **Next**.

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 4-4   displays the Server Information screen for the installation

Step 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. The default user name for the SQL connection will be **sa** and the default password will be **Z1ppyf0rever**. Click **Next**.
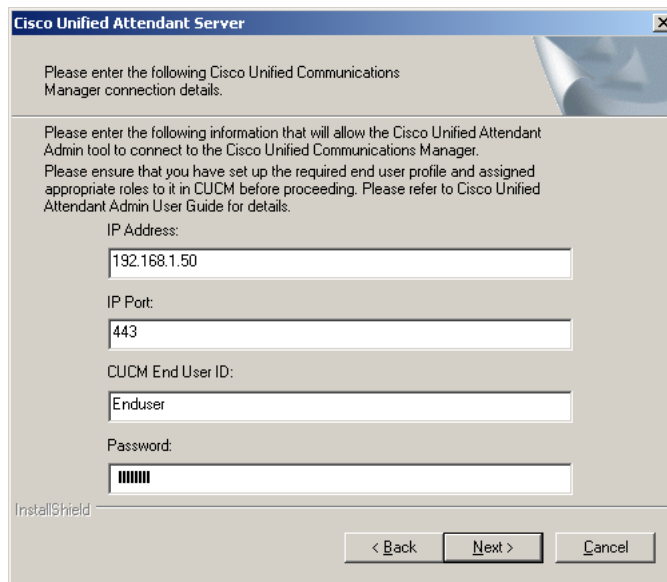
Note   If MS SQL Server is not installed on your machine, it will be installed automatically by Cisco Unified Attendant Server Installation. Please refer to Step 1.
IMPORTANTLY - If the SQL Server is installed this way, the following screen will not appear.

Figure 4-5   displays the Server Login Information screen for installation

Step 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**.
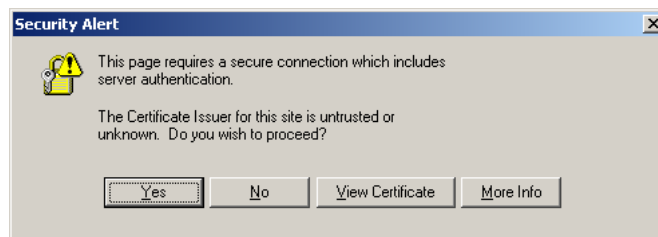
Figure 4-6   displays the CUCM information screen

Step 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 4-7   displays the confirmation to access CUCM

Step 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 4-8   displays the screen to specify location for the files to be installed to
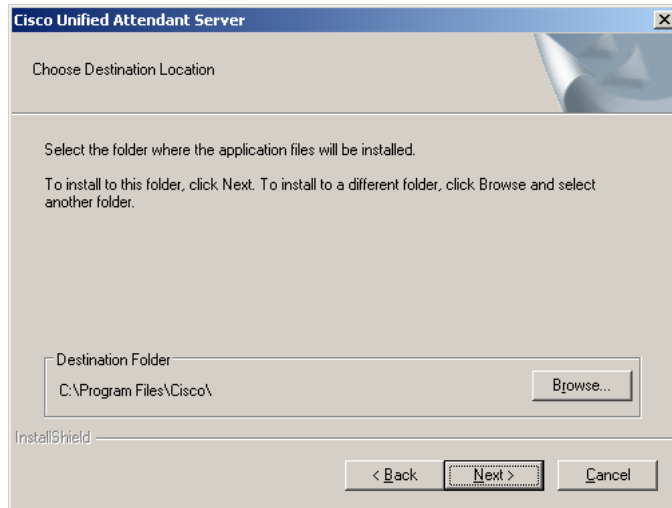
Step 9   In the next window, the summary for the current settings specified will be displayed. Click **Next** to proceed with installation or click **Back** to edit the settings made on the previous screens.

Figure 4-9   displays the summary for the configuration made
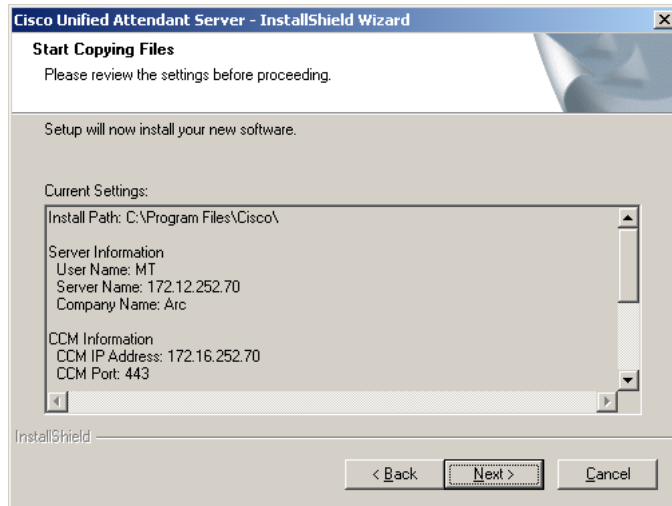
Step 10   The next screen will display the progress bar for the installation.

Figure 4-10 ***displays the progress bar for the installation***
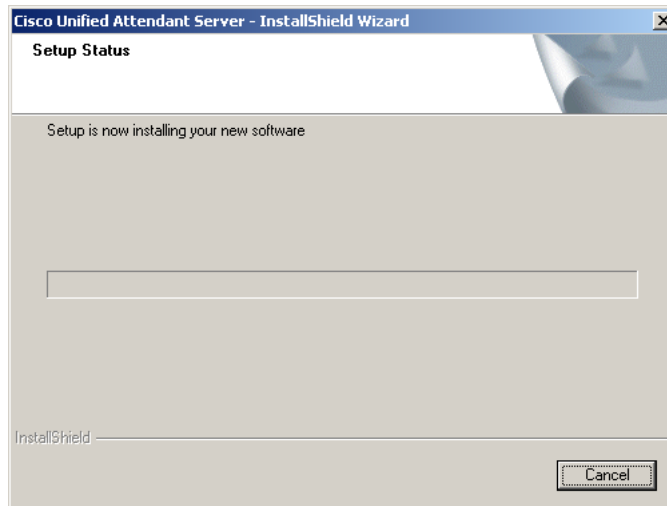
Step 11   Once the application has been installed, the *Database Wizard* will create and configure the databases for the application. Click **Next**.

Figure 4-11 ***displays the Database Wizard welcome screen***
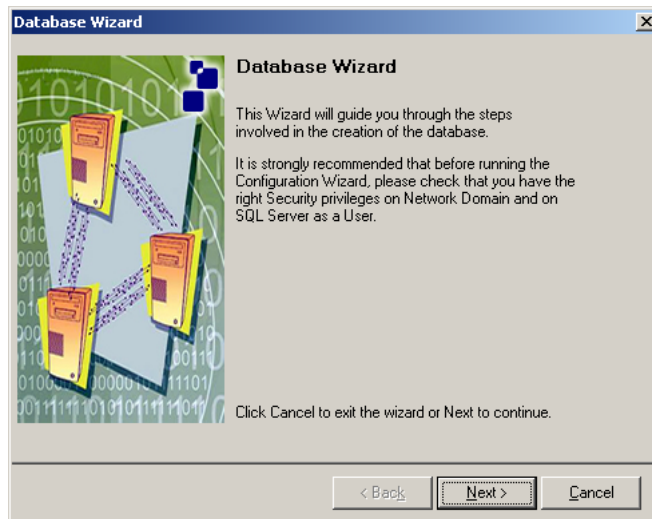
Step 12   In the next window, the status of database installation will be displayed. Once the installation is complete.

Figure 4-12   displays the installation progress of the databases
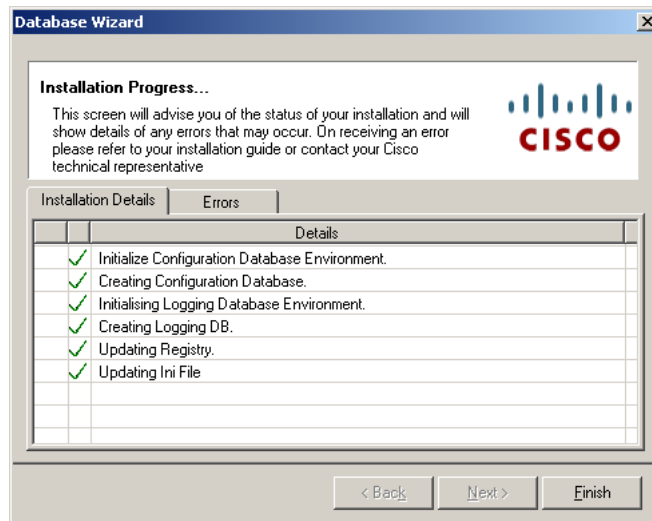
Step 13   The application has now been installed successfully. It is recommended that you restart your computer. Click **Finish**.

Figure 4-13   displays the screen once the installation is complete
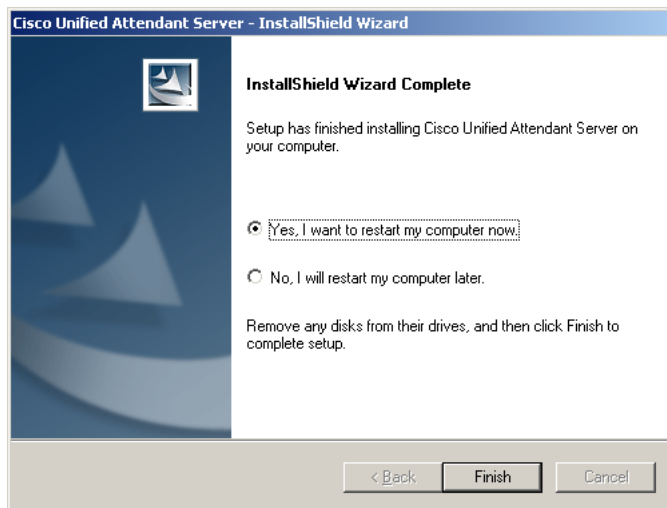
Note   After the restart and before using the software, the Cisco TSP and Cisco TAPI Wave driver have to be installed and configured. This is covered in Appendix C "TAPI Configuration" on page C - 1

Installing Cisco Unified Enterprise Attendant Console Client

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

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

Step 2   The first window appears displaying a message that Cisco Unified Enterprise 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 Enterprise Attendant Console.

Figure 4-14   displays the first install screen
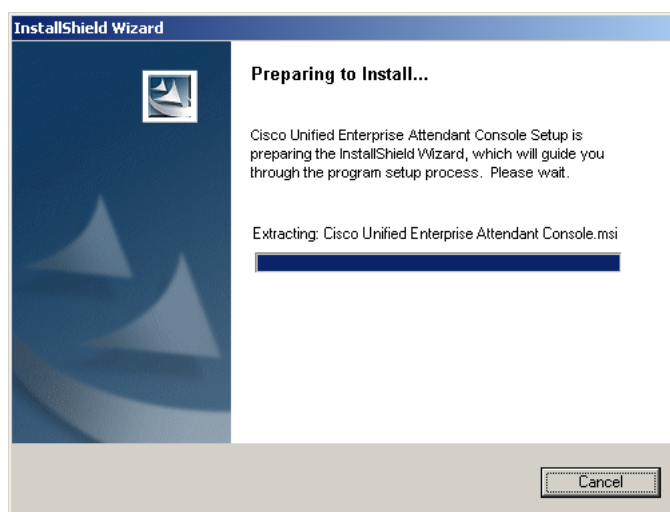
Step 3   The new window that is displayed after the *Preparing to Install* window, shows a welcome note. This screen specifies that Cisco Unified Enterprise Attendant Console and its components will be installed on your computer. To continue, click **Next**. If you wish to exit from the setup at this point, click **Cancel**.

Figure 4-15   displays the welcome screen to installation
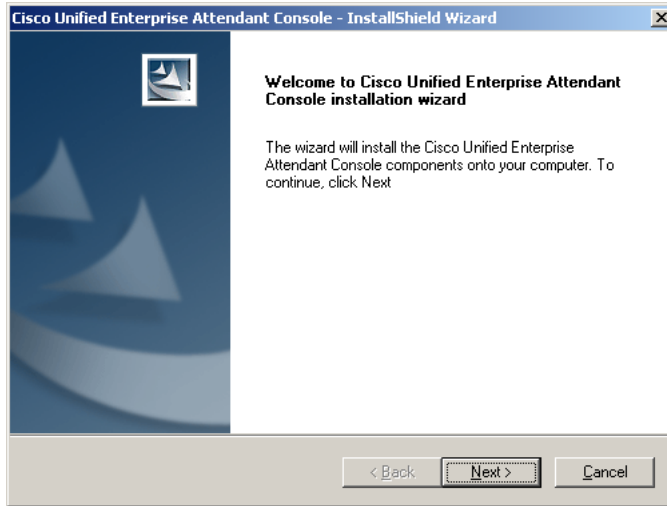
Step 4   The next window contains the registration information. In the *Name* text box, type the name of the registered owner of Cisco Unified Enterprise Attendant Console, and type the owner's company name into the *Company* text box. Click the **Next** button to proceed.

