Cisco Unified CallConnector for Microsoft Windows®, Server/Mobility Edition

Administrator Guide (Version 1.5.0)

Cisco Unified CallConnector for Microsoft Windows®, Server/Mobility Edition

Administrator Guide (Version 1.5.0)

Table of Content

CHAPTER

1

Preface

This chapter introduces Cisco Unified CallConnector Server for Microsoft Windows® (referred to as the Unified CallConnector Server or as the UCC Server) and the Cisco Unified CallConnector Mobility for Microsoft Windows® (referred to as the Unified CallConnector Mobility or UCC Mobility), describes the purpose of this document, and outlines the required software. This document describes the configuration of the UCC Server and UCC Mobility version 1.5)

The chapter includes the following topics:

- Purpose
- Audience
- Organization
- Related Documentation
- Required Software
- Supported Windows Platforms
- Conventions
- Obtaining Documentation
- Documentation Feedback
- Cisco Product Security Overview
- Obtaining Technical Assistance
- Obtaining Additional Publications and Information

.

Purpose

This manual is intended for system administrators and technical support individuals who will be setting up and configuring the Unified CallConnector Server and the Unified CallConnector Mobility Service.

Unified CallConnector Server consists of a set of server applications that provide shared access to control of telephones, database and services to the Unified CallConnector clients. This purpose of this guide is to provide step-by-step instructions to install and setup these server applications.. The document also provides instructions for using the diagnostic tool to isolate problems encountered in the operation and usage of the CallConnector solution.

This document also provides links to additional product information and the methods and options for accessing support. The last chapter provides some troubleshooting information to allow you to isolate problems that you might be experiencing.

Audience

This manual is intended for system administrators and technical support personnel who will be setting up and configuring the Unified CallConnector Server and the Cisco Unified CallConnector Mobility and supporting the Unified CallConnector end-users.

The administrative guide assumes that you know the basics of using your computer and are familiar with Windows, using a mouse and selecting items from a dialog box.

Organization

This guide contains nine chapters:

Preface -	This chapter provides an overview of the Administrator Guide and describes how to use the manual.
Overview -	This chapter provides an overview of the Unified CallConnector Solution and describes the configurations for the Unified CallConnector server.
Installation-	This chapter describes how to install and register the Unified CallConnector Server.
Configuring Cisco Unified CME-	This chapter provides instructions for setting up the required parameters on the Cisco Unified CME router.
Configuring UCC Server -	This chapter describes how to setup and configure the Unified CallConnector Server application and the users.
Configuring UCC Mobility -	This chapter describes how to setup and configure the Unified CallConnector Mobility application and the users.
Starting and Stopping -	This chapter describes how to start and stop the Unified CallConnector server applications which run as Windows services.
Managing Data -	This chapter describes how to manage the configuration and transaction data associated with the Unified CallConnector server.
Using Diagnostic Tool -	This chapter provides step-by-step instruction for running the diagnostic application and the problem isolation tests.
Troubleshooting UCC Server-	This chapter describes the tools and procedures for troubleshooting problems with your the Unified CallConnector solution.
Troubleshooting UCC Mobility-	This chapter describes the tools and procedures for troubleshooting problems with your the Unified CallConnector solution.

Related Documents

For more information about the Unified CallConnector please visit the Cisco System site:

http://www.cisco.com/go/unifiedcallconnector

Required Telephone Systems

The Unified CallConnector supports the following Cisco Systems Unified Communications managers and telephones. Please visit the Cisco Systems site for the Unified CallConnector for the latest product compatibility list.

Cisco Unified Communications Manager Express version 4.1, 4.2 (XW9), 7.0 12.4(20)T1).

Supported Windows Platforms

The following Windows operating systems and application versions are supported by the Unified CallConnector Server. Please visit the Cisco Systems site for the Unified CallConnector for the latest product compatibility list

Windows 2003 Server, Windows XP SP2, Windows Vista and Windows 2008 Server
Microsoft Internet Explorer version 6.0 and 7.0

Conventions

The following conventions are used in this 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 brackets and separated by vertical bars.
string	An unquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information that 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 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 hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

Conventions Used

The following conventions are used in this guide:

Most of the operations of the Unified CallConnector Server applications can be initiated by using either the mouse or keyboard. The administrator guide provides the instructions for both these methods. The body of the text describes the operation in more detail.

The names of keys appear in bold capital letters: **ENTER**

Information that you type appears in small, light typeface: Unified CallConnector

Menu commands appear in bold and are abbreviated in the text. For example the **Print** command on the **File** menu is indicated by **File-Print**. The names of buttons in dialog boxes also appear in bold.

Actions you take or procedures for you to follow are indicated by indented and bulleted steps.

Terminology

The following terms are used frequently in the manual to identify different kinds of individuals and objects.

Term	Meaning
Administrator	The person responsible for the administration of the Unified CallController system.
UCC	Unified CallConnector for Microsoft Windows.
Group	A collection of users. A group is also displayed as the department in the corporate directory.
Manager	The person responsible for a group of users.
Mobility	Unified CallConnector Mobility Service applications providing the user with Single Number Reach and Dial-In Access capabilities.
SNR	Single Number Reach applications that provides a find-me/follow-me function.
Database	A database is a file that contains information in a tabular format.
Record or Entry	Each row of the database table is called an entry or a record.
Field	Each column of the database table is called a field.
Directory	A directory is a database that usually contains names and related information.
Presence	Real-time availability status of a user. Presence status can include availability, location , telephone status and away messages.
Server	Unified CallConnector Server applications or the Windows Server PC.
Users	Individuals who are authorized to use the system.
Dialog	Popup window from which options are selected.
Window	An area of the screen where the application displays information.
SIP	Session Initiation Protocol – a standardized set of messages and methods for setting up communication sessions.
Service	An application running as a Windows Service. These applications do not present a user interface.
RADIUS	Remote Authentication Dial In User Service (RADIUS) is an AAA (authentication, authorization and accounting) protocol for applications such as network access or IP mobility.
Port	Sub-address used in setting up TCP connections.

Using the Mouse

The following terms are used in the manual when describing mouse-based operations:

Term	Meaning
Point	Move the mouse pointer on screen to the desired item or location.
Select	Click on the item of choice.
Click	Quickly press and release the left mouse button.
Right-Click	Quickly press and release the right mouse button.
Double-Click	Quickly press and release the left mouse button twice in succession.
Drag & Drop	Click down on item, holding down the button, move the mouse pointer to desired location, and then release the button.

Obtaining Documents

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/univercd/home/home.htm

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:
http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:
http://www.cisco.com/go/marketplace/

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to:
bug-doc@cisco.com

You can submit comments 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

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 can perform these tasks:

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

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from 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 them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

Emergencies—security-alert@cisco.com
Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*. Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&ex act=on

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support 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 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 TAC 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 TAC 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

Definition of Service Request Severity

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

Severity 1 (S1)—Your 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 operation 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 your network is impaired, but 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 Information

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

Cisco Marketplace provides a variety of Cisco books, reference guides, 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

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

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

Unified CallConnector Server Overview

This chapter provides an overview of the Cisco Unified CallConnector solution including the Client, Server and the Mobility components. It describes the key features, the different modes of operations. It also provides an overview of each of the graphical user interface components of the Unified CallConnector.

This chapter describes the following in more detail:

Key Features -	Describes the key features of the Unified CallConnector.
CallConnector Models -	The CallConnector supports a standalone, server and mobility components. This section describes these UCC models Personal, Server and Mobility.
CallConnector Toolbars -	Describes the components of the Unified CallConnector Toolbars in Microsoft Explorer and Outlook.
CallConnector Sidebar/View -	Describes the components of the Unified CallConnector Sidebars in Microsoft Explorer and View windows in Outlook.
Popup -	Describes the Popup applications and its menu.
QuickSearch -	Describes the QuickSearch user interface.
Monitoring Presence Status-	Briefly describes the Presence capabilities of the Unified CallConnector.
Mobility Service -	Briefly describes the Mobility features and the Single Number Reach capabilities of the Unified CallConnector.
Configuration Overview-	Describes the configuration sets for of the Unified CallConnector.
Getting Help -	Describes how to get Unified CallConnector help information.

Unified CallConnector Overview

Cisco Unified CallConnector delivers a new way to handle the everyday task of communicating with others within the business or with customers and vendors. As a fully integrated communication management solution with presence (your current availability), you will find greater productivity and business efficiency leveraging your PC-based data to initiate voice, messaging or collaboration sessions. Cisco Unified CallConnector is not just another application for the Windows, but is embedded within your line of business application such as Microsoft Outlook and Internet Explorer.

The Cisco Unified CallConnector offers these features:

- Simple to use toolbar within Microsoft Outlook and Internet Explorer for dialing numbers, controlling the call, and setting your availability and location status.
- Brings together all your contacts (personal, corporate, and Outlook) for QuickDialing or for starting a new email or Instant Message to the contact.
- Quick Search feature to find a contact quickly with display of all contact numbers and messaging methods plus location and availability for fellow employees without leaving your current application.
- Quick Message, an Instant Messaging Client included for short communications with fellow employees.
- Screen pop for placed and received calls with Outlook contact name allowing clickable options to take the call, send the call to voice mail or send a quick message.
- Quick Dialing from any application, including web pages, by highlighting a number, and selecting dial.
- Quick Presence conveniently displays availability, location and notes for contacts in directories and search results.
- Optional Mobility Service is an add-on providing Single Number Reach call routing services to allow your business calls to reach you at any number based on the rules you have set.

Unified CallConnector Models

Cisco Unified CallConnector is available in three configurations:

Personal	Delivering call control features for the individual user using Cisco's Unified Communications Manager Express (Cisco Unified CME) TAPI TSP.
Server	Server based application installed at each site giving users call control plus Presence/Instant Messaging and Rules-based Automation Services based on a SIP Client Server architecture.
Mobility	Add-on to the server application, the Unified CallConnector Mobility provides single number reach to a number.

Unified CallConnector Personal

Cisco Unified CallConnector Personal is a separate install on each Windows workstation with a Cisco Unified IP Phone connected to Cisco Unified CME router. Each user of Cisco Unified CallConnector Personal delivers the call control features listed in the table below and is supported with any PC running Microsoft Windows.

Features with Cisco Unified CallConnector Personal

Unified CallConnector Personal Feature	Description	Benefit
Call Control toolbars within Microsoft Outlook and Internet Explorer	Toolbars for easy access to features without the need for any additional desktop applications. Can be used within Outlook or Internet Explorer	Provides easy to use features such as finding contacts, executing phone features, and streamlining communications for the user
CallConnector Contacts	Within Outlook & Internet Explorer brings together all personal, corporate and Outlook contacts, history of calls and speed dial lists.	Makes it easy to find contacts, view missed calls from your everyday applications
QuickConnect from any Contact	Easy click-to-dial or click-to-send on any contact with option to show all numbers (Work, Cell, Home) and send addresses (email, IM, SMS) associated with the Contact	Saves time where call is placed in a few seconds without manual dialing a number or starting other communication sessions.
Quick Transfer /Hold /Conference	Easily transfer, hold or setup conferences using context menus within Outlook or Explorer.	Ease of transferring or setting up conference calls using PC Mouse. Callback from email or conference to a number in the web page.
QuickSearch though Contacts	Use pause/break key on PC to quickly find contact and then quick dial number, or send email.	Easy way to search though all contacts without opening new applications or switching pages.
Speed dial	Option to create Icon based speed dials for frequently called numbers.	Common numbers are easy to find and dial quickly.
Call Popup with Outlook Caller ID Lookup	Incoming calls will show a screen pop with callers name lookup from Outlook contacts. Clickable Option to answer or send call to voice mail.	Always know who is calling with option to answer call or ignore and send to voice mail.
QuickDial from any application	Highlight a phone number in any application like Microsoft Word, PowerPoint, Email or web page, then double-click phone icon to place call.	Quick and easy way to place a call without reading number and manually dialing. Saves time, and improves productivity
CallConnector Call Logs	Missed, Received, and Dialed calls stored on PC in addition to the IP Phone. Use Quick Dial to return calls missed while out of the office	Save time returning calls missed while away from the office. History log of calls received and placed can be used for billing.

Cisco Unified CallConnector Server

The Cisco Unified CallConnector Server application delivers the features as described above with the added benefit of Presence and Instant Messaging. The Cisco Unified CallConnector Server gives your employee's information about colleagues' location, availability, and phone status using the same CallConnector toolbars from within Outlook and Internet Explorer. Using simple icons and colors to show location and availability, users are able to reach colleagues quickly the first time and reduce phone tag – helping them to be more productive.

The table below lists the additional features available with Cisco Unified CallConnector Server.

Cisco Unified CallConnector brings together easy to use call control, presence, instant messaging, directories and call routing rules to simplify the communication experience, helping work teams and colleagues share information faster and communicate in real time.

Cisco Unified CallConnector provides status of co-workers if available or busy before trying to contact them. Similar to popular instant messaging status, the user can set his or her status from the Cisco Unified CallConnector toolbar. This status information is updated automatically to all users from the Cisco Unified CallConnector Server and can be accessed from the toolbars in Internet Explorer, Outlook or Quick search results window. By seeing who online, offline, available, or busy is or with custom message like "on vacation" or "in a meeting" can also be shared to let users know why someone is unavailable or busy. Knowing whether contacts are available helps to reduce communication delays between workers, thereby enabling faster decision making and enhanced productivity.

Features with Cisco Unified CallConnector Server

Unified CallConnector Server Feature	Description	Benefit
Dynamic Presence Information	Real Time display of users Location, Availability, IP Phone Status, plus optional custom message.	Reduces phone tag, and gives employee's information of who is in the office or on the road.
User Selectable Location	User can set their location shown by Icon (Work, Home, Travel, Vacation) or custom message displayed to other users.	Allows others (including operator) to see who is in office, out to lunch or away on travel.
User Selectable Availability	User can set their status shown by color, Available, Busy, Away, other.	Lets fellow employee's know who is available to receive calls or Instant Messages
Dynamic IP Phone Status	All phones Connected to the Cisco Unified CME router have status auto updated for others to see.	Reduces phone tag providing more efficient communications
QuickMessaging	Simple Instant Messaging for the Small Office launched though CallConnector Contacts Quick Dial. Option to launch other IM clients installed on PC though Contacts Quick Dial.	Easy to use Instant Messaging Client for productivity gains between employees. Alternative to use of external public IM Clients due to security concerns
QuickSearch with Presence information	Quick Search results bar shows Location, Availability and Phone Status for colleagues in addition to contact numbers.	Quickly find phone numbers for colleagues plus presence info to know if available before calling.
User Customizable Automation Rules	Set rules for basic call handling and notification though email or SMS when calls are received	Gives users option to send notification to pager, cellular or smartphones about important calls missed while away from the office.
Operator or Admin can change Location or Availability of others	Gives key personal option to change presence information shown to others	Provides up to date information to users to improve communications.
Easy Install without configuring TAPI TSP at each Workstation	Users receive email invite with clickable link for easy install from Server	Users are able to self-install for reduced installation costs

Cisco Unified CallConnector Mobility

Cisco Unified CallConnector Mobility brings the business calls to the workers at their current location and to a phone of their choice. An optional part of the Cisco® Unified CallConnector family of products, the CallConnector Mobility is an add-on server application that integrates with Cisco Unified CME router to monitor incoming business calls and then route or bridge them based on user-specified call handling rules. Whether at home or from remote locations, the workers can place or receive calls through the Cisco Unified CME router and leverage the business's Unified Communications infrastructure.

Cisco Unified CallConnector Rules Interface allows the workers to setup automation rules to bring the business calls to them based on their availability and location.
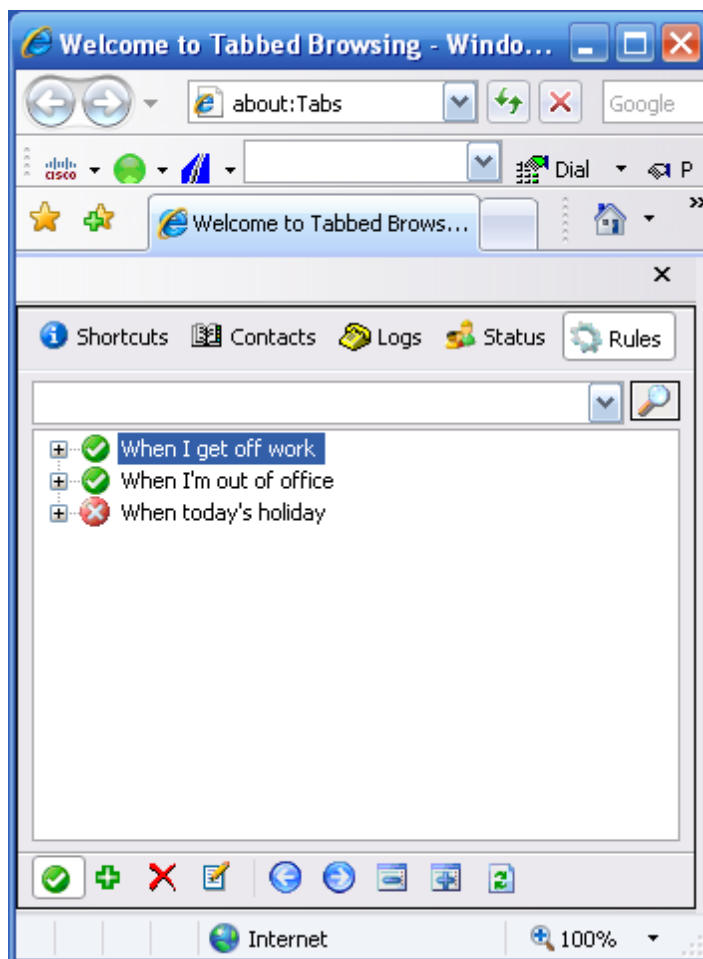
The Cisco Unified CallConnector Mobility is an add-on application to the Cisco Unified CallConnector. The solution monitors user's presence status (availability and location) and calls placed to their Cisco Unified IP phone. Users can associate rules with their presence status and location to route selected callers to a specified number, like a cell phone. As an option, calls can be bridged to both the IP Phone and the remote phone. When a call is bridged, it appears both at the user's IP Phone and the other phone allowing the call to be taken at either device. Calls routed to a remote phone are announced to the user who is given a choice to accept the call or send the caller to voice mail.

The Cisco Unified CallConnector Mobility offers the following features:

Single Number Reach

Cisco Unified CME router users can now provide a single phone number to their business contacts and be immediately connected to their business calls at the most convenient and available telephone. Callers can be routed to a home phone if tele-working or the mobile phone when in transit or any other accessible phone. With the Cisco Unified CallConnector Mobility, workers can provide more responsive service to customers without having to distribute multiple and private mobile phone numbers. .

Single Voicemai/ Box

If the user is unreachable at their specified single business number, the Cisco Unified CallConnector Mobility will forward the call to voice mail, using Cisco Unity Express or Cisco Unity. When calls are routed, an SMS (text message) or email can automatically send notification of the missed call to the user. The single voice mailbox allows the user to easily manage all business voice messages saving time and money.

User Customizable Rules for Routing

The Cisco Unified CallConnector Mobility is fully integrated with the Cisco Unified CallConnector toolbars to allow users to setup rules based on availability and location to specify the reach numbers and routing for business calls. Rules can be easily changed from everyday used business applications like Internet Explorer and Microsoft Outlook. The Cisco Unified CallConnector Mobility combines the power of Single Number Reach with user settable routing rules to provide a flexible and user controlled solution for the mobile workers.

Integration with Presence

Call handling automation rules can be based on the presence status of the user, where as the status changes, call routing rules are triggered automatically. The Cisco Unified CallConnector for Microsoft Office allows users to change both availability (available, busy, away, unavailable) and location (work, home, on-the-road, etc), which can also set call routing rules. Using location information, the Cisco Unified CallConnector Mobility will know if the user is at home and available, can route business calls to their home number, but when busy the call is sent to voice mail with notification to the user.

Reach At Any Phone

The user can specify any telephone number as their single number reach telephone. This can be the home phone, the mobile phone or the telephone at their current location. The different reach numbers can be specified for their different presence locations settings.

Validated Delivery

The Cisco Unified CallConnector Mobility verifies the user at the reach number using a password to ensure that the business calls are delivered only to the user. The users can set their own access passwords.

Device Switching without Interrupting Calls

With Cisco Unified CallConnector Mobility, single number reach calls can be bridged on the IP Phone to allow mobile workers to continue the call after they arrive at the office and take advantage of speakerphone or other IP phone services. The call can be continued at either device without interruption, and users can use the best available IP Phone or mobile device.

Benefits of Cisco Unified CallConnector Mobility

Cisco Unified CallConnector Mobility Feature	Description	Benefit
Simultaneous Ringing	The incoming call rings on the Cisco Unified IP Phone and the user specified number.	Call rings at both the Cisco Unified IP Phone and mobile phone. The call can be picked up at either device.
Bridged Calls	In bridged single number calls, the incoming call is available on both the Cisco Unified IP Phone and the remote telephone.	This allows users to walk into the office and switch the call from the mobile phone to the Cisco Unified IP Phone.
Routed Calls	In routed single number calls, the incoming call is transferred to the remote telephone.	User never misses important calls and customers are connected instead of going to voice mail.
Validated User	Users need to enter a password before the call is delivered to the remote telephone.	The business calls are always delivered to the user. If someone else answers, then the call is sent to voice mail.
Single Voice Mailbox	If the user is not available then the call is routed to the business voice mail box.	User needs to manage only one voice mail box for their business calls. Less time is needed for users to check multiple voicemail systems
User-customizable automation rules	Users can set rules for single number reach call handling.	User's setup their own rules for filtering and routing calls to their reach number. Different reach numbers can be set based on availability.
Integration with Presence and Location	Allows the automation rules to be triggered based on the current user availability and location.	As the user's availability and location changes, the calls can follow them to the most appropriate telephone device.
Switching between telephone devices	Allows the call to be switched from mobile to the Cisco Unified IP Phone and visa versa.	Based on the needs of the moment, users can take advantage of the reliability of the wired office phone or the convenience of the mobile phone.
Privacy for bridged calls	When the call is bridged, it cannot be picked up from the associated desktop phone.	Access to the call from the desktop is allowed as soon as the remote connection becomes active. This prevents the possibility of an unauthorized person listening in on that call.

CallConnector Toolbar Overview

The CallConnector toolbar runs within Microsoft Internet Explorer and Outlook and provides a unified one-click access to call handling, ability to quickly locate your contacts, initiate messaging and collaboration sessions. The Contacts button allows you to open information windows for viewing contacts, call logs or the presence status of your colleagues.

CallConnector Toolbar in Outlook
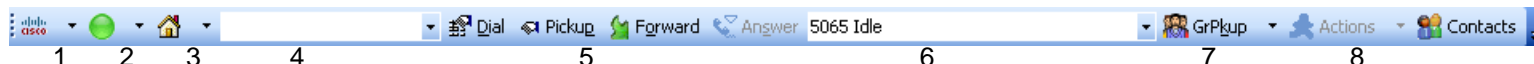
1. Cisco Icon/About Menu provides access to Help and links to more information on the Unified CallConnector and access to support and problem reporting resources.
2. Availability: Allows you to set your current availability status and publish it to your colleagues.
3. Location: Lets you change your current location and indicate whether you are at work or away on business.
4. Search Bar: Enter number to make a call or enter text to search for a contact. The pull down list lets you view the last numbers dialed or contacts located.
5. Call Control Buttons: You can control the call on your phone from these buttons. The buttons are context sensitive and change with the different call states.

    Idle State: The Idle toolbar allows you to dial a new call, pickup a ringing or held call and forward your line to another number.
    Ringing State: For an incoming call, you can answer the call.
    Connected State: The Call Control buttons change to provide Transfer, Conference, Hold, Hang-up and Park options.
    Held State: When a call is on hold, you can resume the conversation.

6. Line Display Menu: The line display is a pull down list showing you the state of the 'lines' or extensions configured on your phone. For each line, it displays the extension number, the call state and the calling party information.
7. Telephony Features Menu: This provides a list of all the supported telephony features.
8. Action Menu: The Action menu is a contextual menu providing access to the additional contact numbers, collaboration and communication methods for the currently active caller. The menu is populated with the caller's contact details.
9. Contacts Button: The Contacts button opens a side window in Outlook and Explorer. These provide access to directories, logs, presence and availability status of the users,
10. Note: The Internet Explorer has two additional buttons:
11. Speed Dial Menu: Pull-down arrow to the right of the dial button displays the speed dial names.
12. Highlighter: Before the Contacts button allows you to convert telephone numbers in the Web pages to clickable numbers.

Handling Calls Using the Toolbar

The CallConnector Toolbar allows you to control the calls on you IP Phone from your PC using the mouse and keyboard. You have access to most of the telephone features available on you phone, but now they are integrated with your PC based data and accessed from a graphical interface.

IDLE STATE:

INCOMING STATE:
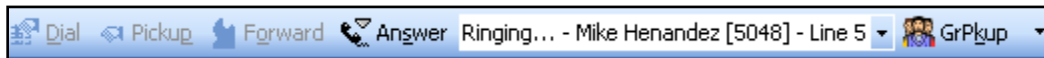
CONNECTED STATE:

HELD STATE:

Locating Contacts from the Toolbar

You can quickly locate and setup communication sessions with your contacts using the Toolbar QuickSearch. Communication options include making calls to work or mobile numbers, launching Email, SMS or Instant Message or opening up collaboration sessions.

QUICKSEARCH BAR
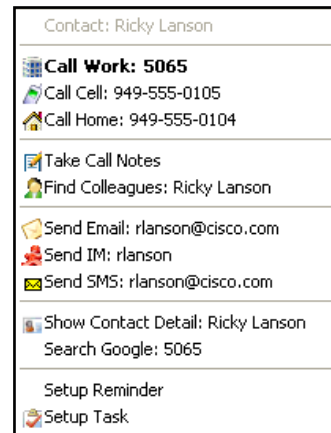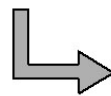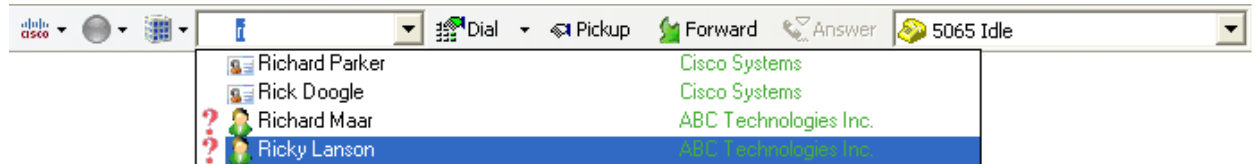
Accessing CallConnector Applications

The Unified CallConnector provides a suite of contact and presence management applications that are available from within Internet Explorer and Outlook. The figure below shows the CallConnector applications in Outlook. The availability and location of the UCC users is displayed as icons on the left side of the Contacts window.
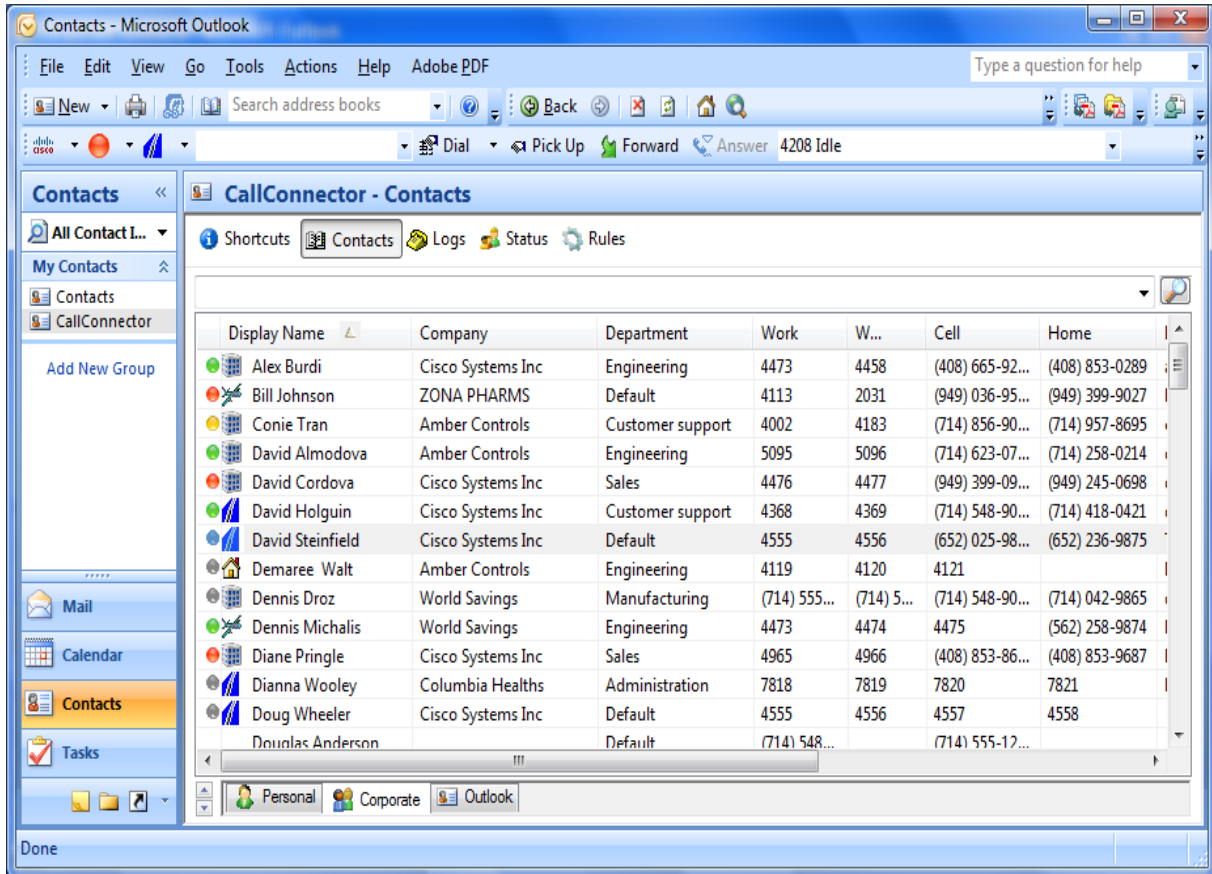
Managing Contacts

The CallConnector supports three contact databases – Corporate for shared organization contact information, Personal available for each individual user and the Outlook contacts. The Contacts window allows you to search, view and manage this information.

From this window users can search to locate a contact, click to dial the primary work number or right click to access a menu, as shown below, to auto-dial alternate numbers and access other communication services.
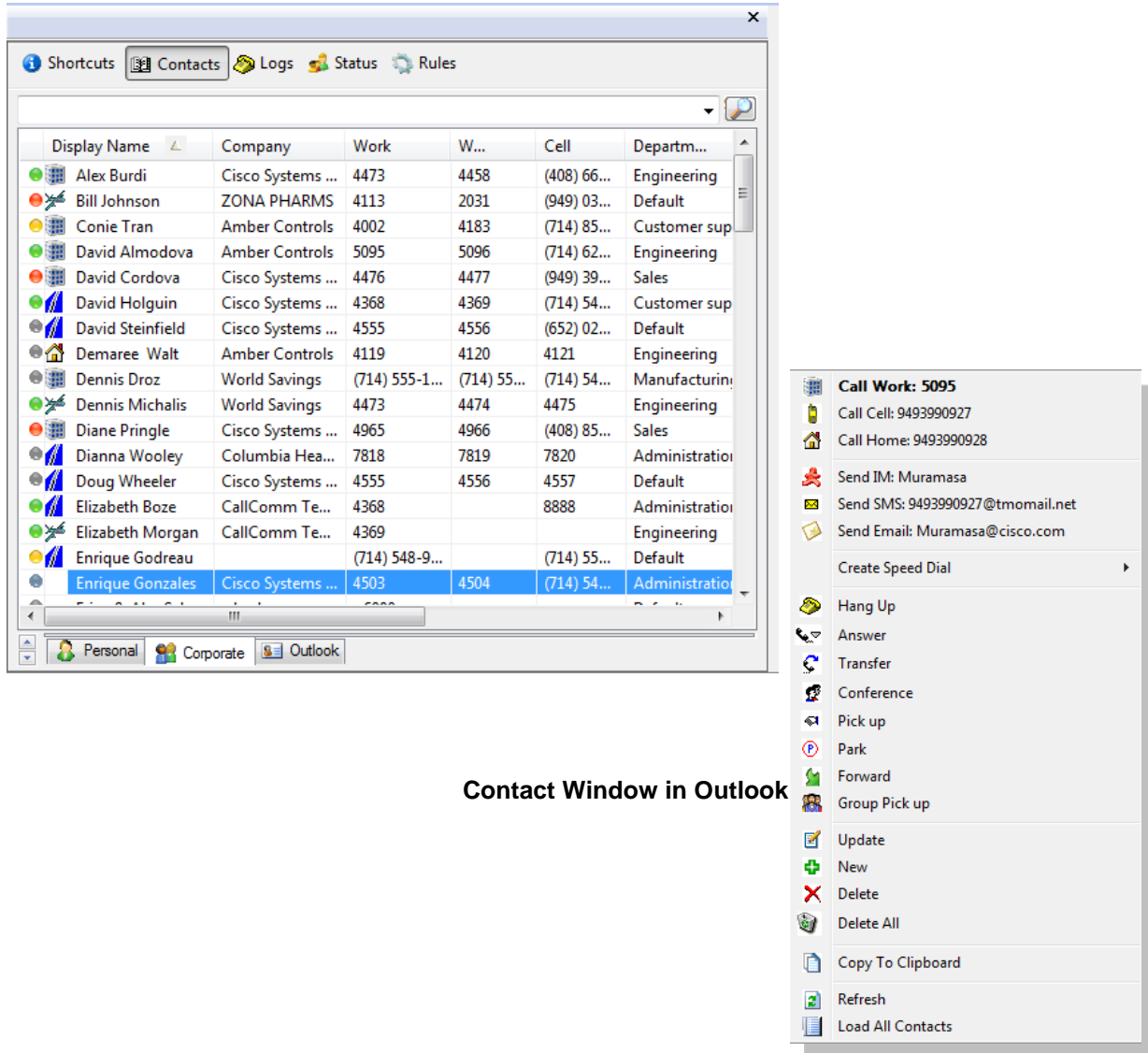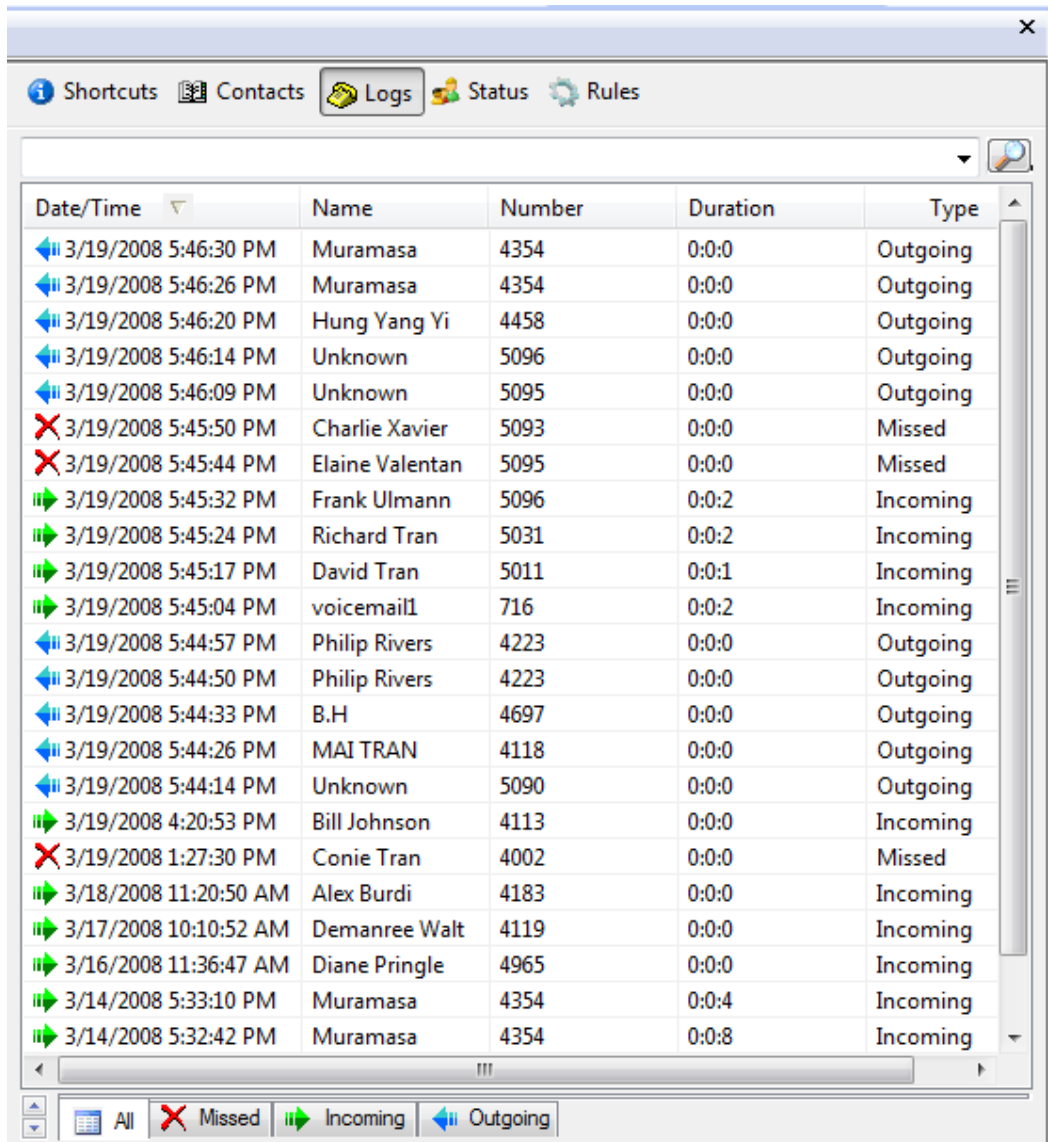
Contact Window in Outlook

Viewing Call Log

The Unified CallConnector Call Logs displays all a list of all calls made and received from your UCC program. It allows you to view important information about phone calls and lets you quickly search calls with specific attributes. It also allows you to perform telephony actions from the right-click action menu. The Call Logs also allows you to sort your call logs by date/time, name, number, and call type. You may also view each type of call individually.

The Call Log window displays the history of the calls that have been made to or from your phone.

Date/Time	Name	Number	Duration	Type
3/19/2008 5:46:30 PM	Muramasa	4354	0:0:0	Outgoing
3/19/2008 5:46:26 PM	Muramasa	4354	0:0:0	Outgoing
3/19/2008 5:46:20 PM	Hung Yang Yi	4458	0:0:0	Outgoing
3/19/2008 5:46:14 PM	Unknown	5096	0:0:0	Outgoing
3/19/2008 5:46:09 PM	Unknown	5095	0:0:0	Outgoing
3/19/2008 5:45:50 PM	Charlie Xavier	5093	0:0:0	Missed
3/19/2008 5:45:44 PM	Elaine Valentan	5095	0:0:0	Missed
3/19/2008 5:45:32 PM	Frank Ulmann	5096	0:0:2	Incoming
3/19/2008 5:45:24 PM	Richard Tran	5031	0:0:2	Incoming
3/19/2008 5:45:17 PM	David Tran	5011	0:0:1	Incoming
3/19/2008 5:45:04 PM	voicemail1	716	0:0:2	Incoming
3/19/2008 5:44:57 PM	Philip Rivers	4223	0:0:0	Outgoing
3/19/2008 5:44:50 PM	Philip Rivers	4223	0:0:0	Outgoing
3/19/2008 5:44:33 PM	B.H	4697	0:0:0	Outgoing
3/19/2008 5:44:26 PM	MAI TRAN	4118	0:0:0	Outgoing
3/19/2008 5:44:14 PM	Unknown	5090	0:0:0	Outgoing
3/19/2008 4:20:53 PM	Bill Johnson	4113	0:0:0	Incoming
3/19/2008 1:27:30 PM	Conie Tran	4002	0:0:0	Missed
3/18/2008 11:20:50 AM	Alex Burdi	4183	0:0:0	Incoming
3/17/2008 10:10:52 AM	Demanree Walt	4119	0:0:0	Incoming
3/16/2008 11:36:47 AM	Diane Pringle	4965	0:0:0	Incoming
3/14/2008 5:33:10 PM	Muramasa	4354	0:0:4	Incoming
3/14/2008 5:32:42 PM	Muramasa	4354	0:0:8	Incoming

Call Log Window showing history of all user's calls

Call Popup Window

The CallConnector Popup Window displays information on the calls at your phone. Each call is represented by one window. The Popup looks up the phone number in your contact database or Outlook and displays the name and organization information. The Popup window provides two call control buttons and the blue arrow for the Action menu.
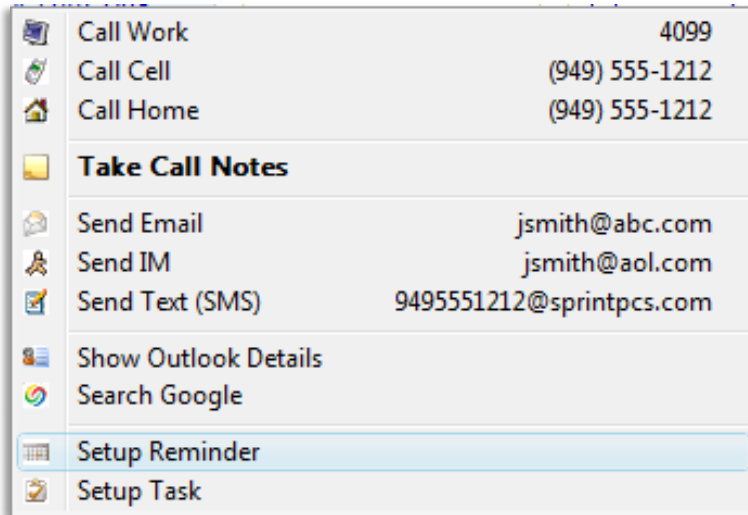
Action Menu

Call Control Buttons:

Button	Description
Answer	Answers a ringing call
Busy	Activates the Do-Not-Disturb phone settings
Hang Up	Disconnects the call
Hold	Places the call on hold
Resume	Re-connects the held call
Action	Opens the contextual actions menu for accessing additional communication and collaboration choices

Using QuickSearch

From within any application, you can quickly locate and setup communication sessions with your contacts using QuickSearch. Communication options include making calls to work or mobile numbers, launching Email, SMS or Instant Message windows or opening up collaboration sessions. To use enter the first few letters of the first name.
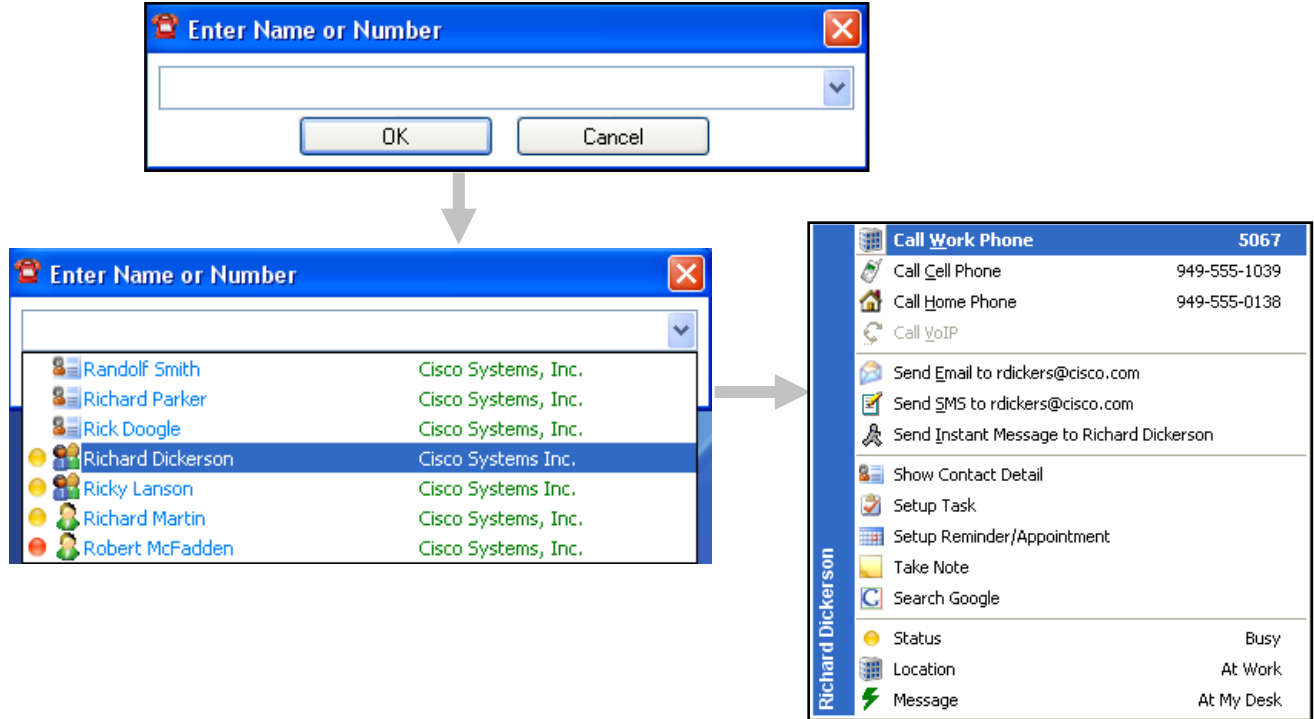
QuickSearch Window with Search Results and Details

Monitoring Presence Status

The CallConnector Presence Service collects information about a user's availability and location, including whether or not they are using their telephone at a particular time. This information is made available to the CallConnector users from within their every day business applications such as Internet Explorer or Outlook. The presence information is also displayed when you use the CallConnector QuickSearch to locate contacts. Using this real-time presence information, users can connect with colleagues more efficiently through determining the most effective method for communicating with them at that time thus avoiding phone or message tag.

The CallConnector Status window provides a real-time view of the entire organization with information on the availability of users and groups, location of people and whether they are on call. Users can manage their own presence status, make calls and send instant messages from this window.
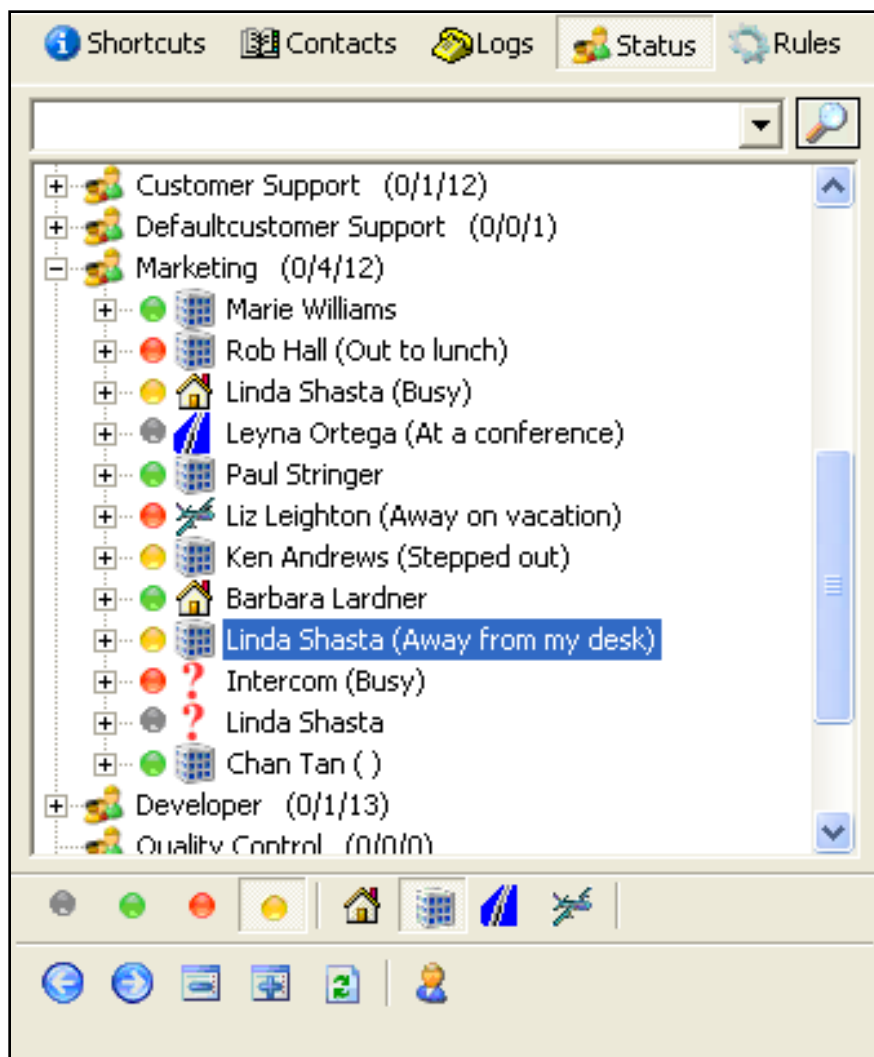
Status Window

Updating Availability

The CallConnector maintains three components of a user's presence information: Availability – this is the user's current Busy, Available, Away and Unavailable status; Location – the place where the user is situated and the Away Message – providing additional notes on their availability. In the server configuration, this information is broadcast to the CallConnector subscribers.