Figure 4-16   displays the screen for Registration Information
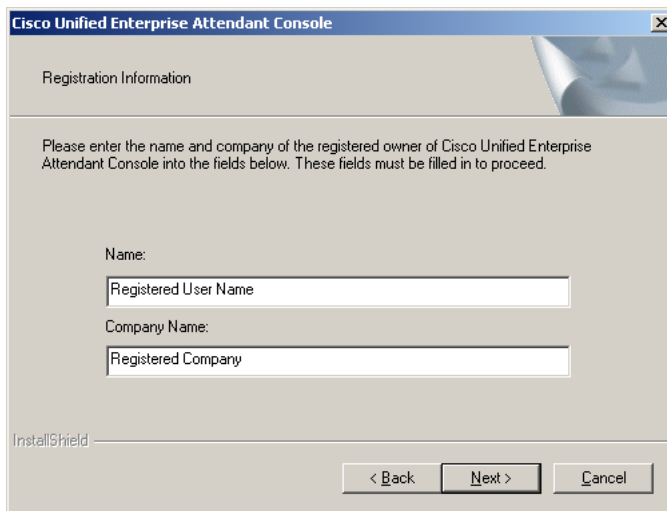
Step 5   In the next window, select the folder where you wish to install the application. It is recommended to use the default destination folder specified on the screen. The default destination folder is created on the following path:

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 4-17   displays the screen used to select a location where the application must be installed
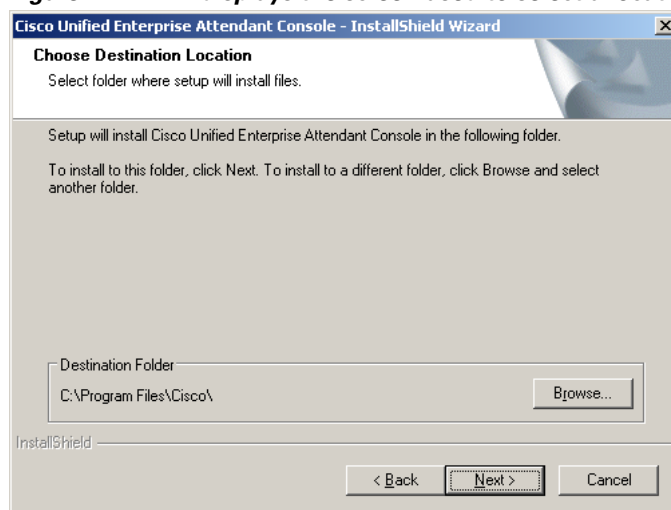
Step 6   In the next window, enter the *IP Address* or *name* of the machine running Cisco Unified Attendant Server. This is required in order to enable communication between Cisco Unified Enterprise Attendant Console and Cisco Unified Attendant Server. Click **Next** to proceed.

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 4-18   displays the screen for Server Information
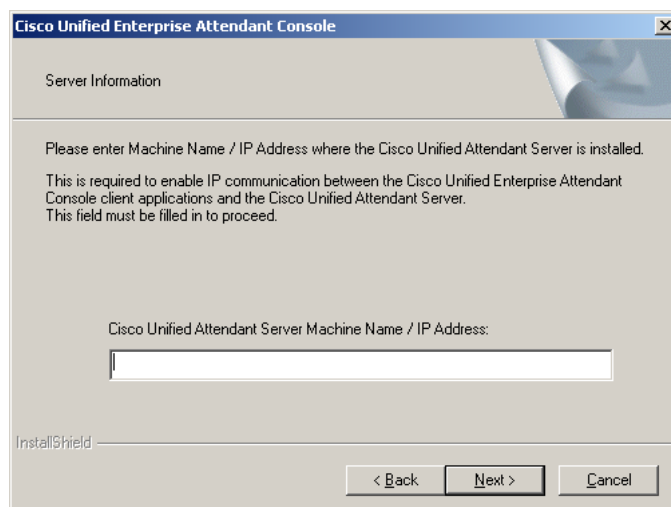
Step 7   In the next window, you must select the language in which you want to install the application. Click **Next** to proceed.

Note   Where a DNS Server is not present on the network or the Servers Machine Name cannot be resolved, the Hosts file (WINDOWS\system32\drivers\etc\) should be amended to reflect the IP Address and Server Machine Name of the server

Figure 4-19   displays the screen used to select the language for the application
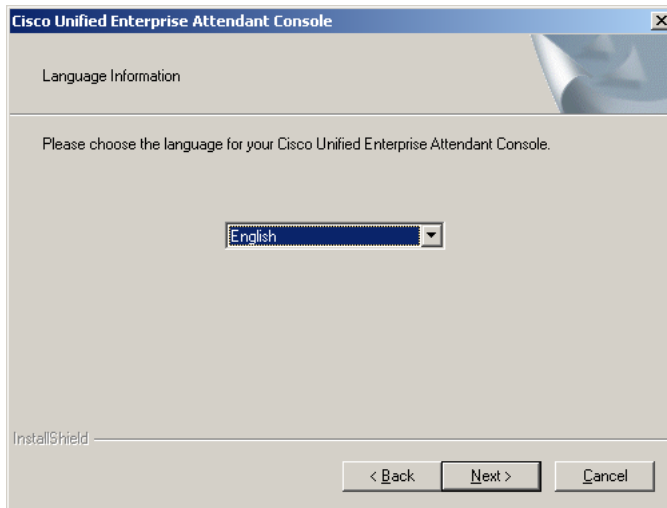
Step 8   In the next window, select the check box to add an icon for Cisco Unified Enterprise Attendant Console on the desktop. Click **Next** to proceed.

Figure 4-20   displays the screen that asks to add an icon to desktop
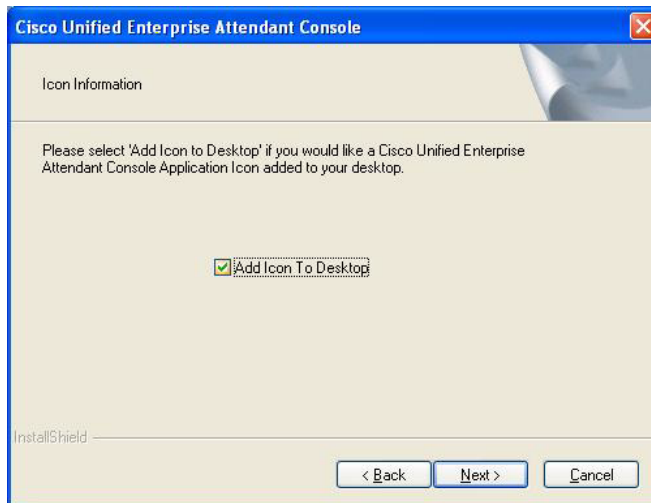
In the next window, the installation wizard displays the summary of the information you have entered so far. You can review these settings on this screen and click **Back** if you wish to edit some information. If you are satisfied with the settings, click **Next** to allow the setup to start copying the files.

Figure 4-21   *displays the screen that shows the summary for the setup*
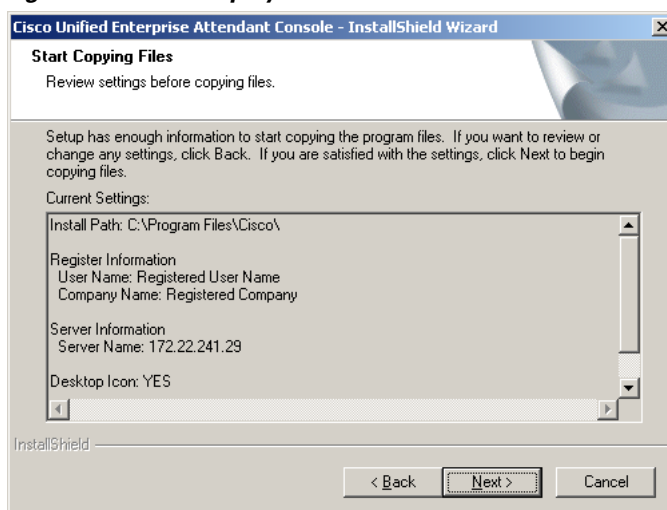
Step 9   In the next window, a progress bar is displayed that shows the status of the installation configurations and the files being copied. If you wish to exit the setup at this point, click **Cancel**.

Figure 4-22   *displays the progress bar for the software configuration*
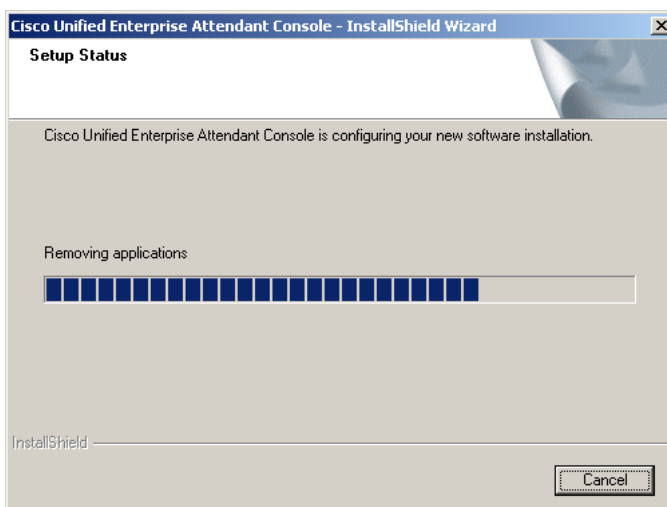
Step 10   The final window displays the confirmation that Cisco Unified Enterprise Attendant Console has been installed successfully. Click the **Finish** button.

Figure 4-23   *displays the screen notifying that the installation is complete*
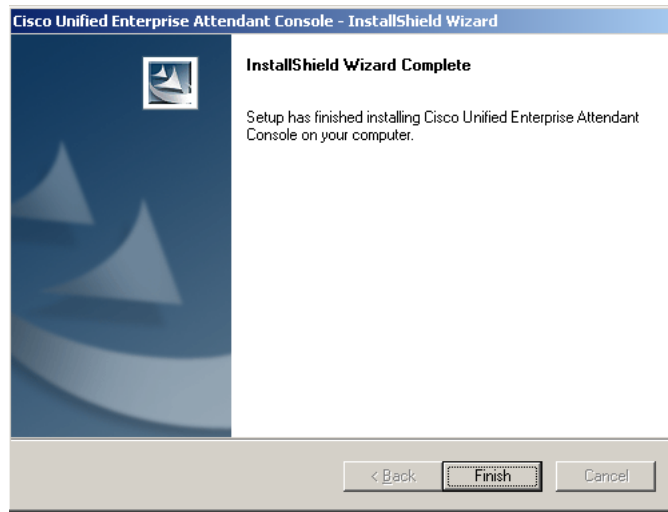
C H A P T E R 5

Cisco Unified Enterprise Attendant Admin

Revised: February 20th, 2009, OL-18667-01

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

System configuration provides the facility to manage synchronization of devices and directories with Cisco Unified Communications Manager. Cisco Unified Enterprise 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 Enterprise 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 Enterprise 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 5-1   displays URL entered in the Internet Explorer address bar
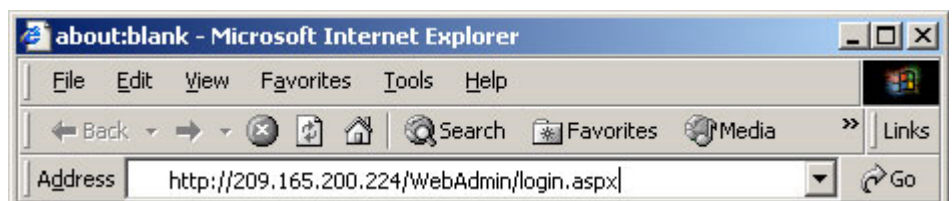
You must login to Cisco Unified Enterprise Attendant Admin in order to configure settings for Cisco Unified Enterprise Attendant Console.

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

Table 5-1   *provides the description for the icons used in the user guide*

Icon	Description
	Submit
	Reset Password
	Test Connection
	Repair Database
	Start Server
	Stop Server
	Information Icon: Used to view runtime information for a service.
	Refresh
	Synchronize with CUCM

Administrator Login

Cisco Unified Enterprise Attendant Admin requires authentication for users, and is accessible only to Administrators for making new configurations for Cisco Unified Enterprise Attendant Console or updating them. Most of the settings configured using Cisco Unified Enterprise 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 Enterprise Attendant Admin,

Step 1   Enter the URL specified by your network administrator to access Cisco Unified Enterprise Attendant Admin.

Step 2   The **Logon** page will open.

Step 3   Enter *User name*.

Step 4   Enter *Password*.

Step 5   Click **Submit**.

Figure 5-2   ***Figure 2: displays the login page for the application***

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

Table 5-2   ***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 password used by the Administrator to log in.

To clear the contents of the User name and Password fields, 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 5-3   ***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 Enterprise Attendant Console configuration.
Help	Provides help information and also includes a section for licensing the applications.

As well as the configuration options the Home Page also displays version numbers and the registration status.