Availability Icon	Description	Location Icon	Description
🟢	Available	▦	At Work
🟡	Busy	🏠	Currently at Home
🔴	Away	🛣	On the Road
⚫	Unavailable	✈	Away on Vacation
?	Don't show my status	?	Location undefined

Sending Instant Messages

Instant messaging in the workplace can allow you to quickly resolve a question or communicate without interrupting the work flow. With the Unified CallConnector Server, users can send brief Instant Messages and Text (SMS) messages to their colleagues.
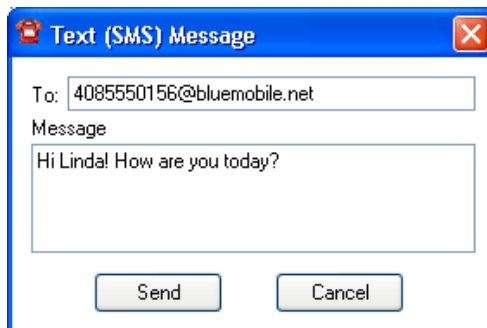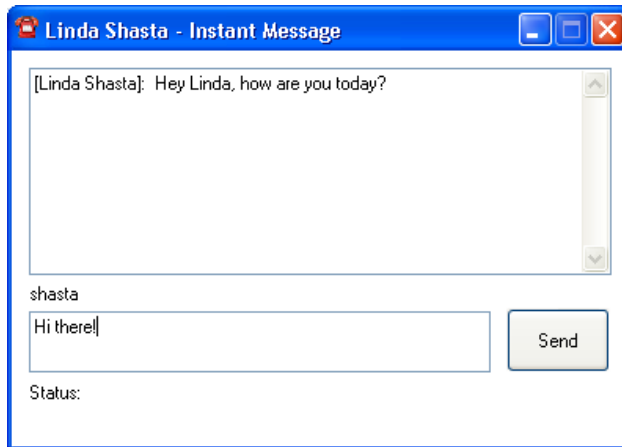
Instant Message and Text (SMS) Message Windows

Outlook Menu Extensions

Some of the Outlook menu have been extended to add in the user contact information and telephony action choices. These menus are described in this section.
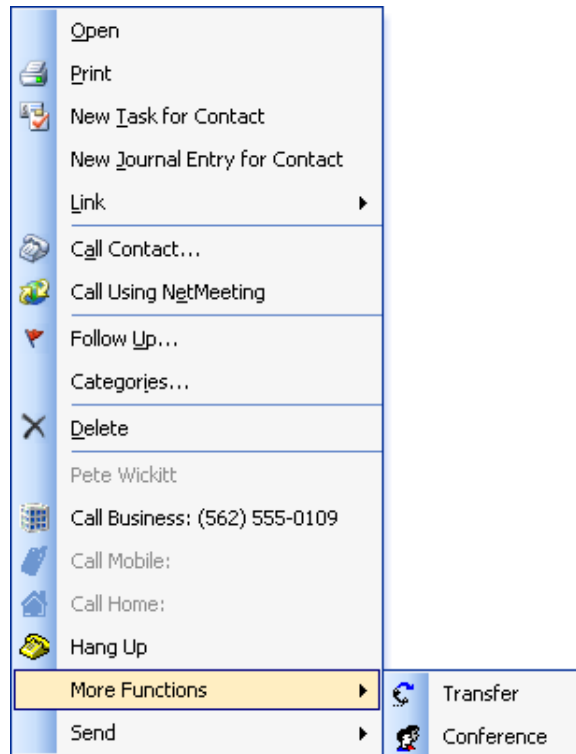
Getting Help

To get help on the operation of the Unified CallConnector client, click on the Cisco icon on the toolbars and select Help. This will display a CallConnector Help window form which you can browse and search to locate the topic of interest.

For more information on the Unified CallConnector you can also go to the Cisco web site at:

http://www.cisco.com/go/unifiedcallconnector

Mobility Service

Cisco Unified CallConnector Mobility Service allows you to receive your business calls at any of your contact numbers. If you are not available, then the caller is able to leave a message in your voice mailbox. The Mobility Service can be personalized in some of the following ways:

- You can setup routing rules based on your availability (available, busy, away, and unavailable) and/or your location (work, home, on the road or vacation).
- You can select which calls are forwarded to you.
- You can condition the routing rules to account for work days, weekend and holidays and for work hours and non-work-hours.

In addition to routing your incoming calls, the Cisco Unified CallConnector Mobility Service allows you to dial-in and make calls leveraging your company telephone resources and access the following features:

- Record the conversation or ask your called party to leave a voice message in your mailbox.
- Add additional parties (up to six) in to the conversation.
- Switch the call to your work, home or mobile number.

The Cisco Unified CallConnector Mobility Service is available as an optional component of the Cisco Unified CallConnector Server. The call routing rules are setup from within Microsoft Internet Explorer and Outlook using the Unified CallConnector client.

Single Number Reach

The Single Number Reach feature routes your incoming business call to your specified reach numbers. These numbers all ring simultaneously. If you answer at one of these numbers then you will be connected to the caller, otherwise the incoming call is sent to your Cisco Unity Express voice mailbox. Each user can customize the Single Number Reach routing of calls. The rules can be setup to specify when and which call is to be routed. You can also specify the numbers you are to be reached based on your availability and location setting. The Unified CallConnector Single Number Reach feature can be viewed as an intelligent user-controlled routing of business calls.

You can give your business contacts a single number to reach you no matter where you are. You can then control which calls and the time periods in which to receive business calls. Your personal numbers are not visible to the business callers.

The Single Number Reach service can ring one or more of following phone numbers simultaneously:

- Work phone
- Home phone
- Mobile phone
- Any other alternate phone number

There can be different call routing rules for:

- Holidays
- Workdays or weekends
- Working hours and after work hours

Personal Routing Rules

The Single Number Reach service requires you to setup rules specifying how to handle your incoming business calls.

Rules are setup from the Unified CallConnector Rules window. Each rule consists of two sections – a set of conditions and the actions to be executed when these conditions are met. Conditions are specified values for selected parameters that are constantly monitored by the Unified CallConnector. Actions are the tasks that are performed automatically on your behalf when all the condition parameters are true.

You can select from some of the following rule conditions when setting up a rule:

Trigger the rule when an Incoming call rings your IP Phone. (<u>This condition must be selected for Single Number Reach rules</u>).

Condition	Description of Options
Telephone number of the caller	Whether the caller's number is in your personal contacts, speed dial list, corporate directory, or in a list of telephone numbers
Your current availability	Available, Away, Busy, or Unavailable
Your current location	Home, Work, On the Road, or On Vacation
If the day is:	Holiday, a workday or a particular day of the week
If the current time:	Is in working hours or after work hours

Tasks that can be performed automatically on behalf of the user

Actions	Description of Action Choices
Route incoming calls	To the user's work, home, or mobile phone
Update the user's availability status	To Available, Away, Busy, or Unavailable
Update the user's location	To Home, Work, On the Road, or On Vacation
Update the user's status message	To Busy, Be right back, Stepped out, Away from keyboard, On the phone, or a Custom message

Mid-Call Features

The Unified CallConnector Mid-Call feature is an option that allows you to access Cisco Unified Communication Manager Express (Cisco CME) features such as transferring to their voice mailbox, extending the current Single Number Reach call to a multi-party conference and more.

For example, you are on a call extended through the Single Number Reach service and you need to add in a colleague to the call. You can enter the 'Add Number' access code and the colleague's telephone number. If available, the number is joined to your call.

You can also change your availability status and location using keypad access codes. This can not only inform colleagues of your current status but can also be used to trigger previously setup call routing rules. For example if you want to be reached on your mobile phone, then you can change your location to "On the Road" to activate the "On the Road rule". The Mid-Call features can also be used to move the call from the current phone to another telephone instrument.

Dial-in Access

The Mobility Service Dial-In Access feature allows you to access the Cisco CME features for your business calls when you are away from the office. To place long-distance or international calls, you can call in and use your company's telephones lines to place these calls. You can also access the Cisco CME features such as setting up a multi-party conference call and more from their mobile or home phones. With the Dial-In Access, you can establish a phone conference from your mobile phone without access to the IP phone physically.

UCC Server Configuration Overview

The Unified CallConnector Server requires a number of parameters to be configured on the Cisco Unified CME and Cisco Unified CUE. These features have to be <u>first provisioned on the CME</u> and CUE and <u>then the corresponding parameters have to be configured on the UCC</u> system. This section provides an overview of the CME and CUE setup requirements.

Cisco CME Setup for UCC Server

1. Settings on Cisco CME required to support UCC Server include:
2. Provisioning the user's ephones on CME to allow 'TAPI' connections.
3. Setting up Radius accounting parameters to send messages to UCC Server.
4. Setting the CME Dial Plan to allow extension and PSTN Dialing
5. Notes for connecting multiple CME/CUE to one UCC Server
6. Network connection between routers and UCC Server needs to support UDP transport and TCP connections.
7. Set up Radius accounting parameters with the same port and password across all routers.
8. Provision ephone user names to be unique across all routers.

Steps to Configure UCC Server

After the Cisco Unified CME has been configured, the following need to be configured on the UCC Server using the Server Administration Wizard.

1. Configure the UCC Server communication parameters. Select database backup options.
2. Configure the Radius port and password. Verify that you can receive the radius messages.
3. Configure Cisco Unified CME location, features settings and dialing rules. Setup any exception dialing translations if needed. Verify digit translations.
4. Download the ephone configuration from CME and select the ephones that will be controlled by the UCC Server. Verify that the ephones can be accessed from Server.
5. Add the Group Names – these are the departments that the users are grouped under. Setup the publishing and restrictions rights.
6. Configure the users with their contact details.
7. Associate the user with their ephone.

UCC Mobility Configuration Overview

The Unified CallConnector Mobility Service makes use of additional features of the Cisco CME and Cisco CUE. These features have to be provisioned on the Cisco CME and Cisco CUE and then the corresponding parameters have to be configured on the UCC system. This section provides an overview of the CME and CUE setup requirements. Following chapters provide a step-by-step tutorial on how to setup the environment for Cisco CallConnector Mobility Service to work.

Additional CME/CUE Setup for Mobility

Settings for CME/CUE for Single Number Reach Service

1. Provisioning of mobility ephones on CME for use by the Mobility Service
2. Setting up Hardware Conferencing including Ad-Hoc conferencing
3. Uploading CUE Transfer to voicemail script and setup pilot numbers

Setting on CME/CUE for Dial-In Access Service

1. Provision additional mobility ephones on CME for use by the Dial-In Access Service
2. Setup call routing – hunt group or Basic-ACD to route incoming calls to the Dial-In mobility ephones.

Steps to Configure Single Number Reach Service

After the Cisco Unified CME has been configured with the additional parameters for the Mobility Service, the following need to be configured on the UCC Server using the Server Administration Wizard.

1. Select the mobility-ephones previously configured in the CME
2. Configure Single Number Reach system parameters.
3. Setup ephone pools for the Single Number Reach Service.
4. Assign ephones to the ephone pools that'll be used by the SNR Service.
5. Configure user contact information including the voicemail box and Tel PIN.

Steps to Configure Dial-In Service

1. Select the additional Mobility ephones configured in the CME for the DISA feature.
2. Configure Dial-In Access system parameters.
3. Setup ephone pools for the Dial-In Access service.
4. Assign ephones to the ephone pools that'll be used by the DISA Service.
5. Configure user contact information including the DISA password for users

Installing Server Software

This chapter describes the steps for downloading and installing the Unified CallConnector Server software. The following topics are discussed:

Installation Overview -	Provides an overview of the Unified CallConnector Server installation process.
Pre-requisites for Installation -	Describes the information you need to have on hand during the installation of Unified CallConnector Server.
System Requirements -	The minimum requirements for the server computer for different user configurations.
Download Site -	Site from which the Unified CallConnector software can be downloaded.
Installing the UCC Server	Describes the steps and options for installing Unified CallConnector Server components.
Registering the Software -	The Unified CallConnector software has to be registered before it can be used. This describes the options presented to you during this process.
Performing an Upgrading	Describes the steps for upgrading an existing Unified CallConnector with a new install program.
Removing the UCC Server	This section describes the steps for removing and un-installing the Unified CallConnector Server and all its components.

.

Unified CallConnector Server Installation

The Unified CallConnector Server software is installed on a Windows computer to provide shared access to call control, contact data and presence status for the Unified CallConnector users. The server installation program checks your system configuration, copies the software to the hard disk and makes the required configuration settings for you. This installation program can be download from the Cisco site and run as described in the sections below.

The installation of the Unified CallConnector Server software involves the following steps:

1. Collecting the information required for obtaining and configuring the Unified CallConnector. This includes obtaining access to the download site or the installation program and the information that you will require during the installation process. See the Pre-requisites for Installation section below for these parameters.
2. Preparing a Windows computer system on which you will install the Unified CallConnector server software. See Minimum System Requirements for the Unified CallConnector Server in the sections below.
3. Configuring the Cisco Unified CME IP Phone and RADIUS parameters. You will also need to user name and password for a telnet account to the Cisco Unified CME for downloading the phone configurations.
4. Acquiring the Unified CallConnector Server installation program. This can be downloaded from the Cisco Software Download Site or obtained from your Cisco channel partner.
5. Logging into the Windows server computer with an administrative or power user account. This is required to register and run the server software.
6. Running the Unified CallConnector Server installation on the computer, and entering the configuration information requested by the installation wizard.
7. Registering your Unified CallConnector Server with the Cisco Activation server. This will require access to the Internet.
8. Setting up the Unified CallConnector Server configuration parameters from the Server Configuration wizard.
9. Start the Unified CallConnector Server software and verifying that the services start up and run.
10. Verifying that the users are able to log in and access the Unified CallConnector services.

This chapter describes the steps for installing and activating the Unified CallConnector Server software. The next two chapters cover the configuration and setup of the UCC Server and the required settings on the Cisco Unified CME.

Pre-Requisites for Server Installation

As a part of the installation of the Unified CallConnector Server, you need to have certain network connectivity and configuration information. These are summarized in the table below and described in the following paragraphs.

Item	Description	Source
Access to Download Site or Installation Software	Download or otherwise obtain the Unified CallConnector installation program	Service Provider or Sys-Admin
UCC Server PAK-ID or Serial Number	Licensed version of the Unified CallConnector Server requires a PAK-ID or serial number. You can get started with an evaluation version if you do not have a PAK-ID.	Service Provider or Sys-Admin
Admin or Power User Name and Password	Login access to the Windows PC on which the UCC Server software ins to be run.	Sys-Admin
Internet Access	Internet access is required for registering the UCC Server. This can be a direct access or through a Proxy server.	Sys-Admin

Table 3.1 Pre-requisite information for installing the Unified CallConnector Server

Access to Download Site: The installation files can be downloaded from the Cisco software download site. You can also obtain a copy of the installation files from the Cisco solution partner.

UCC Server PAK-ID: The Unified CallConnector Server software requires a Product Authorization Key (PAK-ID) or a serial number to operate. This PAK-ID is provided to you when you purchase the software. There is an evaluation option for a limited time period that can be a started by entering 'trial' in the serial number field during the installation process.
Admin or Power User Account of Installation PC: The installation program requires access to Windows registry and installation of services. These changes can only be performed with an account with admin or power user rights to the Window's computer.
Internet Access: The CallConnector Server software has to be registered to the Unified CallConnector License Server via an activation process. This requires access to the Internet. The Internet access can be through a Proxy Server. In this case the Internet Explorer on the PC should have the proxy settings defined.

Windows Access Rights:

During the installation of the Unified CallConnector, you need to have local admin rights to the personal computer. This is to allow various system files to be loaded and Windows registry entries to be written.

Note: If you are not logged in to the PC with the required access rights, the installation may fail or not run through completion.

Minimum System Requirements

Your system must meet the minimum system requirements described in this section. We recommend that your system exceed the minimum when possible to ensure better performance.

Computer and Windows OS

The table specifies the minimum computer requirements for three different size systems. The system requirements vary depending on the number of users logged on to the UCC Server. The number of users here refers to the number of concurrently logged on Unified CallConnector clients.

These are minimum requirements and deal with only the Unified CallConnector Server requirements. If the computer is running other application or services, those requirements should be added to these specifications.

	25 User System	75 User System	250 User System
Processor	Pentium PC 2Ghz	Pentium Dual Core 3Ghz or Greater	Pentium Quad Core 3Ghz or greater
Memory (RAM)	1 Gbyte RAM with 350 Mbyte available for UCC Server	2 Gbyte RAM with 1 Gbyte available for UCC Server	4 Gbyte RAM with 2 Gbyte available for UCC Server
Operating System	Microsoft Windows XP Professional Service Pack 2 or Microsoft Windows 2003 Server	Microsoft Windows 2003 Server	Microsoft Windows 2003 Server
Disk Space	200 Mbyte available for UCC Server	400 Mbyte available for UCC Server	800 Mbyte available for UCC Server

Table 3.2 Recommended minimum computer system for the Unified CallConnector Server

Note: Available memory in the computer can be determined by opening the Windows Task Manager to the performance tab and viewing the used and available before running the UCC Server.

Application Software

Unified CallConnector Server uses the settings of Internet Explorer for navigating through proxies servers. If you are using a Proxy server to access the Internet, first verify the connection using the IE browser.

Internet Explorer Version 6.0 with Service Pack 2, Internet Explorer 7.0

Telephone System

Communication Systems

The UCC Server provides shared access to telephony service to the UCC clients. The UCC Server supports the following Cisco Systems communication systems. For the most current list, see the data sheets on http://www.go.cisco.com/unifiedcallconnector/

Connecting to multiple Communication Systems:

The Unified CallConnector Server can be connected to multiple Cisco Unified Communications Manager systems. The number of systems that can be connected is dependent on the network connecting the systems, the number of users in each system and the capacity of the computer system hosting the Unified CallConnector Server. Please consult with your Cisco System Engineering resource or channel partner for your specific configuration needs.

IP Phones:

Please see the Customer Release Notes for the list of IP phones qualified for the version of the Unified CallConnector software you are using, The Unified CallConnector Customer Release Notes can be found at:

http://www.cisco.com/en/US/products/ps7274/prod_release_notes_list.html

LAN Access and Ports

The Local Area Network is used in multi-user environments to share the directory data and to access services such as E-mail and the Telephony Service. Access to the Internet is also required for the activation process.

The following network connections are made between the applications running on the Unified CallConnector Server and the Unified CallConnector clients and the Unified Communication Systems:

Connections to:	Type	Server Ports (Default)
Communication Servers – SCCP	TCP	Available TCP ports
Communication Server – RADIUS	UDP	1646
Communication Server – Telnet	TCP	23
UCC Server Application	UDP + TCP	5060, 39984, 5061, 5062, 5063, 5071, 5072-5077
UCC Clients Receive Port	TCP	5065
Server Wizard (to verify activation)	TCP	80
Email (SMTP Server)	TCP	25

Table 3.3 TCP/UDP Ports used by the Unified CallConnector Server

Download Site

The Cisco Unified CallConnector can be downloaded and installed from the Web. Go to the link below, select the Unified CallConnector for Microsoft Office, and download the installation files.

<http://www.cisco.com/cgi-bin/tablebuild.pl/callconnector-ms>

Note: A valid CCO User ID and Support Contract are required to access the software download center. If you don't have access, contact your Cisco reseller.

Your Installation Package

Before installing the Unified CallConnector, carefully check your package contents.

Your package should contain the following items:

> Unified CallConnector Installation Program.
> Quick Reference Guide

Installing the Unified CallConnector Server

During the installation process, the Unified CallConnector Server install program will check your system's components and determine what files need to be upgraded. It will copy program files to an installation folder of your choice and system files to the Windows System directory.

The installation program also sets up the Unified CallController Server applications to run as Windows Services.

Step 1: Download the Installation Program

Log in to the Cisco Software Download site for the Unified CallConnector and download the latest Unified CallConnector client installation program. You can also obtain this from your Cisco Channel Partner.

Step 2: Run the Unified CallConnector Installation

Login to Windows under Admin account: The installation program writes to the Windows registry and requires access rights available under the administrative account.

Close all Windows Applications: Close all open applications. Disable the screen-saver if the PC has one enabled. If you have un-installed a previous version of the Unified CallConnector software then it is recommended that the PC be rebooted before the new installation.

Verify that you have Internet Access: The license registration process at the end on the installation requires Internet access. Open the Internet Explorer and verify that Internet is accessible.

To Install Unified CallConnector Server: Launch the Unified CallConnector Server install program by double-clicking on it.
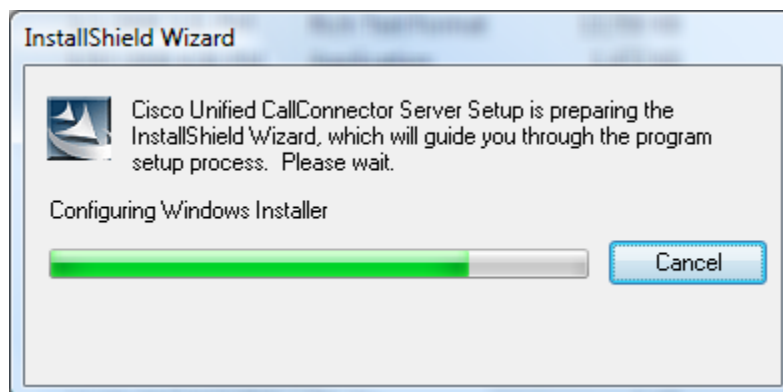
Once the install program is loaded, it will present the Welcome dialog.
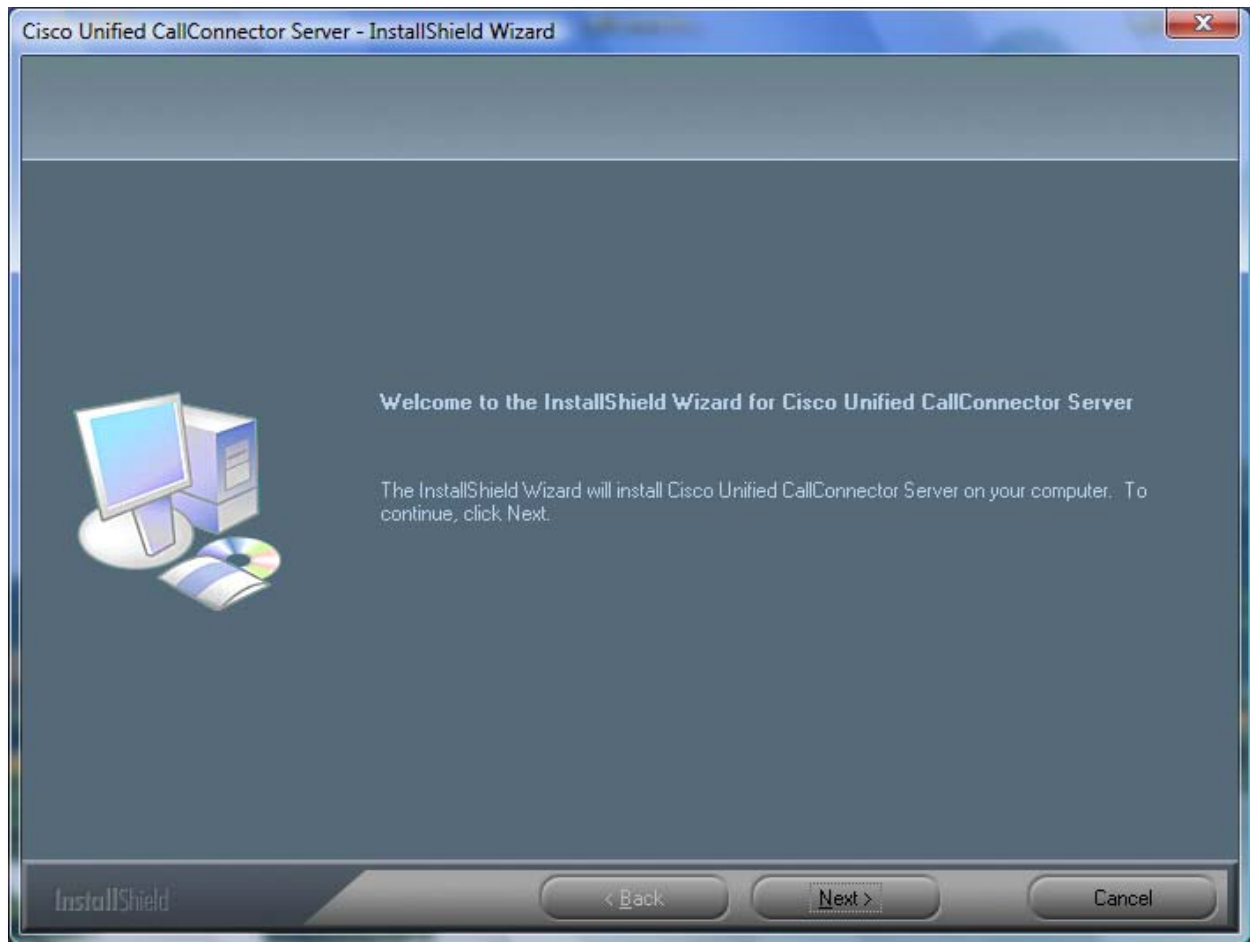
Click on **Next** to display the Software License Agreement statement.

Please read the Software License Agreement statement and click on **Yes** to accept the license and Next button for the Customer Information window.

Enter your contact information in the following fields:

User Name: The name of person under which the software will be registered.

Company Name: The name of registering person company or organization.

Email: The email address of the registering person. The email address and the PAK-ID (or serial number) will be required if you need support related to the license activation.

Display Language: The Server Wizard user interface can be presented in one of several languages. You can select your preferred display language from the pull-down list.
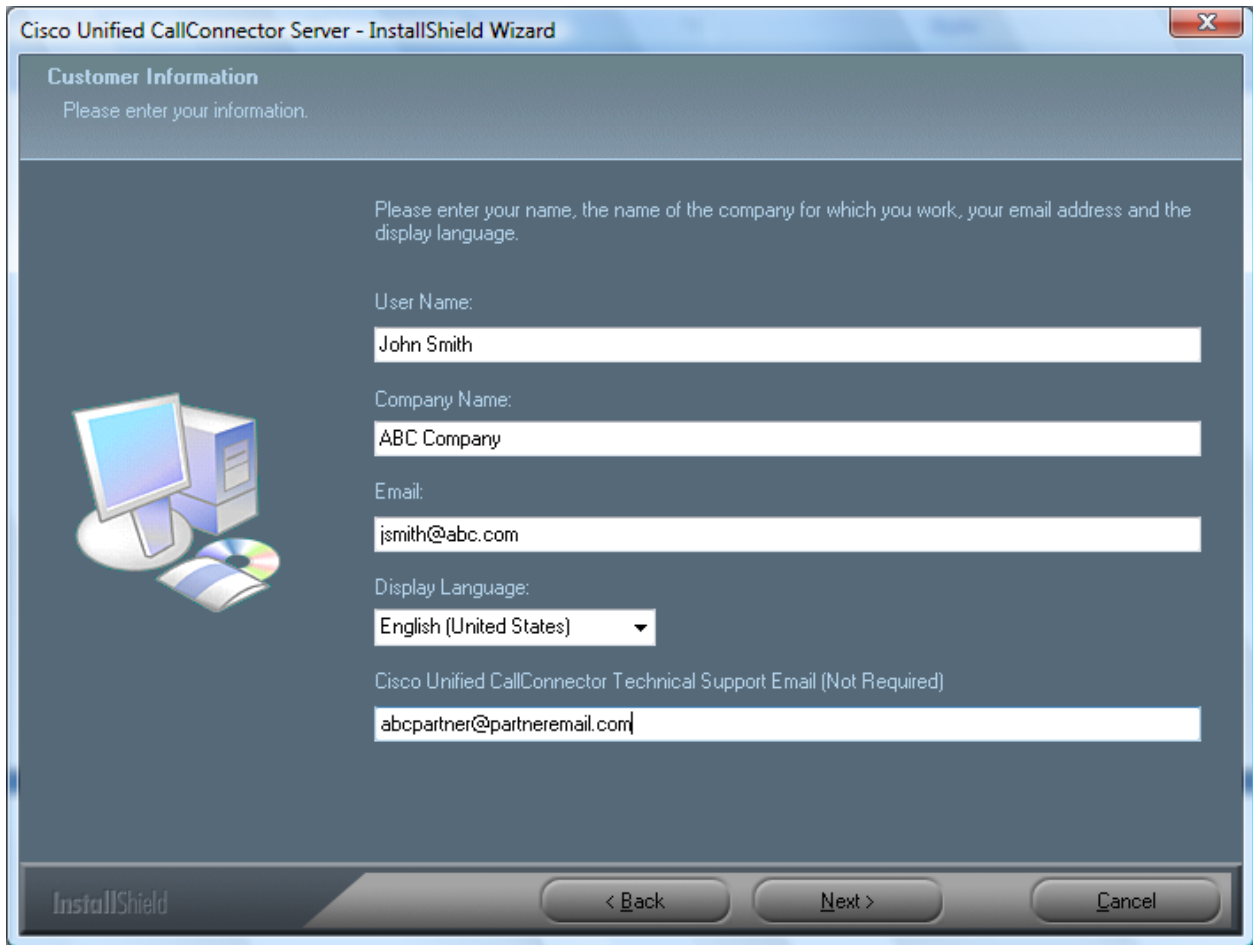
To proceed:

Enter your name, company and e-mail address and select the display language. Note the email address is a mandatory field and will be required during the license registration process.

The Display Languages include English, French, German, Italian, Danish, Dutch, Finnish, Portuguese, Spanish and Swedish. Please see Unified CallConnector Wiki site for latest language files.

Click **Next** or press the **ENTER** key.

Program Files Location:

The next window allows you to specify the location to which the Unified CallConnector program files will be copied. Click on the Browse button to select a folder other than the default.
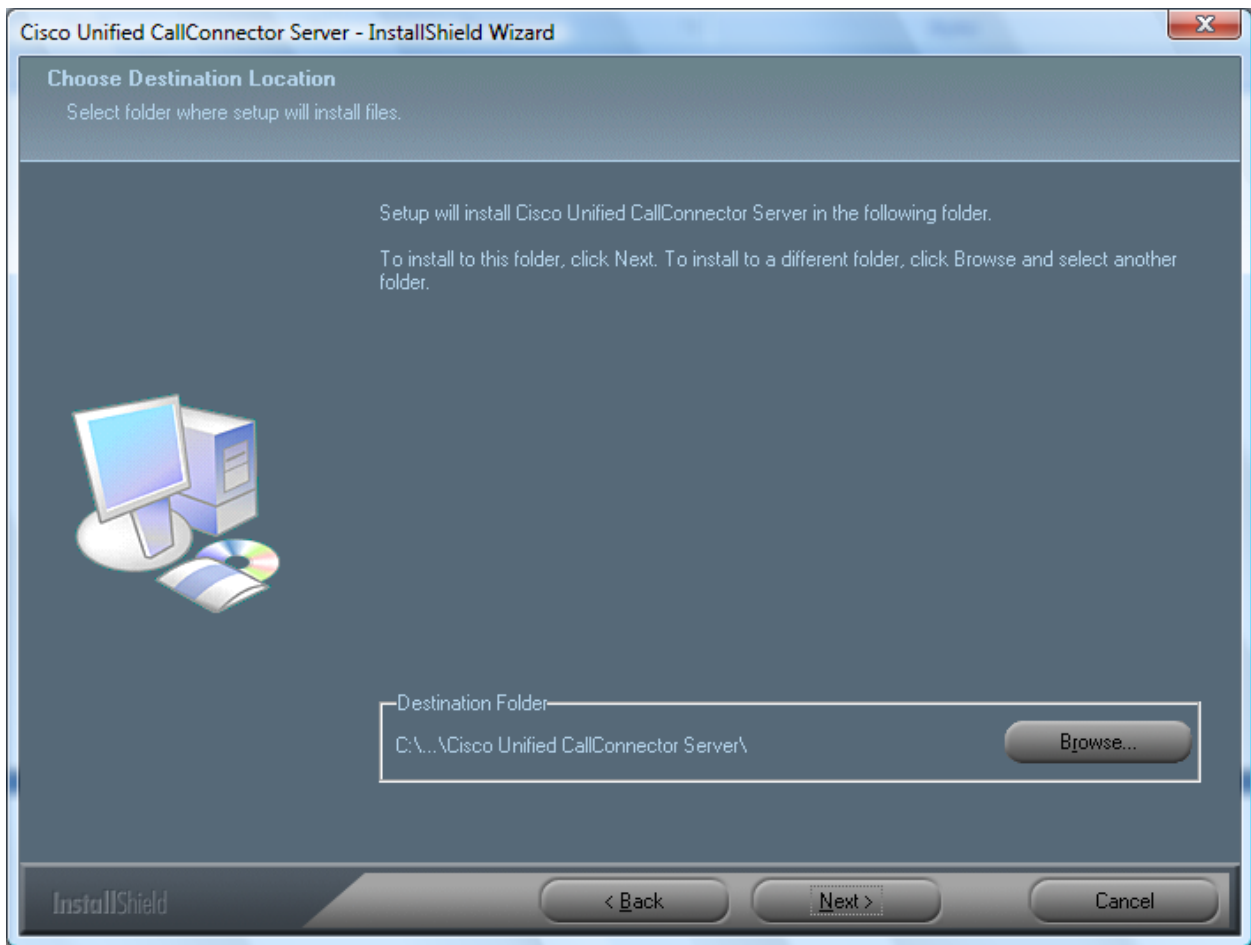
To proceed with the installation:

> Choose the default program path or click on the **Browse** button and specify the desired path.
>
> Click on **Next** to proceed with the installation.

The installation will copy the program and system files and update the registry and XML configuration file settings.

Once the files have been copied, you will be provided with the licensing option for the Unified CallConnector software.
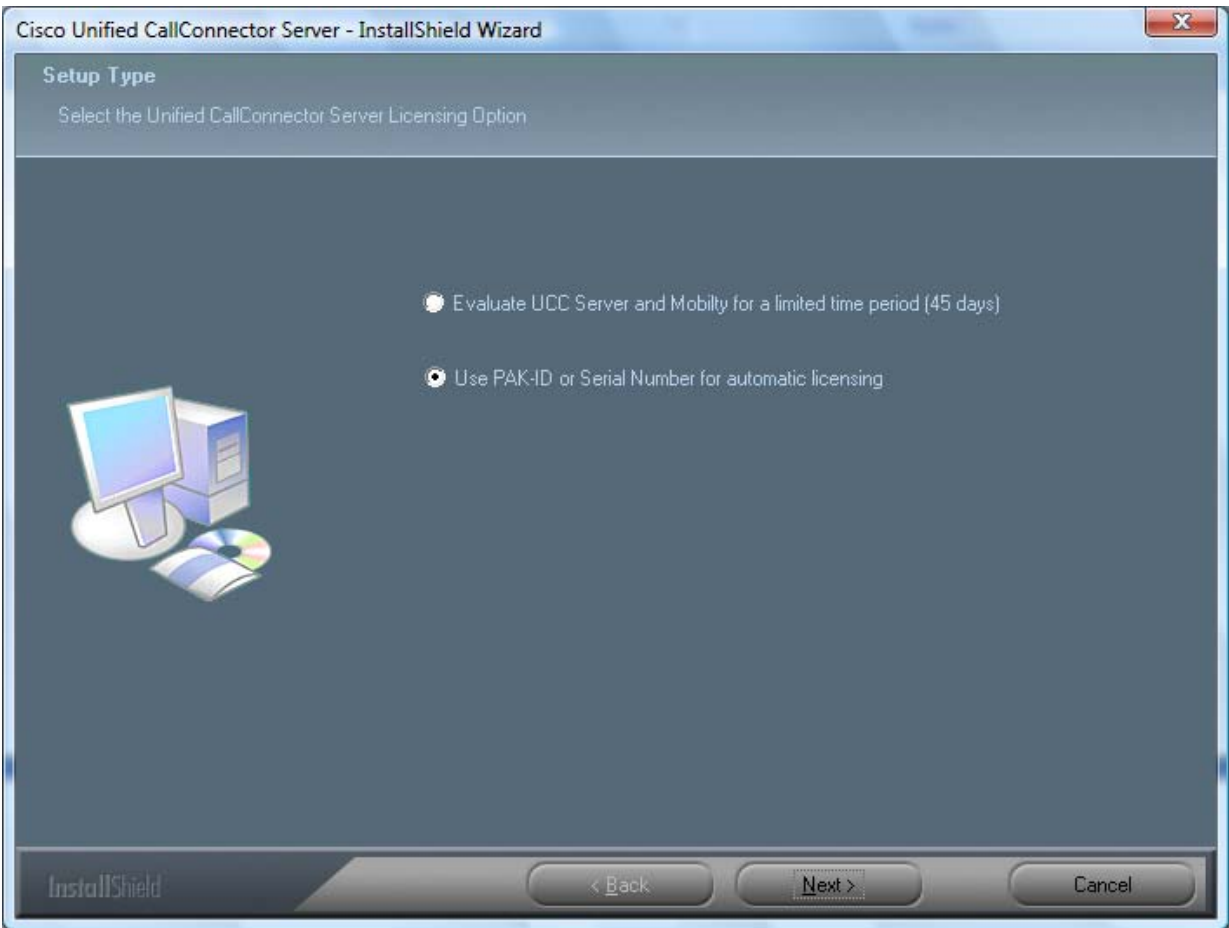
Select one of the Licensing Option:

Evaluate UCC Server and Mobility for a limited time period: Use this option if you have not purchased the UCC Server or do not have the Product Authorization Key (PAK-ID) or a Serial Number. This option will enable to the UCC Server and UCC Mobility Service for a period of 45 days. At the end of this time, you will need to register with a valid PAK-ID.

Use PAK-ID or Serial Number for automatic licensing: This option is used to register your UCC Server or Mobility license. If you have a PAK-ID or Serial Number for the software then select this option

Click on **Next** to proceed with the installation.

Notes on the Licensing Options:

1. Both these licensing options require Internet connection from the Server PC.
2. Internet Explorer needs to be installed on the Server PC.
3. The registration service uses HTTP methods to send your PAK-ID and machine information to the UCC License Server. It supports some HTTP Proxies and requires the Internet Explorer to be configured for such proxy support. Proxies requiring password are not supported.
4. You will need a PAK-ID or Serial Number associated with your purchase of the UCC Server/Mobility software. If you do not have a PAK-ID then you will only be able to install in the 'Trial' mode.
5. Trial mode can only be run once on one machine for a duration of 45 days. If you have trialed the UCC Server or Mobility on this PC for previous version of the software, then the trial request will be rejected.
6. During the 'Trial' period, Internet connection is required to allow for the daily verification of the license.
7. Enable all network adapters that will be used on the Server PC during normal operation of the UCC Server applications. You should disable the network adapters that are not in use.
8. If you are installing the UCC Server with Mobility Service then the registration page will be presented for the activation of each license separately.
9. The automatic registration is a two-step process. When the PAK-ID is registered, the UCC License Server returns a trial serial number. This can be used to immediately start using the UCC Server applications (if the previous trial has not expired). The server applications automatically check for the PAK-ID registration to be authorized. In this case a authorization serial number is returned by the UCC License Server. This replaces the trial serial number.
10. When the Pak-ID is authorized and the UCC Server applications have a valid authorizing Serial Number, then the daily on-line checking is turned off.
11. In the event the Server PC does not have Internet access, or there are some issues are encountered with the automatic registration process, an alternate registration method can be accessed using the Advanced Options button. This method requires a PAK-ID and is described below.
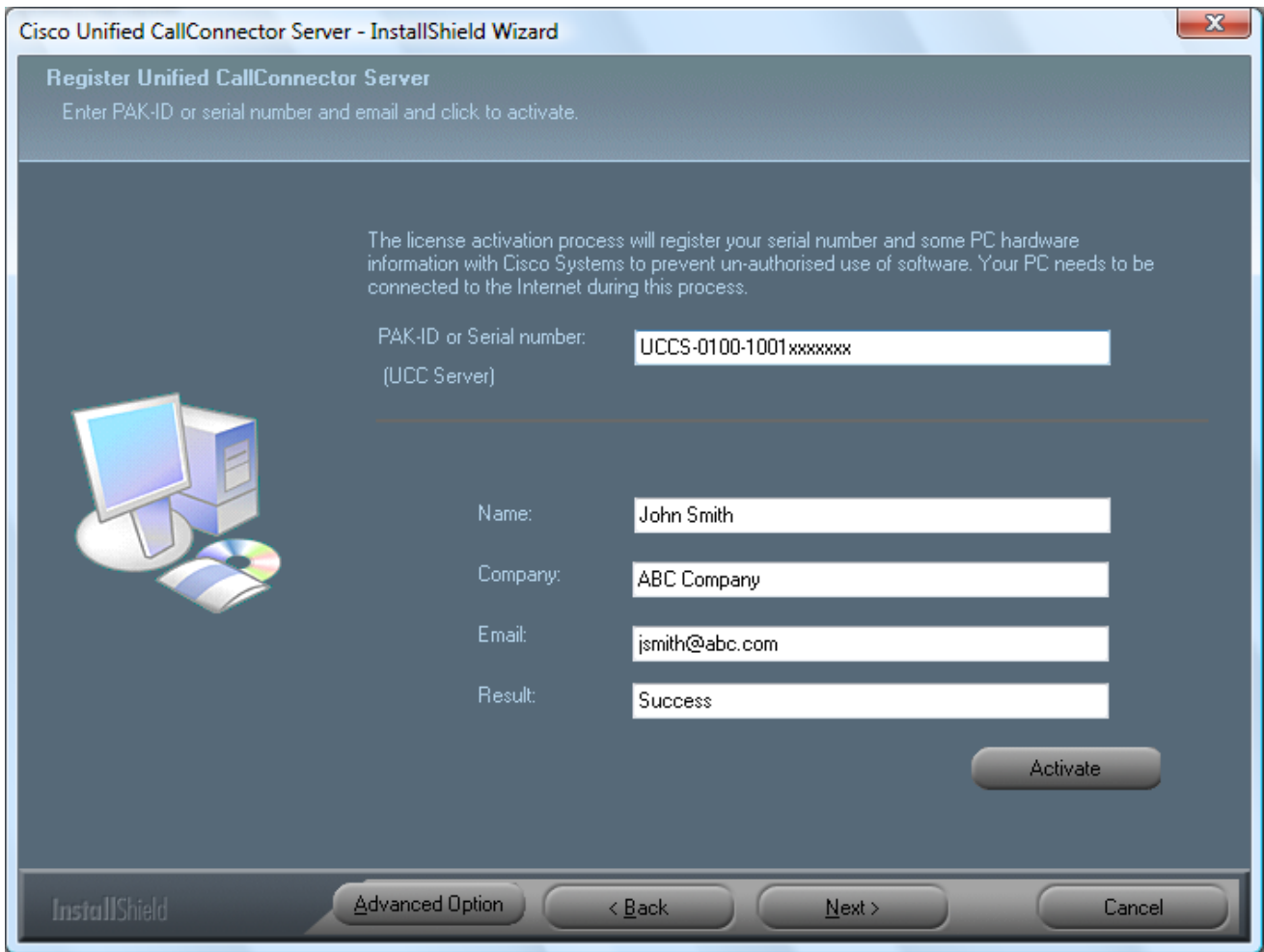
To Proceed with Registering the UCC Server:

Enter the PAK-ID. This Product Authorization Key is shipped to you with your purchase of the UCC software. (In some cases, you may have a Serial Number. This starts can be of the format UCCS-01001-xxxxxxxxxx. A valid serial number for the UCC Server can also be entered as a part of the registration.

Verify your contact information. The email address is mandatory and is used locate your license record for support purposes.

Click on the Activate button to start the registration process. The installation program will connect to the UCC License Server over the Internet and submit your PAK-ID, contact information some and machine information. If the registration was successful, then the results field will display this information.

Click on **Next** to proceed with the installation.

If this installation program includes the UCC Mobility Service, then a second license registration page is displayed to allow you to activate the Mobility Service license.

To Proceed with Registering the UCC Mobility Service:

Enter the PAK-ID. This Product Authorization Key is shipped to you with your purchase of the UCC software. (In some cases, you may have a Serial Number. This starts can be of the format UCCM-0100-xxxxxxxxxx. A valid serial number for the UCC Mobility can also be entered as a part of the registration. Note you will need unique serial numbers for the Server and Mobility registrations however the same or a different PAK-ID can be used depending on the UCC products that were purchased with that PAK-ID.

Verify your contact information. The email address is mandatory and id used locates your license record for support purposes.

Click on the Activate button to start the registration process. The installation program will connect to the UCC License Server over the Internet and submit your PAK-ID, contact information some and machine information. If the registration was successful, then the results field with display this information.

Click on **Next** to proceed with the installation.