Figure 5-3   displays the Cisco Unified Enterprise Attendent Console home page.
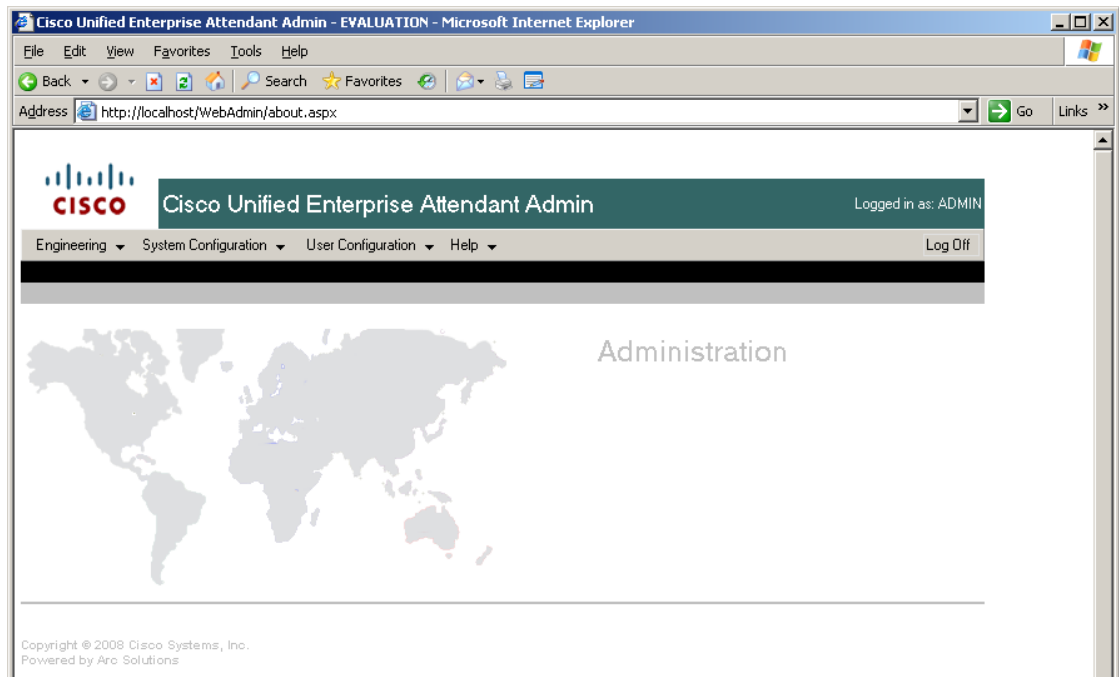
These configurations are explained in detail in the following sections

Engineering

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

- Administrator Management
- Database Management
- Service Management
- Cisco Unified Communications (CUCM) Connectivity
- CUPS Connectivity
- Logging Management

Administrator Management

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

To change password,

Step 1   Go to *Engineering > Administrator Management*.

Figure 5-4   displays the menu option for Administrator Management
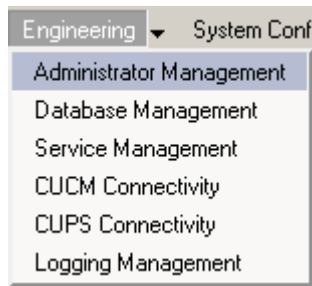
Step 2   Enter *Old Password*.

Step 3   Enter *New Password*.

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

Step 5   Click 💾 **Submit** to save changes.

Figure 5-5   displays the Administrator Management page

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

Table 5-4   descriptions 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.

The Configuration database will be created at the time of installation. Only the connectivity details can be modified through this page.

To manage database,

Step 1   Go to *Engineering > Database Management*.

Figure 5-6   *displays the Database Management menu option*
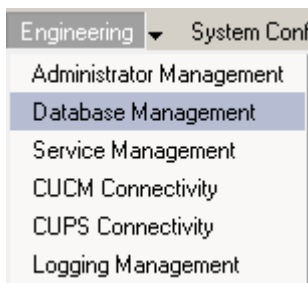
Step 2   In the Server field, specify the name of the machine where the SQL Server is installed.

Step 3   Enter *User Name*.

Step 4   Enter *Password*.

Step 5   To save changes, click ![save] **Submit**. You will be prompted that Cisco Unified Enterprise Attendant Server must be restarted for the changes to take affect. If you select the option, Cisco Unified Enterprise Attendant Admin can restart server automatically.

Step 6   To test the database, click ![test] **Test Connection**.

Step 7   To repair database, click ![repair] **Repair Database**. You will be prompted that Cisco Unified Enterprise Attendant Server must be stopped before repairing the database. If you select the option, Cisco Unified Enterprise 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 5-7   ***displays the Database Management page***

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

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

Field	Example	Description
Server	209.165.202.128	In this field you specify the IP Address of the machine where MS SQL Server 2005 is installed.
User name	username1	You must enter the user name used to connect to SQL Server. If MS SQL Server was installed through *Cisco Unified Enterprise 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 Enterprise Attendant Server Installation Wizard*, the password would be **Z1ppyf0rever**.

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
3. Cisco Unified Attendant CUPS Plug-in
4. Cisco Unified BLF Plug-in

The following controls are available,

Table 5-6   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.
Refresh		The **Refresh** button and the icon shown on the left allow you to see the current status of the server.

Figure 5-8   displays the Service Managment page
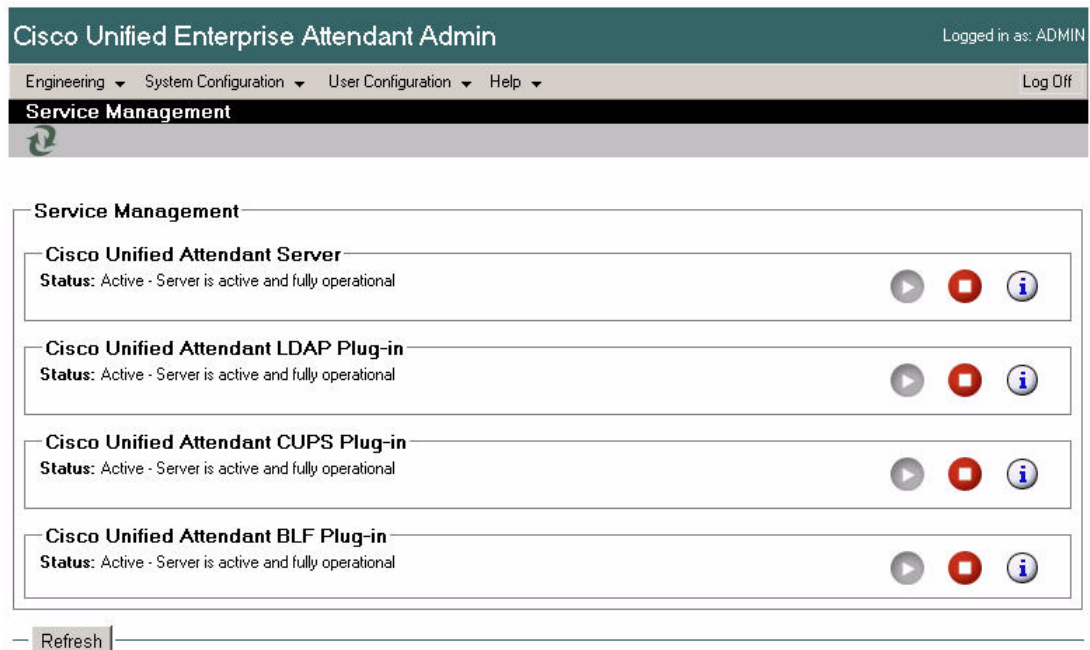
The status window will display the statuses of the following for Cisco Unified Attendant Server,

- CUCM Link
- Configuration Database
- Logging Database
- Event Network

The status window will display the statuses of the following for Cisco Unified LDAP Plug-in,

- Primary Server
- Configuration Database
- Logging Database

The status window will display the statuses of the following for Cisco Unified CUPS Plug-in,

- Primary Server

The status window will display the statuses of the following for Cisco Unified BLF Plug-in,

- CT Link
- DRM
- COMMS

Table 5-7   displays the statuses for the Service Management page,

Status	Description
Connected	The server and databases are connected.
Not Connected	The server and databases are not connected.
Standby	This status can be viewed for Logging Database only. It specifies that the connection between the service and the Logging Database is currently not in use.

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,

Step 1   Go to *Engineering > CUCM Connectivity*.

Figure 5-9   displays the menu option for CUCM Connectivity
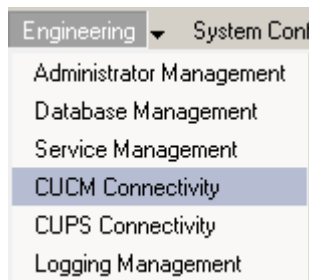
Step 2   Enter *CUCM name*. This is the IP Address of the Cisco Unified Communications Manager Publisher.

Step 3   Enter *CUCM Port* number. This should be left as 443 by default.

Step 4   Enter *User name* and *Password* of the End User profile that is used to connect to Cisco Unified Communications Manager.

Step 5   To save, click 💾 **Submit**.

Step 6   To test, click 🖥️ Test Connection.

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

Figure 5-10   *displays the CUCM Connectivity page*

Table 5-8   *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   **The Username and Password provided here are case-sensitive. Please make sure you enter the information in these fields in proper case.**

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 Attendant CUPs Plug-in with the Cisco Unified Presence Server, which is available with CUCM 6.0 upwards.

To manage connectivity details,

Step 1   Go to *Engineering > CUPS Connectivity.*

Figure 5-11   displays the menu option for CUPS Connectivity
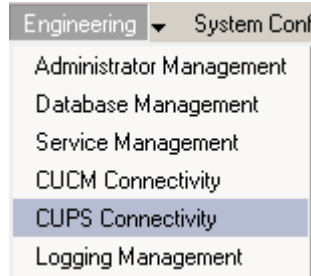
Step 2   Enter *CUPS name or IP*. This is the IP Address of the Cisco Unified Presence server.

Step 3   Enter *CUPS Port* number.

Step 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.

Step 5   Enter *User name* and *Password* of the End User profile that is used to connect to Cisco Unified Presence Server .

Step 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).

Step 7   Enter *Certificate nickname* and the *Certificate Database password* if TLS has been enabled.

Figure 5-12   displays the CUPs Connectivity page

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

Step 9   To test, click 🗹 Test Connection.

Table 5-9   *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   **The Username and Password provided here are case-sensitive. Please make sure you enter the information in these fields in proper case.**

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 A - 6

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,

Step 1   Go to *Engineering > Logging Management*.

Figure 5-13   *displays the menu option for Logging Management*
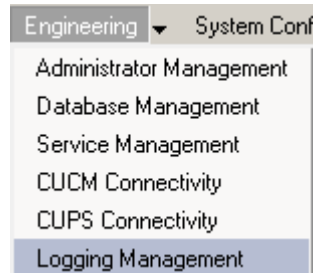
Step 2   Enter Cisco Unified Attendant Server Logging Management details.

Step 3   Enter Cisco Unified Attendant LDAP Plug-in Logging Management details.

Step 4   Enter Cisco Unified Attendant CUPs Plug-in Logging Management details.

Step 5   Enter Cisco Unified Attendant BLF Plug-in Logging Management details.

Step 6   Click [icon] **Submit** to save changes.

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

Figure 5-14   displays the Logging Management page

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

Table 5-10   *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.
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.

Table 5-10   *provides the description for the fields on the Logging Management page*

Field	Example	Description
Lines per file	10000	In this field you specify the number of lines each log file can contain.
Cisco Unified Attendant BLF 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,

Step 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.

Step 2   You must specify the *Logging path* and *file name* where the log must be created.

Step 3   Specify the number of log files that must be created in the *Number of files* field.

Step 4   Specify the number of lines each log file can contain in the *Lines per file* field.

Step 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,

Step 1   Select the *Logging Level* for LDAP Plug-in. Cisco Unified Enterprise Attendant Admin provides the following options:

- Detailed
- Advanced
- Minimum
- Full

Step 2   Specify the *Logging path* and *file name* where the log must be created.

Step 3   Specify the number of log files that must be created in the *Number of files* field.

Step 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,

Step 1   Select the *Logging Level* for CUPS Plug-in. Cisco Unified Enterprise Attendant Admin provides the following options:

- Detailed
- Advanced
- Minimum
- Full

Step 2   Specify the *Logging path* and *file name* where the log must be created.

Step 3   Specify the number of log files that must be created in the *Number of files* field.

Step 4   Specify the number of lines each log file can contain in the *Lines per file* field.

Cisco Unified Attendant BLF Plug-in Logging

Cisco Unified Enterprise 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 BLF Plug-in's performance and activity, determine functionality loss and the configuration issues.

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

Step 1   Select the *Logging Level* for BLF Plug-in. Cisco Unified Enterprise Attendant Admin provides the following options:

- Detailed
- Advanced

- Minimum
- Full

Step 2   Specify the *Logging path* and *file name* where the log must be created.

Step 3   Specify the number of log files that must be created in the *Number of files* field.

Step 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 the synchronization of devices and directories with Cisco Unified Communications Manager. The following configurations are available under this menu,

1. System Device Management
2. Synchronise with CUCM
3. Directory Synchronization
4. Directory Field Mappings
5. Directory Rules

System Device Management

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

To add devices,
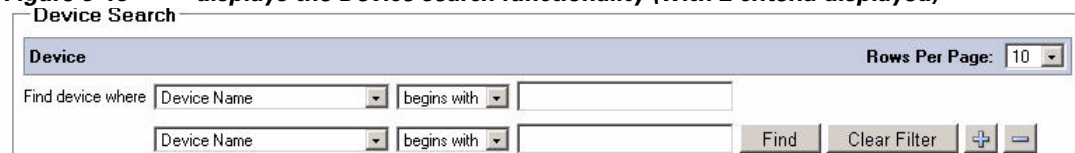
Step 1   Go to *Engineering > System Device Management*.

Step 2   Select a *Template Device*. All device properties (such as device pool, partition, calling search space) of the selected device will be mapped onto new devices being created.When you click on *Find Template Device* you are able to search by a variety of criteria. This criteria is broken into the following entities:-

- Device type e.g. Device Name, Description, Directory Number.
- Search critera e.g. Begins with, Contains, Ends with, etc.
- Specific criteria: The variable to search.
- There is also facility by using the [+] [−] to add additional search criterias. This would be used to narrow the search.

Step 3   Click on *Find* to run the Query.

Figure 5-15   displays the Device search functionality (with 2 criteria displayed)

Step 4   Enter a device range for each of the following:

- CT Gateway Devices (See "CT Gateway Devices" on page 3 - 2)

- Service Devices (See "Service Queues" on page 3 - 2)
- Park Devices (See "Park Devices" on page 3 - 2)

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*

Step 5   Click ![save icon] **Submit** to save changes.

Step 6   Clicking ![sync icon] **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 5-16   *displays the System Device Management page*

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

Table 5-11   *provides description for the fields on the System Device Management page*

Field	Example	Description
Template Device		
Copy all device properties from this device		When you click on *Find Template Device* you are able to search by a variety of criteria. This is criteria is broken into the entity • Device type e.g. Device name, Description, Directory Number. • Search critera e.g. Begins with, Contains, Ends with, etc. • Specific Criteria: The variable to search. There is also facility by using the [+] [−] to add additional search criterias.(To a maximum of 10).
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		

Table 5-11   *provides description for the fields on the System Device Management page*

Field	Example	Description
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.

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,

- Queue Locations
- CT Gateway Devices
- Service Devices
- Park Devices

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

Figure 5-17   displays the devices that will be synchronized with CUCM

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

Table 5-12   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 initialized, 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.

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

Table 5-13   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.
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		

Table 5-13   *provides description for the fields mentioned on the CUCM Sync Report*

Field	Example	Description
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 5-14   *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.
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.

Table 5-14 provides error codes that may be displayed in the CUCM Sync Report

Error Code	Error Description
-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.
9900	An unknown error occured - This is an unknown error.

Directory Synchronization

The *Directory Synchronization* web page provides the ability to synchronize the contact details for the Cisco Unified EnterpriseAttendant 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. **Auto Synchronization:** You can set preferences for automatic synchronization. The following options are available to do so,

   – **On start-up:** If this checkbox is checked then the synchronization is started when Cisco Unified Attendant Server starts.

   – **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.

3. **Route Partition:** In this section you specify the Route Partition. Select from either ALLPartitions or choose a specific partion if required.This will prioritize which DN to import when identical DN's in different partitions are copied over.

4. **Schedule Settings:** This section requires information on the scheduling of the synchronization. You must enter the following information,

   – **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

   – **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)**.

   – **Start date:** This field is used to specify a date to start the synchronization.

   – **Start time:** This field is used to specify the time to start the synchronization.

To configure directory synchronization for Cisco Unified Enterprise Attendant Console,

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

Step 2   Enter specifications for the above-mentioned sections.

Step 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 5-19   displays the settings for Directory Synchronization

Directory Field Mapping

This web page is used to manage information coming from the Cisco CallManager database to the Cisco Unified Attendant Server. The table is broken into a selection column, a Source Field (CUCM), Destination Field (Attendant Server) and a default value if the source file is empty.

Figure 5-20   *displays the Directory Field Mapping*

To Add a New Field for Mapping

Step 1   Go to *System Configuration > Directory Field Mapping*.

Step 2   Click on *Add New*.

Step 3   On the Field MappingInformation, select a *Source field* from the dropdown selection.

Step 4   Select a *Destination field* from the drop down selection.

Step 5   Enter a default value which will be entered if the original Source field is empty.

Step 6   Click Submit to save the changes.

The following image shows the Field Mapping Information screen when a new field is added via the *Add New* button.

Figure 5-21   *displays the Field Mapping Information*

Directory Rules

This web page is used to manage rules that are used to filter the LDAP information coming from the Cisco CallManager database to the Cisco Unified Attendant Server.

Tip   Multiple rules can be created, each with a seperate filter then the import will use each one seperately, using an 'OR' i.e. Rule 1 is lastname = T* and Rule 2 is Department = Product. The result will be an import that includes all people with a lastname beginning with T and all people that are in the product team.

Ifyou create multiple filters within a single rule then an 'AND' is used. i.e. lastname = T* Department = Product, will result in all people in the Product team that have a last name starting with T

The table is broken into a selection column, a Rule Name and a Filter Counter.

Figure 5-22   displays the Directory Rules

To Add a Directory Rule

Step 1   Go to *System Configuration > Directory Rules*.

Step 2   Click on *Add New.*

Step 3   On the RuleFilter Information, select a *Source field* from the dropdown selection.

Step 4   Select an *Operator* from the drop down selection. The selection includes Equal (=), Approx_Equal (like), Less_Equal (<=), Greater_Equal (>=).

Step 5   Enter a default value which will be entered if the original Source field is empty.

Step 6   Click *Submit* to save the changes.

The following image shows the Rule Filter Information screen when a field is addded.

Figure 5-23   displays the Directory Rules - Rule Filter Information

User Configuration

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

- General Properties
- Queue Management
- Operator Management

General Properties

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

1. **Internal/External Access:** These settings allow Cisco Unified Enterprise 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,

   – **Minimum internal device digit length:** This text box requires you to enter the minimum number of digits being used for an internal device.

   – **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. This can be set to manage an internal device with a number of up to 24 digits.

   – **External access number:** This field specifies the access number when making a call to an external number.

   – **External international access number:** This is the number that is to be dialled when making a call to an international external number.

   – **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,

   – **Hold recall:** This is the maximum time limit a call can be put on hold by an operator.

- **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.

- **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.

- **Camp On recall**: When an operator transfers a call to an extension that is busy. the Operator can put that call on Camp On. The Call will wait for that extension to be free for the time as set in 'Camp on Recall' Timer. After that time call returns back to the Operator.

4. **Working Days:** This section allows you to set specific days and hours when the Attendant Console queues will be active. You must specify the following fields,

- The checkboxes provided allow you to select the days the queues are active.

- 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.

Tip   Working Days is a global setting, and may not be suitable in a situation where Queues are specifc to offices that are in different time zones. This scenario could be managed by using *No Operator Overflow* which can be found in *User Configuration > Queue Management.* This would provide the facility to push calls to a specific extension if No Operators are logged into the queue. This does not apply to a queue where an operator is unavailble, i.e. busy with a call.

To configure General Properties,

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

Figure 5-24   displays menu option for General Properties
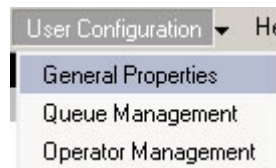
Step 2   Enter specifications for the above-mentioned sections.

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

The following image shows the *General Properties* page used to configure Cisco Unified Enterprise Attendant Console.

Figure 5-25   *displays the setting made on the General Properties page*

Queue Management

The *Queue Management* web page allows you to manage the configuration for existing queues.

To find a Queue,

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

Step 2   To find a queue using the filter options. Select either Name or DDI, then enter search criteria option and then the specific criteria. This criteria is broken into the following entities

- Queue type: Name and DDI number.

- Search critera e.g. Begins with, Contains, Ends with, etc.

- Specific criteria: a variable to search.

- There is also facility by using the ⊞ ⊟ to add additional search criterias. This would be used to narrow the search.

Step 3   Click on *Find* to run the Query.

Figure 5-26   displays the Queue Management screen)

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,

    –   **Name:** This field specifies the name of the queue.

    –   **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.

    –   **Priority:** You can assign a priority number to a queue that determines which queue must be given priority when calls are being routed.

    –   **Salutation**: A specific salutation or greeting can be entered here.

2. **Emergency :** 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,

    –   **Overflow number:** In case of an overflow the exceeding number of calls will be transferred to the number specified in this field.

    –   **Maximum calls:** This field allows you to set the total number of calls that can wait in a Queue at any given time.

    –   **No operator overflow:** If there is no operator logged in to this selected queue, an incoming call will be immediately routed to the *Overflow number* if this checkbox is selected.

4. **Night Service:** This section allows you to specify a *Night service number.* The calls made outside of the days and time specified for working day, are routed to this number.

To manage queues,

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

Figure 5-27   displays the menu option for Queue Management
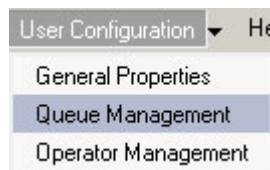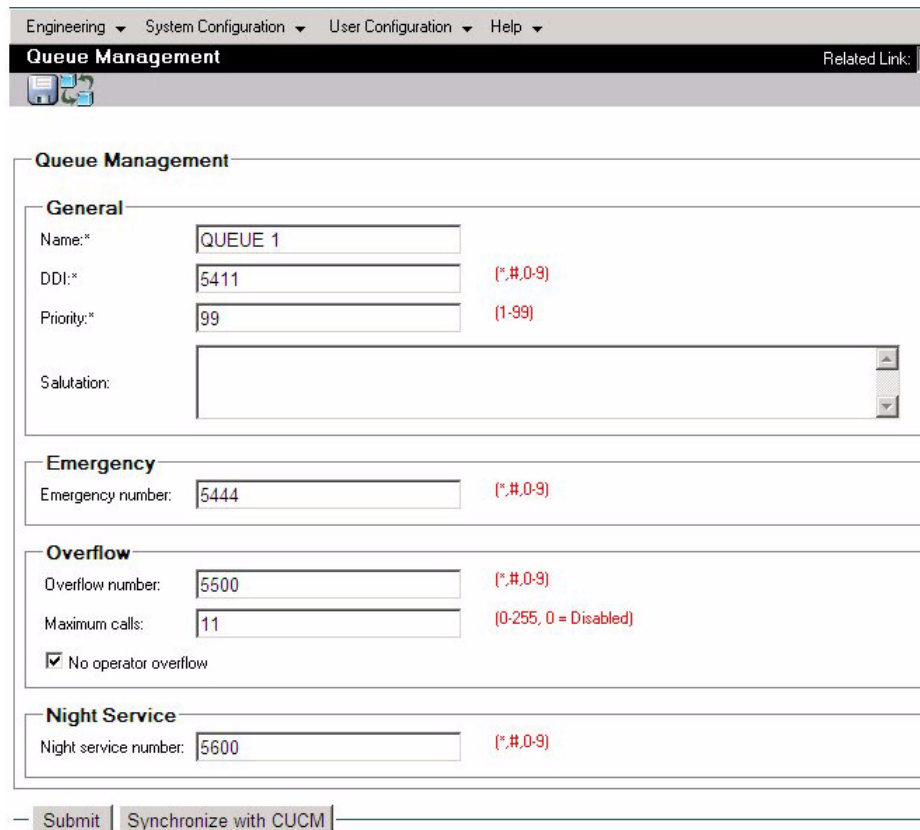
Step 2   Select the queue profile that needs to be modified. Once the queue is selected, the form will be automatically loaded with the queue configuration.

Step 3   Edit the specifications for the above-mentioned sections.

Step 4   Once you have modified the configuration, click ![floppy icon] **Submit** to save the changes.

Step 5   Click ![sync icon] **Synchronize with CUCM** will redirect to *Synchronizing with CUCM* page.

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

Figure 5-28   **displays the Queue Management page for Cisco Unified Enterprise Attendant Console**

Operator Management

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

To manage operators,

Step 1   Select *User Configuration > Operator Management*.

Figure 5-29   *displays the menu option for Operator Management*

Step 2   Select the operator profile that needs to be modified. To use the *find* option enter the following criteria,

- Login Name.
- Search critera e.g. Begins with, Contains, Ends with, etc.
- Specific criteria: The variable to search.
- There is also facility by using the [+] [−] to add additional search criterias. This would be used to narrow the search.

Step 3   Click on *Find* to run the Query.

Step 4   Once an operator profile is selected, the form will be automatically loaded with the operators profile information.

Step 5   Edit *Login name*.

Step 6   Change *Password*.

Step 7   Re-enter password to confirm in the *Confirm password* field.

Step 8   Click 💾 **Submit** to save changes.

Step 9   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 Enterprise Attendant Console.

Figure 5-30   *displays Operator Management page*

To Associate Queues to an operators profile,

Step 1   Select *User Configuration > Operator Management*.

Step 2   Select the operator profile that needs to be modified. To use the *find* option enter the following criteria,

- Login Name.

- Search critera e.g. Begins with, Contains, Ends with, etc.

- Specific criteria: The variable to search.

- There is also facility by using the [+] [−] to add additional search criterias. This would be used to narrow the search.

Step 3 Click on *Find* to run the Query.

Step 4 Once an operator profile is selected, the form will be automatically loaded with the operators profile information.

If any Queues have been associated, they will be listed in the Associated Queues dialogue box.

Step 5 To Add to that list, or create an association, click on *Queue Association*.

A new screen will appear where you can select any Queues that need to be associated.

Figure 5-31   *displays Queue Association page*

There is an option to search for a specific queue if it is not displayed by using either:-

- Queue Name.

- Search critera e.g. Begins with, Contains, Ends with, etc.

- Specific criteria: The variable to search.

- There is also facility by using the [+] [−] to add additional search criterias. This would be used to narrow the search.

Step 6 Click on *Find* to run the Query.

Step 7 Tick the respective Queues that are required to be associated then click on *Save Selected/Changes* to return the operator profile. Click on *Submit* to complete the process.