Advanced Options (Alternative Licensing Options)
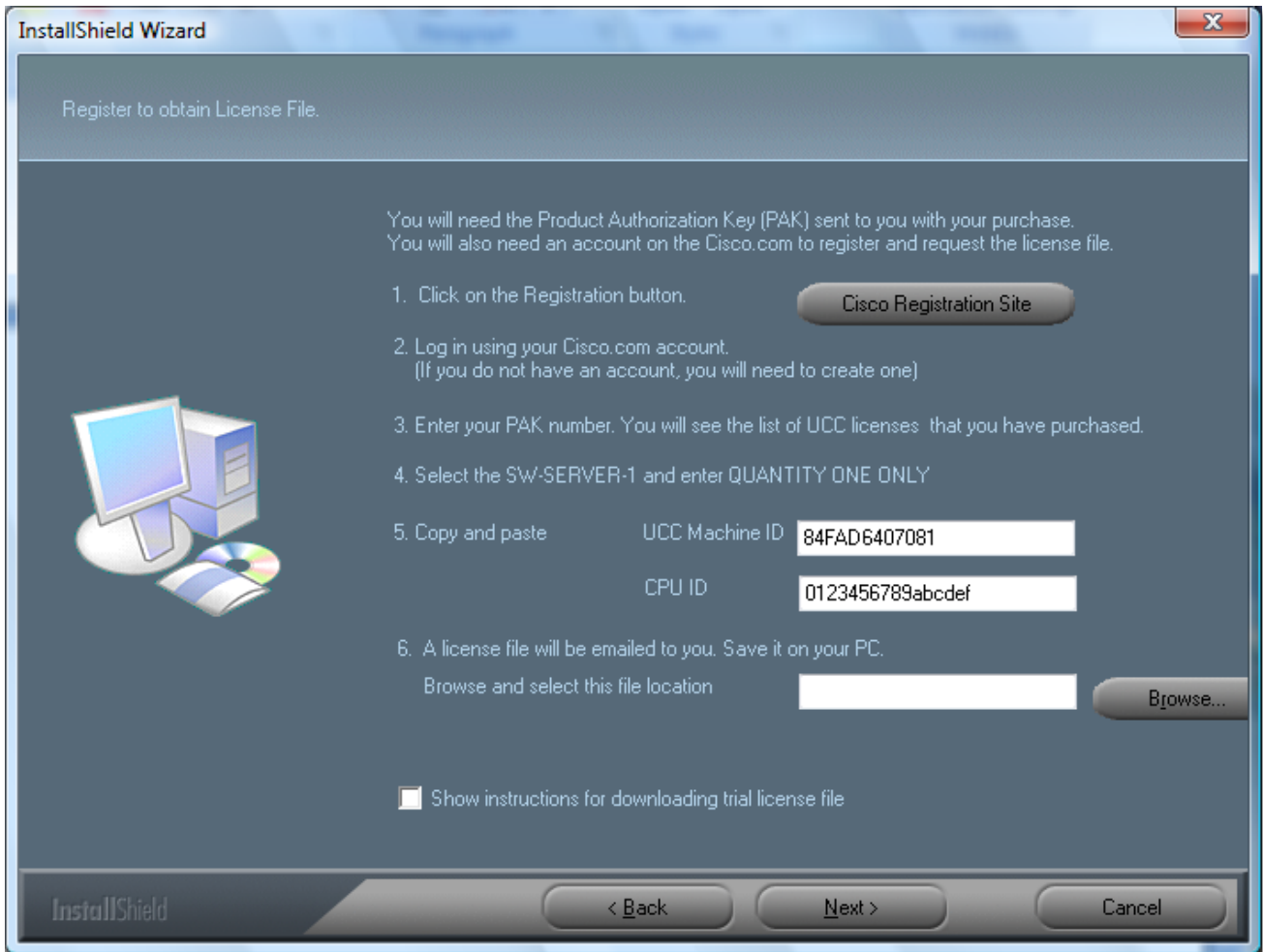
You will need the following information to generate a license file for the Unified CallConnector:

PAK ID: This is shipped to you as a part of your purchase from Cisco Systems.

Access to Cisco License Registration Site:
http://www.cisco.com/go/license

CCO Account: This is used to log in to the Cisco License site. If you do not have an account, you can create one on-line at
http://tools.cisco.com/RPF/register/register.do

UCC Machine ID and CPU ID: This information is needed for each client or server upon which UCC software will be installed. The UCC installation program identifies this information during the installation process. There is also a standalone UCC Machine ID utility that specifically identifies this information.

The steps for generating the license file are given below.

1. Click on the Cisco Registration Site button. This will take you to the Cisco System license registration site: http://www.cisco.com/go/license. Login using a valid CCO Account. If you do not have an account, you will need to create one on-line at http://tools.cisco.com/RPF/register/register.do

2. Enter your **PAK ID** in the field labeled **PAK ID** and click on **Submit** or press Enter.

3. The License Server will retrieve the license purchase information and will display the ordered, fulfilled and available quantities of UCC licenses.

4. If you are installing the Unified CallConnector client on your desktop, then enter **QUANTITY ONE (1) ONLY for SW-UCC-CLIENT-1**. If you are installing the Unified CallConnector Server or Mobility Service then enter **QUANTITY ONE (1) ONLY for each of SW-UCC-SERVER and/or SW-UCC-MOBILITY**. Click on Continue.

5. **WARNING:** You can run only one license on a computer. If you select more than one, then these licenses will not be available for use on other computers.

6. Copy and paste the UCC Machine ID and CPU ID obtained in step one, above, and enter your contact information and email address. Click on **Accept Agreement** and Continue.

7. Verify the information you have entered. If there is an error or if you have selected more than quantity one, then go back and correct this information.

8. Once you have completed the online registration, your License file will be emailed to you. Save it on the desktop then proceed with the UCC software installation process.

9. Click on the Browse button and navigate to the folder that contains the saved license file.

Click on **Next** to proceed.
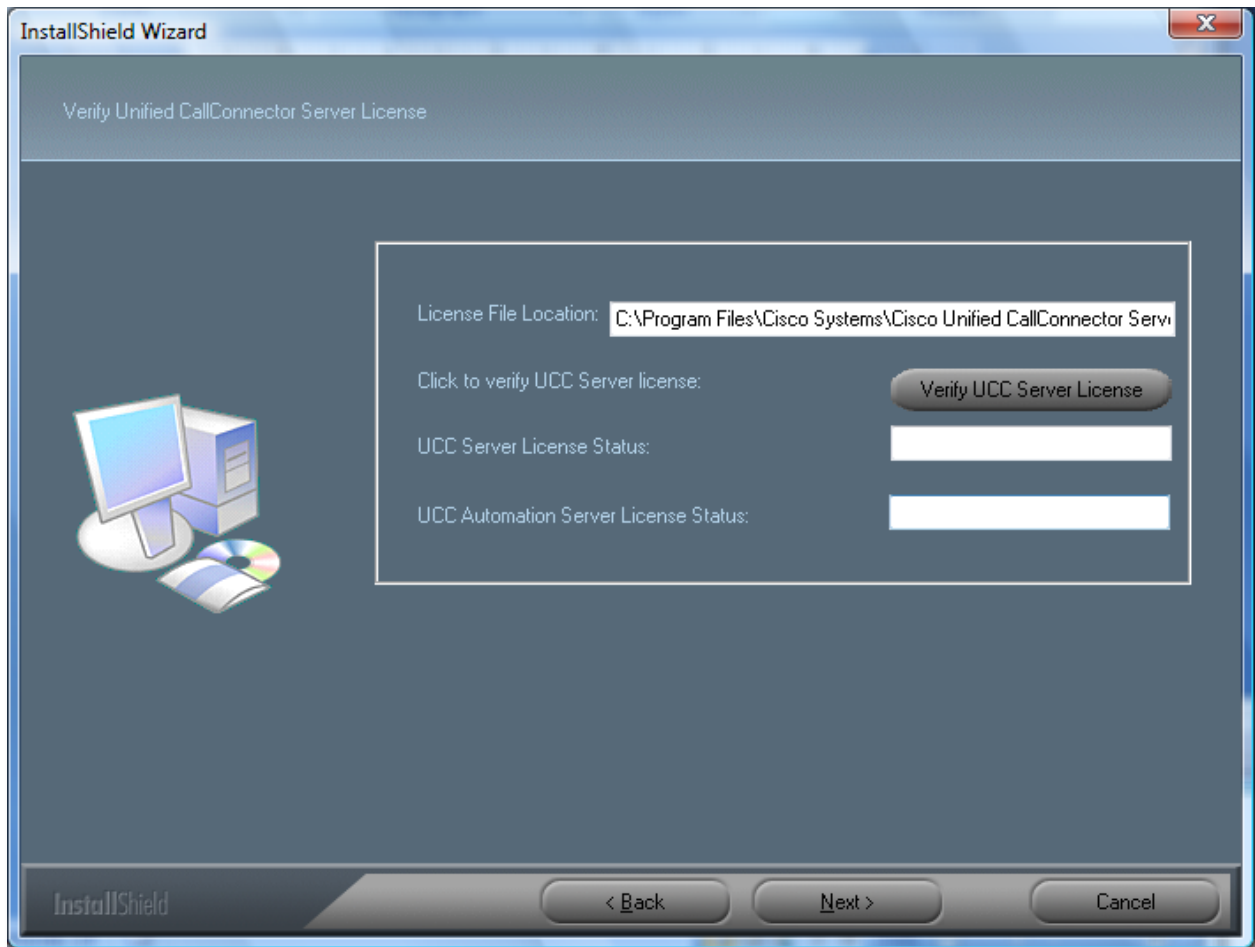
Click on the Verify UCC Server License button.

The licensing status of the UCC Server and UCC Mobility is displayed in the fields below.

Click on Next to complete the installation.

Note: You will need to restart the computer once the activation has been completed to apply the registry updates.

Problems with Activation

The license activation process can fail for a number of reasons. Some of these are discussed below.

Cannot Access the Internet

The activation process cannot access the Internet. Among other reasons, this can be due to:

> Firewall blocking the Server Wizard from accessing the Internet
>
> If a Proxy Server is being used, verify that the Internet can be accessed from the Internet Explorer. Also verify that it is a supported Proxy server. The activation process supports the Socks and HTTP proxy servers. The proxy parameters are read from the Internet Explorer Proxy server settings.

Cannot Access the License Server

This error indicates that the Internet is accessible but the License Server cannot be accessed.

To verify License Server availability you can browse to the License Server site:

http://www/unifiedcallconnecor.com

Trial (Evaluation) Period has Expired

The trail period for the Unified CallConnector Server on this computer has expired. You will to purchase a server license and run the Server Wizard to enter the new license.

Note: When the trial period expires, the Unified CallConnector Server applications will stop operating.

License has been Activated on Another Machine

The serial number that you have entered is invalid and is being used on another computer. You will need to purchase a valid Server serial number.

Serial Number is Invalid

The serial number that you have entered is invalid. Check the number you have entered. You will need to purchase a valid Server serial number for the Server applications to operate.

Activation Information has been Modified

Once the serial number has been activated, a set of information is stored in the Windows registry. If this information is deleted or changed, then the activation checking will fail and you will need to re-activate the software.

Trial License has been blocked

Please contact Cisco support as the trial license has been blocked.

Restart the Computer:

The installed server components are only available once the computer has been restarted. Please restart the server PC.

Performing an Upgrade

If you want to upgrade your Unified CallController to a newer version, then you can download and run a later installation program. The installation program will ask you if you want to upgrade the Unified CallConnector files. Click on Yes to continue with the upgrade. Make sure that you have closed all instances of Internet Explorer and Outlook and the Unified CallConnector Server programs. The install program will then copy the newer versions of the files to your computer.

Removing Unified CallConnector Server

You can remove the Unified CallConnector and all its files from the Windows Add/Remove program.

From the Widows Start menu, select Settings and open the Control Panel.

Double click on Add/Remove Programs

Select Cisco Unified CallConnector Server and click on the Remove button.
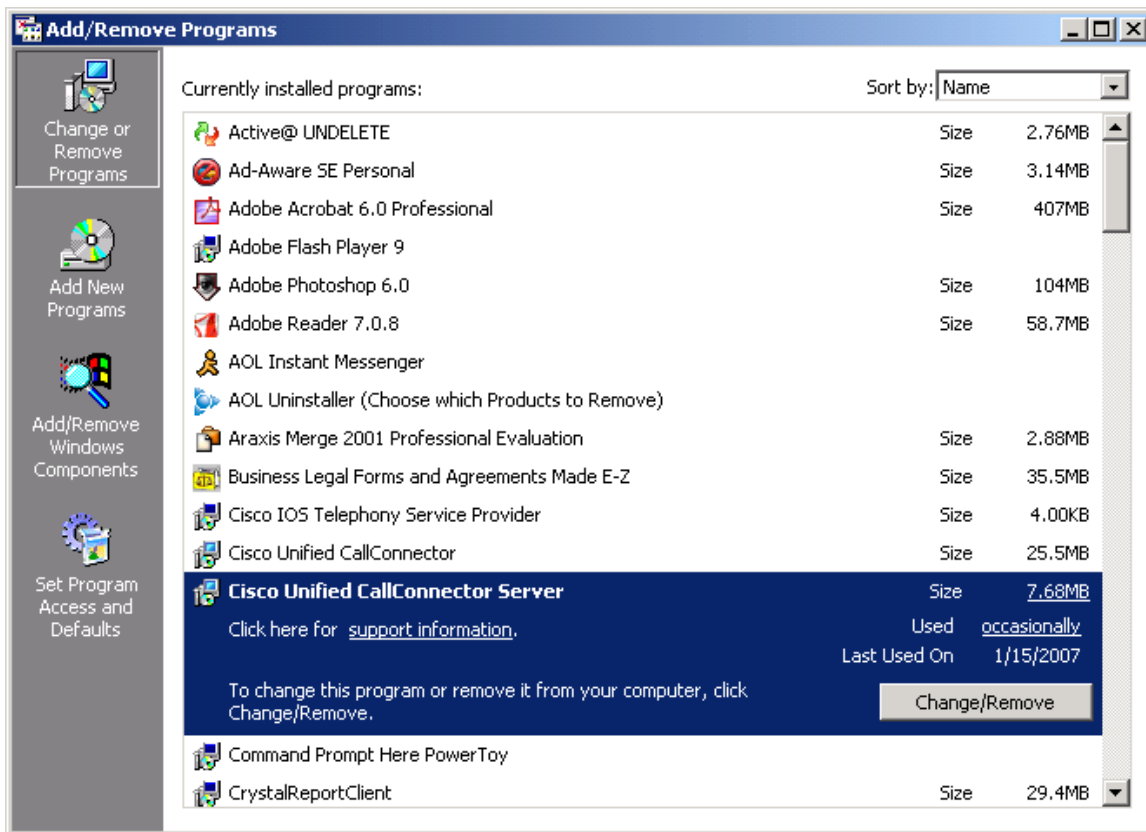
The Unified CallConnector Installation program will run. Click on the Remove button and next.
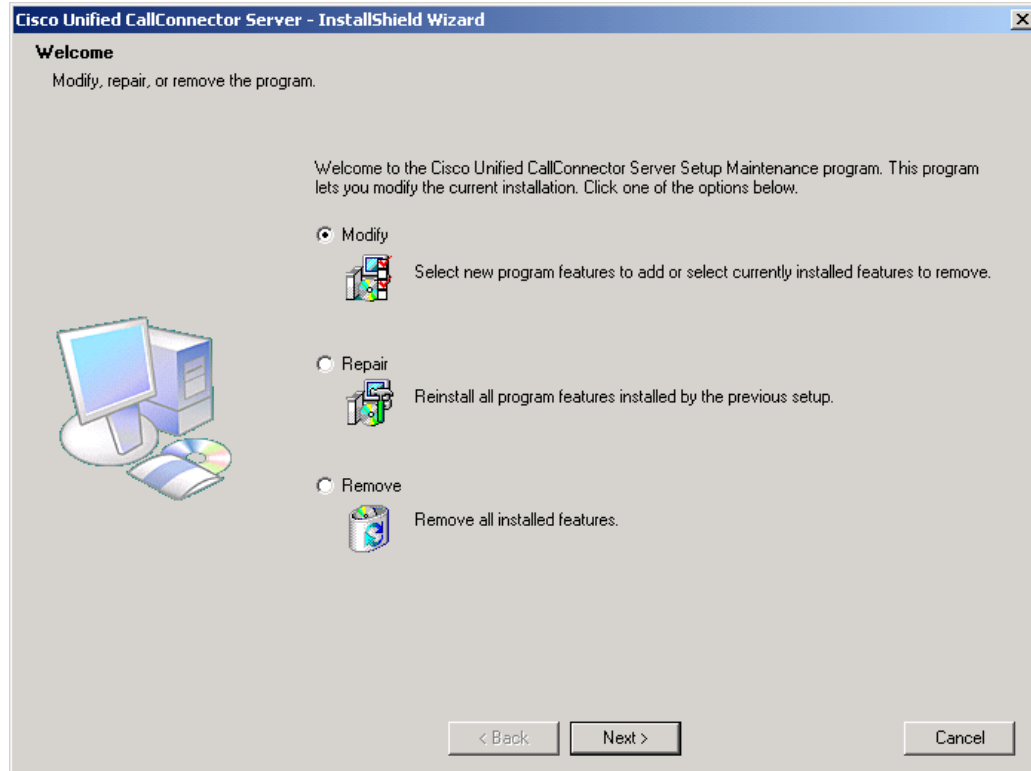
The Unified CallConnector will be un-installed from your computer.

Note: The Modify and Repair functions are not supported.

CHAPTER

4

Cisco Unified CME
Router Configuration

The Cisco Unified CallConnector Servers (UCC Server) connect to the Cisco Unified Communications Manager Express (Cisco Unified CME) routers to receive call status information, to control the call on the user' IP Phones. Both ends of these connections, the Cisco Unified CME router and the Cisco Unified CallConnector Server, need to be configured to allow the Cisco UCC Server to operate correctly.

This chapter describes the configuration required on the Cisco Unified CME routers to allow the Unified CallConnector Server to access and control the IP Phones. The sections include:

CONFIGURATION SUMMARY

Interfaces to Cisco CME -   Describes the interfaces or inter-working between the Cisco Unified CME router and the Unified CallConnector Servers.

CME Configuration Summary-   Provides an overview of the CME configuration required for the UCC Server.

Multiple Routers for Server-   Describes the configuration rules and network requirements for multiple Cisco Unified CME routers to connect to one Cisco UCC Server.

CME CONFIGURATION FOR UCC SERVER

Ephones Parameters -   Describes the parameters that have to be configured on the ephones to allow the CallController Server to open communication sessions.

Radius Parameters -   Describes how to configure the Radius parameters on the Cisco Unified CME router to allow the Presence Server to receive accounting packets.

CME CONFIGURATION FOR MOBILITY SERVICE

Mobility Ephones **-**   Describes the parameters that have to be configured for the ephones that are to be used by the Mobility Server.

Hardware Conferencing **-**   Provides an overview of the steps for setting up the CME hardware conferencing for use by the Mobility Server.

Direct Transfer to Voicemail -   Describes the steps to load and setup the CUE script to transfer a call to a voicemail box.

Hunt Group -   Describes the steps to setup a hunt group to route calls to the Dial-In Access mobility ephones.

Cisco Unified CME Connections

The Unified CallConnector Server applications make the following connections to the Cisco Unified CME:

SCCP connection to Cisco Unified CME: The CallController Server application connects to the Cisco Unified CME ephones using the Skinny Call Control Protocol. For the mobility application, the media is terminated over RTP/UDP protocol.

Connection for Radius Messages: For receiving Radius accounting packets for the call events on the Cisco Unified CME router.

Telnet Connection for Configuration: This is an optional connection used during configuration to download the ephone parameters to simply the configuration process.

The table below shows these connections and the information/configuration required on each of the systems.

	Configuration on UCC Server	Configuration on Cisco Unified CME
Telnet	Cisco Unified CME IP Address Telnet User name Telnet Password and Exec Password	Setup a Telnet account for downloading the configuration information.
Call Control from UCC Server	Cisco Unified CME IP Address Ephone User Name and Password	Configure user name and password on all the ephones that are controlled from the UCC Server
Radius Accounting Messages	Configure Password (Key) Configure Port	Configure the Radius Accounting Parameters on Cisco Unified CME router Verify that the password and port are the same as the UCC Server

CME Configuration for UCC Server

The Unified CallConnector Server requires a number of parameters to be configured on the Cisco Unified CME and Cisco Unified CUE. These features have to be <u>first provisioned on the CME</u> and CUE and <u>then the corresponding parameters have to be configured on the UCC</u> system. This section provides an overview of the CME and CUE setup requirements.

CME Setup for UCC Server

Function	What needs to be setup
Ephones username and password	The UCC Server connects to the user's ephones to allow the user to control and manage calls from the desktops. It uses the Cisco Unified CME TAPI connection – a SCCP connection that is parallel to the IP phone connection to the Cisco Unified CME.
	The TAPI connections require the ephones to be configured in the CME with user name and password.
	Each ephone that is to be controlled by the UCC Server needs to have a unique username and password configured.
	Note: In multiple router configurations, ephone user names must be unique across all routers.
Radius Accounting Parameters	RADIUS accounting messages can be generated by CME for calls that originate or terminate on the CME endpoints. The UCC system uses these messages to obtain the call state and calling/called numbers. The UCC Server <u>includes a RADIUS server</u> functionality and only requires the CME to be setup to send the RADIUS accounting messages of the required format, type and frequency to the UCC server. The section on 'Setting Up Radius Accounting' provides details on the CME setup, corresponding configuration on the UCC Server and tools for verifying that the Radius messages are being received – are described in the next chapter.
Telephony Service Parameters	The following general parameters need to be set in the Telephony Service section of the CME configuration:
	Keep Alive Timeout for the TAPI messages. This is set as following: "keepalive 10 auxiliary 10". The TAPI timeout value is the number after auxiliary multiplied by three in seconds.
	Transfer-System should be set to Full Consult as shown below: "transfer-system full-consult".

Additional CME Configuration for UCC Mobility

The Unified CallConnector Mobility Service makes use of additional features of the Cisco CME and Cisco CUE. These features have to be provisioned on the Cisco CME and Cisco CUE and then the corresponding parameters have to be configured on the UCC system. This section provides an overview of the CME and CUE setup requirements. Following chapters provide a step-by-step tutorial on how to setup the environment for Cisco CallConnector Mobility Service to work.

CME/CUE Setup Summary for Mobility Service

Function	What needs to be setup
Mobility ephones	The Mobility Service uses ephones for answering the Single Number Reach calls and for making the reach out calls. These ephones need to be configured in the CME and then selected and associated with the Mobility application using the Server Wizard.
	The mobility-ephones have specific attributes:
	A 'virtual MAC-address' is assigned to each mobility-ephone.
	Each ephone needs to have at-least three single-line ephone-DN configured
	Ephones need to have Ad-hoc conference control capability
	Note: In multiple router configurations, mobility-ephones have to be provisioned from each of the routers as the Mobility Service uses ephones that are on the same router as the user's ephone.
Ephone DNs for Mobility	Three single channel DN need to be configured for each Mobility Ephone.
CME Conferencing Options	The Mobility Service uses the CME conferencing feature to bridge the caller and user calls. Both hardware and software conferencing is supported by the Mobility Service. However hardware conferencing is required for the Mid-call and DISA features. If hardware conferencing is enabled on the CME, then ad-hoc conferencing has to be configured for use by the mobility-ephones.
Transfer to Voice Mail	When a user cannot be reached at their specified numbers, the call is returned to the user's voice mailbox. A voice mail box must be configured for each user with SNR service. Additionally the CME and CUE have to be setup to allow the transfer of the call directly into the user's voice mailbox. Several methods for transferring a call to a user's voice mail are supported by the Mobility Service. The most common method uses the Transfer-to-Voicemail script. This script has to be uploaded to CUE and configured through the CUE administration interface. On the CME side a dial-peer has to be setup with a 'Transfer-Pilot Number' to send to call to the CUE Transfer-to-Voicemail' script.
	Note: This is the voice mail pilot number. In multiple CME configurations, CUE needs to be configured on each router.

Hunt Group for the DISA numbers	The Mobility Service DISA feature use ephones to receive authenticate and provide CME feature access to the UCC user. Since multiple ephones are normally configured for DISA, a hunt group pointing to the primary ephone-DN on each of these ephones needs to be setup in the CME to route the DISA callers to the mobility ephones. The hunt group can be setup to sequentially hunt for an idle ephone-DN.
	Note: The hunt group list should include only the primary ephone-DN from each of the DISA mobility ephones.
Additional Mobility ephones and ephone-DN for the DISA service	The Mobility DISA service can be setup to share the ephones from a general pool with the SNR feature or it can have a set of ephones dedicated to this service. Sufficient numbers of mobility-ephones need to be configured for the required traffic levels.

Multiple Routers for UCC Server

A single UCC Server can be shared by users on multiple Cisco CME systems. Such configurations can be used to support branch offices with their individual Cisco Unified CME working with a centralized UCC Server.
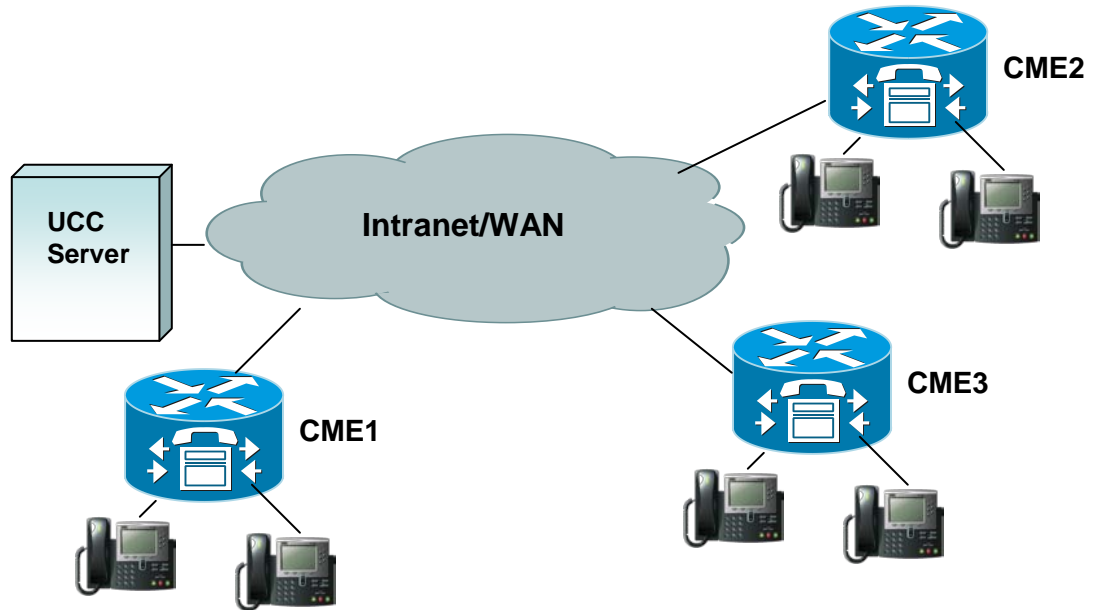
UCC Server Connected To Multiple Cisco Unified CMEs

In multi-site configurations, users at any UCC Client will be able to:

- View the availability and locations settings of their colleagues across the organization.
- See the current telephone status for all the extension numbers maintained in the UCC corporate directory.
- Share the organizational contact information with ability for click to dial.
- The mobility services, if configured, can be available to all the users.

There are a number of configuration rules and network requirements for such multi-router systems.

Configuration	Description
Maximum Number of Routers	It is recommended that no more than 5 ISR/UC500 routers be connected to the UCC Server
Maximum number of users per UCC Server	The maximum number of users per UCC Server is 250 users
TCP/UDP Control Messages	Network must provide bandwidth and minimum latency for the control messages. RADIUS messages are transmitted as UDP messages. TCP sessions are used to transport the SCCP/Skinny messages between the CME router and the UCC Server
UDP Media for RTP messages	Calls handled by UCC Mobility Service include the SNR and DISA calls. The media for these calls flows from the CME router with the PSTN Gateway to the UCC Server. The UCC Server only supports G.711 codecs (64 KBPS for each voice direction)
Network Bandwidth Requirement	If the routers are in different locations connected via private network, the network should have sufficient capacity to support:
	SCCP/Skinny traffic between the UCC Server and each of the routers. The traffic to the UCC Server will be the number of ephones controlled by the UCC Server multiplied by the bandwidth required for one SCCP session.
	Voice Media -- RTP (G.711 encoded) 128 Kbps for each call handled by the Mobility Services. The network should have the bandwidth and latency for the peak or maximum number of calls that can handled by the Mobility Service.
	Radius Messages -- UDP traffic from each router to the UCC Server.
	SIP Messages – TCP & UDP traffic between the UCC clients and the UCC Server
	Note: The network should also allow the transport of UDP traffic between the routers and the UCC Server.
Location of Routers	Generally the UCC Server should hosted with the largest CME router in a multiple router configuration. The UCC Services are not sensitive to the location of the routers, although it is assumed that the routers are in one country.

Resources Required on each router for the Mobility Services	The Mobility Service requires the following to be configured on each router:
	Mobility-ephones and ephone-DNs. The Mobility Service requires available mobility-ephone in the router of the SNR user's ephone for processing the SNR calls. If the ephones are not available, then the service is not launched.
	Conferencing resources – since the mobility-ephones are from each router and these ephones request the conferencing services, the conferencing and DSP resources have to be configured on each CNE router from which the users will be using the Single Number Reach service.
	CUE and Voicemail boxes – the user's calls are returned to the user's voice mailbox. Each router is required to have CUE installed, together with the Transfer-to-Voice Mailbox script and a distinct pilot number to that router's transfer-to-voice mailbox script.
	Since the Mobility Service utilizes the resources of each router, the CME features of shared DNs, Pickup, Transfer and Conference need to be configured on each router for use by the mobility service.
	RADIUS accounting parameters must be setup tp send messages to the UCC server.
Dialing Plans and Dialing Rules	The UCC Server allows administrators to setup the location, extension number lengths, outside access codes for each router. The UCC Server also provides per router a digit manipulation table for pre-processing the telephone numbers for dialing and lookup.
Unique Extension Numbers	The UCC Server matches the extension numbers to the user in the corporate directory and propagates this information as telephone status. This requires that the extension numbers in multiple router configurations be unique and non-overlapping.

Setting up Ephone Parameters

The Cisco Unified CallConnector Server connects to the Cisco Unified CME IP Phones to allow the user to control their phones from the Unified CallConnector clients such as the toolbars. These connections are made over the TAPI port of the Cisco Unified CME router.

The Unified CallConnector server application – CallController Server registers and establishes a connection over the Cisco Unified CME TAPI port to each of the ephones that have been configured for use by the Unified CallConnector. To establish this connection each ephone much have the username and password field provisioned on the Cisco Unified CME router.

Steps to Configure Username/Password for a Ephone

Below are the steps for configuring a typical ephone. The specific requirement for the UCC Server is highlighted in bold and includes the username and password. In this case the username is "john" and the password is "Cisco".

- Click Start -> Run
- Type *telnet xxx.xxx.xxx.xxx* (xxx.xxx.xxx.xxx would be your CME router IP address)
- Enter the username and password
- Enter config t
- Type *ephone x* (x would be the ephone id)
- Type mac-address 0013.C307.E9C0 (MAC address of the ephone)
- Type type 7960
- Enter username john password cisco
- Type button 1:a 2:b 3:c 4:d
- a, b and c are the ephone DNs for the user extensions.
- Type *exit* when finished

Example of Ephone Configuration

```
ephone-2 Mac:0013.C307.E9C0 TCP socket:[11] activeLine:0 REGISTERED in
SCCP ver
6 and Server in ver 5
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
caps:7
IP:192.168.1.5 50179 Telecaster 7960  keepalive 132940 max_line 6
button 1: dn 4  number 5014 CH1   IDLE
button 2: dn 5  number 3 CH1    IDLE
button 3: dn 6  number 5015 CH1   IDLE
button 4: dn 43 number 5043 CH1   IDLE        CH2   IDLE
Username: john Password: cisco
Tapi client information

Username:john  status: REGISTERED Socket : [46]
 Tapi Client IP address:  192.168.1.17  Port: 3426
```

In this example, the ephone-2 has been configured with username john and password cisco. It also shows that a TAPI client (UCC server), an IP-address 192.168.1.17; port 3426 is connected to this ephone.

Notes for Ephone Username and Password

1. Username and password are required to allow a TAPI connection to the IP Phone.
2. Username and password have to be <u>less than 15 characters in length</u>. (This is a Cisco CME restriction.)
3. The IP-Phone has to be in service and registered for the 'TAPI' to be successful. If the phone is disconnected, after a timeout the TAPI connection will fail.
4. The CME supports only one 'TAPI' connection to an ephone. Any additional connection requests get rejected.
5. When a TAPI session is established, the TAPI client information can be viewed using the 'Show Ephone TAPI' command. The TAPI client information displays the status 'REGISTERED' and the Client IP address.
6. The Cisco CME enforces unique usernames for the ephones; however in multiple router environments, the system administrator will need to ensure that the usernames are unique across the routers. The UCC Server will change duplicate username to DUP-ip-address-username.
7. Ephone soft-key templates do not affect the UCC Client as the soft-keys are available to the TAPI session even if they are not configured for the ephone.

Pre-Requisites for Connecting to Ephones:

- Ephone must be configured with user name and password
- There must be a phone device registered to that ephone
- There must be network access for the TCP connections between the Cisco Unified CME router and the UCC Server
- There must be no existing TAPI connections to that ephone. (The Cisco Unified CME router supports only one TAPI connection per ephone.)
- The ephones must be selected using the Server Administration Wizard for it to be controlled and must be associated with a user for the user to manage call using the client.

Connection Recovery and Timeouts

The Unified CallConnector Server tries to establish connections to all the ephones configured for the UCC Server. Normally these ephones will be a sub-set of all the ephones in the Cisco Unified CME. In the event these connections fail either at startup or during operation, the Unified CallConnector CallController Sever will try to re-establish these connections. The recoveries of these ephone connections follow these rules:

- The UCC Server will try to establish connection to the ephone multiple times up to the Max-Retry count – an internal configurable parameter.
- When the Max-Retry count is exceeded, the UCC Server will stop trying to connect to the CME for a period of time. This interval between the retries is a configurable period and is set to 6 minutes by default.
- If the connection cannot be re-established within the maximum retries, then UCC Server will wait for a configurable time period and then return to trying to re-establish the ephone connection.

To Verify TAPI Connection to Ephone

Complete the Cisco Unified CME and the UCC server configuration and start up the server applications from the UCC Services Manager application.

From the Cisco Unified CME router:

From the command line interface, use the 'show ephone tapi' command to list the ephones with TAPI connections.

-

cc2800#show ephone tapi

```
ephone-2 Mac:0013.C307.E9C0 TCP socket:[11] activeLine:0 REGISTERED in
SCCP ver
6 and Server in ver 5
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
caps:7
IP:192.168.1.5 50179 Telecaster 7960  keepalive 132940 max_line 6
button 1: dn 4  number 5014 CH1   IDLE
button 2: dn 5  number 3 CH1    IDLE
button 3: dn 6  number 5015 CH1   IDLE
button 4: dn 43 number 5043 CH1    IDLE          CH2    IDLE
Username: john Password: cisco
Tapi client information

Username:john  status: REGISTERED Socket : [46]
 Tapi Client IP address:  192.168.1.17  Port: 3426
```

From the command line interface, use the 'debug ephone register' command to monitor the registration of the TAPI connections to the ephones.

From the Unified CallConnector Server

- Open the UCC Diagnostic Tool. See Chapter 9 for more details.
- Make a few calls from on the IP Phones.
- From the CallController Server tests, run the Display All Phone Statistics test.
- This will display the registered ephones and some basic call statistics.

To Reset the TAPI Connection to Ephone

Cisco Unified CME version 7.0 and greater allow the TAPI session to be reset from the command line.

From the Cisco Unified CME router:

Click Start -> Run
Type *telnet xxx.xxx.xxx.xxx* (xxx.xxx.xxx.xxx would be your CME router IP address)
Enter the username and password
Enter config t
Type *ephone x* (x would be the ephone id)
Type reset tapi (This is drop the current TAPI connection)

Setting Up the Radius Accounting

The Cisco CME and its underlying IOS platform can be setup to generate accounting packets for the calls being handled within the system. These accounting messages can provide information on the start-time and end-time of the calls as well as the caller/called numbers. The accounting messages are sent to RADIUS servers using a standard protocol, that is extended with Cisco specific

The Unified CallConnector Presence Server has an integrated RADIUS server interface to connect with and receive these Radius accounting messages from the Cisco CME systems.

Notes:

The Cisco CME router has to be configured to enable the voice Radius accounting packets to be sent to the Unified CallConnector.
The Unified CallConnector Server acts as the Radius Server and the Cisco CME router is the Radius client that generates and transmits the radius packets.
Cisco RADIUS VSA Voice Implementation Guide provides more details on the Radius setup options. The configuration of the Radius parameters on the router for providing telephone status information to the Presence Server.
In multiple router configurations, each router must be configured to send the RADIUS accounting packets to the UCC Server. Note – the authentication password and the account port are required to the same on each router.

Radius Parameter Setup Summary

- Enabling AAA accounting
- Enabling Connection-based Accounting
- Setting up the Radius Server IP address and port
- Entering the Authentication Key or password
- Enabling the Cisco Accounting Attributes – Vendor Specific Attributes
- Enable accounting for the gateways
- Setup source address for the Radius packets

Radius Configuration Notes

Item	Description
Accounting Port 1646	This is the port on the UCC Server to which the RADIUS messages are sent by the CME. The port value is set in the CME and must be the same on the UCC Presence Server – Radius Server Parameters page. In multiple router configurations, all accounting ports to the UCC Server must be the same. Note: Verify that the port is available on the UCC Server.
Authentication Key (Password)	The value of the Authentication Key is set in the CME router. This same value must be configured on the UCC Presence Server. In multiple router configurations, the Authentication Key must be the same on all routers.
Radius Server IP address and port	This parameter specifies the IP Address of the Radius Server – in this case this will be the IP Address of the UCC Server. Note: The port value setting must be the same on the router and on the UCC Server.
Cisco Accounting Attributes	The Radius messages can contain Cisco specific attributes. The UCC Server requires these attributes and the VSA setting must be enabled on the router.
Source address for the Radius packets	The Cisco routers can have multiple network adapter cards and the Radius messages can be sent over any of these adapters. The UCC Server requires that the Radius messages must be sent over the same network adapter i.e. have the same source IP Address as the CME IP Address used by the IP Phones.

To Setup Radius Parameters on CME Router

The table below displays the commands for setting up the Radius parameters on the CME router using the Command Line Interface.

Command	Description
enable Router> enable	Enter Exec mode
Configure terminal Router # configure term	Enter global configuration mode
aaa new-model Router (config)# aaa new-model	Enables AAA
aaa accounting connection h323 start-stop radius Router (config)# aaa accounting connection h323 start-stop broadcast group uccserver	Enables connection based accounting and send stop and start packets
aaa group server radius uccserver server 192.168.1.18 auth-port 1645 acct-port 1646 Router (config)# aaa group server radius uccserver	Specifies the IP address and ports for the servers that are in the group uccserver above
aaa accounting update newinfo Router (config)# aaa accounting update newinfo	Enables sending update packets for new information for the interim call states
radius-server host Router (config)# radius-server host 1.1.1.1 auth-port 1645 acct-port 1646	Specifies the Radius Server IP-Address and accounting port. The IP Address and Port should match the setting on the Presence Server Radius configuration.
radius-server key Router (config)# radius-server key cisco	Sets the password for authenticating the Radius server. This password should also be entered in the Radius configuration on the Server Wizard Radius Window,
radius-server vsa send accounting Router (config)# radius-server vsa send accounting	Sends vendor specific attributes. The UCC Server uses the Cisco specific attributes in the accounting messages.
aaa session-id common Router (config)# aaa session-id common	Set common session id
gw-accounting syslog gw-accounting aaa Router (config)# gw-accounting aaa	Enable accounting for gateway endpoints to send Radius messages for the PSTN ports
ip radius source-interface Router (config)# ip radius source-interface GigabitEthernet 0/0	Set the source ip address of the Radius messages to be the same as the CME IP Address for skinny messages. The is required for the Single Number Reach service.

Below is an example of the router configuration file showing the Radius parameter settings.

```
aaa new-model

aaa group server radius uccserver

 server 192.168.1.116 auth-port 1645 acct-port 1646

aaa accounting update newinfo

aaa accounting connection h323 start-stop broadcast group uccserver

aaa session-id common

gw-accounting syslog

gw-accounting aaa

radius-server host 192.168.1.116 auth-port 1645 acct-port 1646 key
uccserver

radius-server vsa send accounting

radius-server vsa send authentication

ip radius source-interface GigabitEthernet 0/0
```

Sending Radius Messages to Multiple Addresses

If your environment has multiple Radius servers and you need to configure the router to send to the UCC Server and the other Radius servers then the following settings can be used:

Group parameter in the aaa accounting connection setup can be used to send messages to a list of Radius servers.

The Radius Server IP Addresses is specified in aaa group server radius group-name as shown below.

aaa accounting connection h323 start-stop radius Router (config)# aaa accounting connection h323 start-stop broadcast **group uccserver group syslogserver**	Enables connection based accounting and send stop and start packets
aaa group server radius uccserver server 1.1.1.1 auth-port 1645 acct-port 1646 aaa group server radius **syslogserver** server 1.1.1.2 auth-port 1645 acct-port 1646 Router (config)# aaa group server radius uccserver	Specifies the IP address and ports for the servers that are in the group uccserver above
radius-server host Router (config)# radius-server host 1.1.1.1 auth-port 1645 acct-port 1646 key uccserver Router (config)# radius-server host 1.1.1.2 auth-port 1645 acct-port 1646 key cisco	Specifies the Radius Server IP-Address and accounting port. The IP Address and Port should match the setting on the Presence Server Radius configuration. This key (password) will apply only to this radius server. Note: Remove the Key setting from Router (config)# radius-server **key uccserver**

Below is an example of the router configuration file showing the Radius parameter settings for sending Radius messages to multiple Radius servers.
```
aaa new-model
!
aaa group server radius uccserver
 server 192.168.1.2 auth-port 1645 acct-port 1646
!
aaa group server radius syslogserver
 server 192.168.1.3 auth-port 1645 acct-port 1646
!
aaa accounting update newinfo
aaa accounting connection h323 start-stop broadcast group uccserver group
syslogserver
!
aaa session-id common
```

```
!
!
gw-accounting syslog
gw-accounting aaa
!
radius-server host 192.168.1.2 auth-port 1645 acct-port 1646
radius-server host 192.168.1.3 auth-port 1645 acct-port 1646
radius-server key uccserver
radius-server vsa send accounting
radius-server vsa send authentication
!
```

Verifying Radius Settings

- Use the 'Show Running Config' from the CLI to verify your router settings.
- Verify that each router is sending the accounting messages to the correct UCC Server IP Address and port. Use the Debug Radius Accounting and see example below.
- Verify in the debug messages that you are getting Radius messages for Off-hook, Ring, Connect and Hang-up.
- Verify that the source IP address in the Radius messages is the same as the CME IP Address being used by the IP Phones.
- Once the UCC Server has been setup, you can verify using the 'View Radius Message' utility to view the messages being received from the routers.
- Verify that the Radius parameters have been setup correctly on all the routers.

Example of Radius Accounting Debug Messages

Note: The Send Accounting Request to IP-Address and the corresponding response indicating receipt and acknowledgement from UCC Server.

```
26 20:19:56.442: RADIUS(000549E7): Send Accounting-Request to 192.168.1.99:1646 id
1646/138, len 867
26 20:19:56.442: RADIUS:  authenticator 58 A6 38 48 9F 73 B4 92 - 44 05 5E 12 37 B5 8F A1
26 20:19:56.442: RADIUS:  Acct-Session-Id    [44] 10  "000A92A9"
26 20:19:56.442: RADIUS:  Calling-Station-Id [31] 6   "4002"
26 20:19:56.442: RADIUS:  Vendor, Cisco      [26] 61
26 20:19:56.442: RADIUS:  h323-setup-time    [25] 55  "h323-setup-time=*12:19:54.786 central
Wed Dec 26 2007"
26 20:19:56.442: RADIUS:  Vendor, Cisco      [26] 40
26 20:19:56.442: RADIUS:  h323-gw-id         [33] 34  "h323-gw-id=cc3845.yourdomain.com"
26 20:19:56.442: RADIUS:  Vendor, Cisco      [26] 56
26 20:19:56.442: RADIUS:  Conf-Id           [24] 50  "h323-conf-id=C1535895 B32611DC
B4D0D9D2 5FE6F9B4"
26 20:19:56.442: RADIUS:  Vendor, Cisco      [26] 31
26 20:19:56.442: RADIUS:  h323-call-origin  [26] 25  "h323-call-origin=answer"
26 20:19:56.442: RADIUS:  Vendor, Cisco      [26] 32
26 20:19:56.442: RADIUS:  h323-call-type    [27] 26  "h323-call-type=Telephony"
26 20:19:56.442: RADIUS:  Vendor, Cisco      [26] 65
26 20:19:56.442: RADIUS:  Cisco AVpair      [1]  59  "h323-incoming-conf-id=C1535895
B32611DC B4D0D9D2 5FE6F9B4"
```

26 20:19:56.442: RADIUS: Vendor, Cisco   [26] 30
26 20:19:56.442: RADIUS: Cisco AVpair   [1]   24 "subscriber=RegularLine"
26 20:19:56.442: RADIUS: Vendor, Cisco   [26] 134
26 20:19:56.442: RADIUS: Cisco AVpair   [1]   128 "feature-vsa=fn:TWC,ft:12/26/2007
12:19:54.786,cgn:4002,cdn
frs:0,fid:471652,fcid:C1535895B32611DCB4D0D9D25FE6F9B4,legID:58BBB"
26 20:19:56.442: RADIUS: Acct-Input-Octets [42] 6   0
26 20:19:56.442: RADIUS: Acct-Output-Octets [43] 6   0
26 20:19:56.442: RADIUS: Acct-Input-Packets [47] 6   0
26 20:19:56.442: RADIUS: Acct-Output-Packets [48] 6   0
26 20:19:56.442: RADIUS: Acct-Session-Time [46] 6   0
26 20:19:56.442: RADIUS: Vendor, Cisco   [26] 63
26 20:19:56.442: RADIUS: h323-connect-time [28] 57 "h323-connect-time=*12:19:56.434
central Wed Dec 26 2007"
26 20:19:56.442: RADIUS: Vendor, Cisco   [26] 66
26 20:19:56.442: RADIUS: h323-disconnect-tim[29] 60 "h323-disconnect-time=*12:19:56.434
central Wed Dec 26 2007
26 20:19:56.442: RADIUS: Vendor, Cisco   [26] 32
26 20:19:56.442: RADIUS: h323-disconnect-cau[30] 26 "h323-disconnect-cause=10"
26 20:19:56.442: RADIUS: Vendor, Cisco   [26] 35
26 20:19:56.442: RADIUS: Cisco AVpair   [1]   29 "h323-ivr-out=Tariff:Unknown"
26 20:19:56.442: RADIUS: Vendor, Cisco   [26] 24
26 20:19:56.442: RADIUS: Cisco AVpair   [1]   18 "release-source=1"
26 20:19:56.442: RADIUS: Vendor, Cisco   [26] 28
26 20:19:56.442: RADIUS: h323-voice-quality [31] 22 "h323-voice-quality=0"
26 20:19:56.442: RADIUS: Vendor, Cisco   [26] 47
26 20:19:56.442: RADIUS: Cisco AVpair   [1]   41 "gw-rxd-cgn=ton:0,npi:0,pi:0,si:0,#:4002"
26 20:19:56.442: RADIUS: User-Name   [1]   6   "4002"
26 20:19:56.442: RADIUS: Acct-Status-Type   [40] 6   Stop   [2]
26 20:19:56.442: RADIUS: NAS-Port-Type   [61] 6   Virtual   [5]
26 20:19:56.442: RADIUS: NAS-Port   [5]   6   60000
26 20:19:56.442: RADIUS: NAS-Port-Id   [87] 15 "EFXS 50/0/358"
26 20:19:56.442: RADIUS: Service-Type   [6]   6   Login   [1]
26 20:19:56.442: RADIUS: NAS-IP-Address   [4]   6   192.168.1.122
26 20:19:56.442: RADIUS: Acct-Delay-Time   [41] 6   0
26 20:19:56.442: RADIUS: Received from id 1646/135 192.168.1.99:1646, Accounting-response,
len 20
26 20:19:56.442: RADIUS: authenticator B5 42 1C 4B 5B 29 6E CB - 79 F5 3E 83 56 D1 94 2C
26 20:19:56.442: RADIUS: Received from id 1646/136 192.168.1.14:1646, Accounting-response,
len 20
26 20:19:56.442: RADIUS: authenticator BE 4D 8E 20 BB ED A2 E9 - 91 6A 0C FE 9B 74 34 02
3845#

Example 2:

On the Cisco Unified CME:
From the command line interface, use the debug command to view the radius accounting messages being sent:

The debug message below was generated on an off-hook and sent to Radius-Server at IP Address 192.168.1.17 from IP Address 192.168.1.121

Note: Use of debug commands, especially verbose debug command, can place a heavy load on the router and can impact other functions on the router.

cc2800#debug radius verbose
cc2800#term mon
cc2800#
*May 13 13:27:00.648: RADIUS/ENCODE(0007DEA8):Orig. component type = VOICE
*May 13 13:27:00.648: RADIUS/ENCODE: Skip encoding 0 length AAA attribute dnis
*May 13 13:27:00.648: RADIUS(0007DEA8): Config NAS IP: 0.0.0.0
*May 13 13:27:00.648: RADIUS/ENCODE(0007DEA8):Orig. component type = VOICE
*May 13 13:27:00.648: RADIUS/ENCODE: Skip encoding 0 length AAA attribute dnis
*May 13 13:27:00.648: RADIUS(0007DEA8): Config NAS IP: 0.0.0.0
*May 13 13:27:00.648: RADIUS/ENCODE(0007DEA8):Orig. component type = VOICE
*May 13 13:27:00.648: RADIUS/ENCODE: Skip encoding 0 length AAA attribute dnis
*May 13 13:27:00.648: RADIUS(0007DEA8): Config NAS IP: 0.0.0.0
*May 13 13:27:00.648: RADIUS/ENCODE(0007DEA8):Orig. component type = VOICE
*May 13 13:27:00.648: RADIUS/ENCODE: Skip encoding 0 length AAA attribute dnis
*May 13 13:27:00.648: RADIUS(0007DEA8): Config NAS IP: 0.0.0.0
*May 13 13:27:00.652: RADIUS/ENCODE: Best Local IP-Address 192.168.1.121 for Radius-Server 192.168.1.17
*May 13 13:27:00.652: RADIUS(0007DEA8): Send Accounting-Request to 192.168.1.17:1646 id 1646/149, len 565

Configuring Mobility Ephones/Ephone pools

The UCC Mobility Service uses CME ephones to make and receive calls to provide the Single Number Reach and Dial-In Access services.

These ephones have to be configured in the Cisco CME for each of the routers connected to the UCC Mobility Service. The mobility ephones have a specific configuration requirement as described below:

Mobility Ephone Attributes

Configuration	Description
Ephone MAC Address Example: AAAA.BBBB.1000	This 'Virtual MAC Address' is used as an identifier for the ephone. This should be unique for the UCC System and is required to be unique for each router. (Since there are multiple mobility-ephones configured for each router, you cannot use the UCC Server MAC address. In addition the CME requires MAC Address field to follow the MAC address format, but does not require this to be a physical MAC address.)
Ephone Type 7960	Default phone type for the Mobility-ephones
Ephone DNs	Three single line DN that are not shared, for each mobility ephone.
Conference Control	Keep Conference – so that when the when the Mobility Service drops out the call is maintained
Feature Set	Standard ephone feature set with pickup, conference, transfer etc.
Codec	G711 codec

Setting up a Mobility-ephone in CME

You would need to configure an ephone to have one or more shared-DN. Please follow the steps below:

Click Start -> Run

Type *telnet xxx.xxx.xxx.xxx* (xxx.xxx.xxx.xxx would be your CME router IP address)

Enter the username and password

Enter config t

Type *ephone x* (x would be the ephone id)

Type mac-address AAAA.BBBB.1000

Type type 7960

Type keep conference

Type username ucceph1 password cisco

Type button 1:a 2:b 3:c

a, b and c are single-line ephone DNs created for the mobility service.

Type *exit* when finished

Example of mobility-ephone

Extract from 'Show run'

```
ephone  28

 username "38user28" password cisco

 mac-address AAAA.BBBB.4307

 type 7960

 button  1:648 2:649 3:650

keep-conference
```

Extract from 'Show ephone'

```
ephone-28 Mac:AAAA.BBBB.4307 TCP socket:[124] activeLine:0
REGISTERED in SCCP ver 3 and Server in ver 3

mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0
debug:0 caps:3

IP:192.168.1.14 1889 Telecaster 7960  Telstrat keepalive 132
max_line 16

button 1: dn 648 number 4648 CH1   IDLE

button 2: dn 649 number 4649 CH1   IDLE

button 3: dn 650 number 4650 CH1   IDLE

Username: 38user28 Password: cisco
```

Setup an ePhone with Share-Call Appearance:

The shared call appearance on the mobility-ephones is used to support the option to pickup the SNR call from the user's ephone by pressing the line button. The user's primary ephone-DN needs to be configured on the shared mobility-ephone. When a call arrives at the user's ephone, it will also ring at the shared mobility-ephone. If the rule conditions are met, then the Single Number Reach service will use this shared mobility-ephone to answer the call and try to locate the user at the specified numbers.

The configuration for the shared appearance mobility-ephone is similar to the mobility-ephone except that you configure an additional button with the the user's primary ephone-DN. Please follow the steps below:

Click Start -> Run
Type *telnet xxx.xxx.xxx.xxx* (xxx.xxx.xxx.xxx would be your CME router IP address)
Enter the username and password
Enter config t
Type *ephone x* (x would be the ephone id)
Type mac-address AAAA.BBBB.1000
Type type 7960
Type keep conference
Type username ucceph1 password cisco
Type button 1:a 2:b 3:c
a, b and c are single-line ephone DNs created for the mobility service.
Type button 4:X   where X is the user's primary DN
Type *exit* when finished

Setting up CME Hardware Conferencing

This section provides the summary steps for setting up hardware conferencing on the CME router. Please refer to the document xxxxxxxxxxxxxxxxxx for more details.

Prerequisites
• Cisco Unified CME 4.1 or a later version
• You must have a PVDM2-8, PVDM2-16, PVDM2-32, or PVDM2-64 high-density packet voice digital signal processor module hosted on the motherboard or on a module such as the NM-HDV2 or NM-HD-2VE.
• For Cisco Unified IP Phone 7985, firmware version 4-1-2-0 or a later version

Restrictions
• The maximum number of meet-me conference parties is 32 for one DSP using the G.711 codec and 16 for the G.729 codec.
• A participant cannot join more than one conference at the same time.
• Ad hoc conferencing for more than three parties (hardware-based) is not supported on the Cisco Unified IP Phone 7906 and 7910 and Cisco Unified IP Phone 7914 Expansion Module.
• Ad hoc conferencing for more than three parties is not supported on Cisco Unified IP phones running SIP.
• Hardware-based ad hoc conferencing does not support the local-consult transfer method (transfer-system local-consult command).

Enabling DSP Farm Services for a Voice Card

To enable DSP farm services for a voice card to support multi-party ad hoc and meet-me conferences, perform the following steps.

Summary Steps

```
enable
configure terminal
voice-card slot
dsp services dspfarm
exit
```

Configuring Join and Leave Tones

To configure tones to be played when parties join and leave ad hoc and meet-me conferences, perform the following steps for each tone to be configured.

Summary Steps

```
enable
configure terminal
voice class custom-cptone cptone-name
dualtone conference
frequency frequency-1 [frequency-2]
cadence {cycle-1-on-time cycle-1-off-time [cycle-2-on-time cycle-2-off-time] [cycle-3-on-
time cycle-3-off-time] [cycle-4-on-time cycle-4-off-time]} | continuous
end
```

Configuring SCCP for Cisco Unified CME

To enable Skinny Client Control Protocol (SCCP) on Cisco Unified CME, perform the following steps:

Summary Steps

> enable
> configure terminal
> sccp local interface-type interface-number [port port-number]
> sccp ccm {ip-address | *dns*} identifier *identifier-number* [priority *priority*] [port *port-number*] [version *version-number*]
> sccp ccm group *group-number*
> bind interface interface-type interface-number
> exit
> sccp
> exit

Configuring the DSP Farm

To configure the DSP farm profile for multi-party ad hoc and meet-me conferencing, perform the following steps.
Note: The DSP farm can be on the same router as the Cisco Unified CME or on a different router.

Summary Steps

> enable
> configure terminal
> dspfarm profile *profile-identifier* conference
> codec {*codec-type* | pass-through}
> conference-join custom-cptone *cptone-name*
> conference-leave custom-cptone *cptone-name*
> maximum conference-party *max-parties*
> maximum sessions *number*
> associate application sccp
> end

Associating Cisco Unified CME with a DSP Farm Profile

To associate a DSP farm profile with a group of Cisco Unified CME routers that control DSP services, perform the following steps.

Summary Steps

> enable
> configure terminal
> sccp ccm group *group-number*
> associate ccm identifier-number priority priority-number
> associate profile *profile-identifier* register *device-name*
> end

Enabling Multi-Party Ad Hoc Conferencing

To allow multi-party ad hoc conferences with more than three parties and meet-me conferences, perform the following steps.

Note: Configuring multi-party ad hoc conferencing in Cisco Unified CME disables three-party ad hoc conferencing.

Summary Steps

    enable
    configure terminal
    telephony-service
    conference hardware
    sdspfarm units *number*
    sdspfarm tag number device-name
    sdspfarm conference mute-on *mute-on-digits* mute-off *mute-off-digits*
    end

Configuring Ad Hoc Conferencing Numbers

To configure numbers for multi-party ad hoc and meet-me ad hoc conferencing, based on the maximum number of conference participants you configure, perform the following steps. Ad hoc conferences require four extensions per conference, regardless of how many extensions are actually used by the conference parties.

Note: Ensure that you configure enough directory numbers to accommodate the anticipated number of conferences. The maximum number of parties in a multi-party ad hoc conference on an IP phone is eight; the maximum on an analog phone is three.

Summary Steps

    enable
    configure terminal
    ephone-dn *dn-tag* [dual-line]
    number *number* [secondary *number*] [no-reg [both | primary]]
    conference {ad-hoc | meetme}
    preference preference-order [secondary secondary-order]
    no huntstop [channel]
    end

Configuring Conferencing Options for a Phone

To configure a template of conferencing features such as the add party mode, drop party mode, and soft keys, for multi-party ad hoc, and meet-me conferences and apply the template to a phone, perform the following steps.

Note: The following commands can also be configured in ephone configuration mode. Commands configured in ephone configuration mode have priority over commands in ephone-template configuration mode.

Restrictions

The ConfList (including the Remove, Update, and Exit soft keys within the ConfList function) and RmLstC soft keys do not work on a Cisco Unified IP Phone 7902, 7935, and 7936.

Summary Steps

    enable
    configure terminal
    ephone-template *template-tag*
    conference add-mode [creator]
    onference drop-mode [creator | local]

conference admin
softkeys connected [Acct] [ConfList] [Confrn] [Endcall] [Flash] [HLog] [Hold] [Join] [Park]
[RmLstC] [Select] [Trnsfer]
softkeys hold [Join] [Newcall] [Resume] [Select]
softkeys idle [Cfwdall] [ConfList] [Dnd] [Gpickup] [HLog] [Join] [Login] [Newcall] [Pickup]
[Redial] [RmLstC]
softkeys seized [CallBack] [Cfwdall] [Endcall] [Gpickup] [HLog] [MeetMe] [Pickup] [Redial]
exit
ephone phone-tag
ephone-template *template-tag*
end

Setup Direct Transfer to Voicemail

This section provides a sample configuration for enabling direct transfer to CUE/Voicemail of a user by dialing a speed-dial code. It details how a dial-peer can be created to setup a call to a CUE AA and then send digits for identifying a voicemail mailbox.

Dial plan

Before configuring CME and CUE, you should plan your dial plan for CME IP phones, CUE and bulk speed-dial on CME. The following is a sample of numbers that need to be defined before configuring the system.

Name	Number	Description
IP Phones (with Voicemail)	1001, 1002, 1003	Ephone-dn numbers of IP phones that have a voicemail mailbox.
Bulk speed-dial file for direct access to VM	0	This is the reference to a file that contains entries for bulk speed-dial codes. This is used in conjunction with bulk speed-dial prefix and list entry to address a particular number
CUE AA pilot for direct transfer to VM script	6500	Trigger on CUE for direct transfer to VM script.

To Setup the Transfer-to-Voicemail Script

Open the Cisco Unity Express (CUE) administration page. In this example go to the web page:
http://192.168.1.123\
Login as the administrator:
Username: admin
Password: admin
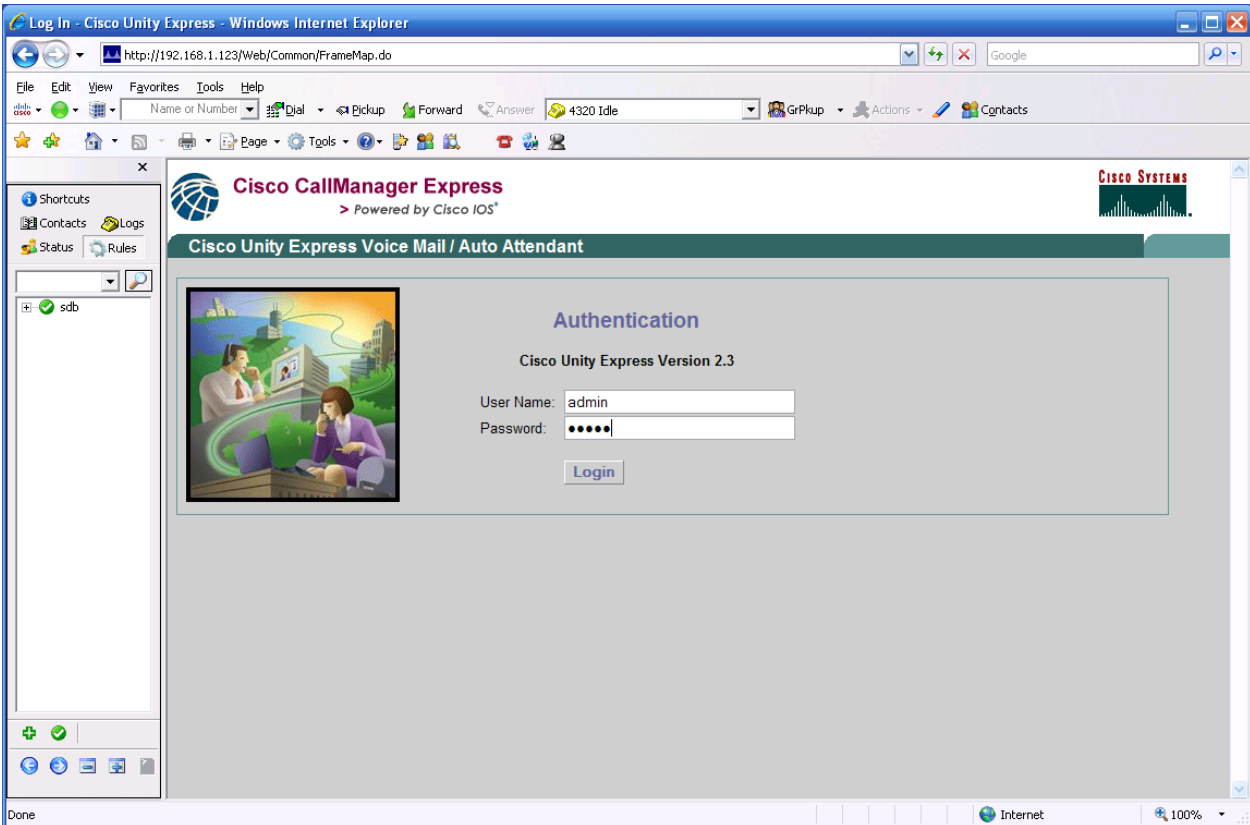
From the Voice Mail menu, select Auto Attendant. The Auto-Attendant pages will display.
Click on the Add button to add the DirectTransfertoVoiceMail script. To update or make changes, you can click on the script name.
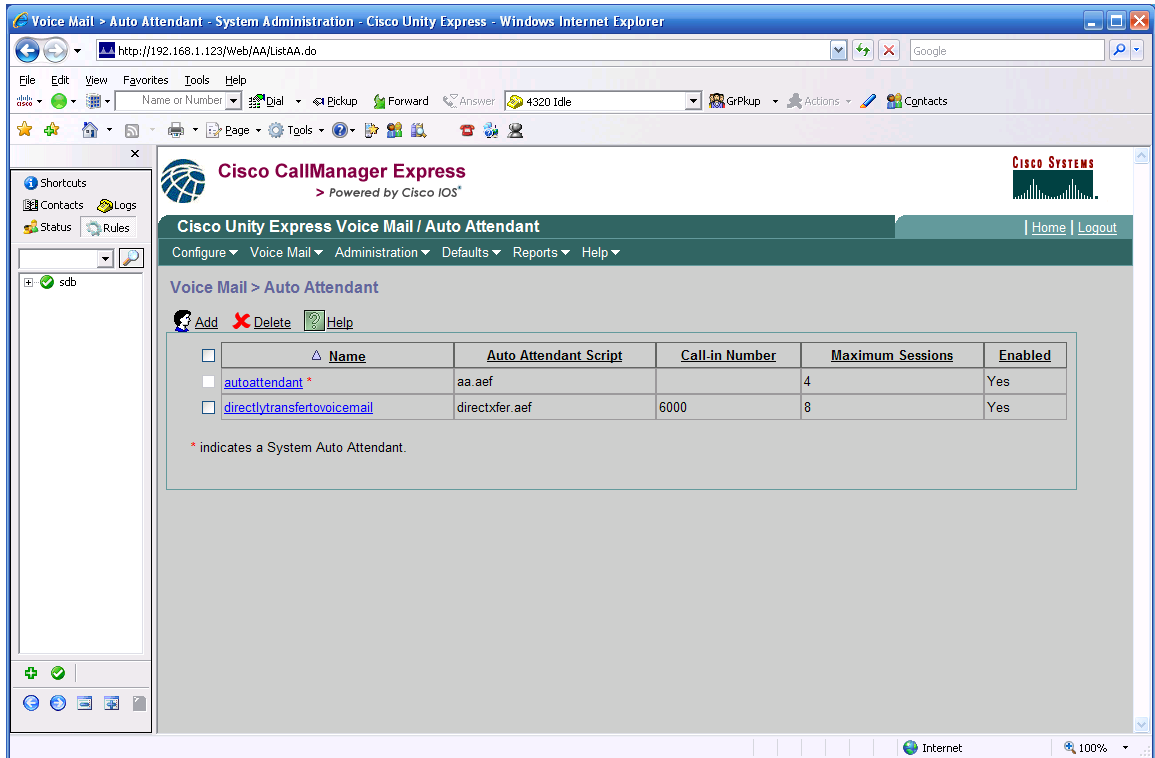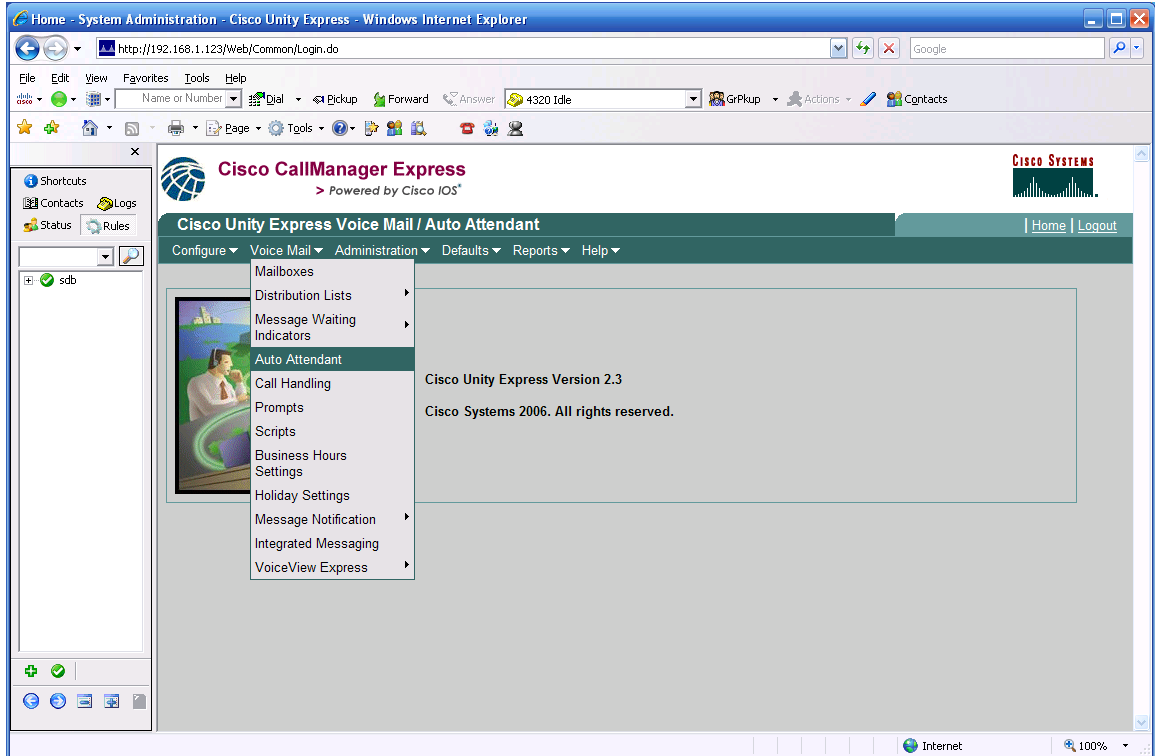
Click on the directlytransfertovoicemail
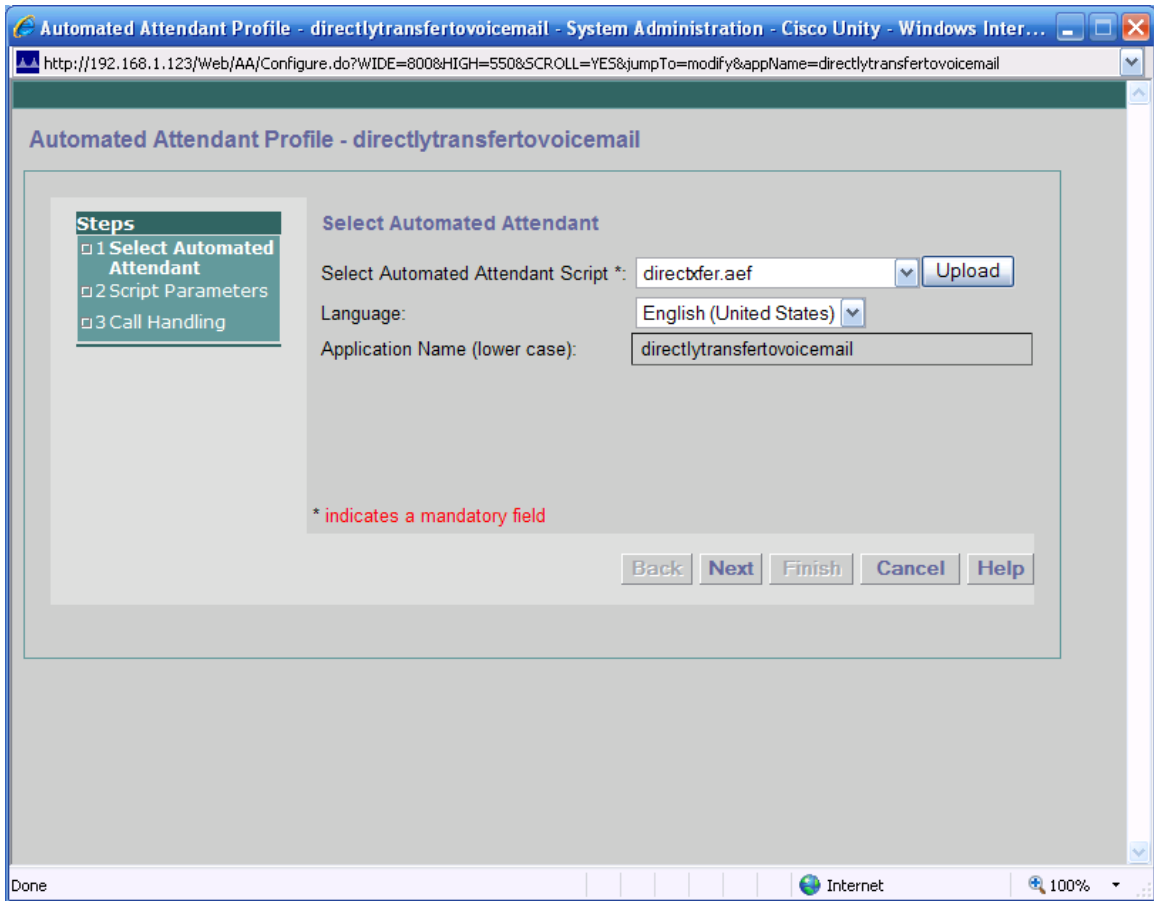
Click Upload the new script, browse to select the script file and click on upload.
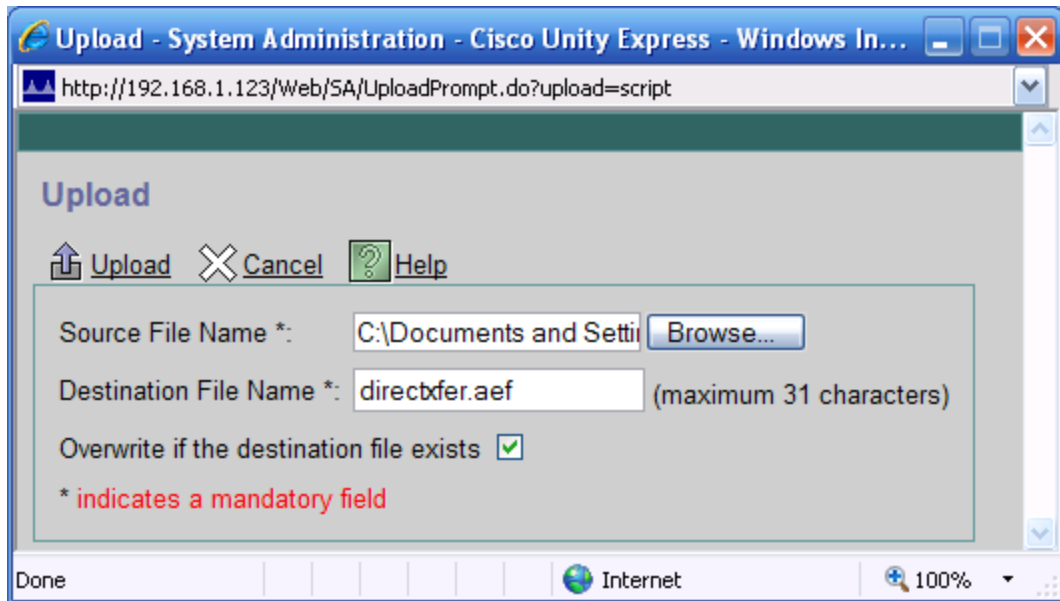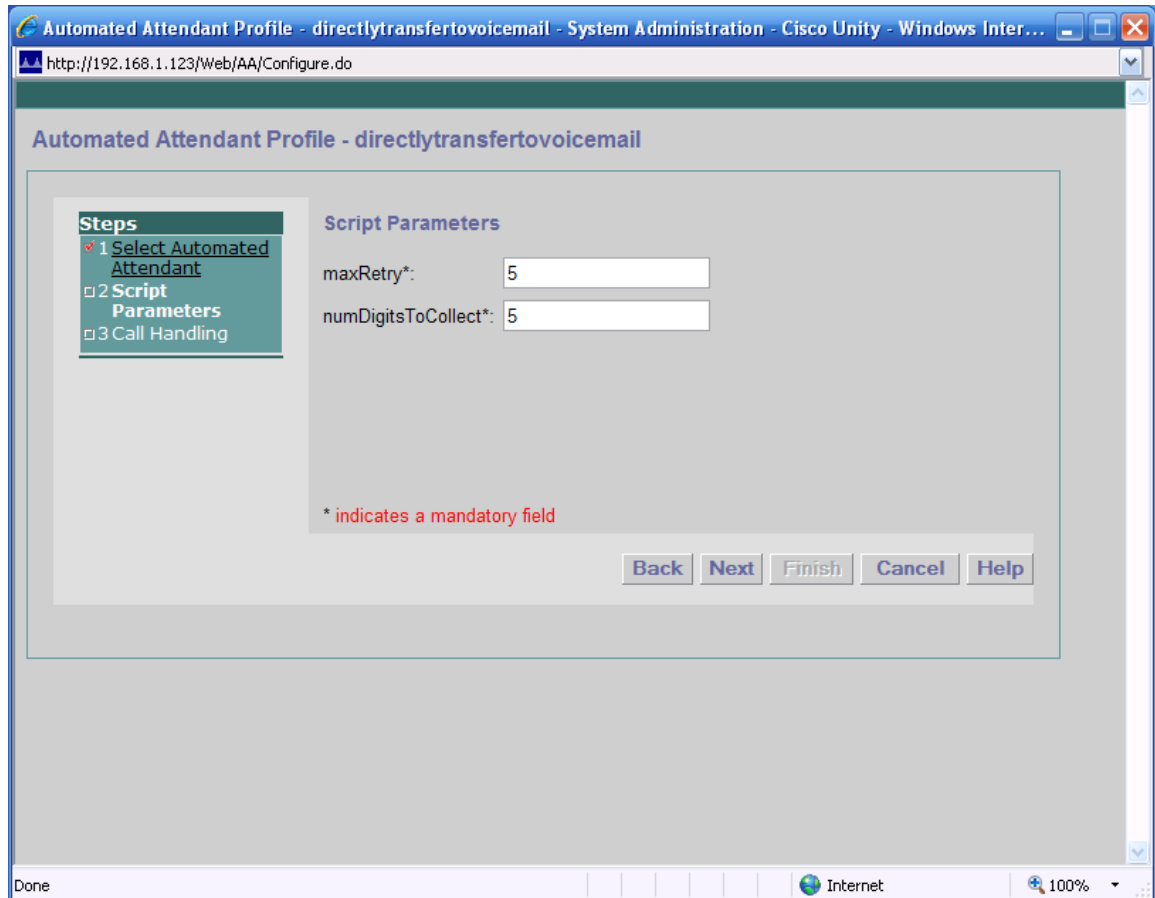
Set the number of digits in the extension. Note CUE will timeout and drop the call after the max re-tries.

Note: Call-in number must be the same as the directory number (DN) on the route point in this case, 6000

Example of Dial-Peer for VM Transfer

```
dial-peer voice 10 voip
 destination-pattern 6...
 session protocol sipv2
 session target ipv4:192.168.1.123
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
```

Setup Hunt Group for DISA calls:

Setup a hunt group to provide a pilot number for the Dial-In Access calls. perform the following steps.

Hunt Group Configuration

Directory numbers to be included in a hunt group must be already configured in Cisco Unified CME.

Summary Steps

enable
configure terminal
ephone-hunt *hunt-tag* {longest-idle | peer | sequential}
pilot *number* [secondary *number*]
list *number*[, *number*...]
exit
end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ephone-hunt *hunt-tag* {longest-idle | peer | sequential} Example: Router(config)# ephone-hunt 23 sequential	Enters ephone-hunt configuration mode to define an ephone hunt group. • *hunt-tag*—Unique sequence number that identifies this hunt group during configuration tasks. Range: 1 to 100. • **sequential**—Ephone-dns ring in the left-to-right order in which they are listed when the hunt group is defined.
Step 4	pilot *number* [secondary *number*] Example: Router(config-ephone-hunt)# pilot 4085551212	Defines the pilot number, which is the number that callers dial to reach the hunt group. • *number*—E.164 number up to 27 characters. This is the number user's will dial to access the DISA services.
Step 5	list *number*[, *number*...] Example: Router(config-ephone-hunt)# list 5001, 5002, 5017, 5028	Defines the list of numbers (from 2 and 20) to which the ephone hunt group redirects the incoming calls. • *number*—E.164 number up to 27 characters. Number assigned to the primary ephone-dn (number of the first button) on each of the mobility-ephones setup for the Dial-In Access service.
Step 26	end Example: Router(config-ephone-dn)# end	Returns to privileged EXEC mode.

Verifying Hunt Groups

Use the **show running-config** command to verify your configuration. Ephone hunt group parameters are listed in the ephone-hunt portion of the output.

Router# show running-config
!
ephone-hunt 2 sequential
 pilot 4085551212
 list 621, *, 623
!

Use the **show ephone-hunt** command for detailed information about hunt groups, including dial-peer tag numbers, hunt-group agent status, and on-hook time stamps. This command also displays the dial-peer tag numbers of all ephone-dns that have joined dynamically and are members of the group at the time that the command is run.
Router# show ephone-hunt

Group 2
type: sequential
pilot number: 4085551212, peer-tag 20098
list of numbers:
123, aux-number A601A0200, # peers 1, logout 0, down 0
peer-tag dn-tag rna login/logout up/down
[20097 56 0 login up]
622, aux-number A601A0201, # peers 3, logout 0, down 0
peer-tag dn-tag rna login/logout up/down
[20101 112 0 login up]
[20100 111 0 login up]
[20099 110 0 login up]
623, aux-number A601A0202, # peers 3, logout 0, down 0
peer-tag dn-tag rna login/logout up/down
[20104 122 0 login up]
[20103 121 0 login up]
[20102 120 0 login up]
*, aux-number A601A0203, # peers 1, logout 0, down 1
peer-tag dn-tag rna login/logout up/down
[20105 0 0 - down]
*, aux-number A601A0204, # peers 1, logout 0, down 1
peer-tag dn-tag rna login/logout up/down
[20106 0 0 - down]

CHAPTER

5

Configuring UCC Servers

This chapter describes how to configure and setup the Unified CallConnector Server applications and covers the following areas.

OVERVIEW

Configuration Overview -	Provides an overview and the steps for configuring the Unified CallConnector Server components.
Pre-requisites	Describes the information you need to have on hand or have setup for use during the configuration of Unified CallConnector Server.

SERVER WIZARD

Server Setup Wizard -	Provides an overview and describes how to start and exit the Unified CallConnector Server Setup Wizard.
Wizard Features -	Describes the UCC Server administrations functions supported by the Server Wizard

SERVER APPLICATIONS

Setting up SIP Parameters -	Describes the SIP Server configuration parameters and the default values.
Database Server Setup -	Describes the Database Server configuration parameters and the default values.
Presence Server Setup -	Describes the Presence Server and RADIUS server configuration parameters.

INTER-WORKING WITH CME

Setting up CallController -	Describes how to setup the CallController server.
Setting up Location -	Allows the administrator to specify the area code, number pattern, extension length etc to allow dialing.
Downloading ephones -	Starts a Telnet session to download the CME ephone and ephone-DN configuration.
Select and Verify ephones -	Specify the ephones that are to be used by the UCC users.

GROUPS AND USERS

Create a List of Group-	Describes how to enter the department or groups for viewing in the Status window.
Adding Users -	Describes how to add, modify and delete the user account information for the Unified CallConnector users.
Configuring User's Phones -	Describes how to associate an ephone with a user.

VERIFYING CONFIGURATION

Verifying Configuration -	Describes some of the steps to verify the UCC Server configuration.

MANAGEMENT FUNCTIONS

Sending Notifications -	Describes how to send out an email notification to the UCC users and the different attachment options.
Reporting Problems -	Describes how to report any problems that you may be experiencing with the Unified CallConnector Server.

Server Configuration Overview

The Unified CallConnector Server is comprised of server applications that run as services on a Windows computer system. Together these server applications provide call control, data access and presence services to the Unified CallConnector clients. In addition to the server applications, the Unified CallConnector Server maintains the user configuration data and the contact and transactional data using a database system.

The UCC Server applications connect to the Cisco Unified CME router to control calls and obtain telephone status information. The Unified CallConnector clients connect to these UCC Server applications to access to the solution features.

The UCC Server Wizard provides the user interface to configure the server applications.

The configuration of the Unified CallConnector Server software requires prior setup of the Windows platform and the Cisco Unified CME. The pre-requisites for the configuration are discussed in the next section.
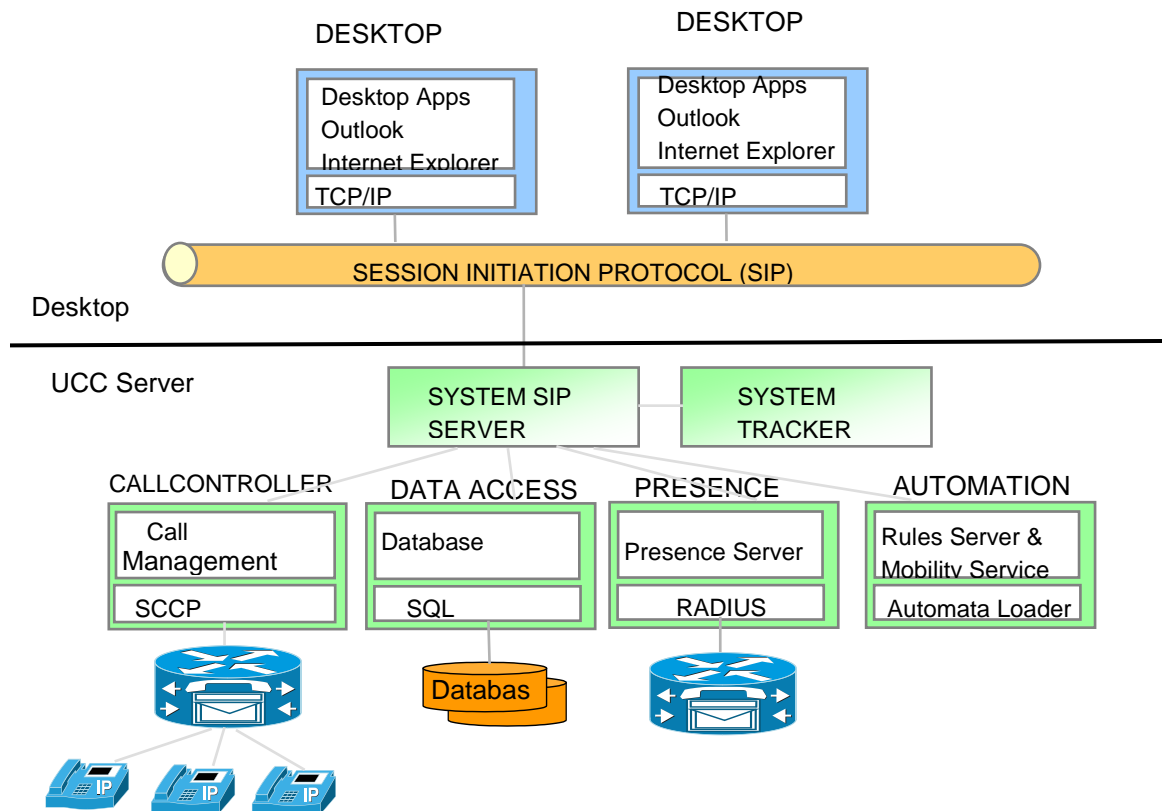
Cisco Unified CallConnector System Diagram

UCC Server Configuration Steps

The following summarize the steps for configuring the Cisco Unified CallConnector Server:

Step 1: Registering the UCC Server License
- The UCC Server applications require the purchased licenses to be registered with the Cisco site.
- The licenses can be registered/activated during the installation process or from the Server Wizard.

Step 2: Setting up Server Application Communication Parameters
- Verify the default settings or enter the IP address and ports for the communication protocols used by the server applications to connect to the UCC clients and to the Cisco CME.
- Verify the default settings or select the option parameters (for example-- Database Purge Duration whose default value is 30 days).

Step 3: Provisioning the UCC Servers to work with Cisco CME
- Specifying the Cisco CME IP Address, Telnet account, location, area code, number pattern and extension lengths.
- Setting up additional dialing rules for patterns not handled by the default dialing rules.
- Downloading the list of ephones and ephone-DNs that have been configured on the Cisco CME
- Selecting the ephones to be controlled by the UCC Server and by the UCC users.

Step 4: Setting up the Groups, User Accounts and User' ephones.
- The UCC users all belong to a department or group. These departments or groups names need to be defined and access rights need to be setup.
- Creating User account with login IDs and contact information. Assigning the users to their groups/departments.
- Associating ephones with the users. Each user account has to be associated with an ephone to allow that ephone to be controlled from the user's UCC client application.

Step 5: Verify the UCC Server configuration.
- Verify that the configuration parameters are correct and the server applications are functioning.

The table below summarizes these steps.

UCC Server	What needs to be setup
Configure the UCC Server communication parameters.	The UCC Server is comprised of a number of communication applications. Each of these requires settings for the IP Address and port on the Server PC to use. Generally you can use the defaults, unless there is a conflict or there are multiple network adapters
Select database backup options.	Select the number of days that the call logs should be maintained in the system. You should also backup the data when the configuration is completed.
Configure the Radius port and password.	Enter the Radius port and the authentication password to match the configuration on the CME. You can also open a utility to view and verify receipt of Radius messages.
Configure CME location, features and dialing rules	For each CME associated with the UCC server, the location, extension lengths and dial-out access codes need to be configured to allow proper formatting of numbers for dialing. Additional dialing rules can be configured to manipulate the numbers for dialing and lookup if required for the location.
Download the ephone configuration from CME	Download the ephone configuration from CME using a Telnet session. This requires the Telnet username and passwords. Then select the ephones that are to be controlled by the UCC Server. Verify that the ephones can be connected from the Server.
Add/Modify the Group Names	The UCC users belong to a group or department for viewing in the Status window. The group names have to be defined first. Setup the publishing rights and restrictions for the groups.
Configure the users with their contact details.	Enter the user login name, password, and contact numbers. Select the group for the user. Specify the user type. Note: Users will use this login name and password to connect to the UCC Server. (Not the ephone User Name)
Associate the user with their ephone.	Select and assign an ephone to the user. When the users login they will be able to manage calls from this ephone only.

Pre-Requisites for Server Configuration

As a part of the installation of the Unified CallConnector Server, you need to have certain network connectivity and configuration information. These are summarized in the table below and described in the following paragraphs.

Item	Description	Source
UCC Server PAK-ID	Obtain the PAK-ID or use 'trail' for a limited time evaluation period	Sys Admin
Server PC Information	This includes: Server PC IP Address Administrative account (Name & Password)	Sys Admin
TCP and UDP Ports	Verify that the required TCP/UDP ports are available on the server.	Sys-Admin
Cisco Unified CME Configuration	Configure the ephones and RADIUS parameters on the router. Including: Radius Password and Port CME IP Address CME Telnet Account CME Location, Area Code, Number Pattern Extension Length, PSTN Access Prefix All the UCC user's ephones need to have the ephone user name and password provisioned in the CME.	Service Provider or Sys-Admin
Department/Groups	The names of the departments or groups at the customer organization.	Sys-Admin
User account and contact information	Obtain the user's contact and account information for creating the user accounts, including: User Names Login Name and Password Group they belong to. User Contact Numbers Ephones assigned to User	Sys-Admin

Table 3.1 Pre-requisite information for installing the Unified CallConnector Server

Server Wizard Features

The Unified CallConnector Server Setup Wizard is an application that runs on the Unified CallConnector Server computer and provides the graphical interface to setup the configuration information for the Server applications and save then in the proper repositories.

The entire UCC Server configuration is setup from the Server Wizard. The administrative functions available are listed in the table below:

Wizard Features	Description
License Registration	Allows you to view the current licensing status and register the PAK-ID with the UCC License Server to allow the UCC Server applications to run beyond the evaluation period.
Server Communication Parameters	Enter the IP Address and port for the UCC Server applications
CME Access Parameters	This sets up the area code for the location, the number patterns and CME extensions and PSTN access codes.
Server Dialing Plan Parameters	When the default dialing plan that ships with the UCC Server needs extensions, this allows dialing rules to be set up to handle these exceptions. (Note: UCC Client dial plan also needs to be setup for each user)
Select and Verify ephones for UCC Server	Download and select the ephones to be used by the UCC Server and UCC users
Setup Groups	Define the Departments or groups in the organization.
Setup user account and contact information	Enter the user's login account and contact information.
Configure the IP Phone for user	Specify the IP Phone for the user. This is the IP phone that can be controlled from the UCC client.

Additional management services available from the Wizard:

Wizard Features	Description
Send Email Notifications	Email configuration information and notifications to the UCC users.
Push Configuration Info to Users	Use the Email methods to attach and send the configuration information to the users
Report Problems	Report problems via email to the UCC team and include select the desired trace log files.

Additional configurations for the Mobility Service:

Wizard Features	Description
Communication Parameters for Mobility (Automation) Server	Enter the IP Address and port for the UCC Server applications
Setup Mobility Service Options	Set the operating parameters for: Single Number Reach (SNR) service Dial-In Access (DISA) to CME Features Caller-ID transmission
Configure ephone pools	Assign the mobility ephones to the SNR or DISA applications
Setup Holiday Schedules	Enter the holidays including the names and dates, work days and working times
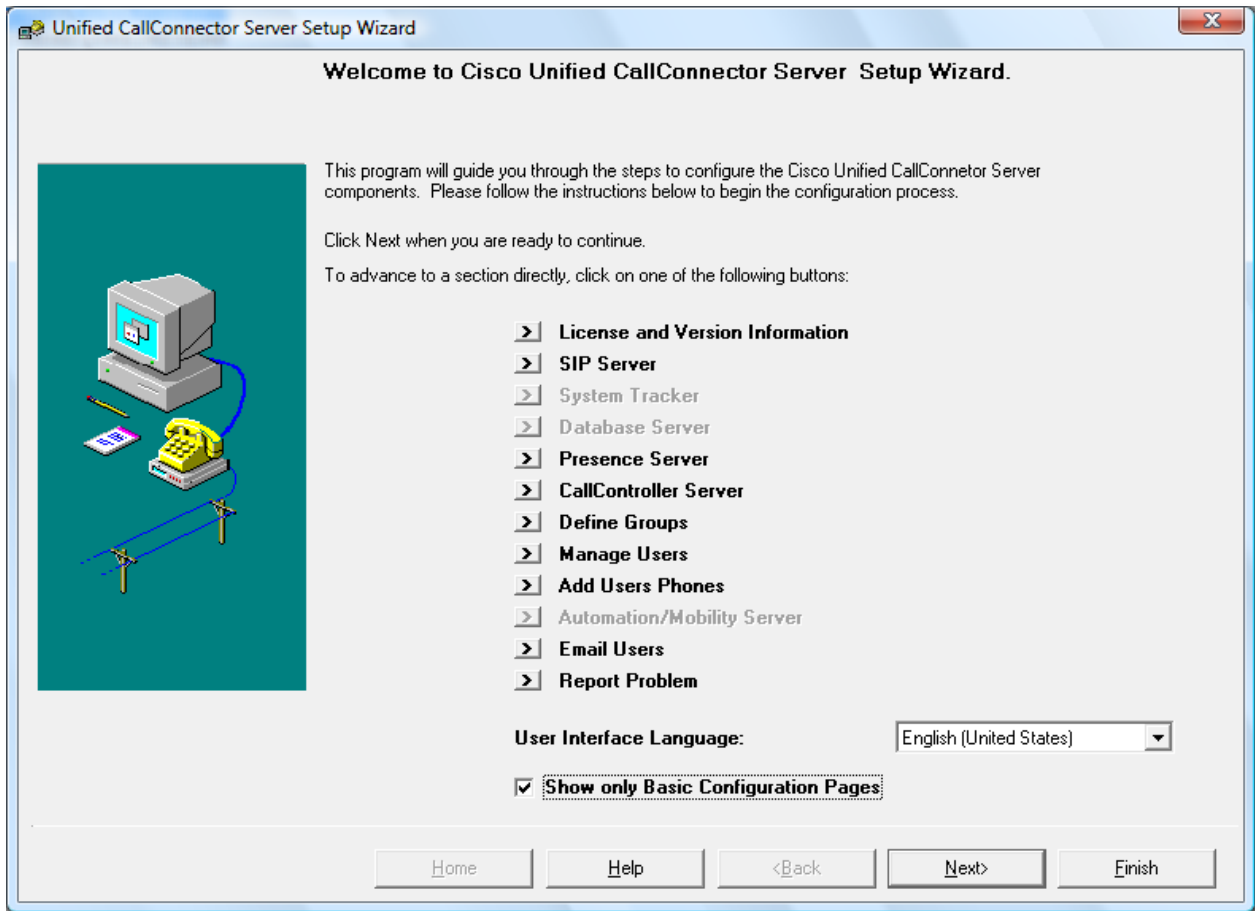
Starting Server Wizard

The Unified CallConnector can be started from:

Start Menu->Programs->Cisco Systems
->Cisco Unified CallConnector Server-> Cisco Unified CallConnector Server Wizard.

The following welcome window displays on startup.

You can jump directly to a section by clicking on the button to the right or click on the Next button to navigate through all the windows. Information in some of the windows is written when you move to the next window. In other cases, the information is written only when you click on the Finish button.

Notes: YOU NEED TO RESTART THE UCC SERVER APPLICATIONS TO APPLY THE WIZARD CONFIGURATION CHANGES.