C H A P T E R 6

Uninstall Attendant Admin

Revised: February 20th, 2009, OL-18667-01

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,

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

Figure 6-1   displays the Add/Remove Programs window
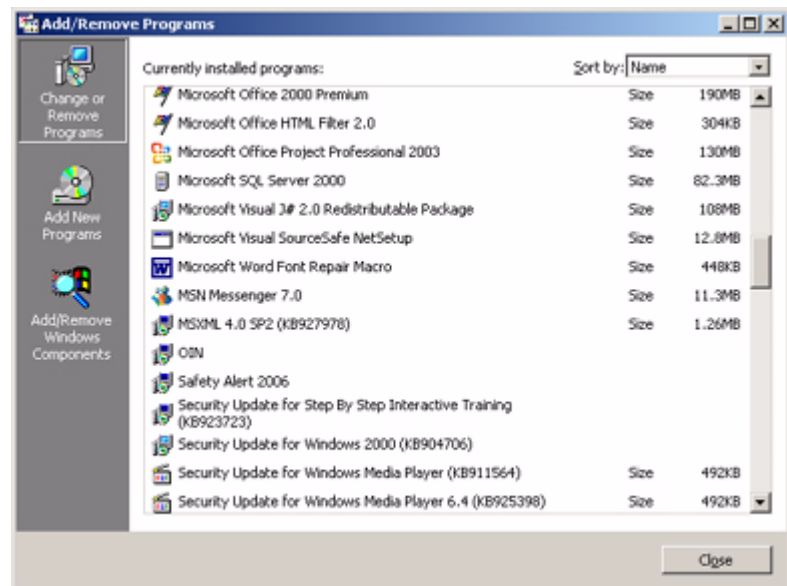
Step 2   Select Cisco Unified Attendant Server from the list of Programs. Click **Remove**.

Step 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 6-2   displays the Preparing to Install screen
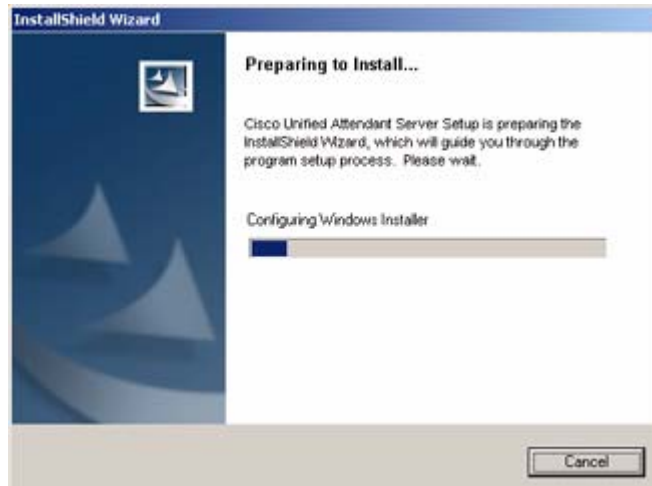
Step 4   The following message box will appear confirming whether you want to remove Cisco Unified Attendant Server from your machine or not. Click **OK** to continue.

Figure 6-3   displays the message box that asks you if you want to remove the application from the system

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

Figure 6-4   displays the un-installation progress of the application
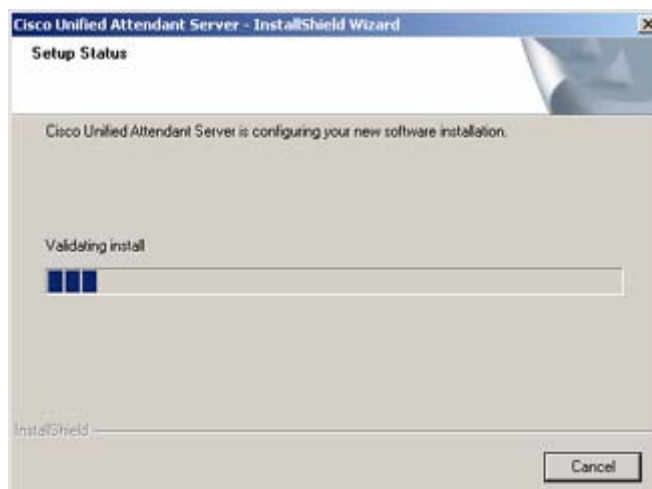
Step 6   Once the files have been uninstalled successfully, the next window will ask whether you wish to restart the computer now or later. It is recommended that you restart the machine. Click **Finish**.

Figure 6-5   *displays the options for restarting the machine*
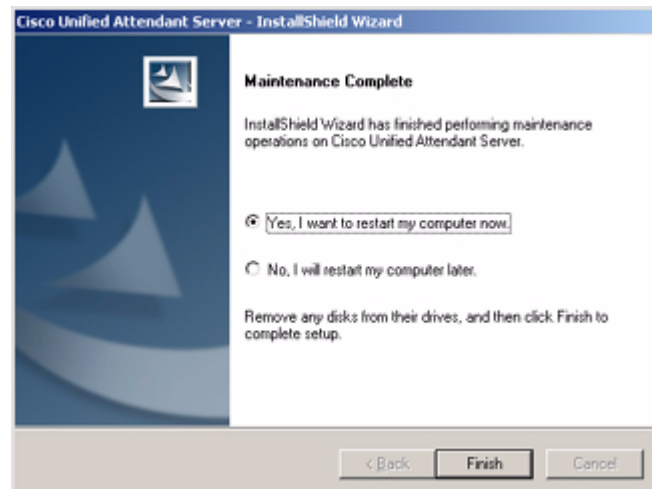
Uninstalling MS SQL Server

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,

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

Figure 6-6   *Figure 6: displays the Add/Remove Programs window*
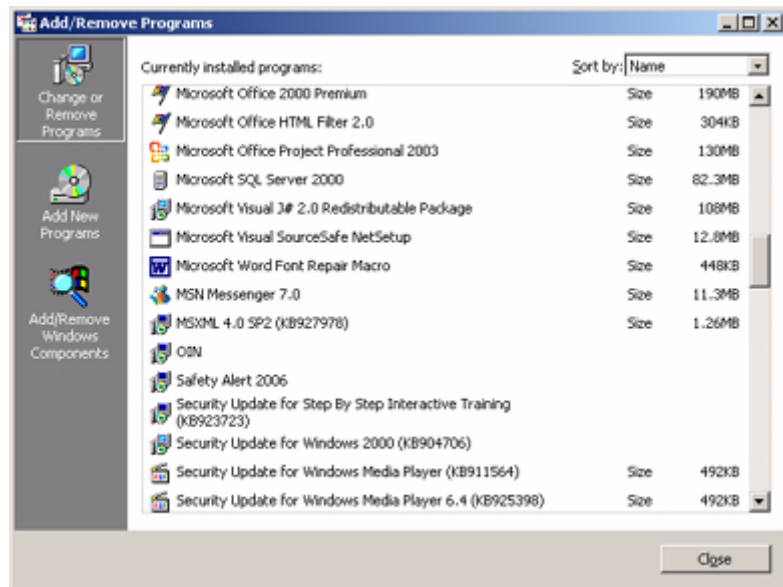
Step 2   Select Microsoft SQL Server from the list of Programs. Click **Remove**.

Step 3   The next window will display the list of server instances. Select the instance that you wish to be removed.

Figure 6-7   *displays the server instance to be removed*
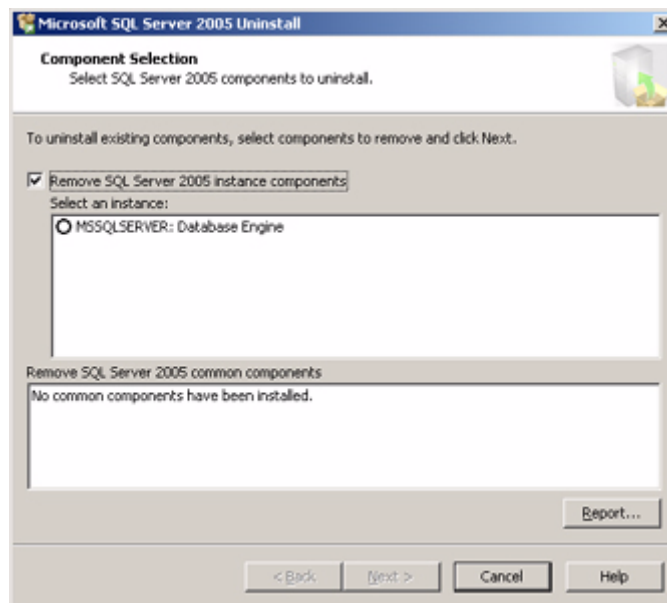
Step 4   The next window will display a summary of the components that will be removed. Click the **Finish** button to proceed. Click **Back** in case you wish to change any of the information.

Figure 6-8   *displays the summary screen for the components that need to be uninstalled*
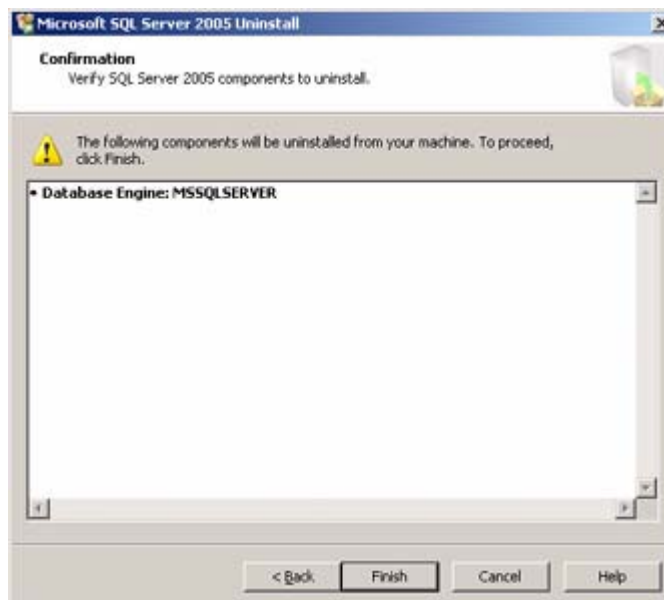
Step 5   In the next window, the status will be displayed for the components removal. Click **Finish** once all the components have been removed.

Figure 6-9   *displays the setup progress*
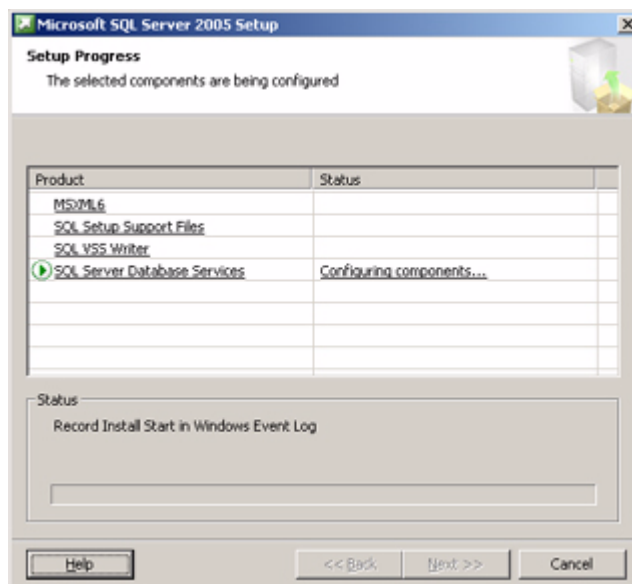
Step 6   Once you have uninstalled MS SQL Server, you must delete the following location and the databases within,

    C:\DBdata\

Uninstalling BDE Utility

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

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

Figure 6-10   displays the Add/Remove Programs window
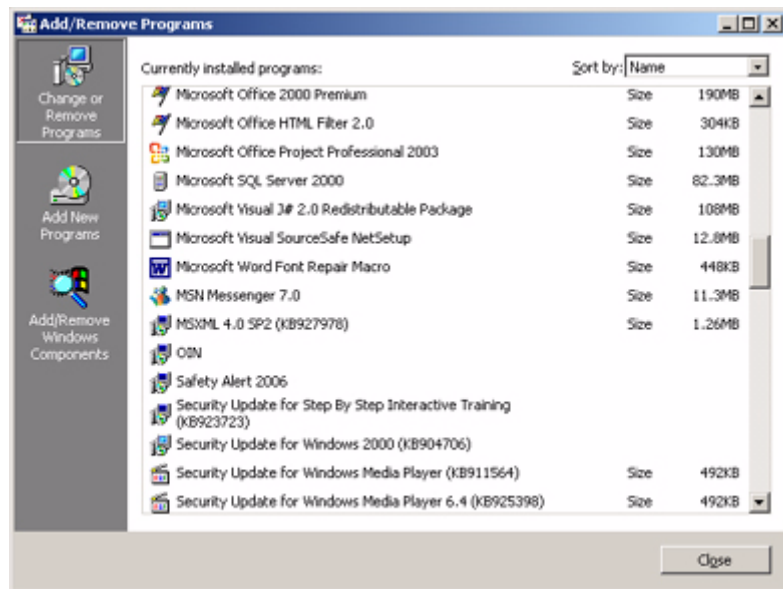
Step 2   Select BDE Utility from the list of Programs. Click **Remove**.

Step 3   The next window that is displayed will show the status of the wizard while the files are being prepared to uninstall BDE.

Figure 6-11   displays the Preparing to Install screen
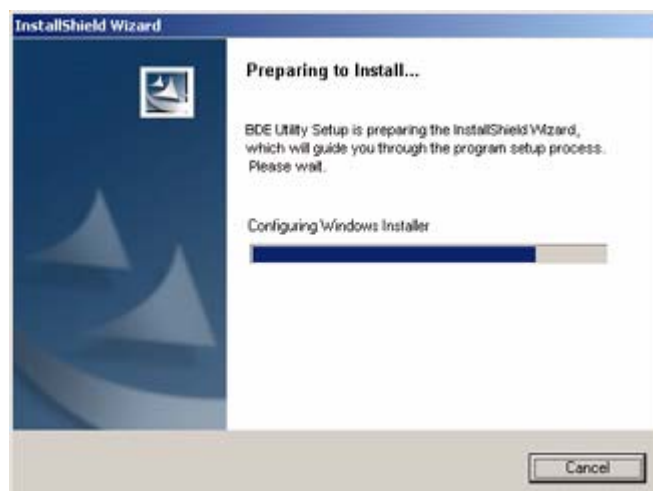
Step 4   The next message box will confirm whether you wish to remove BDE or not. Click **OK** to continue.

Figure 6-12   *displays the message box to confirm whether all features of the BDE Utility need to removed or not*

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

Figure 6-13   *displays the setup status for the uninstallation of the application*
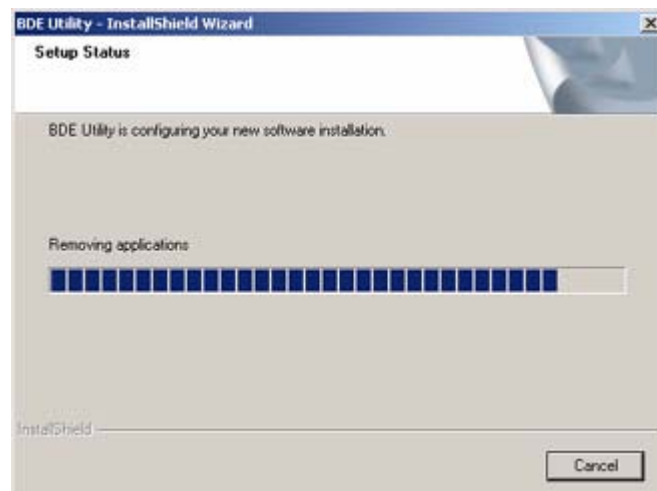
Step 6   Once the BDE Utility has been removed the following screen will appear.

Figure 6-14   *displays the screen that shows that the removal of BDE Utility is complete*
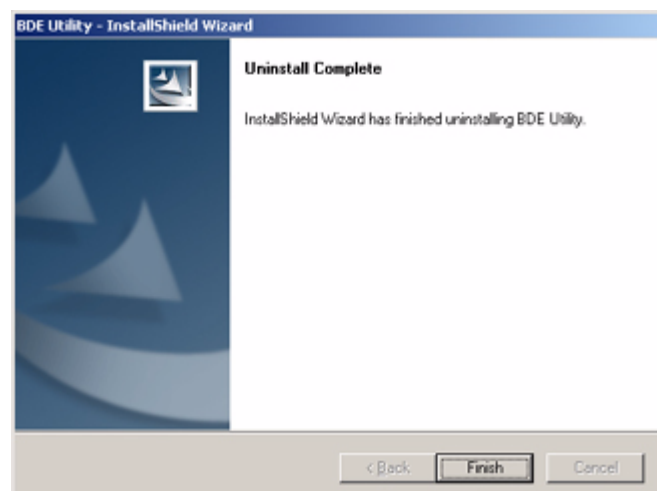
Uninstalling .NET Framework

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

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

Figure 6-15   ***displays the Add/Remove Programs window***
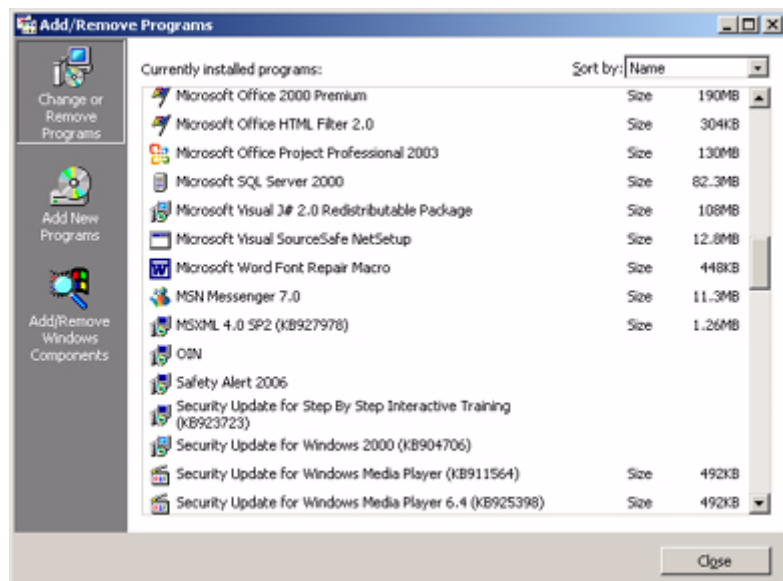
Step 2   Select Microsoft .NET Framework 3.5 from the list of Programs. Click **Remove**.

Step 3   The next window provides you with the option to either repair the installed files or uninstall .NET Framework.

Figure 6-16   ***displays the option to either repair or uninstall .NET Framework***
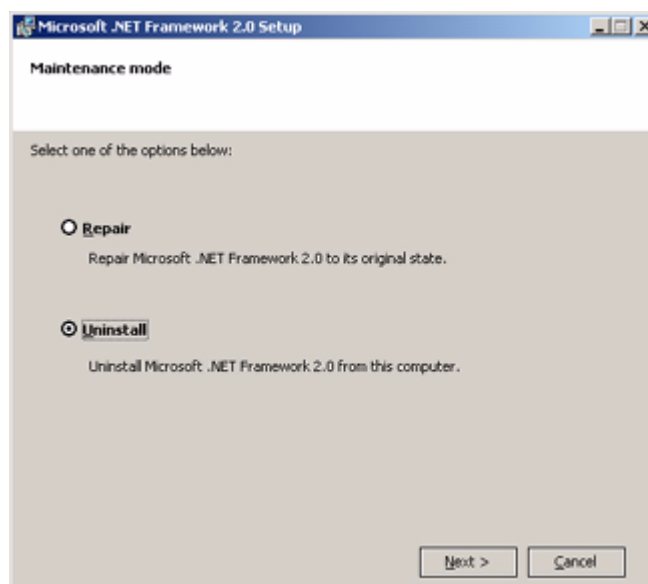
Step 4   The next message box will appear confirming if you would like to remove .NET Framework. Click **OK**.

Figure 6-17   ***displays the message box to confirm whether you wish to remove .NET Framework or not***
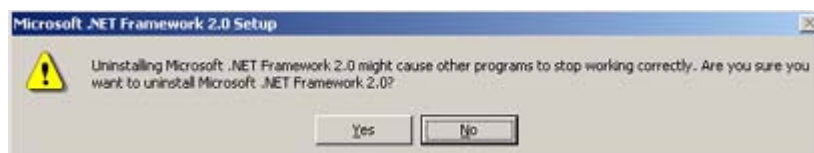
Step 5   The next window will display the setup progress of the components being removed.

Figure 6-18   ***displays the setup progress for the uninstallation of .NET Framework***
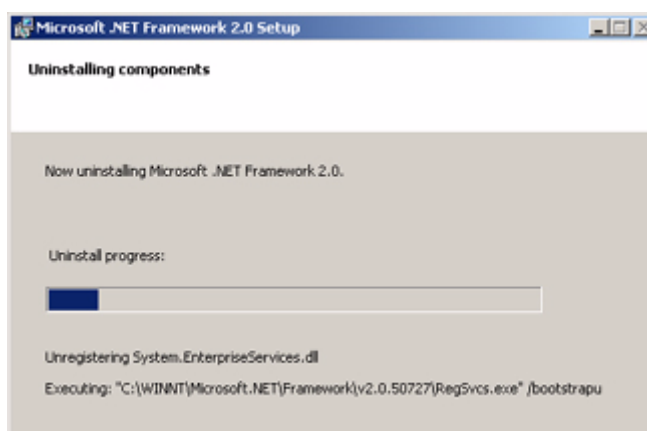
Step 6   The next window will display that the components have been uninstalled successfully. Click **Finish**.

Figure 6-19   ***Figure 19: displays the message that the .NET Framework components have been removed successfully***
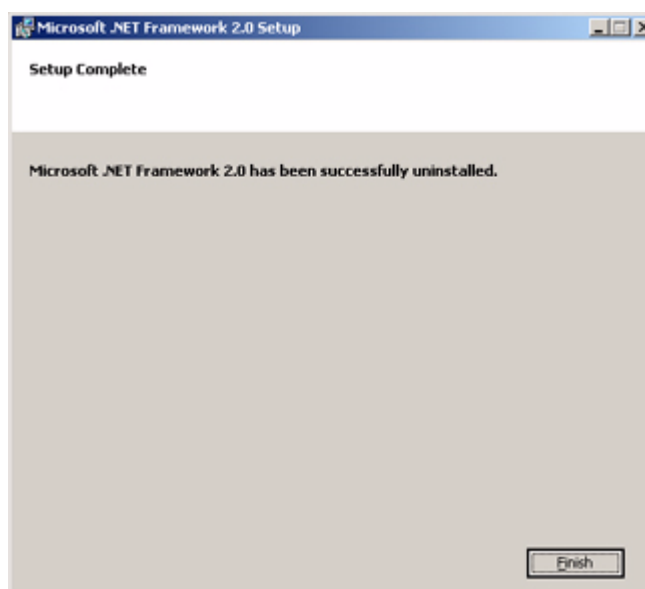
Creating the Attendant Application End User for CallManager 6.x

Revised: February 20th, 2009, OL-18667-01

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 Eneterprise 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 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,

Step 1   Choose *User Management > End User.*

Figure A-1   ***displays menu option for End User configuration***

Step 2   Click the ![plus] button to add a new user.

Step 3   Enter information in the following fields. Please note that the fields mentioned below are mandatory.

- User ID
- Password
- Confirm Password
- PIN
- Confirm PIN
- Last Name

Figure A-2   ***displays the End User Configuration page***

Step 4   Click ![save] **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,

Step 1   Choose *User Management > User Groups*.

Figure A-3   **displays the menu option for User Group**

Step 2   Click the button to add a new user group.

Step 3   Enter *Name* for the new user group.

Figure A-4   **displays the User Group Configuration page**

Step 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,

Step 1   Choose *Back To Find/List > Go* or *User Management > User Groups*.

Step 2   On *Find and List User Groups* page, search for the user group you created.

Figure A-5   **displays the field you may use to search a user group**

Step 3   In the *Search Results*, click on the *Roles* link 🛈 for the user group.

Step 4   Click **Assign Role to Group** to find and list roles for assignment.

Step 5   Select the roles that need to be assigned to this group. The following checkboxes must be selected,

- *Standard CTI Allow Call Park Monitoring*
- *Standard CTI Allow Calling Number Modification*
- *Standard CTI Allow Control of All Devices*
- *Standard CTI Allow Reception of SRTP Key Material*
- *Standard CTI Enabled*

✎
Note   *Standard CTI Secure Connection* should ONLY be enabled if required, as it may affect the operation of the server that is not using CTI secure connections.

Step 6   Click **Add Selected** to assign roles.

Step 7   Click **Save**.

To add the End User to the User Group,

Step 1   Choose *User Management > User Groups*.

Step 2   Click the newly created User Group.

Step 3   Click **Add End Users to the Group** to find and list the users.

Figure A-6   *displays the User Group Configuration page*
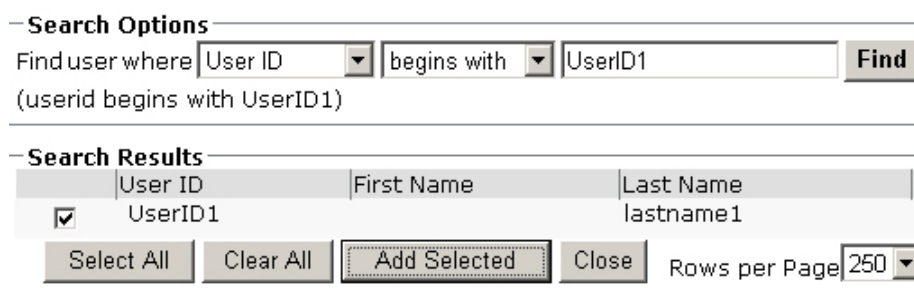
Step 4 Select the newly created End user from the list and click **Add Selected** to successfully add the user to the group.

Figure A-7   *displays the search field you may use to search for a User ID*

Adding the 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,

Step 1 Choose *User Management > User Groups*.

Step 2 Find **Standard Super CCM User** using the search field.

Figure A-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 | **Find**

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

Figure A-9   displays the search result for the user group

Search Results
Name
Standard CCM Super Users

Add New | Select All | Clear All | Delete Selected | Rows per Page 50 ▼

Step 4   Click **Add End Users to the Group** to find and list the users.

Step 5   Select the newly created End user from the list and click **Add Selected** to successfully add the user to this group.