User Interface Language: The UCC Server Wizard supports multiple languages. To switch to a different language, select the language from the pull-down list.

Note – Help pages are provided in English only.

Supported languages shipped with this version include:

English, French

Beta translations for the following languages are also included:

German, Italian, Dutch, Danish, Norwegian, Finnish, Swedish,
 Spanish (Traditional), Spanish (Latin American)

Please download the latest available language files from the Unified CallConnector Wiki site.

Show Basic Configuration Pages: By default, some of the optional server configuration pages are not displayed. Uncheck this option to view all UCC Server Wizard pages. The following additional pages are now displayed:
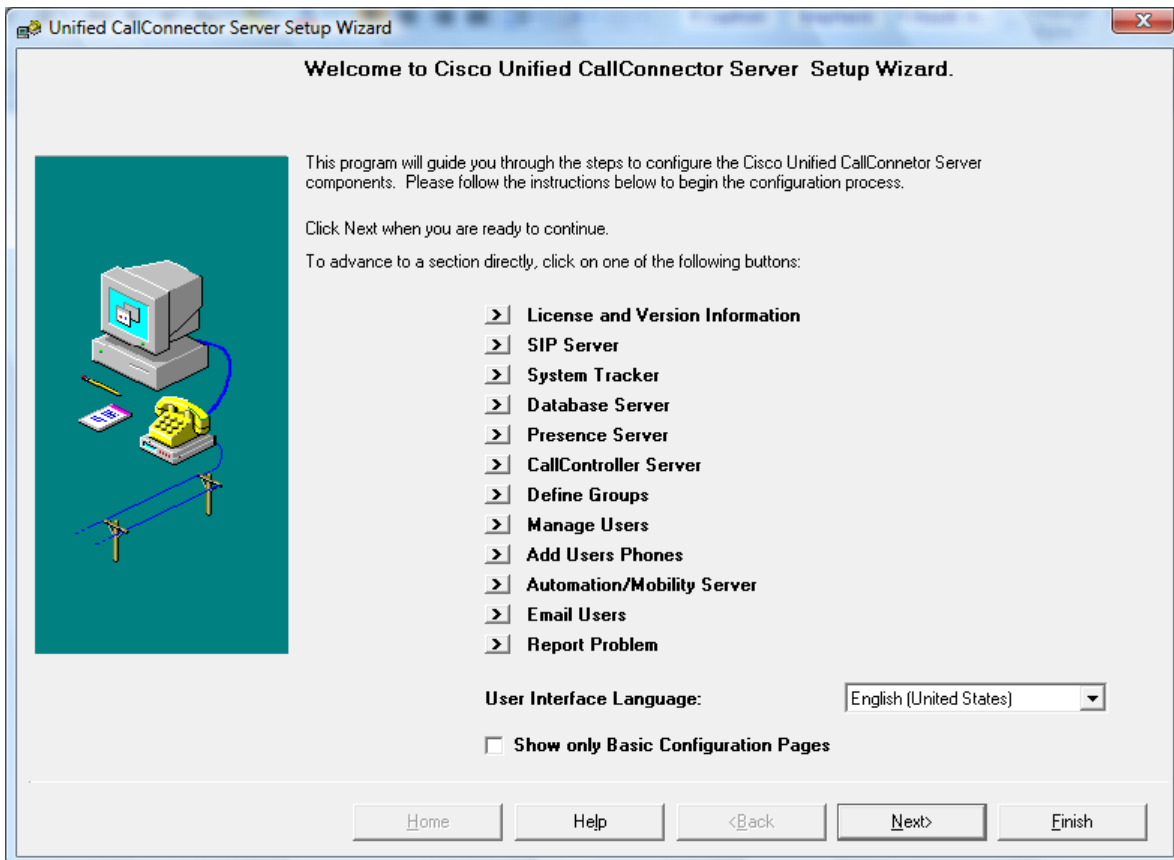
> **Note:** The Mobility Server configuration pages are enabled if the Mobility Service has been licensed or is in Trial mode and "Show only Basic Configuration Pages" is unchecked.

Version Information

The Version Information window displays the file version form each of the Server applications. It also displays the overall Unified CallConnector Server build date and version at the top right of the window. (Uncheck 'Show basic Configuration Pages' to view this page).

Notes

You may be asked to provide this Unified CallConnector Server Build and Version information when reporting any problems.

Exiting Server Wizard

Click on the Finish button to exit the Server Wizard. The Wizard will save the data in the configuration files, registries and the database and then close. You will need to restart the Server applications to apply any of the changes.
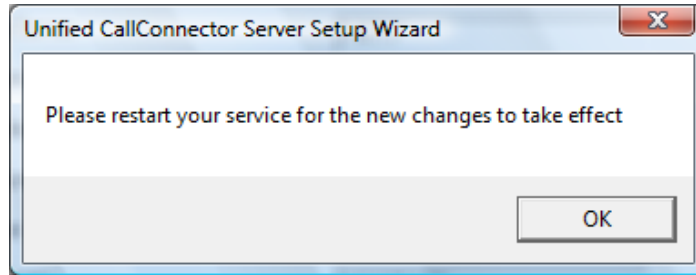
Obtaining Help

Click on the Help button to open the Server Wizard help document. This help document provides access to the Unified CallConnector Server configuration steps and descriptions of the configuration parameters in a Windows Help format. You can search and browse through the help information using the hyper-linked table of contents.

The UCC Server Wizard Help contains all the information that is in this Administrator's Guide.
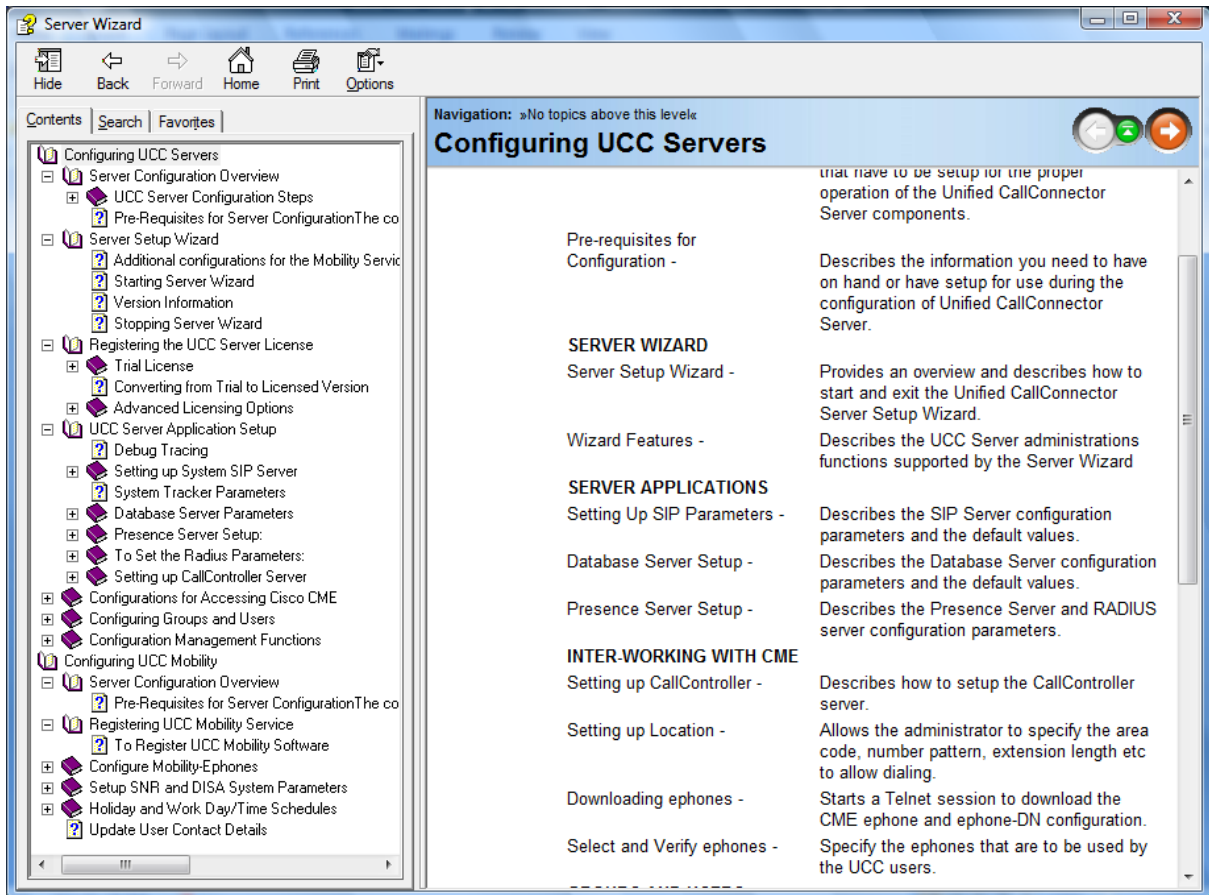
Registering the UCC Server License

The Unified CallConnector Server applications need a registered license to run. During the installation process you can select from one of two options:

> Evaluate the UCC Server and Mobility for a limited time period.

> Use PAK-ID or Serial Number for automatic licensing

If you have selected the evaluation option then the installation process will have automatically obtained a trial license from the UCC License Server.

Trial License

This license is valid for 45 days. It requires access to the Internet and is verified daily. For the duration of the trial period, this license is verified every day by connecting with the UCC License Server over the Internet. When the Server Wizard is run during this evaluation period, it will display the number of evaluation days that are remaining. You can convert from Trial to full license using the Server Wizard.

Product Authorization Key (On-Line Activation)

As a part of your purchase documentation you will receive a Product Authorization Key or PAK-ID. This PAK-ID needs to be registered or activated with the Cisco UCC Licensing Server to receive a 'Serial Number License'. The Serial Number is saved in the Windows Registry. When the PAK-ID has been registered the UCC Server operates in the fully-licensed mode.

Advanced License Options (E-Mailed License File)

The UCC Server also supports an-off-line, email delivered license file for customer situations that do not have access to the Internet or when there is an issue encountered by the automated registration method. This license file is generated on-line by Cisco Systems and is keyed to physical information for that specific computer. To generate the license file, you can use the Advanced License Options to log on to the Cisco System License site and enter the PAK ID, select the UCC Server or UCC Mobility software that you want to license and provide the physical computer information (the UCC Machine ID and CPU ID). The License file will be emailed to you

Converting from Trial to Licensed Version

The evaluation version of the Unified CallConnector Server can be converted to a licensed version by entering a valid Product Authorization Key (or a Server Serial Number).

The server license is registered and activated in a two-step process

- Open the Server Setup Wizard to the License Information page.
- Highlight the Unified CallConnector (UCC) Server in the License Information window.
- Enter the PAK-ID (or Serial Number) in the field below. PAK-Ids have the format 30xxxxxxxxx, Serial Numbers have the format UCxx-0100-xxxxxxxxxx.
- Enter the User's or Installer's Email address – this is a mandatory field and click on the Activate button.
- The Server Wizard will register the PAK-ID with the Unified CallConnector License server. The registration is a two-step process, the license is immediately placed in a "Pending Authorization" state. The UCC Server checks every day with the License Server until this is authorized. At this point the license status changes to "Fully Licensed".
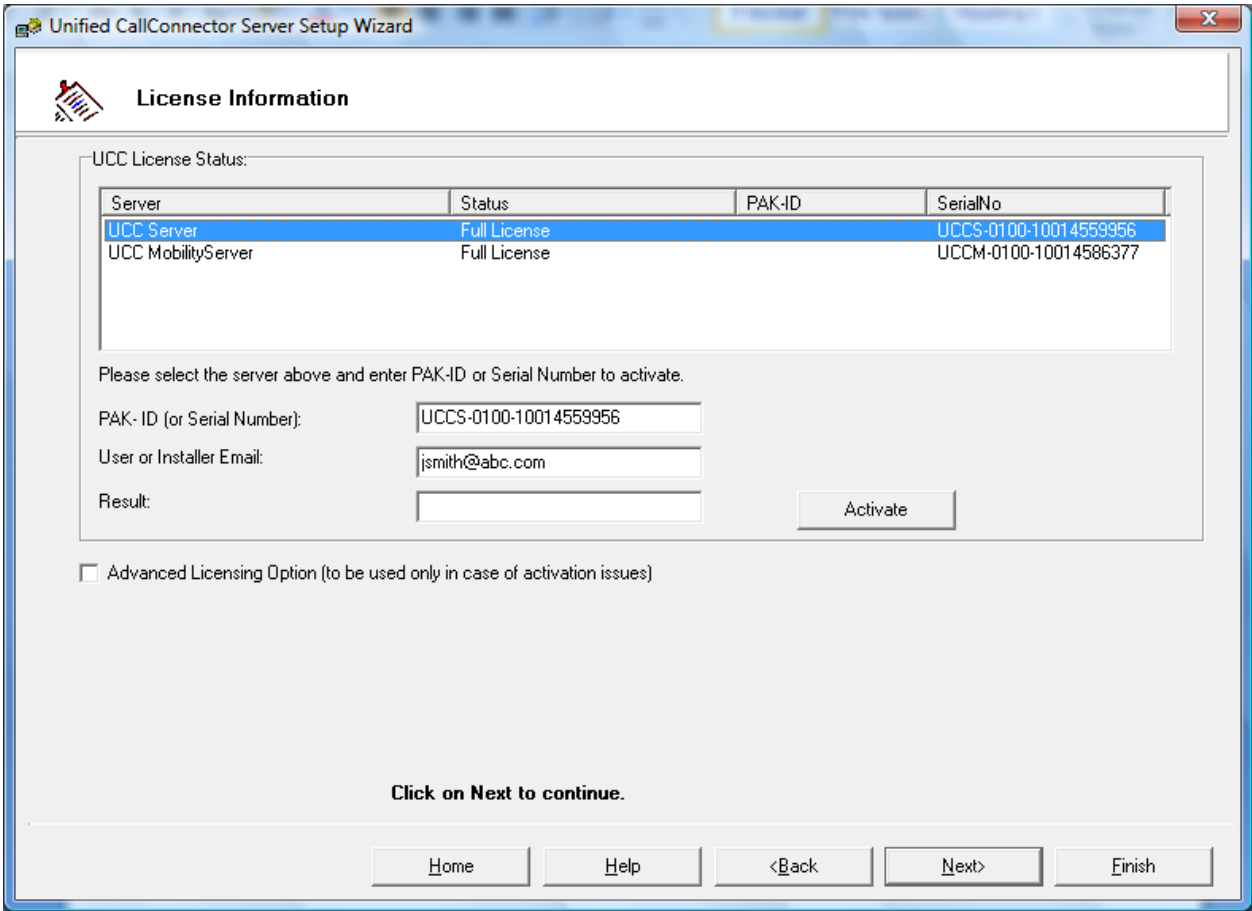
Mobility Server License

The Mobility Server is separately licensed. If you have purchased both the Server and Mobility solutions then the same PAK-ID can be used to register the Mobility Server license.

- To register the Mobility Server, select the UCC Mobility Server and repeat the steps for activating the license.

Advanced Licensing Options

The Unified CallConnector Server supports an alternate licensing method. This method also requires registration with the Cisco License site; however a license file is email as a part of the process. This licensing method can be used for situation where there is no Internet access.

The Cisco Unified CallConnector requires a license file for each personal computer on which it is run. This license file is generated on-line by Cisco Systems and is keyed to physical information for that specific computer. As a part of your purchase, you will receive a PAK ID (Product Authorization Key). The PAK ID identifies the quantities of Unified CallConnector software that you have purchased. To generate the license file, you will need to log on to the Cisco System License site and enter this PAK ID, select the software that you want to license and provide the physical computer information (the UCC Machine ID and CPU ID). The License file will be emailed to you
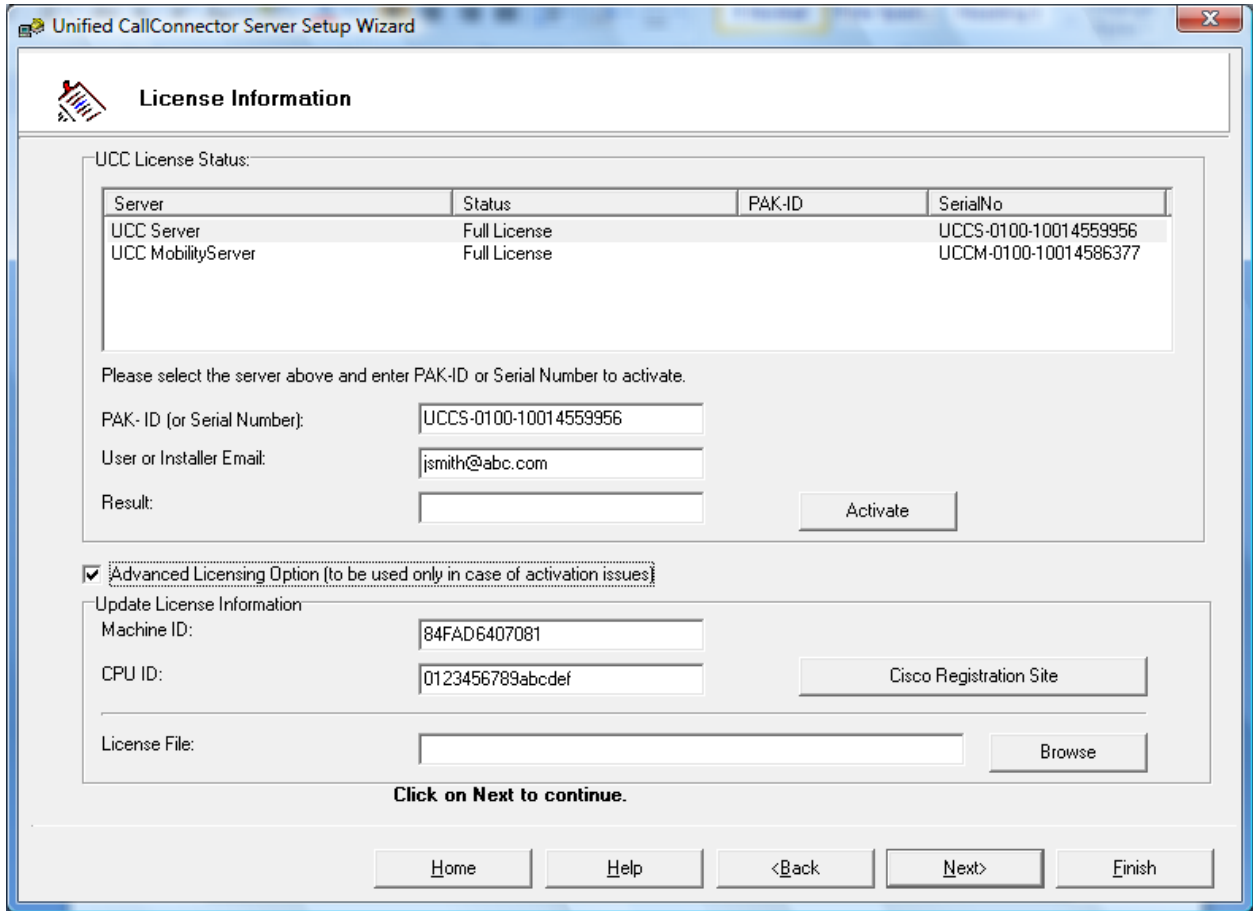
To use the Advanced Licensing Option

- Click on the Advanced Licensing Options check box to enable that section of the Server Wizard window.

- Click on the Cisco Registration Site button to open the browser to www.cisco.com/go/license.

- Login using your CCO account. A valid account is required to access the License Server site.

- Enter the PAK-ID in the Product Authorization Key field and press enter or click on Submit.

- You will see a list of purchased UCC components. Select the UCC Server and UCC Mobility options. (Note – Select quantity ONE only of server and/or mobility. Do not select any UCC Client quantities).

- Enter the Machine ID and CPU ID from the Server Wizard page to the Cisco license web page.

- Enter the email address where you would like to receive the license file.

- The license file will be emailed. Download it to the server PC and use the browse button to select the file.

UCC Server Application Setup

The Unified CallConnector Server is comprised of multiple server applications that run as services on the Windows Server PC.

These server applications communicate with endpoints that are on the network using a number of protocols including TCP, UDP, HTTP, and Telnet. This requires specification of the IP Address and ports of the Server PC that are to be used by the UCC Server applications.

Since the Server PC may have more than one network adapter card connected to different networks, administrators need to select which network card (by specifying the card IP address) should be used by a UCC Server application and the ports on that network card that are available for use.

All the Server application need to be accessible from the UCC client applications from the user's PCs.

The CallController Server can support two separate sets of connections – SIP/TCP & UDP connections to the UCC clients and SCCP/TCP (and RTP/UDP) connections to the Cisco CMEs. If required, these sets of connections can be on different network adapters. By default the CallController Server network adapter card used to connect to the Cisco CME is the same as the network adapter used for the CallController SIP connection.

The Presence Server can support two separate sets of connections – SIP/TCP & UDP connections to the UCC clients and RADIUS/UDP connections to the Cisco CMEs. These sets of connections can be on different network adapters. By default the Radius Server network adapter card used to connect to the Cisco CME is the same as the network adapter used for the Presence Server SIP connection. This can be changed from the Server Administration Wizard.

Notes

1. The Unified CallConnector client/server communication does NOT support traversal across routers using the NAT mechanism. Any router between the UCC client and server PCs must be SIP aware and able to transport SIP messages.
2. Each of the Unified CallConnector Server applications need to be setup and configured to allow them to:

   - Communicate using SIP messages.
   - Accessing the functions for which they are providing services.
   - Enable the debug trace capability and debug file as needed.
   - Setup the Windows environment for these applications to run as services

The configuration information is saved in Windows registry files associated with the server applications as well in files and databases.

Debug Tracing

Each of the server application supports writing trace and debug information to a log file. This trace function can be enabled from the Server Wizard. There are six trace levels defined. For each level, all the trace messages for that level and below are written to the log files.

Critical:	Fatal error – the application will terminate.
Error:	Defect in a feature or function. This does not affect the operation of the application.
Warning:	Generally indicating resources are being depleted.
Information:	Information messages for significant events in the operation of the application.
Debug:	Summary level trace messages to assist in debugging the application.
Trace:	Verbose level trace messages for debugging the application.

The debug messages are written to individual files for each server application. Information is written to the trace file until the maximum size setting for the trace files is exceeded. The current trace file is renamed to .bak and a new trace file is created. If a backup file exists, it is deleted.

Trace Log Folder

The Trace Log folder is a sub-folder of the Cisco Unified CallConnector Server. All the debug log files are saved in this folder.

- To view the current debug information, open the desired server file with the .log extension. When the log file reaches it maximum size, it is renamed with the.bak extension and a new .log file is started.

-

- Internet downloadable applications UltraEdit, BareTail and Bare-Grep can be used to view the debug information.

Setting up System SIP Server

The System SIP Server (ccSSS) provides UCC client and server applications authentication (Registrar function) and routing of the SIP messages (Re-Direct Server function). All UCC clients and servers first login to the System SIP Server at startup. This is the central component that authenticates users and server applications and routes the SIP messages.

Parameters for the System SIP Server and the System Tracker need to be setup to allow the Unified CallConnector server applications and clients to run properly.

A failure of the System SIP Server will affect UCC system in the following ways:

- All UCC clients and Server applications starting up will fail and provide 'unable to connect with SIP Server error message.
- Existing connections will continue to be in place until the subscriptions or registrations timeout and need to be renewed. These attempts will fail.
- The CTI Manager should indicate System SIP Server is stopped.
- All UCC Server applications should be restarted upon SIP Server failure.

System SIP Server Parameters

- Click on the SIP Server button in the welcome page or click Next to get to the System SIP Server Parameters page.

- SIP Domain: Select the IP address of the network adapter card on the computer on which the Unified CallConnector Server software has been installed. The SIP Domain can also be a network address if that domain name has been registered with the local Domain Name Server (DNS). Note: All the Unified CallConnector Server Applications need to communicate with the System SIP Server and connect to this SIP Server IP Address.

- Port: This is the port on which the Unified CallConnector System SIP server will receive messages. The default port for the System SIP Server is 5060. This port is used to receive UDP messages. The System SIP Server also uses a fixed port 39984 (TCP and UDP) to connect to the Database Server for authentication services. The current availability of the port is indicated beside the Verify Port button. Click on the Verify Port button to verify that the port is available.

- Enable Trace Logging: If asked by Cisco Technical Support, enable the debug trace logging and set the Trace level to the requested level. This option is checked at the server application startup, to determine if debug logging is enabled. By default the trace files are saved in the Trace Log folder under the Unified CallConnector Server. To apply this Trace Log setting to all the Server applications, enable the option 'Apply debug trace log setting to all servers'.

- Trace File: The default path and trace file name is displayed.

- Apply debug trace log settings to all servers: Check this option to apply the SIP Server trace logging settings to all the UCC Server applications. This avoids the need to set the debug level for each of the servers individually.

- Apply password to all servers: Check this option and enter a password to apply to all the UCC Server applications. This avoids the need to set the password for each of the servers individually.

Notes

1. The SIP Domain IP address should be used as the SIP Server address for all the UCC Server applications.
2. This SIP Domain IP Address is also used by the UCC clients to connect to the UCC Server.
3. The port 5060 is the standard SIP server port. Please ensure that this port is available for the UCC System SIP Server.
4. The 'Apply debug trace log settings to all servers' and 'Apply password to all servers' is a convenient way to set these parameters once and have them apply to all to the UCC Server applications.

Click on Next to continue.

System Tracker Parameters

The System Tracker supports the automated recovery of the connections in the event of failures. (Uncheck 'Show basic Configuration Pages' to view this page).

It provides the following services to the UCC system:

- The SystemTracker (ccSystemTracker) supports the automated failure recovery capability of the Unified CallConnector components.
- It monitors the status of the Unified CallConnector Server applications by polling them individually.
- Each Unified CallConnector client connects to the System Tracker to receive UCC Server status notification.
- If a UCC Server application stop or get disconnected then the System Tracker determines this information from its polling and notifies the client of this state change – Connected and Disconnected, Ready or Not Ready.
- Clients use this notification to enable or disable the services they make available to the user.
-

A failure of the System Tracker applications will affect UCC system in the following ways:

- UCC clients starting up will not be able to receive the UCC Server status to allow them to continue.
- The UCC client user interfaces will be grayed out; as the clients will assume that all the Server applications are down
- Established sessions (clients) will not know; will not get UCC Server failure notifications.
- Subscription timeouts causing re-subscribe will fail.
- When the System Tracker returns; all subscriptions will need to be re-established
- To recover stop and restart System Tracker.

If you have selected the Trace Log and Password options to apply to all the UCC Server applications and wish to take the default settings for the System Tracker, then click on Next and continue otherwise you can use this window to change the System Tracker parameter settings.
.

- SIP Server Address: This is the IP address of the computer with the System SIP Server as provisioned for the System SIP Server in the previous page.
- Port: This is the port used by the System Tracker to receive messages. The default value is 5071. This port is used for both TCP and UDP connections. If this port is not available, then change this to a port available on the computer.
- Username: This is the well-known name of the System Tracker. This cannot be changed.
- Password: This password is used to authenticate the registration of the System Tracker. Enter the password. This can be any text or number string up to twelve characters in length.
- If asked by Cisco Technical Support, enable the debug trace logging and set the Trace level to the requested level. This option is checked at the server application startup, to determine if debug logs are to be written.

Click on Next to continue.

Database Server Parameters

The Unified CallConnector Database Server provides access to the configuration, contact and transactional data to all the Unified CallConnector servers and clients. (Uncheck 'Show basic Configuration Pages' to view this page).

The Database Server provides gateway functions between SIP messages and the SQL database command. SIP User Agents such as UCC clients' access configuration, contact and transaction data from standard SQL databases by sending SIP messages to the Database Server. The Database Server supports the SIP Message methods. When it receives a database request, it fulfills the request from the attached SQL database and returns the data/response to the requestor.

Database Server supports synchronization feature; allowing add/delete/updates to be kept current

If the Database Server fails, then

- User cannot log-in– cannot be authenticated.
- Call Logs lost for the down-time.
- Existing clients continue to work but loose QuickSearch (non-Outlook) functions.
- If Database Tables corrupted; then database has to be restored from customer backup of UCC Server.

There are two aspects to the configuration – setting up the communication parameters to handle the SIP messages and setting up the access to the database system.

Notes

1. The Database Server uses Microsoft ADO objects to connect to the Access compatible database files stored in the Data folder under Unified CallConnector Server.
2. Windows Data Source tools in the Control Panel Administrative Tools-> ODBC Drivers provides interface to administer and verify settings. Normally the Server Wizard will automatically install and configure the ODBC drivers.
3. The Database Server connects to three databases – Configuration database that contains the provisioning information, Corporate database that contains the corporate directory data and the Logs database that stores the transaction data for example call logs.
4. The databases should be regularly backed up and in the event of corruption or other problems that latest configurations can be restored from the backups.

If you have selected the Trace Log and Password options to apply to all the UCC Server applications and wish to take the default settings for the Database Server, then click on Next to continue to the next window.

SIP Communication Parameters

- SIP Server Address: This is the IP address or network address of the computer with the System SIP Server. If the Unified CallConnector Server components are all installed on one computer, then this address will be the IP address of this machine.
- Port: This is the port used by the Database Server to receive messages. The default value is 5061 and is used for both TCP and UDP connections. If this port is not available, then change this to a port available on the computer.
- Username: This is the well-known name of the Database Server. This cannot be changed.
- Password: This password is used to authenticate the registration of the Database Server. Enter the password. This can be any text or number string up to twelve characters in length.
- If asked by Cisco Technical Support, enable the debug trace logging and set the Trace level to the requested level. By default the trace files are saved in the Trace Log folder under the Unified CallConnector Server.

Click on Next to continue.

Data Management Parameters

The Unified CallConnector supports three separate databases. These include the Corporate Directory Database, the Transaction Log Database and the Unified CallConnector Configuration Databases.
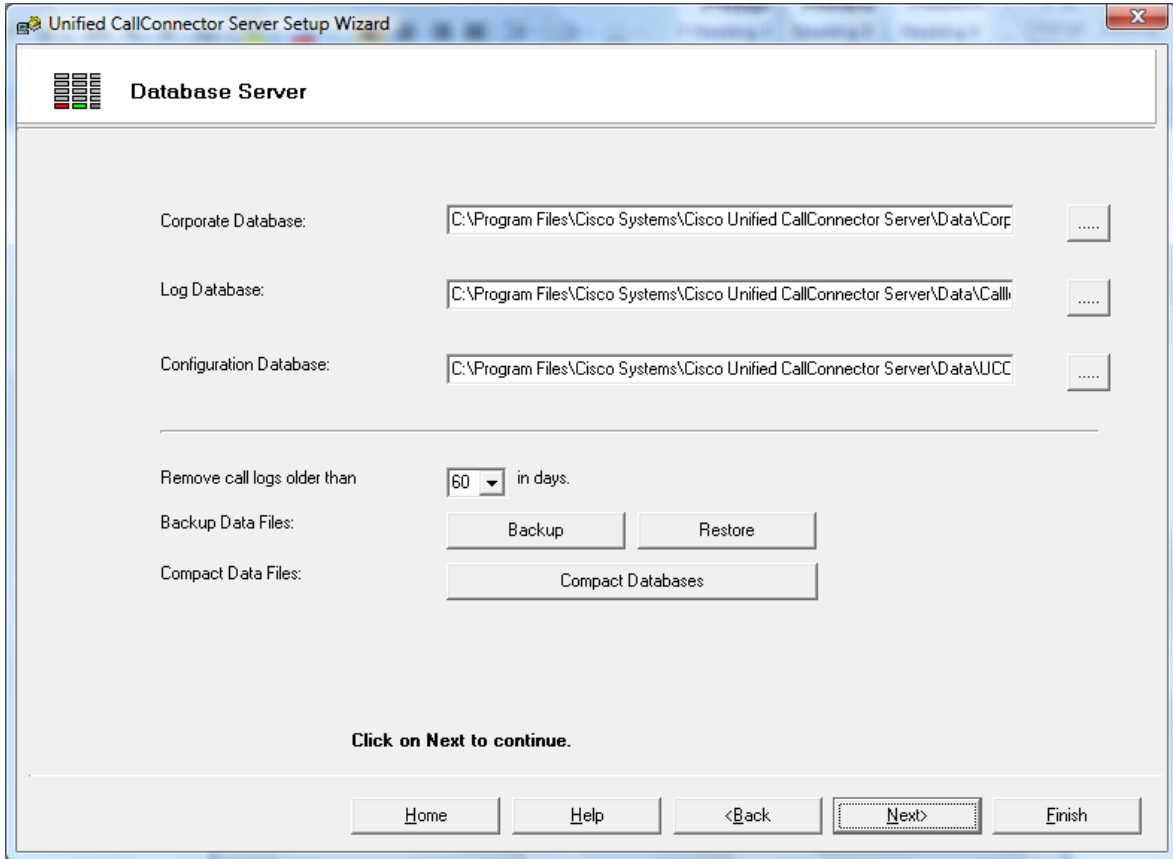
The Server Installation program copies the default database files to the Data folder under the Unified CallConnector Server. This Wizard page allows you to select different files if you have these files saved or backed up in a different folder.

To Select Different Database files

- Click on the Browse button for the database of interest and select the appropriate file.

Notes

The Unified CallConnector must use the databases and tables that have provided by the install program. The database structure, the tables and the fields in the tables cannot be changed. You may backup the database files and from the wizard select these backed-up database files.

Managing the Database files

The following data management options are provided in the Unified CallConnector server:

Removing the Call Log Entries

The call log entries are written to the database for every number for which there is a match with a Unified CallConnector user's contact numbers. Over a period of time a large number of records can be written. Although individual Unified CallConnector users can manually delete their own call log entries, this option allows the administrator to set a policy to automatically delete the call log entries that are older than a certain number of days. Three duration selections are available – 30, 60 or 90 days. To disable this automatic call log entry removal option, select the 0 days option from the pull down list.

Database Backup

The database backup option allows you to save the current database files to a backup folder. You should first stop the Unified CallConnector Server applications. The database files are copied and saved in the DataBackup folder. Any existing database files in the backup folder are overwritten. When you click on the Backup button, you will be prompted to close the server applications.

Database Restore

The database restore option allows you to copy the backed up database files to the current database folder. The Restore operation should only performed if there is a problem with the current data files. You should first stop the Unified CallConnector Server applications. The database files are copied from the DataBackup folder to the Data folder. Any existing database files in the Data folder are overwritten. When you click on the Restore button, you will be prompted to close the server applications.

NOTE: THE DATABASE RESTORE WILL OVERWRITE THE DATABASE FILES AND YOU WILL LOOSE ALL THE DATA THAT CHANGED SINCE THE LAST BACKUP OPERATION.

Compact Database

When entries are deleted in the database, they are marked as deleted but not removed from the database files. The Compact operation removes these deleted records form the database file and recovers disk space. You should first stop the Unified CallConnector Server applications before starting the Compact operation. When you click on the Compact Database button, you will be prompted to close the server applications.

Select the number of days you want to retain the call log entries from the pull down list. Select zero if you do not want to automatically delete log entries.

Click on Next to continue.

Presence Server Setup

The Unified CallConnector Presence Server reads in the user configuration data and the corporate directory information and maintains the user's presence and telephone status information. The Presence Server incorporates a Radius Accounting Server functionality to receive the telephone status updates from the Cisco Unified CME. The user presence information and telephone status is published to all authorized clients in real-time.

Presence Configuration Notes

1. The Presence Server publishes the list of contacts in the Corporate directory database grouped by their departments. It also manages and publishes the presence status (availability and location) and the telephone status of these users in real-time.
2. Contacts in the Corporate directory can be UCC users and non-users. A UCC user has a user login account created via the Server Wizard. Presence status is published for both types of users.
3. For non-UCC users, this provides a bulletin-board type function. The status of such users can be updated by the manager of that user's group or by users with administrative rights.
4. Only the UCC users can update their own status; administrators or managers can change the status of the contacts in the status window.
5. Telephone status is only published if there is a match on the caller or called number with one of the user's work, work-2, home or mobile numbers in the UCC Corporate directory.
6. For the telephone numbers to match, the caller/called number and the numbers in the database must be in the same format – preferably in the canonical format. This requires the server dial plan to be correctly setup.
7. Call logs are only written for the UCC users. The call log entries include the caller/called name if there is a match in the Corporate directory. Names in the user's Outlook contacts are not included in the call logs.
8. Presence Access control can only be applied to the Groups/Departments defined through the Server Wizard. This allows the administrator to control which users can view the availability status of users in other groups.
9. The department field in the Corporate directory can contain department names that are not in the 'Group' list.
10. The status of the users in 'departments' that are not in the Group list, are visible to all the UCC users.

The Presence Server filters out telephone status messages from telephone numbers that are not in the UCC Corporate Directory. Even though you might see the Radius events for a phone number, the telephone status may not display in the Status window. Therefore to receive telephone status events, the following must be properly configured:

1. Router must be configured to send Radius messages to the UCC Server.
2. UCC Server must receive the Radius messages.
3. The telephone numbers (caller or called) must be in the Corporate Directory.
4. The UCC Server Dial plan must be properly setup so that the numbers as provided in the Radius messages can be formatted for lookup. This means that after lookup formatting the incoming number will be identical to the 'canonically' formatted number in the directory.
5. The telephone numbers in the UCC directory is saved in the 'canonical' format e.g. (408) 555-1212. The telephone numbers in the Radius message are not formatted. The

Presence Server uses the UCC Server dialing rules to convert the Radius provided telephone numbers to the canonical format and then searches the Corporate Directory for a match. You will need to verify that the dial plan is correctly configured on the server so that the numbers sent in the Radius messages (as displayed in the 'View Radius Messages' window) are being formatted to allow successful searching.

Presence Server Failure Impact

- If the Presence Server fails, then:
- Status windows in the UCC Clients are grayed out.
- Users cannot change their presence status.
- Status displayed in the QuickSearch will not be current.
- Call Logs are not written and are lost for the duration that the Presence Server is down.
- The Mobility Services including the Single Number Reach will not work.
- Other UCC servers are un-affected.

There are two aspects to the configuration – setting up the communication parameters to handle the SIP messages and setting up the Radius parameters to allow the Presence Server to receive these Radius accounting messages. (Uncheck 'Show basic Configuration Pages' to view this page).

If you have selected the Trace Log and Password options to apply to all the UCC Server applications and wish to take the default settings for the Presence Server, then click on Next to continue to the next window.

Presence Server Communication Parameters

- SIP Server Address: This is the IP address or network address of the computer with the System SIP Server.
- Port: This is the port used by the Presence Server to receive messages. The default value is 5062 over which TCP and UDP connections are supported. If this port is not available, then change this to a port available on the computer.
- Username: This is the well-known name of the Presence Server. This cannot be changed.
- Password: This password is used to authenticate the registration of the Presence Server. Enter the password. This can be any text or number string up to twelve characters in length.
- If asked by Cisco Technical Support, enable the debug trace logging and set the Trace level to the requested level. This is checked at server startup only.

Click on Next to continue.

To Set the Radius Parameters:

The Radius Parameters window sets up the parameters for the Radius Accounting server incorporated in to the Presence Server. The Authentication Key (password) and the Port parameters need to be specified for the Presence Server to receive the accounting packets from the Cisco Unified CME.

- Enter the Authentication Key value. This is the password value used to authenticate the communication between the Cisco Unified CME and the Presence Server. This value must match the Radius Server Key value set in the Cisco Unified CME router. (In the following example, this would be uccserver: radius-server host 1.1.1.1 auth-port 1645 acct-port 1646 key **uccserver**)

- Radius Accounting Port: The Radius Accounting Server opens this port to receive the accounting messages. This value must match the Radius Server Accounting Port value set in the Cisco Unified CME router. (In the following example, this would be 1646: radius-server host 1.1.1.1 auth-port 1645 **acct-port 1646** key uccserver).

- Use this network adapter for RADIUS: If there are multiple network adapter cards in the PC and the adapter card used by the Presence Server cannot reach the Cisco CME then check this option and select the correct Network Adapter IP Address for receiving the RADIUS messages from the router.

- Click on the View Radius Messages to verify that the Radius messages are being received at the UCC Server.

- Click on the Verify Ports button to check is the specified port is available for use by the Presence Server.

Notes

1. See Chapter 4 – Configuration of the Cisco Unified CME router parameters for details of setting the RADIUS accounting messages.
2. Verify that no other Radius servers are running on the UCC Server computer as they might block access to the default Radius accounting port. Specifically the Windows Authentication Server should be closed as it opens the default Radius port.
3. If the Unified CallConnector Server is connected to multiple CME/UC500, then the RADIUS password and port must be the same on all the routers.

To View Radius Messages
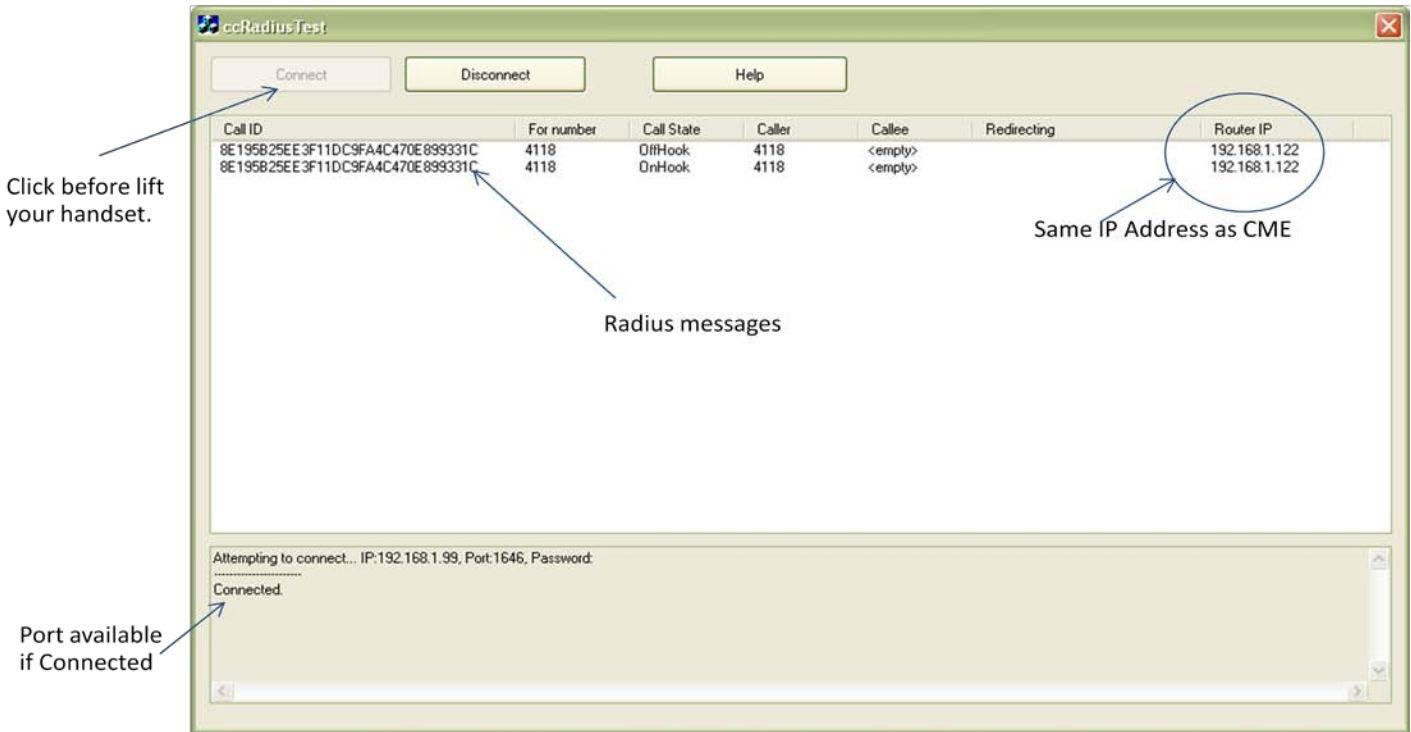
- You can verify that the Radius messages are being received by clicking on the "View Radius Messages" button. Click on the Connect button. If the connection succeeds, then the port has been successfully opened, otherwise some application or firewall is blocking access. (Note: the Presence Server should be stopped before you can run this application)
- Go off-hook or make calls to the phones on each router, the Radius messages should be displayed in the Radius Test window.
- Verify that the Router IP is the same as the CME IP address configured for that Cisco CME in the CallController Server section of the Server Wizard.
- Verify that you can see the call state transitions – ring, connect and hang-up. Note the Radius does not provide the Held call state.

NOTE: If the Radius message is repeated multiple times then the Radius password setting is incorrect.

Examples below show sections from the server log files:

RADIUS SERVER LOG EXTRACT

```
2007-12-21--07:05:22###############Incoming Radius Packet from
192.168.1.122################
DATE & TIME: Fri Dec 21 07:05:22 2007
------------------------------------------------
Identifier: 92
Attributes:
  (44)Acct-Session-ID=000A58F7
  (26)Vendor-Specific: (25)h323-setup-time="h323-setup-time=*07:11:21.049
central Fri Dec 21 2007"
  (26)Vendor-Specific: (26)h323-call-origin="h323-call-origin=answer"
  (26)Vendor-Specific: (1)Cisco AVpair="feature-vsa:fn:TWC,ft:12/21/2007
07:11:21.045,cgn:4225,cdn:,frs:0,fid:464275,fcid:D235EC29AF0D11DCA937D9D25FE6F9
B4,legID:56EEA"
  (40)Acct-Status-Type=1
  (5)NAS-Port=60000
  (87)NAS-Port-ID=EFXS 50/0/225
  (4)NAS-IP-Address=192.168.1.122

2007-12-21--07:05:22<<Radius>> CallInfo event fired for number 4225 with state
OffHook.
2007-12-21--07:05:22[SkinnyCallInfo::Dump()] CallRef:13978 Calling:4225 Called:
OriginalCalled: LastRedirecting: CallType:1 LastRedirRxn:0 Trunk:0 LineInst:0
ExtCallId:D235EC29AF0D11DCA937D9D25FE6F9B4 RouterIp:192.168.1.122
2007-12-21--07:05:22<<Radius>> Updated 0 call(s). Added 1 call(s). Total call
legs: 20.
2007-12-21--07:05:22<<Radius>> Calls cleaned up. Calls:12. Legs:20.
2007-12-21--07:05:22<<Radius>> Call ID Manager entries: 12.
```

PRESENCE SERVER LOG EXTRACT

```
<<ccPresenceServer>>[TRACE]@2007-12-28@10:56:10** <0x08A0>
[+][CRadiusAPI::fire_CallInfo]
<<ccPresenceServer>>[DEBUG]@2007-12-28@10:56:10** <0x08A0>
[CRadiusAPI::fire_CallInfo]: *** CRadiusAPI::fire_CallInfo: CallDirection=0,
CallRef=42 ,CallingParty=902112345678, CalledParty=919493991085, CallState=5,
RedirectedReason=0
<<ccPresenceServer>>[DEBUG]@2007-12-28@10:56:10** <0x08A0>
[CRadiusAPI::fire_CallInfo]: CONNECTED
<<ccPresenceServer>>[TRACE]@2007-12-28@10:56:10** <0x08A0>
[+][GetCurrentDateTime]
<<ccPresenceServer>>[TRACE]@2007-12-28@10:56:10** <0x08A0>   [-
][GetCurrentDateTime]
<<ccPresenceServer>>[DEBUG]@2007-12-28@10:56:10** <0x08A0>
[CRadiusAPI::fire_CallInfo]: ### Call '42' found and being updated
<<ccPresenceServer>>[TRACE]@2007-12-28@10:56:10** <0x08A0>   [CCallInfo::dump]:
*------------------------------------------------
<<ccPresenceServer>>[TRACE]@2007-12-28@10:56:10** <0x08A0>   [CCallInfo::dump]:
* Router           : 192.168.1.122
<<ccPresenceServer>>[TRACE]@2007-12-28@10:56:10** <0x08A0>   [CCallInfo::dump]:
* Call Ref         : (42)
<<ccPresenceServer>>[TRACE]@2007-12-28@10:56:10** <0x08A0>   [CCallInfo::dump]:
* Local Number     : +902112345678
<<ccPresenceServer>>[TRACE]@2007-12-28@10:56:10** <0x08A0>   [CCallInfo::dump]:
* Other Party Number : 9493991085
<<ccPresenceServer>>[TRACE]@2007-12-28@10:56:10** <0x08A0>   [CCallInfo::dump]:
* Ring Duration     : 3813
```

```
<<ccPresenceServer>>[TRACE]@2007-12-28@10:56:10** <0x08A0>    [CCallInfo::dump]:
* Connect Duration   : 0
<<ccPresenceServer>>[TRACE]@2007-12-28@10:56:10** <0x08A0>    [CCallInfo::dump]:
* Direction          : Out
<<ccPresenceServer>>[TRACE]@2007-12-28@10:56:10** <0x08A0>    [CCallInfo::dump]:
* Status             : Completed
<<ccPresenceServer>>[TRACE]@2007-12-28@10:56:10** <0x08A0>    [CCallInfo::dump]:
*----------------------------------------------------
<<ccPresenceServer>>[DEBUG]@2007-12-28@10:56:10** <0x08A0>
[CRadiusAPI::fire_CallInfo]: *** CRadiusAPI::fire_CallInfo: CallDirection=1,
CallRef=42 ,CallingParty=902112345678, CalledParty=919493991085, CallState=5,
RedirectedReason=0
<<ccPresenceServer>>[TRACE]@2007-12-28@10:56:10** <0x0BB0>
[+][CSVRTransactions::PublishCallInfo]
<<ccPresenceServer>>[ERROR]@2007-12-28@10:56:10** <0x0BB0>
[CSVRTransactions::PublishCallInfo]: *** LOCAL NUMBER NOT FOUND (+902112345678)
```

Setting up CallController Server

The CallController Server connects to the Cisco Unified CME router to control the user's IP phones. To setup the CallController, you need to configure the following information:

- Specify the SIP communication parameters for the CallController Server.

- Obtain a list of the IP phones that are present on the Communication Cisco Unified CME router. This can be done manually or by using the automated Configuration Download feature of the Wizard.

- Specify or select the IP Phones that are to be controlled by the CallController Server. You should select only the phones that will be accessed and controlled by the Unified CallController users.

- Verify that the selected phones can be accessed and controlled by the CallController Server.

SIP Communication Parameters

- SIP Server Address: This is the IP address or network address of the computer with the System SIP Server.

- Port: This is the port used by the CallController Server to receive messages. The default value is 5063 and is used for TCP and UDP connections. If this port is not available, then change this to a port available on the computer. Note – in addition to

the SIP connection, the CallController Server sets up one TCP connection for each selected ephone and for the softphones it will setup UDP connections for handling the RTP media.

- Username: This is the well-known name of the CallController Server. This cannot be changed.

- Password: This password is used to authenticate the registration of the Presence Server. Enter the password. This can be any text or number string up to twelve characters in length.

- Use this Network Adapter to connect to the CME: For Server PC with multiple network adapter cards where the access to the Cisco CME is through a different network adapter than the connection to the user's desktop. Click on the check box to select an alternate network adaptor for the Cisco CME.

CallController Server Options

- **Enable speaker when placing or answering a call**: When a call is placed or answered from the UCC client the speaker on the IP Phone is automatically turned on when this option is enabled.

- **Publish call information for shared lines**: Checking this option enables publishing call state information for shared calls. An ephone-DN is considered to be shared if the DN is present on multiple IP Phones. The affect of this option is to disable popup notification for calls on this button. Users will not see the call state changes for this line on their UCC client.

- **Publish call information for monitored lines**: Checking this option enables publishing call state information for monitored calls. An ephone-DN is considered to be monitored in the line button type is set to be 'monitored'. Unchecking this option globally disables popup notification for calls on monitored DNs. Users will not see the call state changes for this line on their UCC client.

- **Enable trace log file**: This option enabled writing to the trace log file. The amount of information written is specified by the trace level field below.

- If asked by Cisco Technical Support, enable the debug trace logging and set the Trace level to the requested level. This is checked at server startup only. By default the trace files are saved in the Trace Log folder under the Unified CallConnector Server.

Click on Next to continue.

Configurations for Accessing Cisco CME

The Unified CallConnector server connects to the Cisco Unified CME routers to control the IP phones based on user commands and to receive call status information. To enable this function, each ephone that is to be controlled has to be specified through the Server Configuration Wizard.

The UCC Server requires the following information from each of the routers to control the calls on the IP Phones.

Configuration	What information is needed
Telnet Access Information	The download method uses the Telnet protocol to access the CME configuration information. You will need to provide:
	CME IP Address
	Telnet account name
	Telnet password and Exec level password
Transfer to Voice Mail	This is only required for Mobility Service: For each selected method, the information required is:
	Using Transfer Script: Transfer Pilot Number
	E164 Routing: Dialing pre-fix number
	Transfer-to-Voice Mail Softkey: None
Ephone and CME Features	CME configuration information including the following:
	CME setup for Hardware Conferencing
	Are you using digital or analog PSTN connections – enable "Receive connect on remote answer" for digital connections.
	Length of the extension numbers
	Prefix for Dialing PSTN Numbers
Configure CME location	For each CME associated with the UCC server, the location information allows the UCC Server to select the dialing parameters for mobility calls: Required parameters include:
	Country
	Area code
	Number Pattern
Ephones for Users	You will also need the list of ephones for the UCC users. Each of these ephones must have the ephone username and password configured.

The configuration changes are made from the Server Wizard - Settings to Access CME/UC500 Features window shown below.

Access CME/UC500 Features Window

CME/UC500 Table:

This table on the left displays the list of Cisco Unified CME router configured for the UCC Server. In multiple router configurations, this list will display each of the routers configured for the UCC Server.

- To add a new router, enter the router related information in the fields to the right and click on the Add button.
- To make changes the router parameters, select the router IP address from the CME/UC500 table, make the changes to the fields in the right and click on the Update button.
- To remove a router from this list, select the router from the CME/UC500 table and click on the Delete button.

Telnet Access:

These fields specify the parameters for the Telnet account to be used to download the Cisco CME ephone and ephone-DN parameters. The login account is specified here and used to initiate the download session in the next window.

Voicemail:

The Voicemail fields select the method for transferring a call to the user's voice mailbox. Several methods are supported, but the recommended method is 'Using the Transfer Script' as it requires the least configuration on the router and Cisco CUE.

Ephones:

The Ephones section includes miscellaneous parameters including the conferencing method and the type of PSTN gateways that are on the router. This information is used primarily during the Mobility Service calls.

The Extension lengths specify the length of the extension numbers defined in the router. There can be multiple extension number lengths; each should be specified, separated by a comma.

The Dial-Out Prefix is the access code that has to be pre-pended to the PSTN numbers to cause it to be routed to the PSTN gateway ports.

CME/UC500 Location:
This information is used to generate dialable numbers and for formatting incoming caller-id to a canonical format for lookup in the directory database.

Buttons:

Clear:	This clears all the information from the fields to allow a new data to be entered.
Add:	Adds this information as an additional router entry in CME/UC500 table.
Update:	Updates the current values for the selected router.
Delete:	The highlighted entry n the CME/UC500 table is deleted.

Parameters for Telnet Access

These parameters are used to setup a Telnet session to the Cisco CME router to download configuration information.

CME IP-Address:	This is the IP Address of the router Cisco CME or UC500. This IP Address is used telnet to the router to download the configuration information.
Telnet User Name:	User name of the telnet account to be used for downloading the configuration information.
Telnet Password:	Password for the Telnet user account.
Exec Password:	Exec level password for some specific configuration parameters. (The exec level password is entered when download is initiated).

Transfer to Voice Mailbox Settings

This lists the supported method for transferring a call to a user's voice mailbox. The Transfer to Voice Mail Script is the recommended method. Note: Transfer to Voicemail is used in UCC Mobility Service to return the caller to the user's voicemail box.

Transfer to Voice Mail Script: This is a CUE script that automatically answers a call and waits for a voicemail box number. The voice message is recorded and saved into that mailbox.
Use E164 Number: In method requires a separate E164 telephone number to be assigned to each voice mail box. The call is then transferred to this number for recording of message for the associated mailbox.

- Use Transfer-to-Voicemail Softkey: This feature requires the version of CME with this Softkey.

CME Features and Extension Dialing

- Use Hardware Conferencing: This parameter specifies that the CME has been configured for hardware conferencing and ad-hoc conference. When this option is checked, the UCC Mobility Service uses the hardware conferencing methods and enables features that require multiparty conferencing.

- Receive connect on remote answer: This parameter is used determine if the call progress states are local or from the far-end device. When analog lines are used to make PSTN calls, the Mobility Server receives ring and connect when the line is seized, while on digital trunks ring and connect states are provided by the terminating end device. The Mobility Server uses this parameter to delay when the prompts are played to the caller. This should be set to true when the CME/UC500 is configured with digital trunks.

- Extension Length: Number of digits in the internal extension. If there are several number plans of different extension lengths, then enter all these number lengths separated by commas.

- Dial Out Prefix: Digits that have to be appended to the PSTN number, but excluding the long distance code, to make an external call.

CME Location Parameters

- Location: The selection of the location sets the country, area code and the number patterns. You can select a pre-defined location or click on Edit to add/modify a location details.

- Country: The country in which the router is located, more specifically this is the country code associated with the PSTN network the router is connected to.

- Area Code: The telephone Area code of the location.

- Pattern: This is the canonical format of the PSTN telephone number for that country and area code.

- Edit Button: This button opens the Edit Location Information window to allow the above location information to be updated.

Editing Location Parameters

Click on the Edit button in the CME/UC500 Location section. The Edit Location Information window will be displayed.
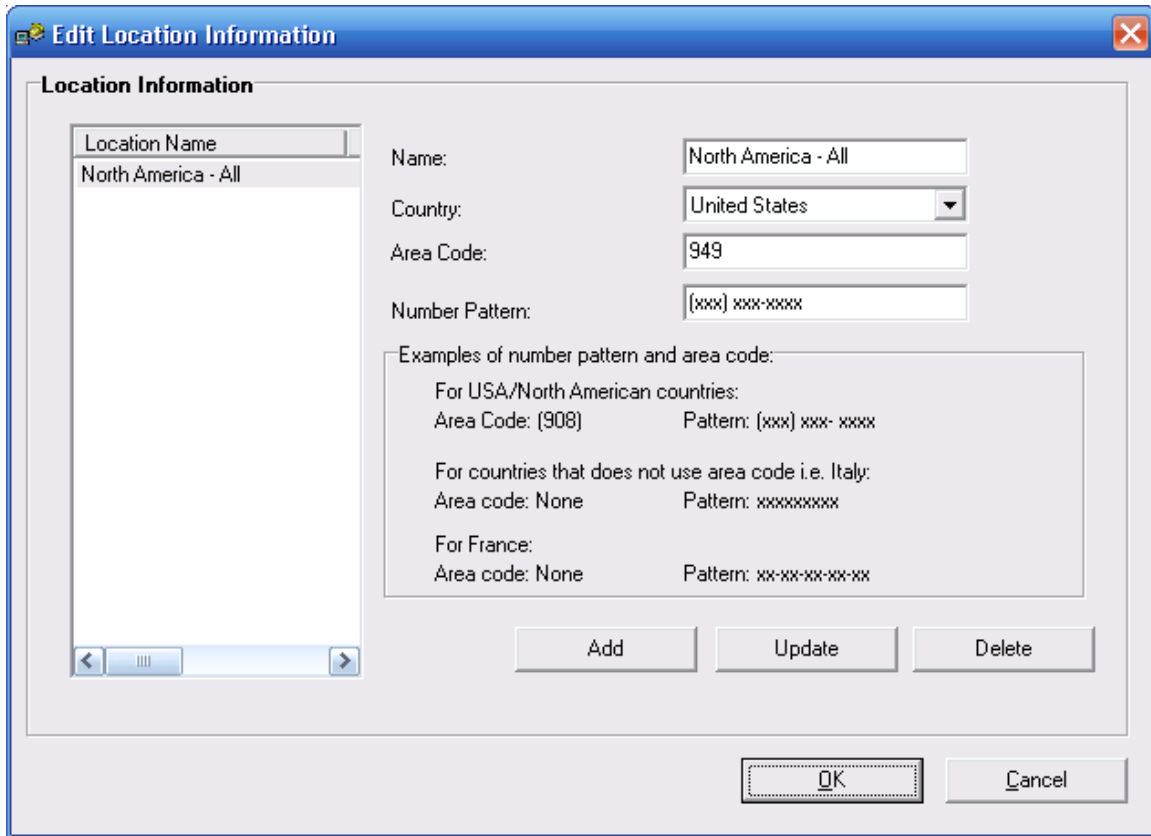
- Click on the Edit button in the CME/UC500 Location section
- Click on an existing location to make changes or enter a new location name.
- Select or change the country setting from the pull down list.
- Enter the area code and number pattern.
- Click on Add to add new location details or Update to modify an existing setting.
- Click on Delete to remove a location setting.
-

Notes

The number pattern is used to convert a caller-id number to a canonical formatted telephone number.
A default set of number patterns are shipped with the UCC Server. If the patterns is incorrect, please enter the correct number pattern in this field.

To Setup the Router Location Parameters:

- Start the Server Wizard
- Click on the CallController Server button in the Home page and then click on Next.
- Select the router that you want to make changes to or enter the information then click on Add to create a new entry.
- Enter the router related information in the "Settings to Access CME /UC 500 Features" page.
- Click on Add to add a new router details or Update to modify an existing setting.

Advanced Dialing Translations for Server

The UCC Server dial plan is used for two different purposes:

- Convert a telephone number to a dialable number. This involves determining if the number is an internal extension or a external PSTN number. In the case of a PSTN number, the Dial-Out Prefix is added to the number and the number formatted for local or long distance dialing.
- Convert an incoming number to the 'canonical' format to allow searching for the number in the UCC directories. Numbers in the UCC Directories are saved in a standard format known as 'canonical' format. For example 4085551212 in the United States is formatted to be (408) 555-1212.

The UCC Server uses the router location specification and the information in the uccDialPlan.xml file to convert to a dialable number and a canonical format. Since there may be special local requirements or dialing configurations that have not been covered, the Advanced Dialing Translation provides a method to manually setup dialing translation rules to handle these requirements.

Warning: Please note the Server Dialing Translations are applied only to two types of calls.

Mobility Service calls made by the Mobility Server. These rules are not applied to the calls made from the UCC clients. The caller, called party numbers received from the Radius messages are converted to a 'canonical format' for lookup by the Presence Server.
At the present time these are the only two call flows that make use of the server dialing rules.

Notes on Dialing Translations

1. The dialing translations are specified for each router. Even if the translations are the same, they will need to be specified for each router.
2. There are two different translations – a) for dialing and b) lookup. Dialing Translation converts a telephone number to a number that can be sent to the CME for dialing out. The lookup translation converts telephone numbers provides from a) Radius messages – both internal extension and external PSTN numbers and b) caller and called numbers provided through the skinny messages. Both have to be specified based on the format of the numbers.
3. The translations are performed in the specified precedence order until a translation rule is encountered. Processing stops at the first rule that can be executed. All subsequent rules are ignored.
4. Patterns specify the format of the input number to the translation. You can use the letter 'x' to specify any digit. For example xxxx indicates any number that is four digits long and between 9999 and 0000. 'x' should be used when the input number has to be of a specific length. The character period '.' is used to denote any subsequent digits regardless of the length. For example '551.' indicates any number starting with 551 that is greater or equal to four digits in length.
5. The 'Strip' function removes the specified number of starting digits from the input. For example Strip=3 will remove the first three digits from the matching pattern.
6. Pre-pend function appends the specified digits to the front of the number once the Strip function has been performed.
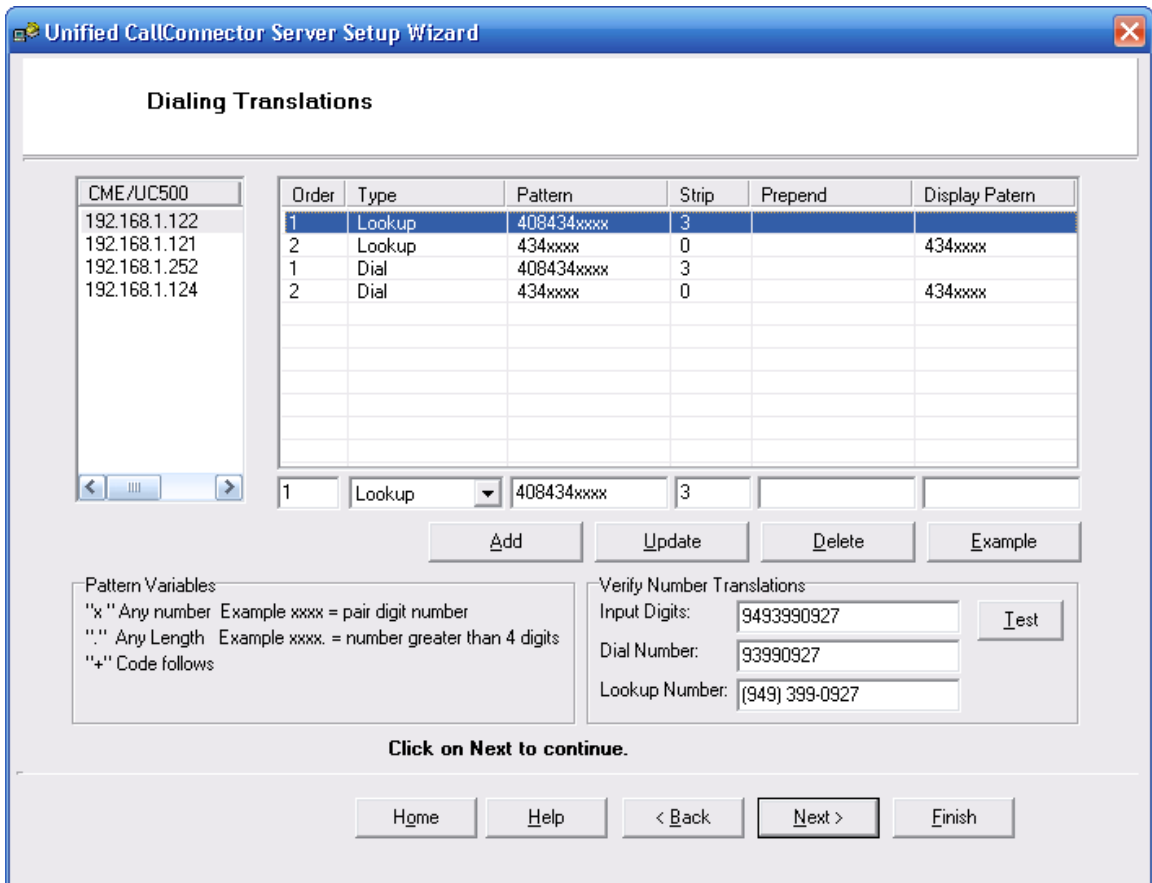
Configuring Dialing Translations

Configuring Dialing Translations

The default dialing and lookup dialing rules are applied to the incoming and the dialing out numbers based on the CME location setting. In a number of situations, these default translations are not sufficient. The Dialing Translations table allows you to setup custom rules to handle any special number translation requirements for your locale.

Dial Translation Parameters:

Options	Description
CME/UC 500	This lists the defined CME/UC500 associated with the UCC Server. The dialing translations are specified for each router. To make or edit dialing translations, first select the router.
Order	Order defined the precedence or execution order for the rules. Lookup and Dialing have their separate execution orders. Rules are processed starting with one and moving down the list. Processing stops when there is a match for a pattern.
Type	There are two types of number translations – Lookup for incoming numbers that have to be converted to the canonical format to enable searching in the directories; and Dialing in which canonically formatted numbers are converted to a dialable number with Dial Out codes and Long Distance and Area codes.
Pattern	Pattern is the specification of the input number for which the translations are to be performed. Here 'x' means any number between 0 and 9; '.' Means any number of that length or greater. Examples of patterns include: xxxx -- any four digit number 555xxxx – any seven digit number starting with 555 408xxx. – any number starting with 408 and greater than six digits.
Strip	Remove the specified number of digits from the right of the input numbers.
Pre-Pend	Add the specified numbers to the left of the input number
Display Pattern	The format to associate with the matching input number
Add	Add this as a new rule
Update	Modify and save the selected dialing rule
Delete	Delete the selected dialing rule
Example	Opens a Dialing Rules Examples help document
Input Digits	Enter a number to verify how it will be converted for dialing and lookup given the existing rules. Note make sure you have selected the correct router.
Test	Click on the Test button after you have entered the input number to generate the dialing and lookup numbers.
Dial Number	Conversion of the Input number to a dialing number based on the location and dialing rules
Lookup Number	Conversion of the Input number to a lookup number based on the location and dialing rules

To Setup the Dialing Rule:

Order   Translation Type Pattern   Strip   Pre-pend

1	Dial ▼	1949xxxxxxxx	4	9	

Add	Update	Delete	Example

- Select the router from the CME/UC500 table at the top left of the window.
- Enter the precedence order for this particular rule, if you have multiple dialing rules. The rules are processed in sequential order, until there is a match in the specified pattern.
- Select Dial from the pull down list. This specified this rule to be a dial translation rule as opposed to a lookup rule.
- Enter the number pattern. The UCC Server will look for this pattern in the dial string. Only if the supplied telephone number matches this pattern, will the translations performed. You may use wild cards in the pattern specification including:
- 'x' for any number between 0 and 9. This is also a place holder that can be used to specify a number string of a specific length.
- '**.**" The dot can be used to specify a variable length number pattern.
- Enter the number of digits from the left that are to be stripped from the input number.
- And enter any digits that are to be added to this number pattern (from the left).
- Click on Add to save the change.

To verify that the translations are working, enter the dialing number in the Input Digits field of the Verify Number Translation Section and press 'Test'. The Dialing Number and the Lookup Number based on the currently router location and the dialing plans setup in the above are displayed.

Verify Number Translations

Input Digits:

Dial Number:

Lookup Number:

Test

To Setup a Lookup Rule:

Order   Translation Type Pattern   Strip   Pre-pend

- Select the router from the CME/UC500 table at the top left of the window.
- Enter the precedence order for this particular rule, if you have multiple lookup rules. The rules are processed in sequential order, until there is a match in the specified pattern.
- Select Lookup from the pull down list. This specified this rule to be a lookup translation rule as opposed to a lookup rule.
- Enter the number pattern. The UCC Server will look for this pattern in the input string. Only if the supplied telephone number matches this pattern, will the translations performed. You may use wild cards in the pattern specification including:
- 'x' for any number between 0 and 9. This is also a place holder that can be used to specify a number string of a specific length.
- '**.**" The dot can be used to specify a variable length number pattern.
- Enter the number of digits from the left that are to be stripped from the input number.
- And enter any digits that are to be added to this number pattern (from the left).
- Click on Add to save the change.

Downloading IP Phone Configuration

This step is provided to help make the installation easier. Information about the IP Phones that are to be controlled by the CallController Server can also be entered manually. When the information is downloaded from the Cisco Unified CME router then you need to only select the required IP Phones from a list.

The Wizard uses the telnet protocol to download the IP Phone information. You will need a telnet account on the Cisco Unified CME router for this function.
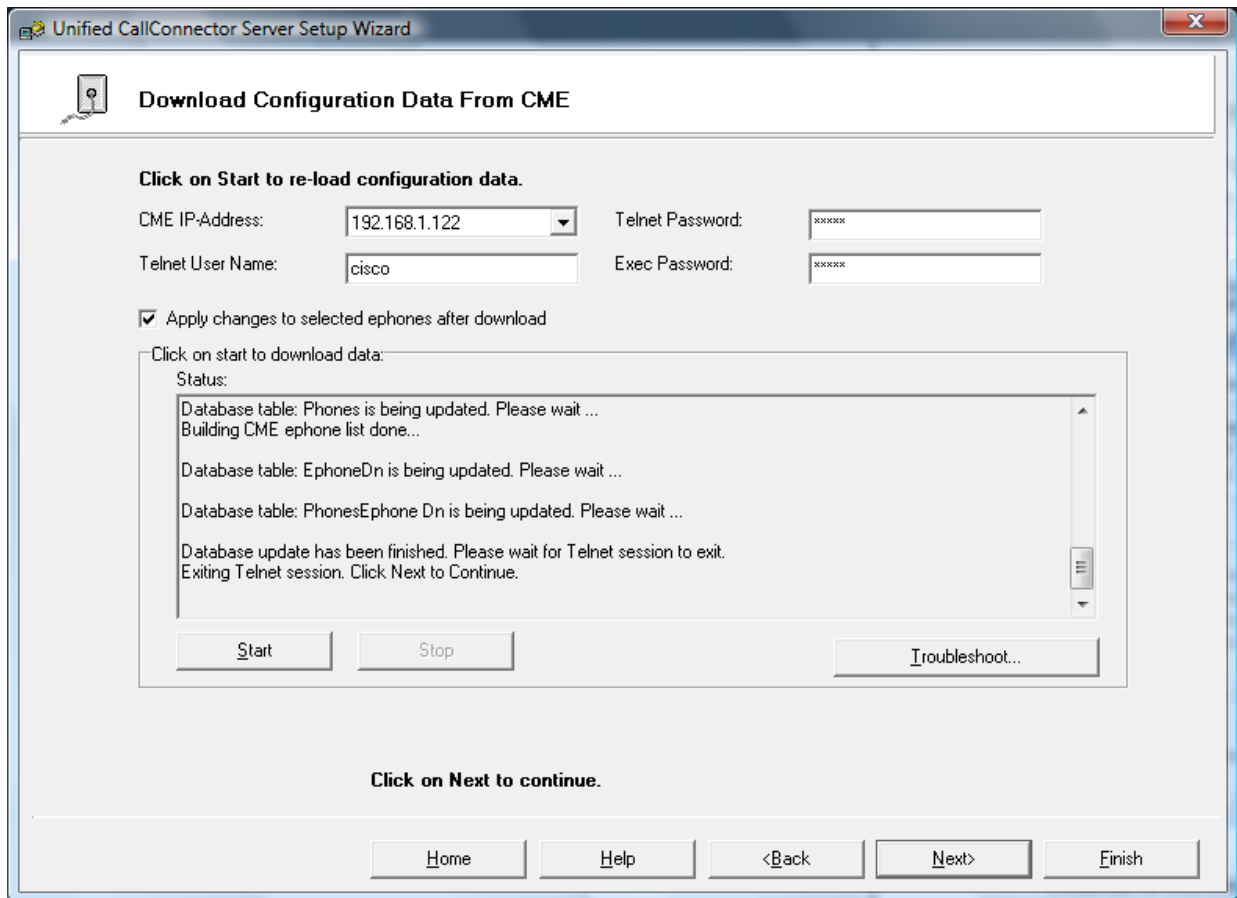
To Download the Cisco Unified CME IP Phone information:

- Select the CME IP Address: This is the IP address of the Cisco Unified CME router.
- Telnet User Name: This is the login user name for the telnet command line access to the Cisco Unified CME router.
- Telnet Passwords: Telnet account password and the Exec password. Enter the Exec level password.
- Click on Start. The Wizard will log in to the Cisco Unified CME router and down load the IP Phone information using the 'Show Ephone' command. This IP Phone information is s saved in the cme.xml file in the Unified CallConnector Server folder.

The download function will run through the following steps. Note this may take a little time.:

```
User Access Verification

Telnet Session finished the passwords verification.

Receiving the ephone-hunt information. Please wait...
Receiving the ephone-dn information. Please wait..

Creating Configuration file: cme.xml. Please wait ...

Configuration file: cme.xml created. Please wait ...

Database table: PhoneSystem is being updated. Please wait..

Database table: Phones is being updated. Please wait ...
Building CME ephone list done...
Synchronizing database...

Database table: EphoneDn is being updated. Please wait ...

Database table: PhonesEphone Dn is being updated. Please wait ...

Database update has been finished. Please wait for Telnet session to exit.

Exiting Telnet session. Click Next to Continue.
```

NOTES:

1. The IP Phone configuration download requires the privilege level access to the router.
2. The Cisco Unified CME router administrator can run the wizard and make the cme.xml file available to the Setup Wizard. This can be used instead of the download as described in the next section.
3. All IP Phones that are to be controlled by the CallController Server need to have the ephone username and password provisioned on the Cisco Unified CME router.
4. The CallController Server supports both control and media termination mode of access to the Cisco Unified CME router. The control mode allows an existing IP Phone to be controlled from the user's desktop. The Media Termination mode is used for the Mobility Server lines only.
   1.

Click on Next to go the 'Select Ephones' window.
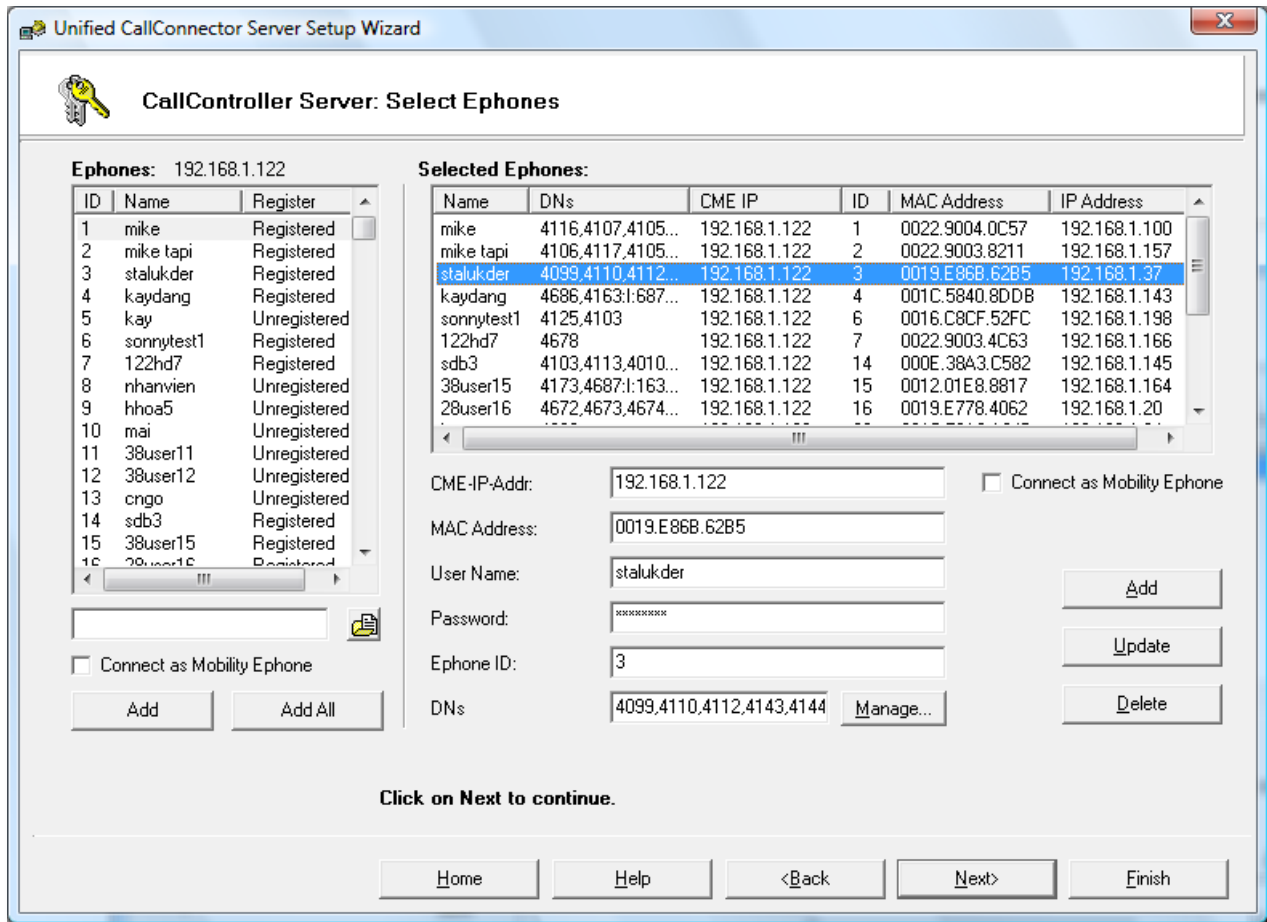
This window allows you to specify the IP phones that will be controlled by the UCC Server. If you have downloaded the IP Phone configuration from the Cisco Unified CME router, then the phones for the CallController can be selected from this list.

Components of the Select Ephones Window

Ephones (All Available Ephones):

This table on the left displays the list of ephones downloaded from the Cisco Unified CME router. The first column is the Ephone ID and the second column lists the directory numbers on that Ephone. If you have not downloaded the configuration then this list will be empty. If you have a cme.xml file of an IP Phone configuration, then you can open this file by clicking on the browse button at the bottom of the Ephone list table. The Add and Add All buttons at the bottom of the Ephones table select the highlighted ephone or select all the ephones respectively.

Connect as Mobility Ephone:

Enable this option only for the ephones that have been configured for use by the Mobility Server. Warning!: Setting this option for IP Phones can cause the phones to be reset.

Selected Ephones (Ephones Controlled by UCC Server):

This table lists the IP Phones that will be controlled by the CallController Server. The table displays the username of the selected ephone, the directory numbers configured on that ephone, the IP address of the router, ID of the ephone. The fields at the bottom of the Selected Ephones table display the parameters of the ephone highlighted in the Selected Ephones table. These fields can also be used to manually enter or change the IP Phone information. The fields and buttons are described below:

Fields:

CME IP Address: IP Address of the Cisco Unified CME router.

MAC Address: This is the MAC Address of the ephone.

User Name: This is the username configured for that ephone in the Cisco Unified CME router.

Password: This is the password configured for the ephone.

Ephone ID: ID or number of the Ephone.

DNs: List of DNs configured on the ephone. This field is provided to distinguish between the ephones.

Checkbox: Connect as Mobility Ephone: Indicates that this ephone has been selected for the Mobility Service

Buttons:

Add: The current values of the ephone parameters are used to add a new entry in the Selected Ephone table.

Update: The current values of the ephone parameters are used to update the highlighted entry in the Selected Ephone table.

Delete: The highlighted entry n the Selected Ephone table is deleted.

Manage: Click on this button to edit the ephone DNs.

To Select IP Phones for the UCC Server

- Download the ephone list from the CME/UC500.
- Click on an entry in the Ephones table. It will be highlighted.
- Click on the Add button at the bottom of the Ephones table. The highlighted entry will be added to the Selected Ephones list. Repeat this step to select all the IP phones for the UCC Server.
- To select all the ephones in the Ephones list, click on Select All button.

To Manually Add IP Phones:

- Enter the User Name, Password, MAC-Address, and CME IP Address in the fields.
- Click on the Add button at the bottom of the Ephones table. A new entry will be added to the Selected Ephones list.

To Delete an IP Phones:

- Click on the Ephone that you want to remove in the Selected Ephones table.
- Click on the Delete button at the bottom of the Ephones table. The highlighted entry in the Selected Ephones list will be deleted.

Click on Next to continue to with the UCC Server Configuration.

Verify Connection to Ephone

This window allows you to verify that the CallController can connect to the IP Phone that you have selected or configured. The verification step is optional and provides a visual confirmation that a) the ephone exists and can be connected for control purposes b) the parameters configured for the ephone are connect.
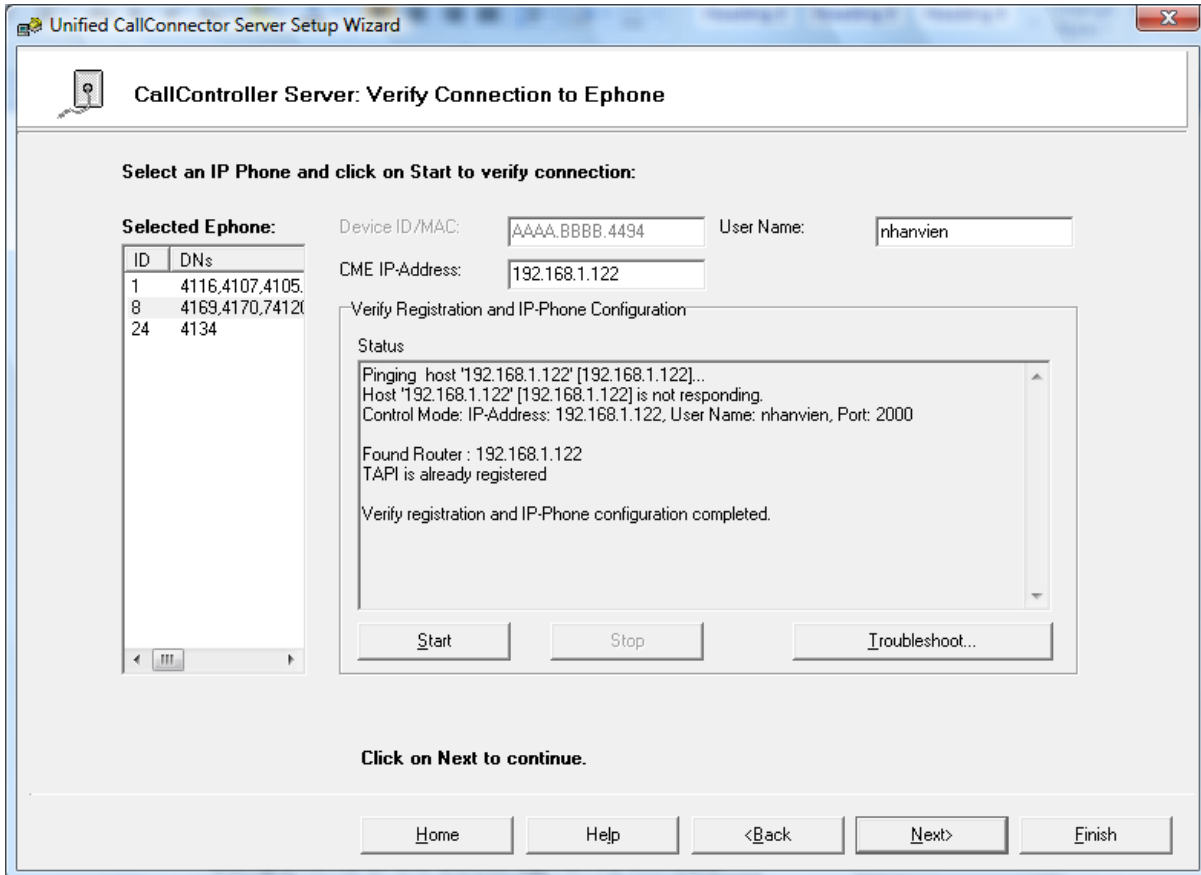
Components of the Verify Connections to Ephones Window

Selected Ephones:
This table lists the IP Phones that will be controlled by the UCC Server. The table displays the ID of the ephone and the directory numbers configured on that ephone. When you click on an ephone in this list the key parameters are displayed in the field to the right. The fields and buttons are described below:

Fields:

MAC Address: This is the MAC Address of the ephone.

User Name: This is the username configured for that ephone in the Cisco Unified CME router.

CME IP Address: IP Address of the Cisco Unified CME router.

Buttons:

Start: Starts the connection process by registering to this ephone.

Stop: Terminates the registration process.

Troubleshoot: Opens the troubleshooting help file.
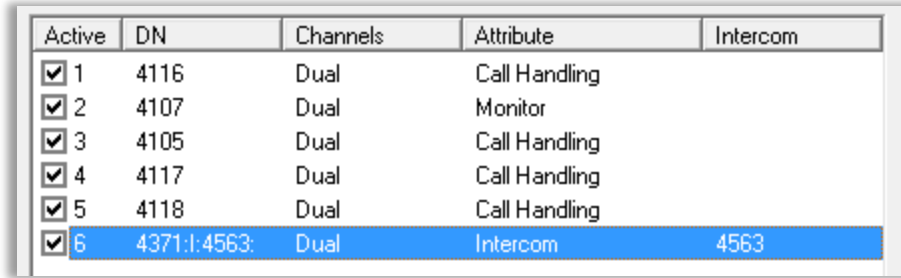
To Verify the connection to an IP Phone:

- Click on an IP Phone in the Selected Ephones table. It will be highlighted and the connection parameters will be displayed on the fields to the right.

- Click on the Start button.

- The Wizard will attempt to register to the Cisco Unified CME router with the specified parameters and display the results.

- If the connection was successful, then the line number and display names for each extension on the ephone will be listed.

- You can click on each ephone and verify connection to the device.

Click on Next to continue to the Call Appearance and Feature Buttons window.
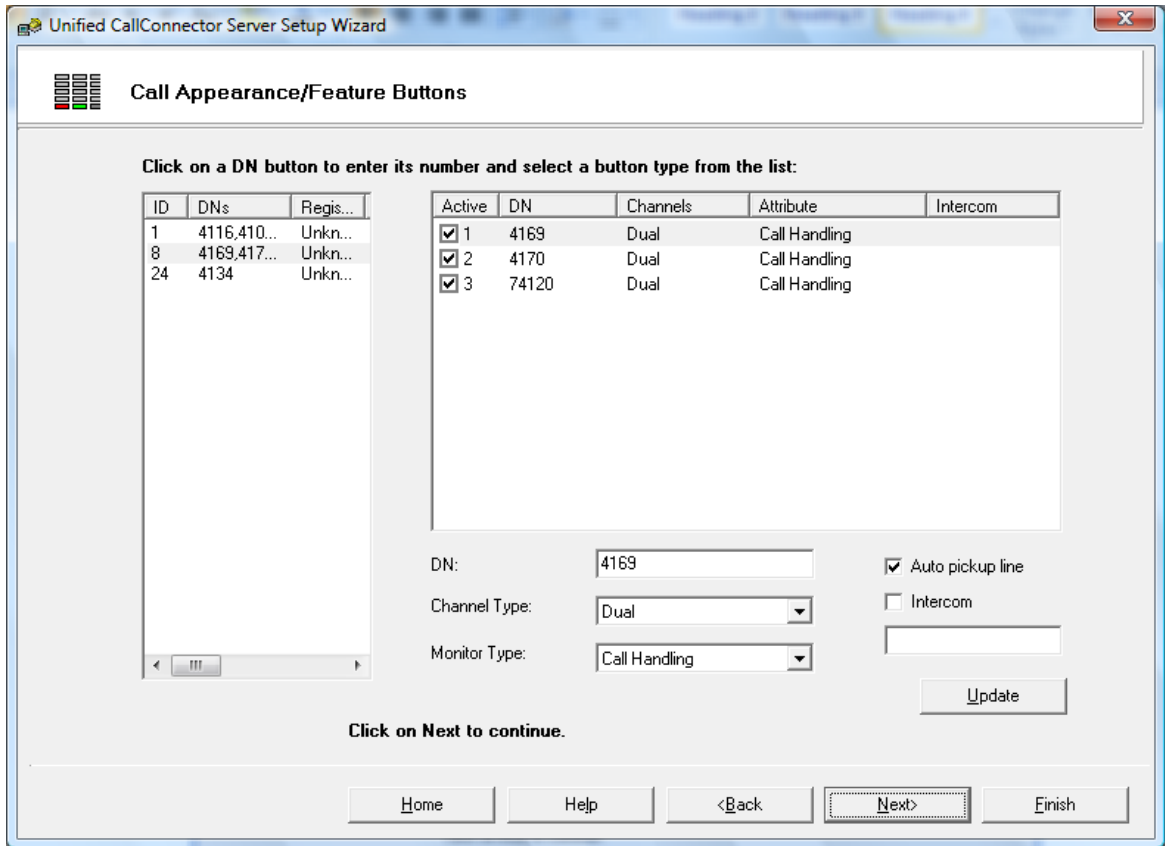
For the selected ephone, this window displays the extensions defined on the buttons with their number, channel type and DN monitoring attribute.

Active	DN	Channels	Attribute	Intercom
☑ 1	4116	Dual	Call Handling	
☑ 2	4107	Dual	Monitor	
☑ 3	4105	Dual	Call Handling	
☑ 4	4117	Dual	Call Handling	
☑ 5	4118	Dual	Call Handling	
☑ 6	4371:I:4563:	Dual	Intercom	4563

Active: The number indicates the button of the IP phone. The check mark indicates that the calls on this button will be presented to the user. If this button is un-checked, then the call information will not be visible in the UCC client.

DN: This is the extension number associated with the ephone-DN configured for this button.

Channels: This is the channel type of the ephone-DN configured on this button. Channel types can be single-line, dual line and octal line.

Attribute: This specified how the DN is being used on this button. The options include:

Call Handling ▼
Call Handling
Monitor
Intercom
Watch
Overlay
Silent ring (beep muted)
Silent ring (beep not muted)
Overlay call-waiting
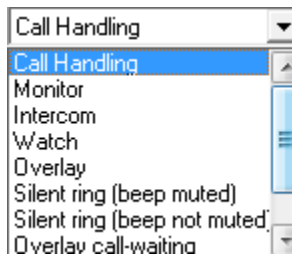
Call Handling: Calls can be made and received on this DN

Monitor: The status of the DN is displayed as idle/busy (or in-use) on this button. If the button or line is selected, then a call is placed to the associated DN.

Intercom: This is an intercom line. Pressing this button places a call to the specified extension and it is immediately connected.

Watch: The button displays the status of the IP phone which has this DN as the primary DN. If the button or line is selected, then a call is placed to the associated DN.

Overlay: There are multiple DNs associated with this button. Calls from each of these DN are presented to the line of button.

Silent Ring: The button is configured to not ring.

Overlay Call Waiting: Indicates that overlay calls are waiting.

Expansion/Overflow: This is a place holder to display the calls from another button.

Intercom: If the button is an intercom, then the intercom number is displayed in this field.

Auto Pickup Line: This specifies the preferred line to be used for making outgoing calls. This option is specified by the Auto-Line parameter in the ephone configuration.

The UCC Server Wizard automatically downloads this information from the CME router. Administrators may override the configuration from this wizard page. The information is provided to allow you to verify the ephone configuration.

Connecting to Multiple Communications Manager Systems

The Unified CallConnector Server can be connected to multiple Cisco Unified CME routers or Unified Communication 500 systems. Please verify the system configuration with your Channel Partner.

To Add Ephones from another CME System

- Return to the Download Configuration Data from CME window.
- Enter the connection information for the CME that you want to connect to.
- Enter the Telnet user name and password.
- Click on start to down load the ephone information from the new router.
- Run through the steps as described above to add in additional ephones that are to be controller by the Unified Connector Server

Click on Next to continue with the user administration.

Configuring Groups and Users

The configuration of users for the UCC server consists of three steps:

- Define the groups or departments in the organization. All UCC users are placed in a group/department. If a group is not assigned, the users are placed in the Default group. The groups have to be defined first so that the users can be placed in those groups.

- Define the UCC users. Each user in the Unified CallConnector system needs to be added in by the administrator. Each user should have a login name and password as well as their other contact information. (This information can be updated in a spreadsheet and imported).

- IP Phone for the User. The administrator needs to assign an IP phone to the user. This is the phone that can be controlled by the user when they log in to the UCC client.