Figure A-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	

Select All | Clear All | Add Selected | Close | Rows per Page 250 ▼

Configuring Access for the Cisco Unified Attendant CUPS Plug-In

It is important that the Cisco Unified Attendant Server Address is added to the firewall information on the CUPS Server.

Step 1   To do this go to Cisco Unified Presence menu, and select Proxy Server and Incoming ACL (access control list)

Figure A-11   displays accessing the Cisco Unified Presence Proxy Server, Incoming ACL menu.
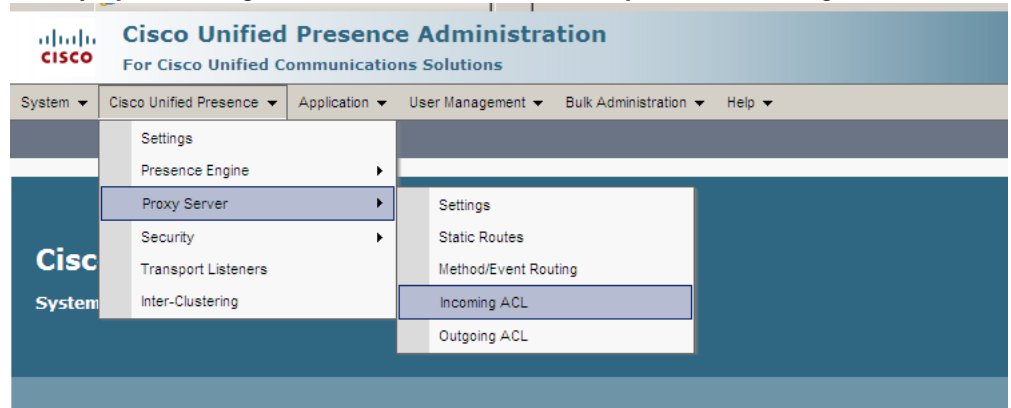
The page *Find and List Allowed Incoming Hosts* will be displayed.

Figure A-12   Displays Find and List Allowed Incoming Hosts page
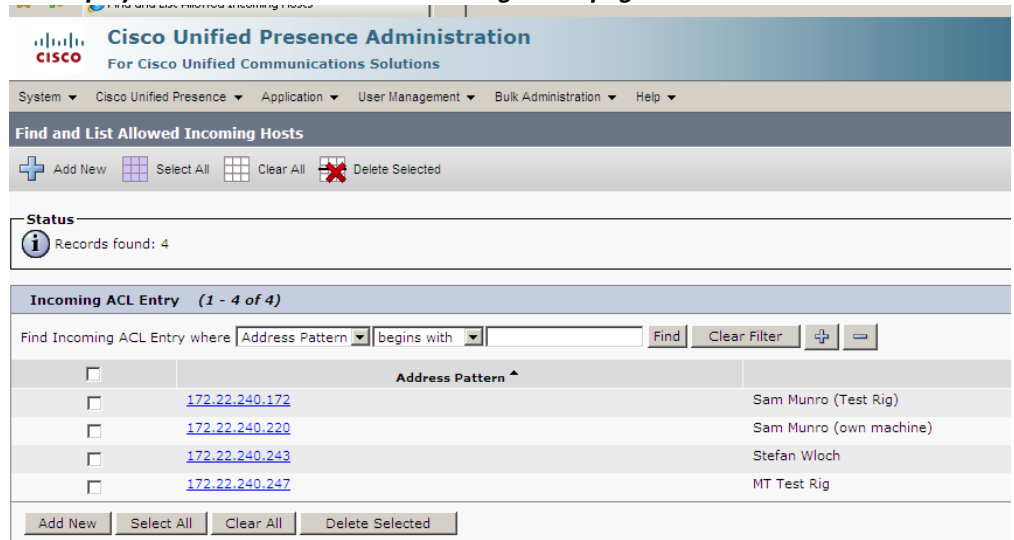
Step 2   Click on **Add New** and enter the **Description** and **Address Pattern**.

Figure A-13   *displays Incoming Access Control List Configuration page*

Step 3   Click on **Save**.

Step 4   Confirm the address and description have been added.

Creating the Attendant Application End User for CallManager 7.x

Revised: February 20th, 2009, OL-18667-01

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 Enterprise 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 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,

Step 1 Choose *User Management > End User.*

Figure B-1   ***displays menu option for End User configuration***
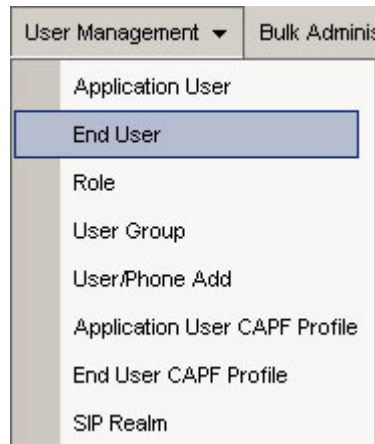
Step 2   Click the ✚ button to add a new user.

Step 3   Enter information in the following fields. Please note that the fields mentioned below are mandatory.

- User ID
- Password
- Confirm Password
- PIN
- Confirm PIN
- Last Name

Figure B-2   ***displays the End User Configuration page***

Step 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,

Step 1   Choose *User Management > User Groups*.

Figure B-3   displays the menu option for User Group
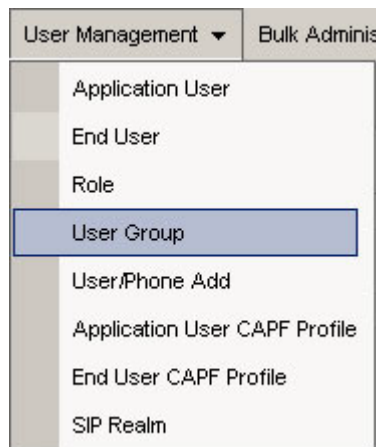
Step 2   Click the ➕ button to add a new user group.

Step 3   Enter *Name* for the new user group.

Figure B-4   displays the User Group Configuration page

Step 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,

Step 1   Choose *Back To Find/List > Go* or *User Management > User Groups*.

Step 2   On *Find and List User Groups* page, search for the user group you created.

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

Step 3   In the *Search Results*, click on the *Roles* link 🛈 for the user group.

Step 4   Click **Assign Role to Group** to find and list roles for assignment.

Step 5   Select the roles that need to be assigned to this group. The following checkboxes must be selected,

- *Standard CTI Allow Call Park Monitoring*
- *Standard CTI Allow Calling Number Modification*
- *Standard CTI Allow Control of All Devices*
- *Standard CTI Allow Reception of SRTP Key Material*
- *Standard CTI Enabled*

Note   *Standard CTI Secure Connection* should ONLY be enabled if required, as it may affect the operation of the server that is not using CTI secure connections.

Step 6   Click **Add Selected** to assign roles.

Step 7   Click **Save**.

To add the End User to the User Group,

Step 1   Choose *User Management > User Groups*.

Step 2   Click the newly created User Group.

Step 3   Click **Add End Users to the Group** to find and list the users.

Figure B-6   *displays the User Group Configuration page*

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

Figure B-7   *displays the search field you may use to search for a User ID*

Adding the 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,

Step 1   Choose *User Management > User Groups*.

Step 2   Find **Standard Super CCM User** using the search field.

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

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

Figure B-9   displays the search result for the user group

Step 4   Click **Add End Users to the Group** to find and list the users.

Step 5   Select the newly created End user from the list and click **Add Selected** to successfully add the user to this group.

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

Configuring Access for the Cisco Unified Attendant CUPS Plug-In

It is important that the Cisco Unified Attendant Server Address is added to the firewall information on the CUPs Server.

Step 1   To do this go to Cisco Unified Presence menu, and select Proxy Server and Incoming ACL (access control list)

Figure B-11   *displays accessing the Cisco Unified Presence Proxy Server, Incoming ACL menu.*

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

Figure B-12   *Displays Find and List Allowed Incoming Hosts page*

Step 2   Click on **Add New** and enter the **Description** and **Address Pattern**.

Figure B-13   *displays Incoming Access Control List Configuration page*

Step 3   Click on **Save**.

Step 4   Confirm the address and description have been added.

A P P E N D I X C

TAPI Configuration

Revised: February 20th, 2009, OL-18667-01

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 Enterprise 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,

Step 1   Select *Application > Plugins*.

Figure C-1   *displays the menu option for plugins*
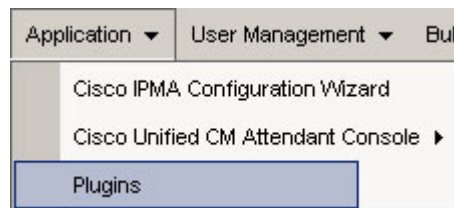
Step 2   Find Cisco Telephony Service Provider using the search field.

Figure C-2   *displays the search option to find and list the required plugin*
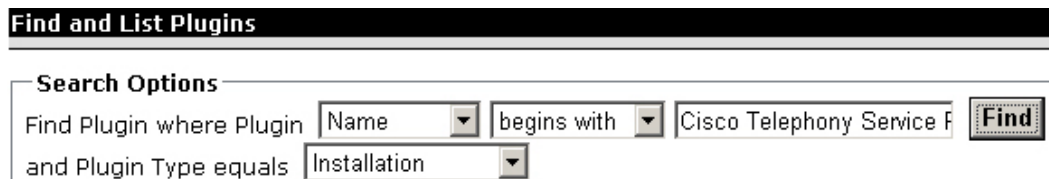
Step 3   In the Search Results, click Download on the Cisco Telephony Service Provider line.

Step 4   Save **CiscoTSP.exe** on your desktop.

Step 5   Double Click the **CiscoTSP.exe** icon on the desktop and follow the on screen instructions to complete the install.

Step 6   During the installation, you will be asked if you want to install multiple instances of TSP. Click **No**.

Figure C-3   ***displays the message box confirming whether multiple instances for TSP are to be installed or not***
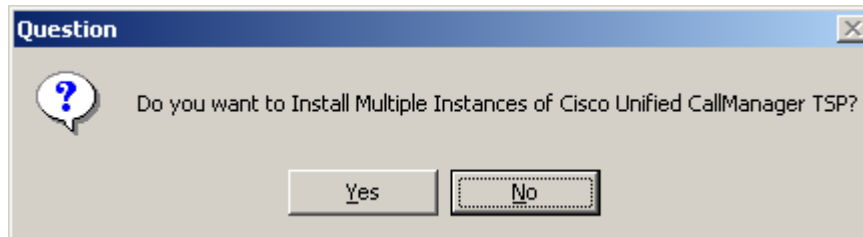
Step 7   After a successful installation the setup will prompt you to restart the system. You must restart the machine for the changes to take effect

.

Configuring the TAPI TSP

To configure TSP.

Step 1   Go to *Start > Settings > Control Panel > Phone and Modem Options*.

Step 2   Select *Advanced* tab.

Step 3   Select CiscoTSP001.tsp.

Step 4   Click **Configure**.

Step 5   Enter the End User ID of the user that was created for the CallManager earlier in the *User Name* field.

Step 6   Enter the password of the user in the *Password* field.

Figure C-4   ***displays the End User ID information to be entered in the fields***
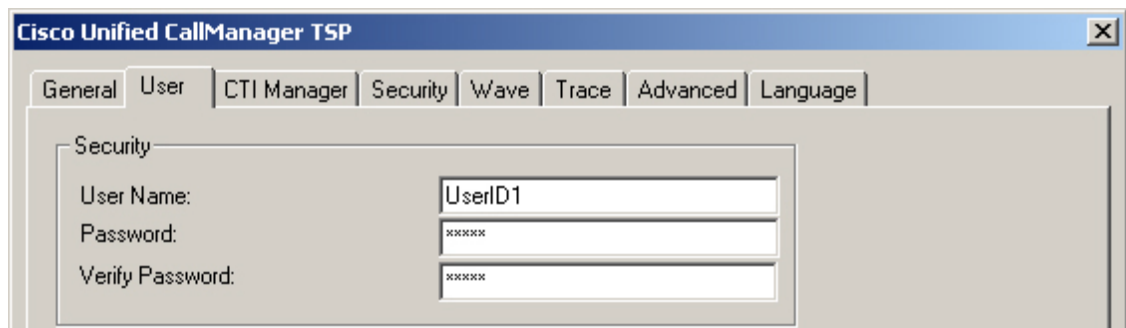
Step 7   Select the *CTI Manager* tab,

Figure C-5   ***displays the CTI Manager information to be entered for the TAPI configuration***

Step 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.

Step 9   Select the *Wave* tab.

Step 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.