Creating Group List:

The administrator needs to setup the groups or department of the organization. This information can be manually entered from the Server Wizard – Update Group window or imported from the GroupsTable.xml file. By default, a list of group is pre-installed. These can be used, modified or deleted based on your organization. Each Unified CallConnector user has to be placed within a group or the system will place them in the Default group.
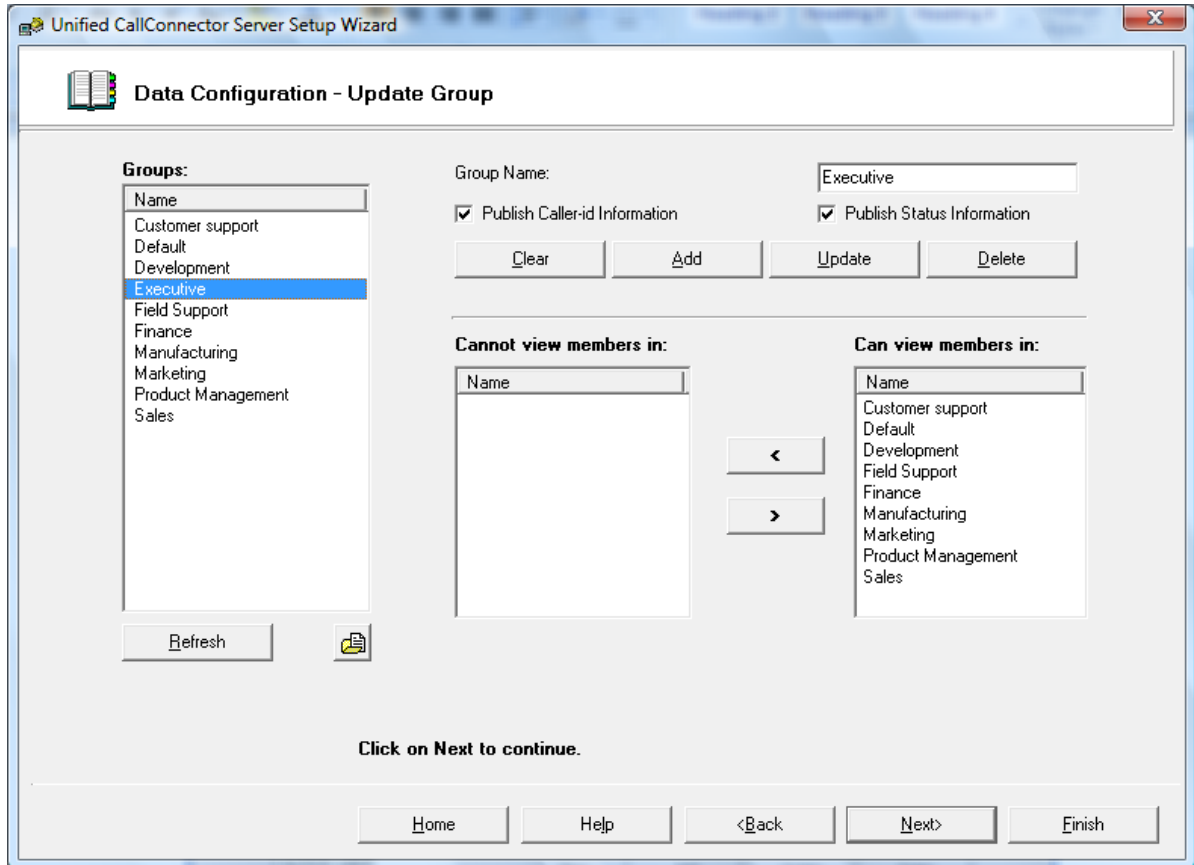
Components of the Group Window

Groups:

This table lists the groups that have been defined for use with the Unified CallConnector. The table displays the Group Names.

Cannot view members in:

This table lists the groups whose users cannot view the presence status of the members of the Group currently selected in the Groups table.

Can view members in:

This table lists the groups whose users can view the presence status of the members of the Group currently selected in the Groups table.

Publish Caller-Id Information:

This option enables the publication of the caller, called numbers with the call status. Uncheck this option to stop publishing caller/called numbers. Only the call state information will be displayed for users in this group.

Publish Status Information:

This option enables the publication of the user's availability status. Uncheck this option to stop publishing all status information for the users in this group.

Group Buttons (at the bottom of the Groups table):

Refresh:	Re-reads the group information from the database and displays it in the table.
Browse:	Allows you to open and import the group-list from the GroupsTable.xml file. This file is saved in the Data folder under Unified CallConnector Server.
Arrow Left:	Moves the currently selected group in the Can-View Group to the Cannot-View Group.
Arrow Right:	Moves the currently selected group in the Cannot-View Group to the Can-View Group.

Fields (fields and buttons to the right of the Groups table):

Group Name:	This is the name of the group.
Buttons:	
Clear:	Clears the Group name to allow you to add an new entry. You will need to click on Add to apply.
Add:	Creates a new entry with the group name specified in the field above.
Update:	Changes the name of the currently selected group with the name in the group name field above.
Delete:	Removes the currently selected group name. If any user was placed in this group then that association is changed to the default group.

To Update an existing Group Name:

- Click on an entry in the Groups table. It will be highlighted.
- Modify the name in the Group Name field
- Click on the Update button. The highlighted group name will be replaced with the new name entered in the Group Name field.

To Add a New Group:

- Enter the group name in the Group Name field.
- Click on the Add button. A new entry will be added to the Groups list.

To Delete a Group:

- Click on the Group name that you want to remove in the Groups table. This group name will be displayed in the fields to the right.
- Click on the Delete button. The highlighted entry in the Groups list will be deleted.

To Restrict Members of a Group from Viewing Status:

- In the Groups table, click on the Group Name to which you want to apply the access restrictions.
- The Can View Group table will display the Groups whose members can view the status of the users in the Group highlighted in the Groups table.
- The Cannot View Group table will display the Groups whose members cannot view the status of the users in the Group highlighted in the Groups table.
- Click on the Group name that you want to restrict in the Can-View Groups table. Then click on Arrow-Left.
- This Group will be moved to the Cannot View Groups list.

To Allow Members of a Group Access to Viewing Status:

- In the Groups table, click on the Group Name to which you want to apply the access restrictions.
- The Can-View Group table will display the Groups whose members can view the status of the users in the Group highlighted in the Groups table.
- The Cannot-View Group table will display the Groups whose members cannot view the status of the users in the Group highlighted in the Groups table.
- Click on the Group name that you want to allow in the Cannot-View Groups table. Then click on Arrow-Right.
- This Group will be moved to the Can-View Groups list.

Click on Next to continue to with the User Configuration.

Managing Users:

The Unified CallConnector users need an account to be setup with login name and password to connect to the UCC Server. The Server Wizard Managing Users window allows you to add, delete and update the Unified CallConnector user information. It allows you to perform the following management functions:

- Add a Unified CallConnector user. Assign the user login name and password.
- Delete a user. This removes the user from the system and will reject login attempts with on that account.
- Change the contact information of the UCC user. Note - users are also able to update their contact information from the Options window.
- Change the user login name and password.
- Assign the user type and the user's group.
- Import the user list from an xml file.

Components of the User Administration Window

User Table:

This table lists the user accounts that have been defined for the Unified CallConnector. Only these users will be able to login to the Unified CallConnector Server. The table displays the User ID of the user and the User Display Name. The ID is an internally used parameter and cannot be changed.

User Table Buttons (at the bottom of the User Table):

Refresh:	Re-reads the user information from the database and displays it in the table.
Browse:	Allows you to open and import the user-list from the users.csv file. An example file is saved in the Data folder under Unified CallConnector Server.

The fields and buttons to the right of the Users Table are described below:

Fields (to the right of the Users Table):

User ID:	This is the ID number of the user and is assigned automatically by the system.
First Name:	This is the first name of the user.
Last Name:	This is the last or family name of the user.
Login Name:	This name is used by the user to login to the Unified CallConnector Server.
Password:	The password to be used to login.
Company:	User's organization or company name.
User Type:	Three types of user accounts are supported.
User:	A standard Unified CallConnector user
Manager:	This user, in addition to the standard user functions, is able to change the status of the other users in the group for which they are the manager.
Administrator:	An administrator is able to change system wide configuration data.
Serial Number:	(Optional) This is the client serial number. It is provided to help with the license number administration. Each user's serial number can also be sent out to the user with the email notification feature of the Server Wizard.
Business:	The work or business telephone number. This would be the primary number provisioned on the user's IP Phone. (Please see note below when a shared number is entered)
Business2:	A second work or business telephone number. (In configurations where the dual-line DN are set to an extension number and the secondary to a DID number, this fields can be used to enter the DID number)
Home:	The home telephone number.
Mobile:	The mobile or cellular telephone number.
Email:	User's email address.
SMS:	User's SMS address. This is typically the mobile-number@service-provider.com
IM:	Instant Message address. This is the login name of the user. This is a non-editable field and is set to the user's login name by default.
Voicemail:	User's voicemail box number. By default this is the primary extension on the IP Phone.

TEL Pin: User's personal Single Number Reach password. When a SNR calls is placed to the user, the system authenticates the user with this password.

DISA Pin: User's personal Dial-In Access password. When the user calls to access the Dial-In Access features the Mobility Server authenticates the user with this password.

Buttons (to the right of the Users Table):

Clear: Clears the user information fields to allow data for a new user to be entered. You need to click on Add to apply the change.

Add: Creates a new user account with the user parameters specified in the fields above.

Update: Changes any changes to the currently selected user's information.

Delete: Removes the currently selected user account.

Note: If the extension number entered in for the Business number is a shared number, then the Server Wizard will display a list of ephones (ephone id, ephone user name and router IP address) to allow the administrator to select the ephone associated with this user.
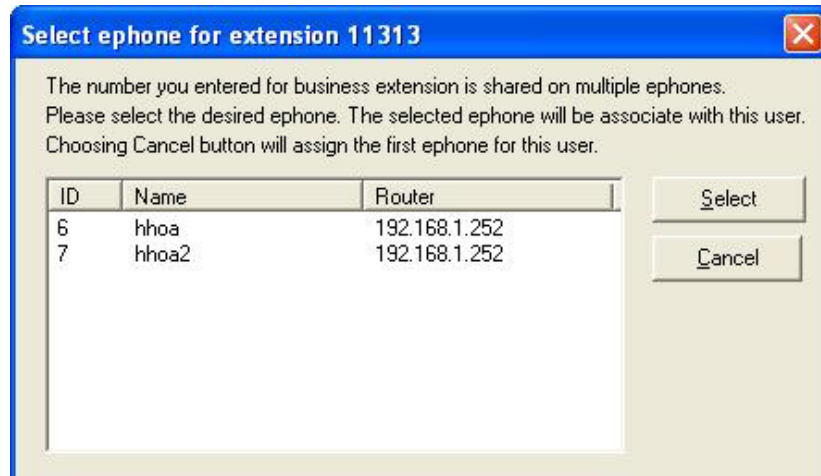
To Update an existing User Account:

- Click on the user name entry in the User Table. It will be highlighted and the user information displayed in the fields to the right.
- Modify the user parameters in the fields to the right.
- Click on the Update button. The highlighted user account information will be replaced with the information entered or changed.

To Add a New User:

- Click on the Clear button to clear the information in the User Parameter fields.
- Enter the user information in the User Parameter fields.
- Click on the Add button. A new entry will be added to the User Table.
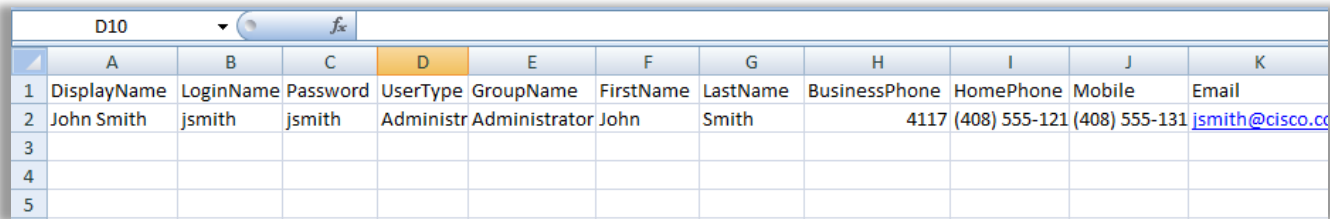
To Delete a User Account:

- Click on the User name that you want to remove in the User Table. This user information will be displayed in the fields to the right.
- Click on the Delete button. The highlighted entry in the User Table will be deleted.

Importing User Information

Administrators can use Microsoft Excel to update user information and import that information using the Server Wizard.

The template text file is provided in the Unified CallConnector Server->Data folder. It is called users.csv. This can be opened with Excel but should be saved back in the Comma Delimited 'csv' format. The header fields and the order of the fields in the text file cannot be changed.

	A	B	C	D	E	F	G	H	I	J	K
1	DisplayName	LoginName	Password	UserType	GroupName	FirstName	LastName	BusinessPhone	HomePhone	Mobile	Email
2	John Smith	jsmith	jsmith	Administr	Administrator	John	Smith	4117	(408) 555-121	(408) 555-131	jsmith@cisco.co
3											
4											
5											

To Add or Update UCC User Information

- Open the users.csv file using Excel. The file can be found in the Unified CallConnector Server->data folder.
- Add and update the user information in the columns of the spreadsheet.
- Save the file in the csv format.
- Open the Server Wizard to the User window and click on the Browse button. Navigate to the updated users.csv file and click OK.
- The user information will be added or updated if the user account already exists in the UCC Server.

Click on Next to continue to with the User's phone Configuration.

Adding Phones to Users

The User's Phone Window displays three tables – User List, Available Phone List and the User's Phone.

Users -- This table displays all the users configured on the Unified CallConnector Server.

User's Phones - For the user highlighted in the Users table, this table displays the phone(s) that are associated with and can be controlled by the user. This is currently restricted to one phone.

Phones -- This table displays all the phones that have been configured for the Unified CallConnector. These phones can be controlled from the Unified CallConnector clients.
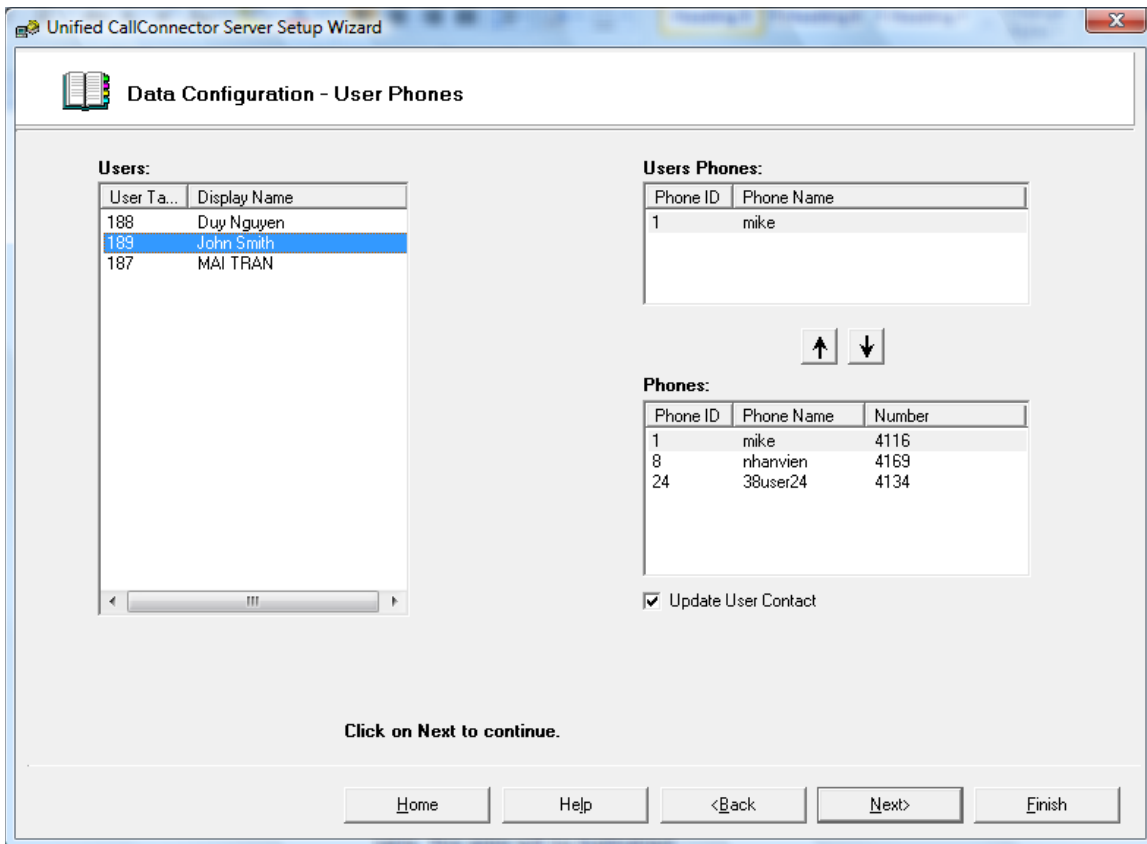
To Associate a Phone with User:

- Select the user by clicking on the user name entry in the User table.
- Click on the IP Phone that you want to have the user control in the Phones table. This entry will be highlighted.
- Click on the Add button to associate this phone with the selected user. The selected phone will be displayed in the User's Phone list.
- 'Update User Contact' checkbox automatically updates the Business phone number with the primary DN on the selected ephone.

Notes

The current release of the Unified CallConnector only supports a single IP Phone per user.

The same IP Phone can be associated with more than one user. However in this situation, all such users have ability to control the call.

To Delete a User's Phone:

- Select the user by clicking on the user name entry in the User table.
- Click on the users IP Phone that you want to delete in the User's Phones table. This entry will be highlighted.
- Click on the Delete button to remove this phone from the user. The selected phone entry will be deleted in the User's Phone list.

Click on Next to continue to Send Email Notifications or Report Problems.

Configuration Management Functions

Sending Email Notifications

The Server Wizard provides a facility to send email messages to the Unified CallConnector users. This email notification facility can be used to send messages to selected users or to all the users.

The Email Notification feature allows you to automatically append the following information with the email:

Append Login Information: When this option is selected, the user's login name, password and serial number are included in the body of the email massage. Each user is send only their login information.

Attach Default Configuration File. The Unified CallConnector client configuration options are saved locally in an xml file. The default configuration file allows the administrator to pre-define or customize this configuration file for the users. When the option is selected, then the configuration file is sent as an attachment.

Quick Reference. This option allow you to attach notes or other documents in the notification email to the user.
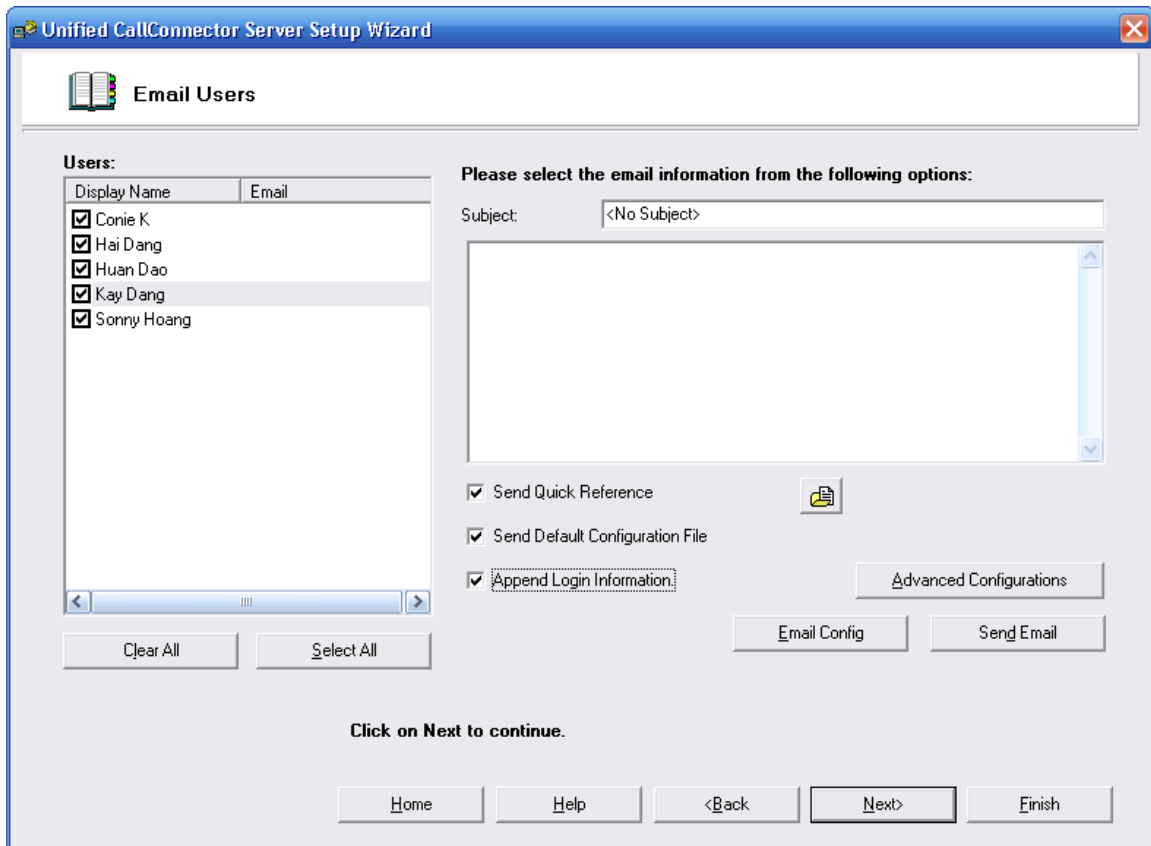
Components of the Email Notification Window

User List:
This table displays a list of the Unified CallConnector users and their email addresses. The check box beside each user allows you to select that user to receive the email message.

Subject: Email subject text for the notification message.

Message Body: Text of the email to be sent to the users.

Buttons:

Clear All: Clears all the selections in the User List table.

Select All: Selects all the users in the User List table to receive the email message

Append Login Information: Automatically adds the user's login name, password and serial number in the email message.

Default Configuration File: Attaches the administrator customized configuration file to the email message.

Advanced Configuration: Opens the configuration file to allow site specific values to be entered.

Quick Reference: Allows you to attach a selected file such as a Quick Reference document to be sent to the user.

Email Config: Opens a window for setting the email account information.

Send Email: Sends email to the selected users.

To Send the Users a Notification Email Message:

- Select the users that you want to send the email message. Click on each user or click on Select All to select all the users.
- Enter the subject and email text.
- Click on the optional information that you want to attach with the email message.
- Click on Send Email to send the message.

To Setup the Email Account:

- Click on the Email Config button in the Send Email Notification window.
- Enter the SMTP email server information and the account you want to use to send the email messages.
- Click on OK to save the information.

Unified CallConnector Server Setup Wizard

Email Configurations: Smtp Settings

Smtp Server:	smtp.1and1.com
Port:	25

☑ Authentication Required

Name:	Shahryar
Email Account:	alukder@callcomm.com
Password:	***********

[OK]   [Cancel]

Advanced Configuration Parameters

The Advanced Configuration Parameters provides a mechanism for the administrator to customize and distribute standard user configuration parameters during the installation process.

The user login/account information, software serial number and UCC client configuration data can be sent to the user via email. This can simplify the UCC client installation as most of the installation parameters can be read from this file by the install program.

When the client install is run, it looks for this configuration xml file in the user's desktop.

The Configuration parameters that can be customized are described below:

Unified CallConnector Server Setup Wizard

Click on the value columns to change:

Parameters	Value
Extension Length	4
Office Code	101
UCC Server Address	192.168.1.14
Local UCC Port	5060
Use Local TAPI Driver	0
Use UCC Server	1
Enable SMTP	1
Authentication Required	1
SMTP Server Address	smtp.yourcompany.com
SMTP Port	25
Phone Services URL	localhost
Phone Services Port	80
MAPI Profile Name	Outlook
Start Services Automatically	1
Local Host	localhost
Local SIP Server Port	5061

OK   Cancel

To Customize the Configuration Values:

- Click on the Advanced Configuration button and change the parameter values.
- Click on OK to save the changes. These settings will be sent in the email to the user by selecting the Default Configuration file option.

Reporting Problems

To report problems to the Unified CallConnector, select all or the desired trace files. Enter the description of the problem and the steps for reproducing them and click on Send Problem Report to send the email with the attachments.

CHAPTER

6

Configuring UCC Mobility

This chapter describes how to configure and setup the Unified CallConnector Server applications and covers the following areas.

Configuration Overview - Provides an overview of the configuration steps for the Unified CallConnector Mobility Service.

Pre-requisites Summary of the information and configuration required for the Mobility Service.

CME Setup for Mobility - Provides an overview of the Cisco CME and Cisco CUE parameters required for Mobility.

Registering UCC Mobility - Describes the steps to register the Mobility License.

Setting up Mobility Ephones - Describes how to download and select the mobility ephones.

Mobility Server Setup - Describes the options for setting up the mobility server communication parameters.

Mobility System Parameters - Describes the system parameters for the Single Number Reach and Dial-In Access features.

Allocating ephones - Describes how procedure for allocating the ephones to the mobility applications.

Creating Pools - Describes the steps for creating the mobility ephone pools.

Setting up Holiday Schedules - Describes how to setup the holiday and business work day and work hours.

Mobility Configuration Overview

The following summarize the steps for configuring the Cisco Unified CallConnector Mobility Service:

Step 1: Registering the UCC Mobility Server License

- The UCC Mobility Server applications require the purchased licenses to be registered with the Cisco site. The licenses can be registered/activated during the installation process or from the Server Wizard.

Step 2: Setting up Automation/Mobility Server Connection Parameters

- Verify the default settings or enter the IP address and ports for the communication protocols used by the Automation/Mobility Server.
- Setting up the Single Number Reach and Dial-In Access system parameters.

Step 3: Setting up Mobility System Parameters

- Setting up the Single Number Reach and Dial-In Access system parameters.

Step 4: Select the Mobility Ephones

- Selecting the ephones to be controlled by the UCC Mobility Server.

Step 5: Add the Mobility-Ephones to the Mobility Application Pools

- Allocate the Mobility-Ephones to the Single Number Reach and Dial-In Service.

Step 6: Verify the UCC Mobility Server configuration.

- Verify that the configuration parameters are correct and the server applications are functioning.

Automation/Mobility Server

The Unified CallConnector Mobility Service is provided by the Automation/Mobility Server. This Mobility Server needs to be installed and registered with the UCC Server. The Mobility Server uses the call control, data access and the presence services from the UCC Server.

The Automation/Mobility Server stores the users single number reach rules. It monitors the state of the user calls, presence status and their personal rules. When a rule is triggered, then the Automation/Mobility Server launches a task to execute the actions specified in the user's rule.

Note: The Mobility Server runs as an add-on to the UCC Server.

Configuration for Single Number Reach Service – Summary

Single Number Reach	What needs to be setup
Select Mobility ephones for the SNR Service	This specifies the ephones that have been configured in the CME for use by the Mobility Service. These ephones must have the option 'Connect as Mobility Ephone' checked and must be configured with a virtual MAC-address.
Configure SNR System parameters	The administrator can set a number of system wide parameters for the Single Number Reach service. These include: Maximum number of reach out calls for each user Maximum number of concurrent SNR sessions Answer timeout --- the maximum wait time for a call to be answered Enable/Disable the Mid-call features In addition the administrator can set the caller-id transmission rules.
Setup holidays and work hours	The administrator can setup a schedule for the holidays observed and the working hours (start and end times) and the working days for the organization.
Add the Mobility-ephone to the SNR pool	The ephones that have been configured for the Single Number Reach service need to be selected for the SNR application allocating them to the mobility applications
Update user contact information for voice mail box and SNR PIN number	For the Single Number Reach service, the users need to have the voice mail box and the SNR PIN or password configured. Users can update this information from their Popup application.

Configuration for Dial-In Service - Summary

Dial-IN Access	What needs to be setup
Select the additional Mobility ephones for the DISA Service	This specifies the additional ephones that have been configured in the CME for the Mobility Dial-In Service. These ephones must have the option 'Connect as Mobility-Ephone' checked and must be configured with a virtual MAC-address.
Configure Dial-In System parameters	The administrator can set a number of system wide parameters for the Dial-In Access service. These include: Enable/Disable the Dial-In Access Restrict only to calls from telephone numbers configured UCC Corporate directory Always require Dial-In password Specify the pick-up numbers or use the DISA ephone-DNs In addition the administrator can set the caller-id transmission rules for DISA.
Add the Mobility-ephone to the DISA pool	The ephones that have been configured for the Dial-In Service need to be selected for the DISA application allocating them to the mobility applications

CME Configuration for UCC Mobility

The Unified CallConnector Mobility Service makes use of additional features of the Cisco CME and Cisco CUE. These features have to be provisioned on the Cisco CME and Cisco CUE and then the corresponding parameters have to be configured on the UCC system. Chapter four of this document provides a step-by-step tutorial on how to setup the Cisco CME and CUE parameters for the UCC Mobility Service. The configuration steps are summarized below for reference.

CME/CUE Setup Summary for Mobility Service

Function	What needs to be setup
Mobility ephones and ephone-DN	The Mobility Service uses ephones for answering the Single Number Reach calls and for making the reach out calls. These ephones need to be configured in the CME. The mobility-ephones have specific attributes: A 'virtual MAC-address' is assigned to each mobility-ephone. Each ephone needs to have at-least three single-line ephone-DN configured Ephones need to have Ad-hoc conference control capability
CME Conferencing Options	The Mobility Service uses the CME conferencing feature to bridge the caller and user calls. Both hardware and software conferencing is supported by the Mobility Service. However hardware conferencing is required for the Mid-call and DISA features.
Transfer to Voice Mail	A voice mail box must be configured for each user with SNR service. The Cisco CME and CUE also have to be setup to allow the transfer of the call directly into the user's voice mailbox. Several methods for transferring a call to a user's voice mail are supported by the Mobility Service.
Hunt Group for the DISA numbers	A hunt group can be setup to sequentially hunt for an idle DISA Mobility-ephone.
Additional Mobility ephones and ephone-DN for the DISA service	Sufficient numbers of mobility-ephones need to be configured for the Mobility DISA service.

Pre-Requisites for Mobility Configuration

The configuration of the Unified CallConnector Mobility Service involves the following steps:

- Purchased license and PAK-ID for the Mobility Service.
- Configuration of the Cisco CME for the UCC Mobility parameters.
- Configuration of the Cisco CUE parameters for the Mobility Service.
- Installed and configured UCC Server.

The following capabilities need to be configured on the UCC Server to support the Mobility Service:

- The Mobility Service applications need to be installed and registered (activated).
- UCC Presence Server needs to be setup to receive the RADIUS messages and be able to look up numbers in the contact directory.
- For each router, the location, dialing access codes, CUE routing methods have to be setup.
- Dialing translation rules for making calls and looking up numbers has to be setup and verified.
- The Mobility Ephones have to be specified for each router.

Registering UCC Mobility Service

For the Single Number Reach, Mid-Call and Dial-In Service features, the UCC Server with Mobility Services has to be installed and the Mobility Service has to be registered.

The UCC Server applications can operate in two modes:

> UCC Server only
>
> UCC Server with Mobility Service

The UCC Server provides presence, telephone status, centralized logs, and instant messaging features. The UCC Mobility Services adds the Single Number Reach, Mid-Call and Dial-In Access Services. UCC Server is required to be installed and registered for the UCC Mobility Services.

When the UCC Mobility Service is registered, the Server Wizard will display the Automation/Mobility Server options and enables access to the mobility configuration pages. To register the Mobility Service you will need the PAK-ID with the UCC Mobility key enabled. The Mobility Service can also be run in an evaluation mode for a 45-day period. This evaluation mode has to be enabled during installation.

To Register UCC Mobility (On-Line Activation)

- Start the UCC Server Wizard from Programs ->Cisco Systems->Unified CallConnector Server-> Cisco Unified CallConnector Server Wizard and go to the License Information page.
- Select UCC Mobility Server in the UCC License Status table.
- Enter the Mobility Server PAK-ID and your email address and click on the Activate button.
- If the activation is successful, then the Status field will display SUCCESS.

.

Notes:

1. The activation process uses the Internet to register the PAK-ID or serial number and your server machine information to the UCC License Server. This process requires access to the Internet.
2. The PAK-ID can be activated on only one physical machine.
3. Virtual Windows environments such as VMWare are not supported.

To Register UCC Mobility (Email License Delivery)

- Enable the check box "Advanced Licensing Option" and click on the Cisco Registration Site button.

- This will take you to the Cisco License site. Log in with your CCO account.

- Enter the PAK-ID and click on Submit to view your purchases.

- If you have already generated a license file for the UCC Server, then select the UCC Mobility, otherwise you can select both the UCC Server and Mobility options. Make sure you select Quantity one for each. Do not select any UCC Client licenses.

- Enter the Machine ID and CPU ID by copying and pasting from the Server Wizard page.

- Once you have received the license file, save it on the desktop and use the browse button on the License Information page to select the file.

- The Mobility Server License status should change to indicate valid license.

Configure Mobility-Ephones

The UCC Mobility Service is comprised of the Single Number Reach and Dial-In Access applications. Each o these mobility applications use ephones to answer the incoming call and make the outgoing calls. These ephones have to be provisioned in the CME and then configured for the Mobility Service using the UCC Server Wizard.

The ephones provisioned in the CME for use by the mobility applications are referred in this document as the mobility-ephones.

Notes on Mobility Ephones

1. The mobility-ephones can be provisioned for two different types of usage – mobility-ephones that can be used to process any user's mobility service requirements and dedicated mobility-ephones which can only process one specific user's mobility service requirements. The dedicated mobility-ephones typically have a shared appearance DN of the user's primary DN.
2. Mobility application use ephones from the router to provide voice prompts to the callers. In multiple router configurations, the mobility-ephones need to be configured on each router.
3. For incoming calls to the Dial-In Access features, the mobility-ephones are used from the router that received the PSTN call.
4. Mobility-ephones are allocated to the Mobility applications using the Server Wizard in groups or pools. Such pools can be shared among multiple mobility applications or they can be 'dedicated' to a single mobility application.
5. The mobility applications acquire the needed ephones form the pools and return them back to the pool.
6. If there are multiple pools associated with the application, ephones are acquired first from the dedicated pools, if none are available then from the shared pools.
7. The mobility applications use one ephone for the duration on the session with the following exceptions:
8. One additional ephone is used when setting up a new call. For example if the Single Number Reach application is making two simultaneous reach out calls, then two additional ephones are used, one for each call. Once the reach out call is processed, the call is terminated and the ephones are returned to the pool. These ephones will typically be in use for less than a minute.
9. If Mid-Call features are enabled, then the SNR session continues for the duration of the call. If Mid-Call features are disabled then all ephones for the SNR session are freed up once the SNR connection is made or the call is sent to voice mail.

Number of Ephones for Mobility Services

The following model can be used to calculate the number of mobility ephones on the CME. The variables include:

- Number of Concurrent SNR Sessions (MAX-SNR): This parameter sets the maximum number of SNR sessions enabled for the Mobility Service.
- Maximum Number of Reach-out calls (MAX-CALLS): This is the maximum number of simultaneous calls made to the user's numbers. This number can be set from the Server Wizard to be from one to four.
- Maximum Number of DISA calls (DISA-CALLS): This is the number of incoming calls allowed to access the Dial-In Access service.
- Shared SNR Numbers (NUM-SHARED): This is the number of shared SNR sessions. Each of these requires a dedicated ephone.

The number of ephones required can be derived from:

- Ephones for General Pool = MAX-SNR + MAX-CALLS
- Ephones for Shared Pool = NUM-SHARED
- Ephones for DISA = DISA-CALLS
- The total number of ephones required for the Mobility Service would be

    (MAX-SNR + MAX-CALLS) + NUM-SHARED + DISA-CALLS

Mobility Ephone Setup

The following is a summary of the configuration steps for setting up the mobility-ephones for use by the UCC Mobility Service.

- Provision ephones for use by the UCC Mobility Service on each CME/UC500.
- From the Server Wizard, download all the provisioned ephones and ephone-DNs.
- Enable the 'Connect as Mobility-Ephone' option before adding the mobility-ephone.
- Verify that the ephones have been provisioned correctly with the required ephone-DNs
- Allocates the ephones to the mobility applications.

Provisioning Mobility Ephones

Mobility ephones need to be provisioned on the routers as described in the previous chapter. You can verify the configuration of these ephones using the 'Show Ephone' command from the Command Line Interface (CLI). Examples of the mobility-ephone is showed below.

ephone-28 Mac:AAAA.BBBB.4307 TCP socket:[124] activeLine:0 REGISTERED in SCCP ver 3 and Server in ver 3

mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:3

IP:192.168.1.14 1889 Telecaster 7960 Telstrat keepalive 132 max_line 16

button 1: dn 648 number 4648 CH1   IDLE

button 2: dn 649 number 4649 CH1   IDLE

button 3: dn 650 number 4650 CH1   IDLE

Username: 38user28 Password: Cisco

Note:

1. Each mobility-ephone has a virtual MAC Address. In this case AAAA.BBBB.4307.
2. Three single channel DN are configured for the ephone

Download CME configuration

The Server Wizard uses the CLI commands over a Telnet connection to download the ephone, ephone-DNs and the hunt group details from the CME. This is a manual step that needs to be repeated if the CME configuration is changed. In multiple router configurations, the ephone details and selection for the UCC needs to be repeated for each router.
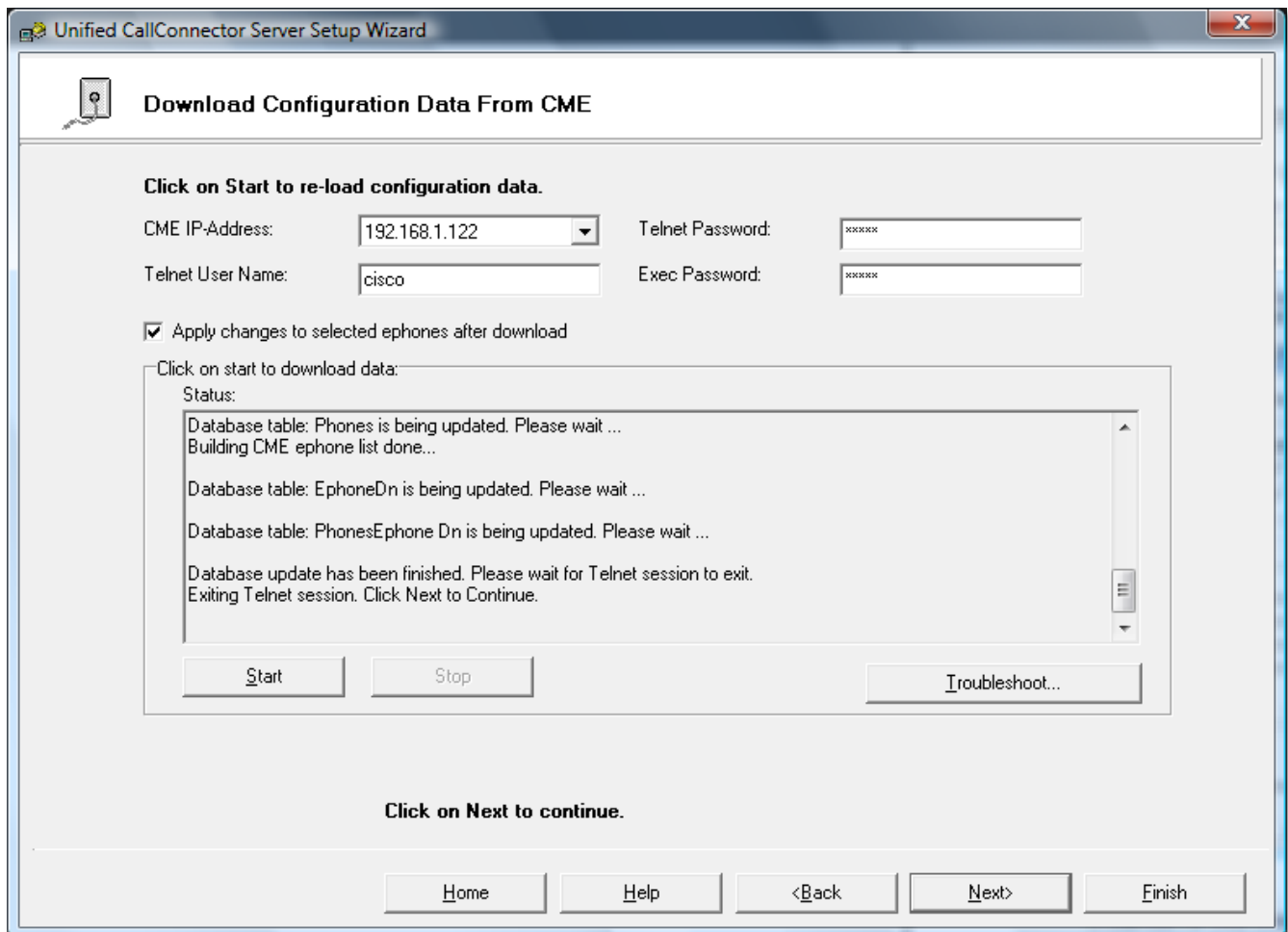
To Download CME Configuration Data

- Open the Server Wizard to the CallController Server and click Next to go to the 'Download Configuration Data from CME' page.
- Enter or select the CME IP Address, the Telnet account name and passwords.
- Click on Start. The status messages will provide feedback on the progress. Note this step may take some time as the Wizard logs in using the Telnet account and obtains the CME configuration information using:

'Show ephone' for ephone configuration
'Show run' for the ephone-DNs
'Show ephone-hunt' for the hunt groups.

The downloaded information is saved in the UCC Databases.

Select Mobility Ephones

The 'Download CME configuration data' downloads the details on all the ephones in the CME. The 'CallController Server: Select Ephones" page displays this list of ephones in the Ephone tables. This includes the ephones provisioned for use by the Mobility Services. In this configuration step, these mobility-ephones are identified to the UCC system.
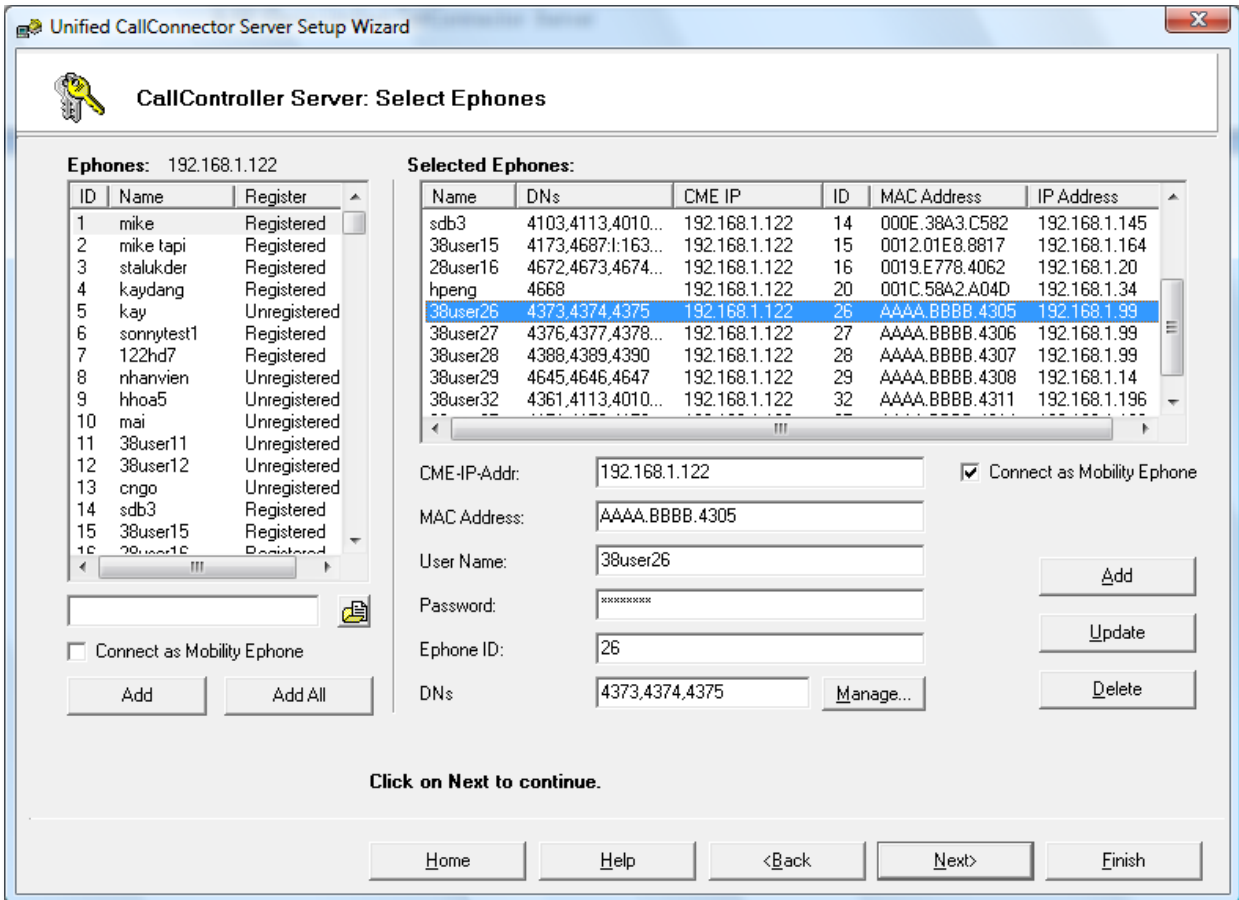
To Select the Mobility Ephones

- From the Ephones list, select one or more of the mobility-ephones. You will need to know the ephone id or the assigned DNs. (Note DNs may not be visible as these ephones will not be registered.)

- Check the 'Connect as Mobility-Ephone' option and click on the Add button below the Ephones list. The 'Selected Ephones' table will display this ephone. The 'Selected Ephones' table contains both the user IP Phone ephone and the mobility ephones.

- Verify the mobility-ephone configuration details in the fields below the 'Selected Ephones' table.

- Repeat this process for all the Mobility-Ephones.

Verify Mobility Ephones

The 'Verify Connection to Ephone' allows you to connect to the CME and register to the selected ephone and verify that the parameters are accurate and that connection can be established to the CME.
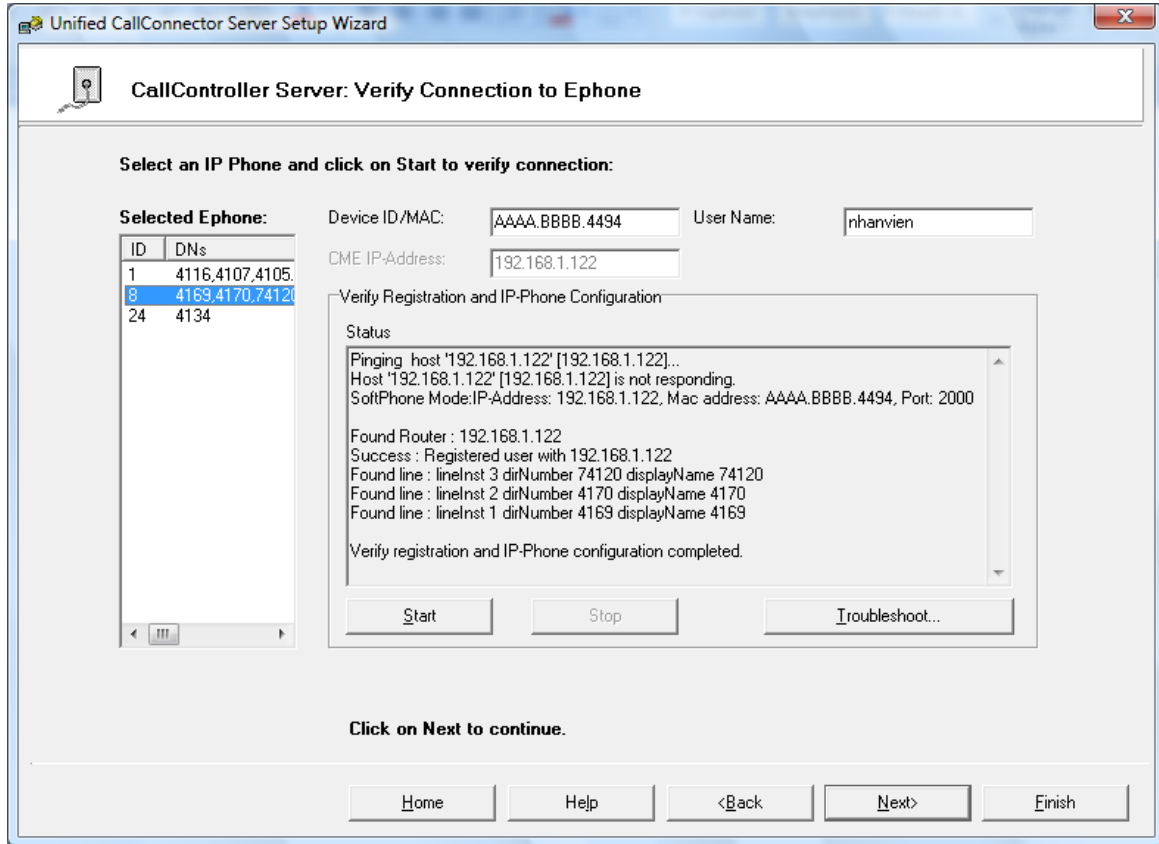
- Click on each ephone and then click on Start

The Wizard will register to that ephone and display the ephone line configuration details.