Figure C-6   displays the Wave configuration for TAPI
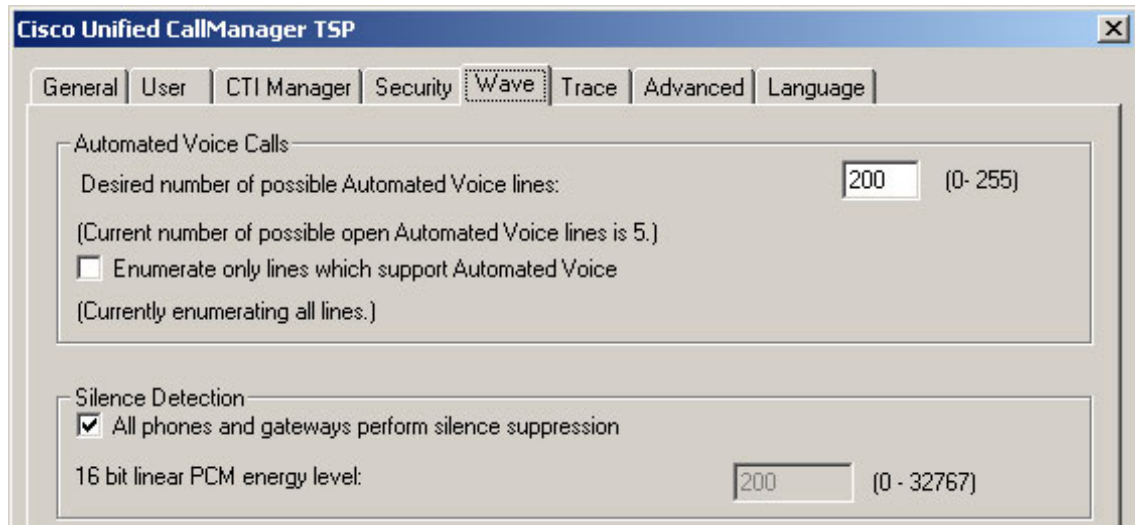
Note   By default Voice lines is set to 5. If when your installation is complete, your devices are not monitored, this should be the first place to check that the number set is sufficient to cover the CTI Ports required.

Note   You will also need to uninstall and reinstall the Cisco TAPI Wave driver every time you change the Voice Lines figure.

Step 11   Click **OK**.

Step 12   Select *Advanced* tab.

Step 13   In the Provider Open Completed Timeout (secs) field enter 300.

Step 14   Click **OK**. Reboot the machine.

Note   After completing the TSP configuration you will need to install the *Cisco TAPI Wave* driver.

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.

Step 1   From Control Panel execute the *Add Hardware* utility. Click the **Next** button.

Step 2   Select **Yes, I have already connected the hardware** Radio button. Click **Next**.

Step 3   Select **Add a new Hardware device** from the list. Click the **Next** button.

Step 4   Select **Install the hardware that I manually select from a list** radio button. Click the **Next** button.

Step 5   Select **Sound, video and game controller** when prompted for hardware type. Click the **Next** button.

Step 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**.

Step 7   Click **Open** to install the Cisco Wave Driver and select **OK**.

Step 8   Highlight the **Cisco TAPI Wave Driver** in Select a Device Driver window and select **Next**. Select **Next** in **Start Hardware Installation** window.

Step 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*.

Step 10   You will be prompted to reboot the server. Do so.

Step 11   TAPI has now been successfully installed.

Downloading, Updating and registering Software

Revised: February 20th, 2009, OL-18667-01
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 Enterprise Attendant Applications

The Cisco Unified Enterprise 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 Unified Enterprise Attendant Console Applications it is recommended that you back up the Cisco Folder, backup of DBs and within the Registry the backup of Arc Solutions folder.

Accessing the Solutions + Website

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

Go the website http://www.cisco.com/go/ac

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

Step 1 Enter your *User Name* and *Password* to **Log In** to the web site.

Figure D-1   Solutions + Log In screen

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 D-2   Cisco User Registration

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 D-3   ***Confirming your Reseller***

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 D-4   ***Completing the Account creation***

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 D-5   ***Welcome Screen***
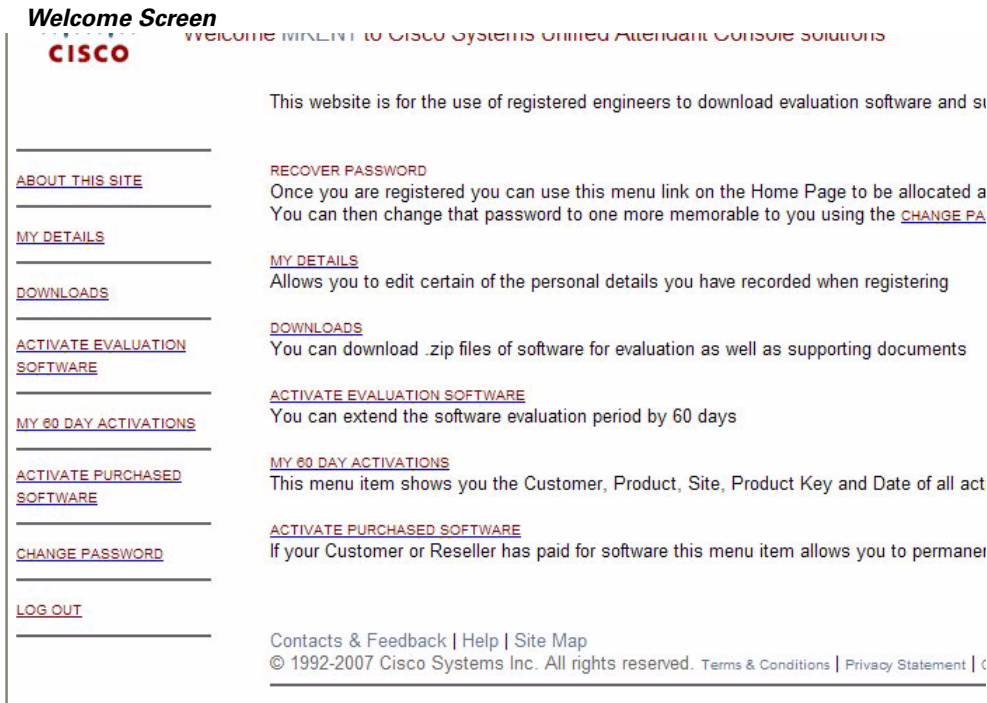
My Details

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.
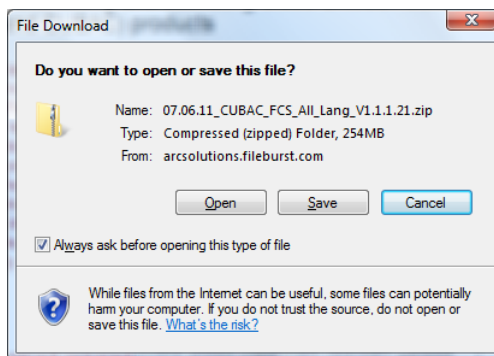
Downloads

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 D-6   *Download Screen*
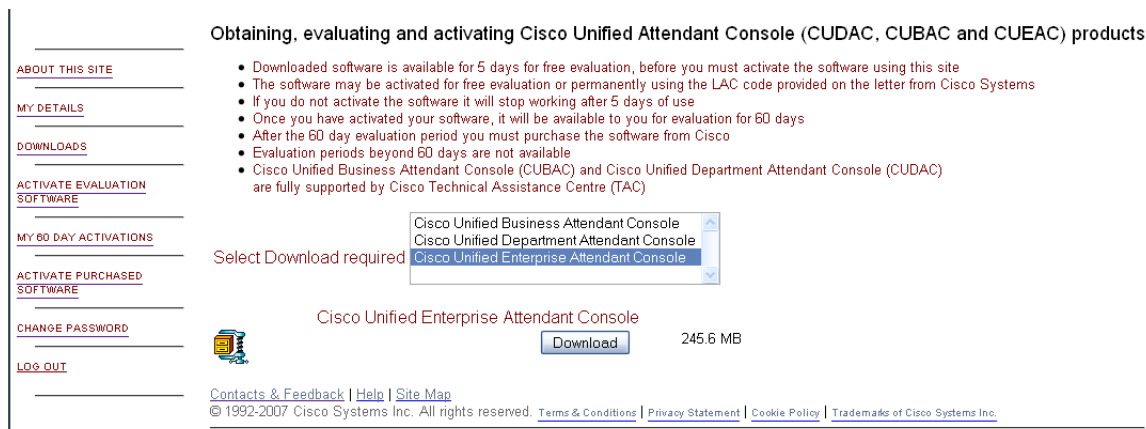
When the software required is selected the screen will display the file format and the size of the download.

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 D-7   *File Download prompt to either Open or Save*

Note   The download for CUEAC is around 250mb. The contents include SQL database, explorer, installs, languages and the software.

When the software has been downloaded, continue with the installation process described in Section 4 Installation Checklist and Procedure for Cisco Unified Enterprise Attendant Admin 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 via a drill down method across three screens.

- Registration code from an installed Cisco Unified Enterprise Attendant Console software. This information is obtained from the *Help* menu within Cisco Unified Enterprise Attendant Console Web Admin.

Figure D-8   License Management screen within CUEAC software

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 D-9   60 Day Software Activation - Selecting a Reseller

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

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

Figure D-10   60 Day Software Activation - Software Activation (Product Key)

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 D-11   60 Day Software Activation - Confirmation screen

Figure D-12   The confirmation email with the activation code

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

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

Figure D-13   License Management screen

Figure D-14   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   After Applying the License the services should be stopped and restarted.

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 D-15   ***Activate Purchased Software***

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

Figure D-16   ***Activate Purchased Sofware - Entering the LAC 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 Enterprise
Attendant Console Web Admin.

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

Figure D-17   *License Management screen within CUEAC software*
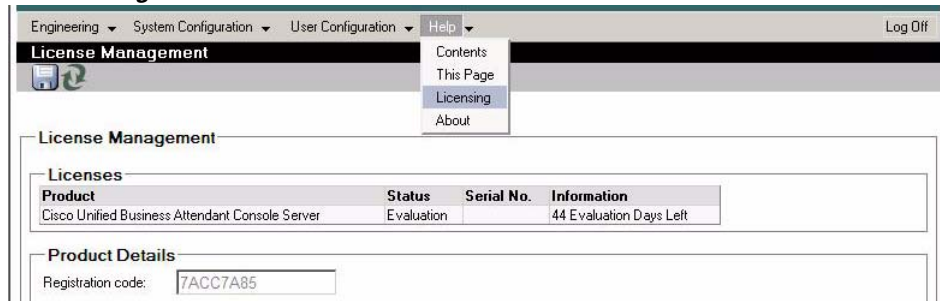
Figure D-18   *Activate Purchased Software - Product Key*
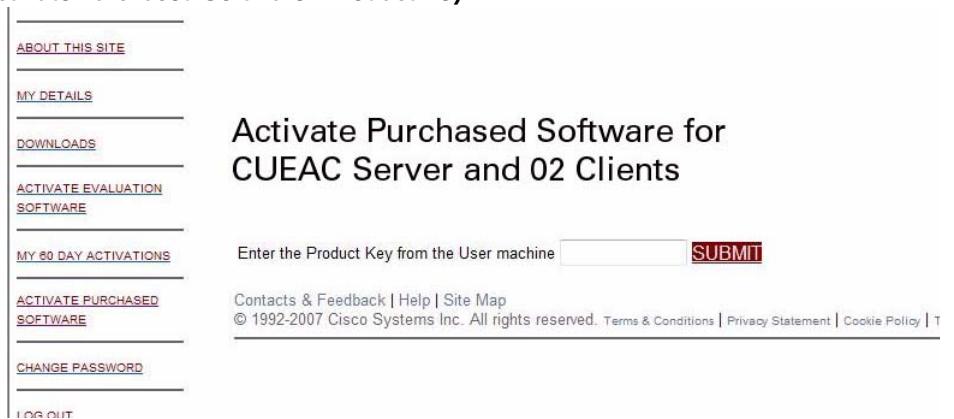
When you click **Submit**. The Activation Code will be emailed out to the registered email address, and a confirmation screen will confirm this.

Figure D-19   *Software Activation - Confirmation screen*
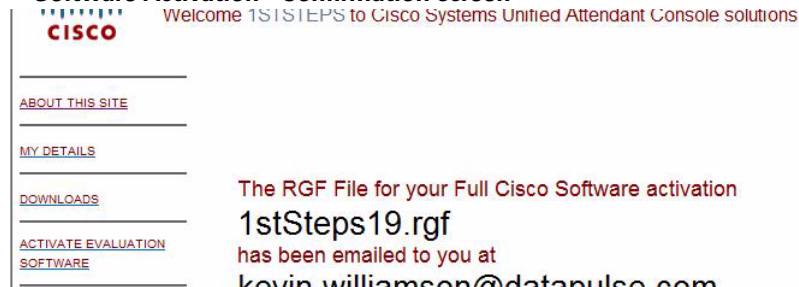
Figure D-20   *The confirmation email with the activation code*
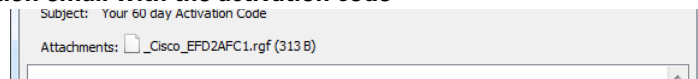
Save the Activation code to a location where it can be browsed to from the Cisco Unified Enterprise Attendant Console Web Admin server.

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

Figure D-21   *License Management screen*
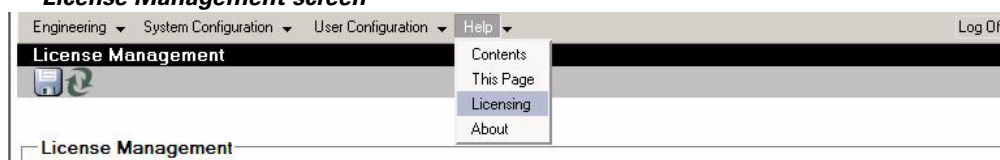
Figure D-22   *License Management screen - Registration File*

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

Note   After Applying the License the services should be stopped and restarted.

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.
CUPs	Cisco Unified Presence is a standards-based platform that collects information about a user's availability and communications capabilities to provide unified user presence status and facilitate presence-enabled communications for Cisco Unified Communications and critical business applications.

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.

C O N T E N T S

U

W