Automation/Mobility Server Setup

The Unified CallConnector Automation/Mobility Server reads in the user rules and monitors the user's presence and telephone status information. The Mobility Server communicates with the UCC Server components – Database Server, CallController Server and Presence Server to implement the mobility services.

Mobility Configuration Notes

1. The Presence Server publishes the list of contacts in the Corporate directory database grouped by their departments. It also manages and publishes the presence status (availability and location) and the telephone status of these users in real-time.
2. Contacts in the Corporate directory can be UCC users and non-users. A UCC user has a user login account created via the Server Wizard. Presence status is published for both types of users.
3. For the telephone numbers to match, the caller/called number and the numbers in the database must be in the same format – preferably in the canonical format. This requires the server dial plan to be correctly setup.
4. The Presence Server filters out telephone status messages from telephone numbers that are not in the UCC Corporate Directory. Even though you might see the Radius events for a phone number, the telephone status may not display in the Status window. Therefore to receive telephone status events, the following must be properly configured:
5. Router must be configured to send Radius messages to the UCC Server.
6. UCC Server must receive the Radius messages.
7. The telephone numbers (caller or called) must be in the Corporate Directory.
8. The UCC Server Dial plan must be properly setup so that the numbers as provided in the Radius messages can be formatted for lookup. This means that after lookup formatting the incoming number will be identical to the 'canonically' formatted number in the directory.

Mobility Server Failure Impact

- If the Presence Server fails, then:
- Status windows in the UCC Clients are grayed out.
- Users cannot change their presence status.
- Status displayed in the QuickSearch will not be current.
- Call Logs are not written and are lost for the duration that the Mobility Server is down.
- The Mobility Services including the Single Number Reach will not work.
- Other UCC servers are un-affected.

There are two aspects to the Mobility Server configuration – setting up the communication parameters to handle the SIP messages and setting up the Mobility application system parameters. (Uncheck 'Show basic Configuration Pages' to view this page).

If you have selected the Trace Log and Password options to apply to all the UCC Server applications and wish to take the default settings for the Mobility Server, then click on Next to continue to the next window.

Mobility Server Communication Parameters

- SIP Server Address: This is the IP address or network address of the computer with the System SIP Server.
- Port: This is the port used by the Mobility Server to receive messages. The default value is 5072 to 5077 over which TCP and UDP connections are supported. If these ports are not available, then change the base port number to a port range available on the computer.
- Username: This is the well-known name of the Automation Server. This cannot be changed.
- Password: This password is used to authenticate the registration of the Presence Server. Enter the password. This can be any text or number string up to twelve characters in length.
- If asked by Cisco Technical Support, enable the debug trace logging and set the Trace level to the requested level. This is checked at server startup only.

Click on Next to continue.

To Set the Mobility System Parameters:

To setup Automation Mobility Service, click on Windows

Start button -> All Programs -> Cisco Systems ->
 Cisco Unified CallConnector Server -> Cisco Unified CallConnector Server Wizard.

Select Automation/Mobility Server from the home menu and click on Next once. The Automation/Mobility System Parameters window will display. The system configuration parameters for Single Number Reach (SNR) and Dial-in System Access (DISA) features are displayed and can be modified.

Single Number Reach Parameters

If you want users to access to the Mid-Call Features then you can check **Allow mid-call to features access** to enable the feature.

The option **Maximum number of calls to locate user** limits the number of simultaneous calls can be made to a user per incoming call.

You can decide the timeout interval (in seconds) for user to answer the reached call. Also, you can specify the maximum number of SNR session to be established concurrently.

Dial-In Access Parameters

In the Dial-in-Access Options, you can enable the DISA features by checking **Allow Dial-in access**.

If you don't want to allow users to access the DISA features from phones that are not in users' contact directory, you can check **Restrict Dial-in to user contact numbers** to restrict users to access the DISA features from their work, home or mobile phone only.

If additional security is required, you can require every user to provide DISA password before they can access the DISA features by checking **Always authenticates with dial-in password**.

Caller ID Transmission (Requires PSTN support)

For both SNR and DISA applications, you can decide whether you want users to be able to view the caller's number when there's an incoming call or they try to reach to other contacts by checking **Show caller number for Mobility Service Calls.**

 You can specify if the length of the caller number is less than certain digits then the caller number either will be transformed to a full length custom PSTN number or the caller number will be appended to the custom prefix number with **as prefix** checked.
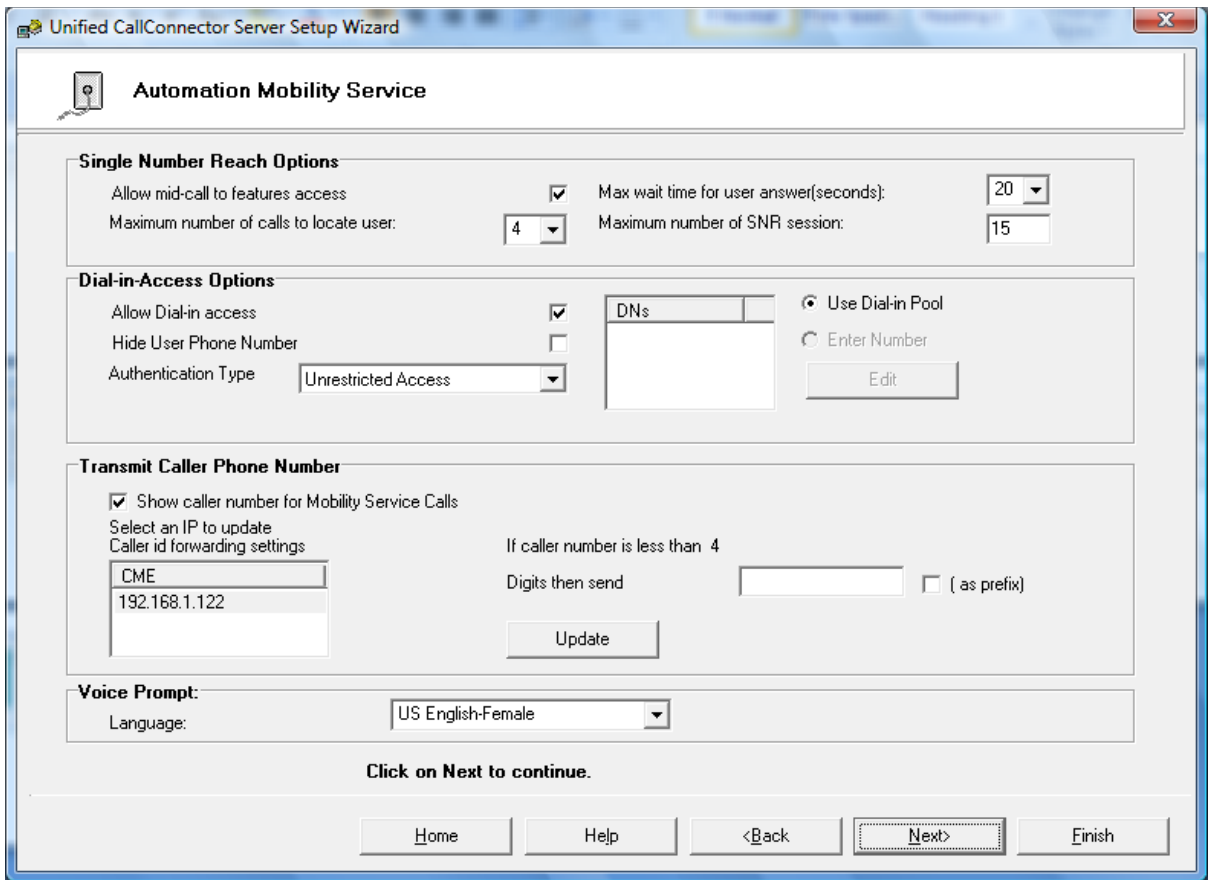
Single Number Reach Options:

Options	Description
Allow mid-call access to features	Check to enable/Uncheck to disable the Mid-Call Features after a SNR session is established.
Maximum number of calls to locate users	Select a number to set the maximum number of calls can be made to locate users.
Timeout for user answer (Seconds)	Select a timeout period (in seconds) for the SNR to hang-up the calls if users cannot be located.
Maximum number of SNR session	Define a maximum number of SNR session can be established concurrently.

Dial-in Access Options:

Options	Description
Allow Dial-in access	Check to enable/Uncheck to disable the Dial-in Access Feature.
Hide Caller Phone Number	This options hides the user personal telephone number by not transmitting it as the caller id, instead the mobility ephone number is displayed.
Authentication Type	Select one of the following Dial In Access Authentication Type from the poll-down list:
	Unrestricted Access: All callers are allowed access to the DISA features.
	Require DISA Password: Check to enforce Dial-in password authentication.
	Restrict Numbers: Only allow calls with calling numbers that are specified in the corporate directory
	Restrict # and Password: Restrict to calls from numbers in corporate directory and additionally require DISA password.
Use Dial-In Pool	This option indicates that the Dial-In Access should answer incoming calls the ephones defined in the ephone pools specified for this feature.

* If the extension number you enter or dial from is shared by other users, you'll still be prompt for your dial-in password even with the option "Authenticate with Dial-in password" disabled.

Transmit Caller Phone Number:

Options	Description
Show caller number for Mobility Service Calls	Check to enable/Uncheck to disable showing caller number to the contacts who are receiving Mobility Service Calls.
If caller number is less than x digits	Specify the length of caller number to be transformed to a custom number.
Fixed number to be sent	Specify the custom number that will be used to display the caller's number.
As prefix	Check to indicate the custom number is a prefix number to be pre-pended to the caller number.

Note: The internal number length and the prefix or fixed number for transmission as the caller-id is specified per router. In multiple router configurations, select each router and setup the parameters.
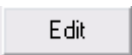
Assign ephones to Mobility Applications

A set of ephone pools or groups for each of the Mobility application is setup by default. You can assign the mobility-ephones from the "Available Ephone" list to a mobility application.
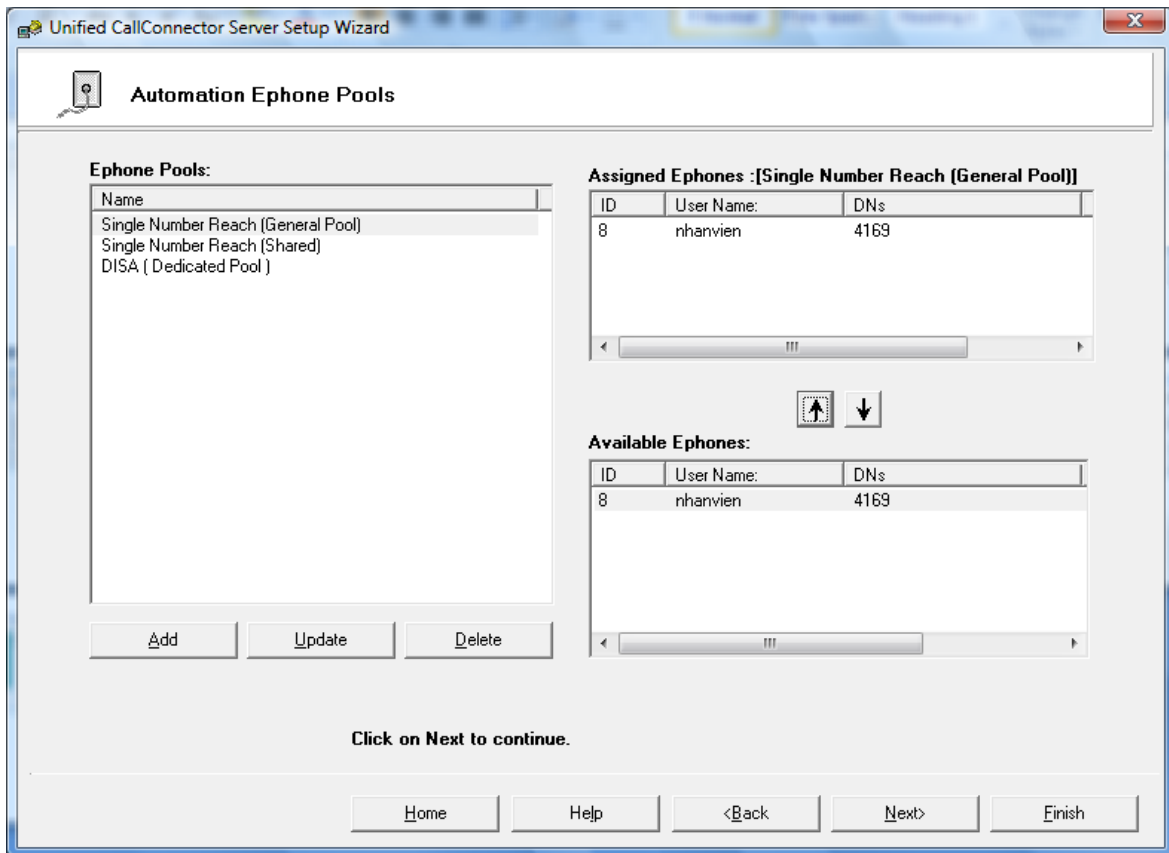
- Select the mobility application or Ephone Pool from the table on the left.

- Select a mobility-ephone from the available ephone list then click ⬆ to allocate the ephone to the mobility application. The ephone being assigned will be listed in the "Assigned Ephones" list.

- Repeat for all the ephones you want to add this ephone pool or mobility application.

- If you want to remove an ephone from the ephone pool, select an ephone from the assigned ephone list and click ⬇ to remove.

Tables	Description
Ephone Pools	A list of ephone pools currently setup for Mobility applications.
Assigned Ephones	A list of ephones that are assigned for the ephone pool selected in the ephone pool list.
Available Ephones	A list of ephones that is available to be assigned to ephone pools.

Buttons	Description
↑	Assign an ephone from the available ephone list to a selected ephone pool.
↓	Remove an ephone from the assigned ephone list.
Add	Add a new ephone pool.
Edit	Edit a selected ephone pool.
Delete	Delete a selected ephone pool.

Allocating Phones to Dedicated Pools

These ephones are associated with individual users.

After you setup one or more ephones that have shared-DNs, you would need to create a separate ephone pool for Share-Call Appearance. When you create a new ephone pool, make sure that you select 'Yes' on the "Dedicated" option and assign applications to the ephone pool from the available application list.

Creating Ephone Pools

There are two different types of ephone pool. One is general ephone pool and the other is dedicated ephone pool. The following table shows the comparison between the two different ephone pool types:

	General	Dedicated
Sharing	The general ephone pool can be shared by different mobility applications	The dedicated ephone pool can only be used for one application at a time
Applications	SNR w/o Share-Call Appearance DISA Features using Mobility Phone	SNR w/ Share-Call Appearance DISA Features using Dial-in Pool

At least one general ephone pool is required for the Single Number Reach (SNR) to work. If you want to use the Share-Call Appearance feature, then at least one dedicated ephone pool will be needed. The following table illustrates the required ephone pool setup for various Single Number Reach functions:

General Phone Pool / Dedicated Phone Pool

SNR Functions	Enable	Disable
Share-Call Appearance	Dedicated and General	General
Mid-Call Features	General	General

The following window allows you to add, update, and remove ephone pools; it also let you assign available ephones to the phone pools.

To Create an ephone Pool

1. To create an ephone pool, click on the ⬚ Add button then an "Add Application Pool" window will pop up for you to assign applications to the ephone pool*.
2. Enter a name for the ephone pool
3. Select YES if it is a dedicated ephone pool**.
4. Assign the applications from the available application list to the ephone pool by selecting an application and click on the ⬚ Add → button. Click OK when finished.
5. If the ephone pool is dedicated, then only one application can be assigned to it.
6. ** For Share-Call Appearance, the ephone pool needs to be dedicated.
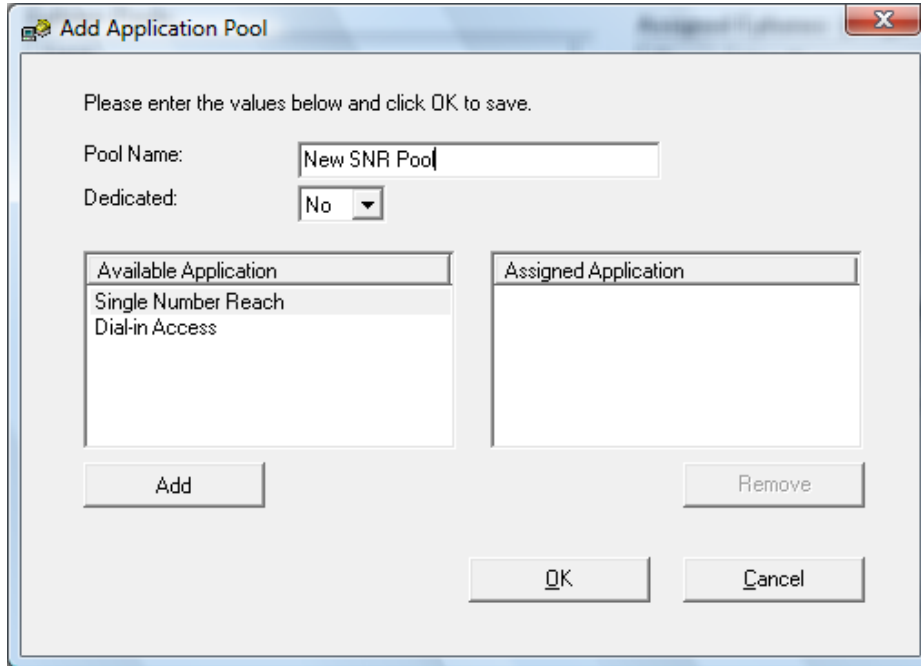
Buttons	Description
	Add a selected application from the available application list to the ephone pool.
	Remove an application from the selected application list.

Options	Description
Pool Name	Assign a name to identify the ephone pool.
Dedicated	Select "Yes" to make the ephone pool dedicated.
Available Application	Applications that are available to be assigned for the ephone pool.
Selected Application	Applications that are added to the list will use the ephones in the ephone pool to make calls.

Holiday and Work Day/Time Schedules

The holiday and work day and work hours are used in the user specified rules for call routing. This Wizard page Holiday Schedule lets the administrator setup this information for the organization.

To Setup Holiday Schedule

- Select the Holiday date from the calendar button.

- Enter the name or description of the holiday and click on Add.

- To Update a Holiday, select that holiday in the Holidays list. Make the changes in the Date and Description fields and click on Update.

- To Delete a Holiday, select the holiday from the Holidays list and click on Delete.

To Setup Working Hours

From the pull down list select the start and end times to set the working hours for the organization.

To Setup Working Days

Check the days which are working days for your organization.

Update User Contact Details

Voice Mail, Tel PIN and DISA PIN have been added to the user's contact information.

Voicemail: This is the user's voice mail box number. By default this is set to the Business number.

Tel PIN: This is the password entered to authenticate the user for SNR calls.

DISA PIN: This is the user's password for using the Dial-In Access features.

CHAPTER

7

Starting and Stopping Services

This chapter describes how to start and stop the Unified CallConnector Server applications and verify that the services are running.

This chapter describes the following in more detail:

Using UCC Services Manager –Describes how to start and stop the Unified CallConnector Server applications using the Services Manager application.

Using Windows Services - Describes how to start and stop the Unified CallConnector Server applications using the Windows Services program.

Verifying Operation - Describes how to verify that all the server applications are running properly.

Starting/Stopping Server Applications Server

These Unified CallConnector Server applications run as Windows services and do not have any user interfaces. When the applications are running their status can be viewed in the Windows Task Manager and Services application.

The Unified CallConnector Server applications can be started in two ways:

From the CTI Services Manager Application
From the Windows Services

Using the CTI Services Manager

The CTI Services manager application is a tool to start and stop the collection of the server applications that comprise the Unified CallConnector server. The CTI Services Manager also displays the current status of each of the CallConnector server applications. It polls the status of the services and displays the current running state.

From the Start-Programs menu, select the Cisco Systems group and select the Cisco Unified CallConnector Server option, then click on CallConnector Service Manager.

The CallConnector Services Manager application will run and display the status of the Unified CallConnector server applications. The CallConnector Services Manager window has a status field that indicates if all services are running or if some are stopped.
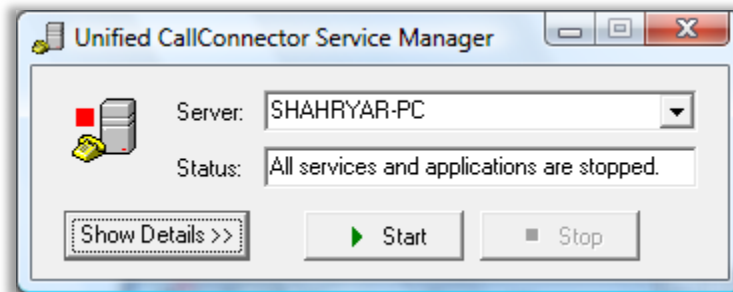
The window has three buttons:

Show Details/Hide Details: This button opens or closes a list of the Unified CallConnector Server applications and their current status – started or stopped.

Start: This button starts all the server applications. This button is only available when all the services are stopped. The services are started in their dependency order.

Stop: This button stops the services. If some services are stopped, then all services have to be first stopped before they can be started from the CallConnector Services Manager.

The window below shows the CallConnector Services Manager with all the services running.
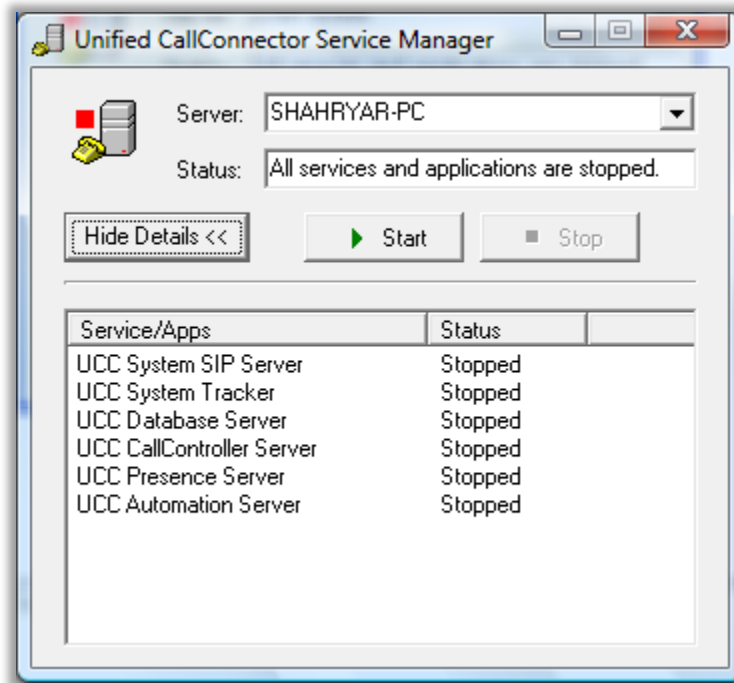
To Start the Server Applications

- Start the Unified CallConnector Service Manager application from the Start-Programs menu.
- If some Server Applications are stopped, then click on Stop.
- If some services do not stop, then open the Task Manager and from the Process window select the Unified CallConnector Server and click on End Process.
- When all the Server Applications are stopped, click on the Start button.

To Stop the Server Applications

- Start the Unified CallConnector Service Manager application from the Start-Programs menu.
- Click on Stop button.
- If some services do not stop, then open the Task Manager and from the Process window select the Unified CallConnector Server and click on End Process.

Minimize to System Tray

- Click on the minimize button, and then will move the Service Manager to the Windows system tray. To re-open, right click and select open.

Using Windows Services Manager

The Windows Services interface displays all the service applications that have been configured for that computer and describes their current status. This window also allows you to start and stop these services. In order for a server application to be displayed in this window, the application has to be configured to run as a service.

The Services management application one of the Administrative tools available with the Windows operating system. To open the Services application, from the Control Panel select Administrative Tools and click on Services.
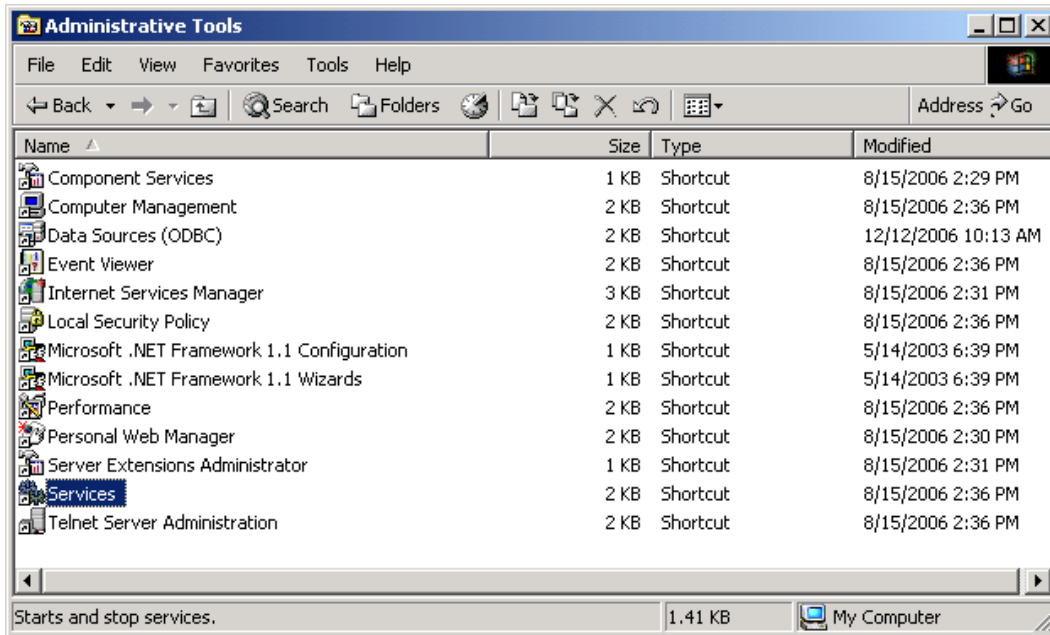
This will open the Windows Services management application. The Unified CallConnector Server applications all start with cc… as shown in the picture below.

From this services window, you can perform some of the following functions:

- Start/Stop a Service
- Setup the service to start with Window Startup
- Define the Recovery actions if the service fails.

The Unified CallConnector installation program will setup the CallConnector Server Applications as manually started Windows services. It also sets the Recovery actions to automatically restart upon failure.

Server Application Dependencies

The Unified CallConnector Server applications should be started in the following sequence:

> System SIP Server
>
> System Tracker
>
> Database Server
>
> CallController Server
>
> Presence Server
>
> Automation/Mobility Server
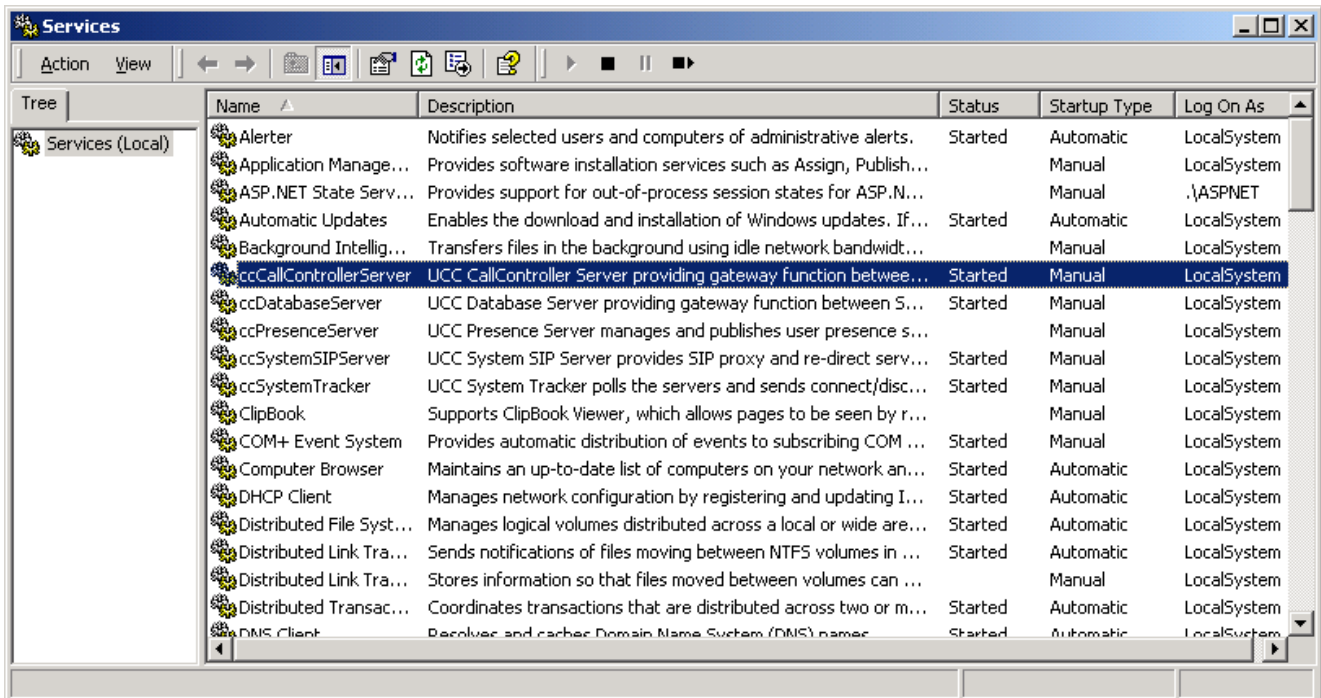
To Start a Server Applications

- Open the Windows Services application from Control Panel->Administrative Tools->Services.
- Select the Service that you what to start by clicking on the service name.
- Click on the Start button or right-click and select Start.
- When the selected service is running, the status will change to Started.

To Stop a Server Applications

- Open the Windows Services application from Control Panel->Administrative Tools->Services.
- Select the Service that you what to stop by clicking on the service name.
- Click on the Stop button or right-click and select Stop.

- When the selected service is not running, the status will change to Stopped. If the service status does not change but displays Stopping, then the Stop operation has failed. Use the Windows Task Manager to End the process.

Starting up with Windows:

The installation program sets up the server applications to be started manually. These applications can also be automatically started when Windows starts.

- Open the Windows Services application from Control Panel->Administrative Tools->Services.
- Right-click on the Service that you what to update.
- From the menu select Properties.
- Change the Startup Type from Manual to Automatic in the General tab.
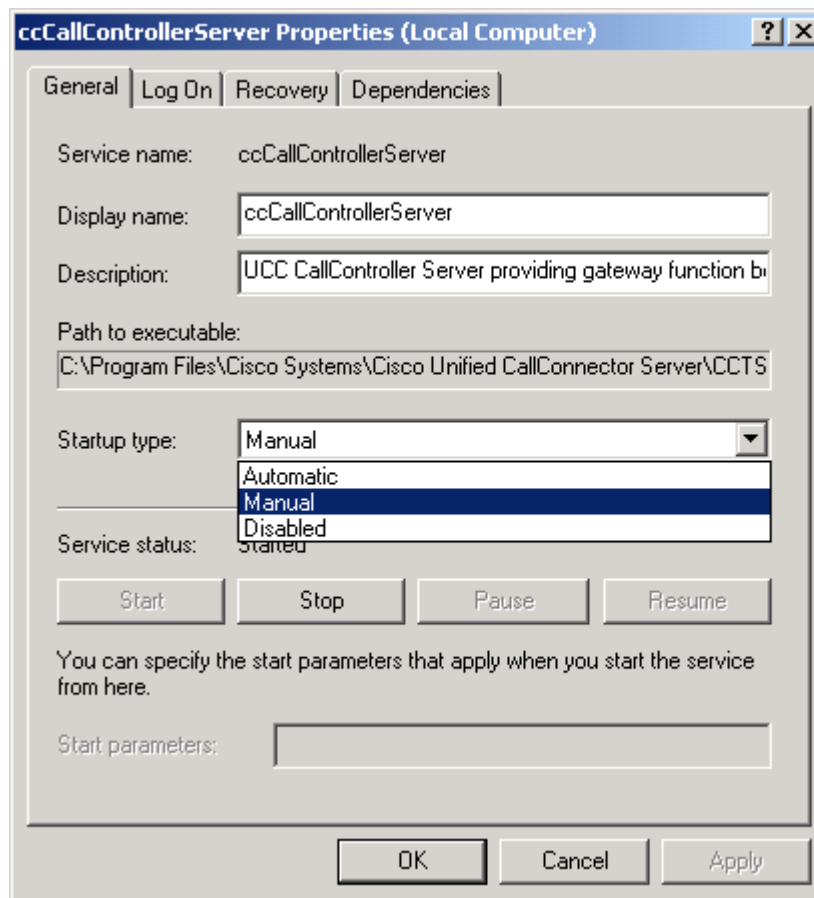
To Modify Recovery Actions

- Open the Windows Services application from Control Panel->Administrative Tools->Services.
- Right-click on the Service that you what to update.
- From the menu select Properties and click on the Recovery tab.
- From the pull down list select the recovery option. By default this is set to restart the service upon failure.
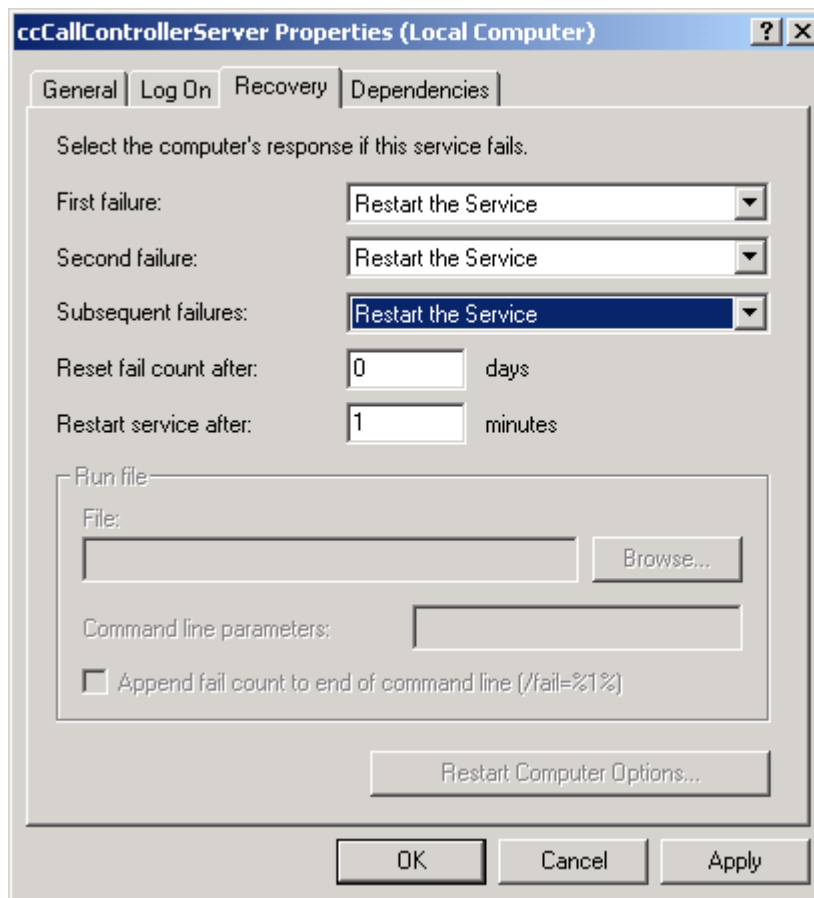
Verifying Server Operation
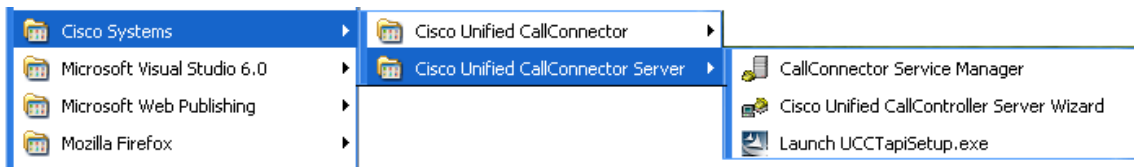
To Stop Unified CallConnector Servers

The Unified CallConnector Server applications can be started in several ways:

- From the CTI Services Manager Application
- From the Windows Services

Stopping Using CallConnector Services Manager

From the Start-Programs menu, select the Cisco Systems group and select the Cisco Unified CallConnector Server option, then click on CallConnector Service Manager.

The CallConnector Services Manager application will run and display the following window.

Stopping from Windows Services

- Open the Windows Services application from Control Panel->Administrative Tools->Services.
- Select the Service that you what to stop by clicking on the service name.
- Click on the Stop button or right-click and select Stop.
- When the selected service is not running, the status will change to Stopped. If the service status does not change but displays Stopping, then the Stop operation has failed. Use the Windows Task Manager to End the process.

CHAPTER 8

Data Management

The Unified CallConnector Server stores configuration, contact and transaction data in databases. This section provides information the procedures for the management of this data. This chapter provides an overview of the Unified CallConnector databases, the server dependencies on the data and the procedures for managing the data. It includes:

UCC Databases:	Provides an overview of the Unified CallConnector databases.
Data Dependencies:	Describes the data requirements for the Unified CallConnector servers.
Managing the Data:	Describes the procedures for maintaining the Unified CallConnector data including backing up and restoring.
Importing Contacts:	Describes the method for importing the corporate database entries.
Transaction Data:	Describes the steps for managing the call log and other Unified CallConnector transactional data.

UCC Database Overview

The Unified CallConnector Server maintains configuration, contact and transaction data in three relational databases - UCCDatabase, Corporate and CallLog. The data is accessed using standard SQL commands through the Windows ODBC drivers. This allows the Unified CallConnector Server to be agnostic to the underlying database system.

For the smaller configurations, the Microsoft Access database is used as the database system.
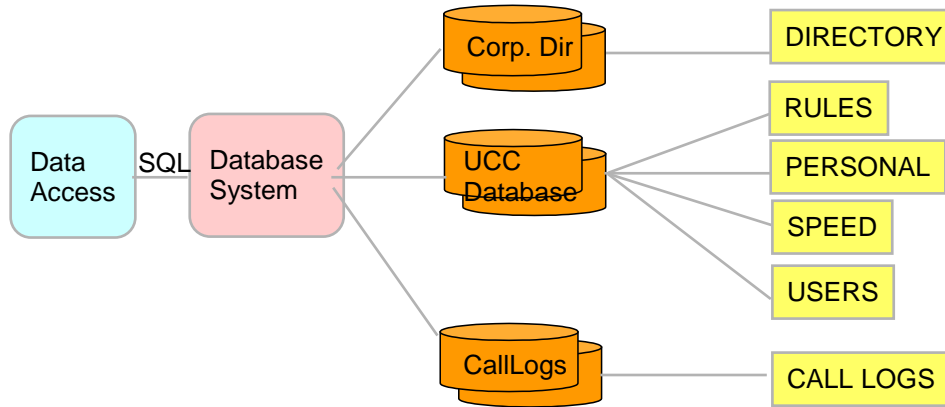
UCC Database

The UCCDatabase maintains the configuration and personal contact information. The main tables and the information they contain is listed below:

USERS - UserID, Login Name, Password, User Type

GROUPS - Group/Department names

PHONES - Phone Name, Password, MAC & IP address

ACCESS CONTROL Blocked users/groups

USER-ASSOCIATION TABLES -- associates user with their resources

PERSONAL – Personal contact data

SPEED – Personal Speed Numbers

RULES -- User's Automation Rules

The information in the Users, Groups, Phones and the Access Control tables are updated through the Unified CallController Server Wizard. The Personal, Speed and Rules tables are updated from the user interfaces in Outlook and Internet Explorer.

Notes on UCC Database

User Login Name

The corporate database can contain both Unified CallConnector user and non-user information. The user login name in the corporate directory distinguishes the record as a Unified CallConnector user. This information is required and should not be changed when the data is manipulated using external database tools.

Department Field

The value in the department field of the corporate database is used to group users in the Status window. In other words the users in the Status view are grouped by the department they belong to. The Status window also displays the number of users in the department that are currently logged in and available.

Telephone Numbers

Telephone numbers in the corporate directory are saved in the canonical format. This means that the number format includes the country code preceded by a plus sign, area code in brackets and separated from the subscriber number with a space. One exception to the canonical formatting is that the country code is not inserted for the current location.

Access Rights

Corporate directory entries can be changed only from administrative accounts. User's can change their contact information from the Popup->Options window. User's can change their availability status using the toolbar buttons.

Corporate Database:

The corporate directory is a key database in the Unified CallConnector server environment. This is used to store shared contact information accessible to all the Unified CallConnector users. The information in the corporate database is used by a number of applications including:

- QuickSearch queries the corporate directory database are returns the resulting results.
- The Corporate window in the Contacts window displays the information from the corporate database.
- The Presence Server generates the Status hierarchical display from the corporate directory data.
- The Presence Server saves the availability status of users in this database. The user's current presence status is displayed in the directory search results.
- Call Logs are generated and written to the call log database only for the Unified CallConnector users. The caller or called number must match one of the user's contact numbers and the user must be a Unified CallConnector user.
- Instant Messages can be sent to Unified CallConnector users. The destination address is obtained from the corporate directory.

The corporate database stores two types of information:

- Shared contact data for the organization.
- Unified CallConnector user contact data.

The Unified CallConnector user information is added to the corporate directory when the users are created using the Server Wizard. Users can change their contact details from the Popup->Options window or from the Contacts->Corporate directory view,

Information about other contacts can be added to the Corporate directory from the Contacts window or imported into the corporate directory.

Notes on Corporate Directory

User Login Name

The corporate database can contain both Unified CallConnector user and non-user information. The user login name in the corporate directory distinguishes the record as a Unified CallConnector user. This information is required and should not be changed when the data is manipulated using external database tools.

Department Field

The value in the department field of the corporate database is used to group users in the Status window. In other words the users in the Status view are grouped by the department they belong to. The Status window also displays the number of users in the department that are currently logged in and available.

Telephone Numbers

Telephone numbers in the corporate directory are saved in the canonical format. This means that the number format includes the country code preceded by a plus sign, area code in brackets and separated from the subscriber number with a space. One exception to the canonical formatting is that the country code is not inserted for the current location.

Access Rights

Corporate directory entries can be changed only from administrative accounts. User's can change their contact information from the Popup->Options window. User's can change their availability status using the toolbar buttons.

Call/Transaction Database:

The CallLog database stores the call transaction logs and the instant message transactions. The transaction data is stored only for the Unified CallConnector users. Several conditions have to be met for a call log to be written to the call log database:

- The Radius service on the router needs to be properly configured to send accounting packets to the Unified CallConnector server.
- The Presence Server has to be running and receiving the accounting records from the router.
- Call Logs are written for the Unified CallConnector users. The users have to be configured using the Server Wizard and their records should be present in the corporate directory.
- One of the user's telephone numbers must match the IP Phone extension number.

Notes on Call Log Directory

User ID

Each call log record is associated with a user based on the user-id parameter. This means the call log is only visible to individual users. If multiple users have the same phone number, then a separate records is written for each user. Users can manage their log entries from the log window.

Name Lookup

The caller and called telephone numbers are matched in the corporate directory to lookup the names. If there is a match then the name is written in the call log database.

Data Dependencies

This section highlights the dependencies between some of the key features of the Unified CallConnector and the data in the database system.

User Authentication

All users need to log in to the Unified CallConnector to access the system features. This authentication is carries out during the SIP registration process. The following data from the Users table in the UCCDatabase is used verify the user account.

- LoginName: This is the login name assigned by the administrator when the user account is created.
- Password: Password used to authenticate the account.

User Type

Each user account needs to be assigned a user type. Three user types are supported – User, Manager and Administrator. The default account type is User. Generally, the user type determines the read/write (or add, modify and delete) rights.

- The user types are defined in the UserType table in the UCCDatabase.
- The foreign key FK_UserTypeID in the user table associates the user account with the type information.

Phone Association and Authentication

Each user account in the Unified CallConnector can be associated with one or more IP Phones. The users are able to view call information from these phone and are able to control these calls.

- The Phones table in the UCCDatabase stores the details of the IP Phones configured in the Unified CallConnector system.
- The UserPhones table maintains the list of the phones associated with the user.

Access Rights

A set of tables contain the list of users and groups that are allowed to access the status informations.

Presence Groups and Users

The Unified CallConnector Status window organizes the user in Groups. This Group is the department that the user belongs to in the organization. Each user can belong to one group.

- The Group names are defined by the Server Wizard and stored in the Groups table in the UCCDatabase.
- The associated between the user and their group is maintained by the UserGroups table.
- Users need to be associated with the groups defined in the Groups table for the access control rights to be applied.

Telephone Status in Presence

The telephone status information is displayed in the Status window. Thus information is only displayed for contacts in the corporate directory whose telephone number matches the extension number of the IP Phone receiving or making the calls.

- Match for the caller and called ID numbers is checked against the BusinessPhone, HomePhone or Mobile numbers in the corporate directory.
- If the number matches then the call state of that number is published to the Status window.

Call Logs for Each User

The call log data is saved in the CallLog database only for UCC users.

- For a call log to be saved in the database the caller or called IP Phone extension number must be in the corporate directory.
- The corporate directory record must be a Unified CallConnector user.

Note: The corporate directory stores both UCC-user and non-user contact information. If you are importing contact information to the corporate directory, the user account information should be maintained.

Maintaining the Data

This section describes how to backup, restore, repair, import, and export the Unified CallConnector databases.

Backing Up Databases

Backing up the directory data allows you to keep a copy of the database for future data recovery. It is recommended to backup your database on a regular basis in order to keep your backup data current.

To Backup the Databases

- Stop the Unified CallConnector Database Server. The server can be stopped from Administrative Tools->Services window.
- Run the Unified CallConnector Server Wizard and go to the Database section.
- Click on the Backup button. The files will be copied to the Databackup folder.
- You can also copy the database files to the backup folder. The Access database files have the .mdb extension.
- Restart the Unified CallConnector Database Server.

Restoring Databases

If a directory database gets corrupted, you may restore the database from backup. Any new information in the database will be lost when the data is restored.

To Restore the Databases

- Stop the Unified CallConnector Database Server. The server can be stopped from Administrative Tools->Services window.
- Run the Unified CallConnector Server Wizard and go to the Database section.
- Click on the Restore button. The files will be copied to the Data folder.
- Copy the specific database file that you wish to restore from the backup folder to the Unified CallConnector Server->Data folder. This will override the existing data file.
- Restart the Unified CallConnector Database Server.

Note: The transaction information such as call logs is stored in the CallLog database, the shared contact information is saved in the Corporate database and the configuration and personal data is stored in the UCC Database

Compacting the Databases

When records are deleted in the database, they are marked as not available. The deleted record remains in the database. The ;Compact' operation removes these deleted records. For databases with frequently changing data, such as the Calllog database, the compacting operation can be used to remove these un-used records.

To Compact the Databases

- Stop the Unified CallConnector Database Server. The server can be stopped from Administrative Tools->Services window.
- Run the Unified CallConnector Server Wizard and go to the Database section.
- Click on the Compact button. The files will be compacted.
- Restart the Unified CallConnector Database Server.

To Compact the Databases from ODBC

- Stop the Unified CallConnector Database Server. The server can be stopped from Administrative Tools->Services window.
- Open the Data Sources (ODBC management) window from Administrative Tools-> Data Sources.
- Click on the System DSN tab. The Unified CallConnector databases will be displayed. Select the database that you want to compact and click on Configure button.
- The Configure button will open the ODBC Microsoft Access Setup widow. Verify that the correct database has been selected and click on Compact.

Restart the Unified CallConnector Database Server.
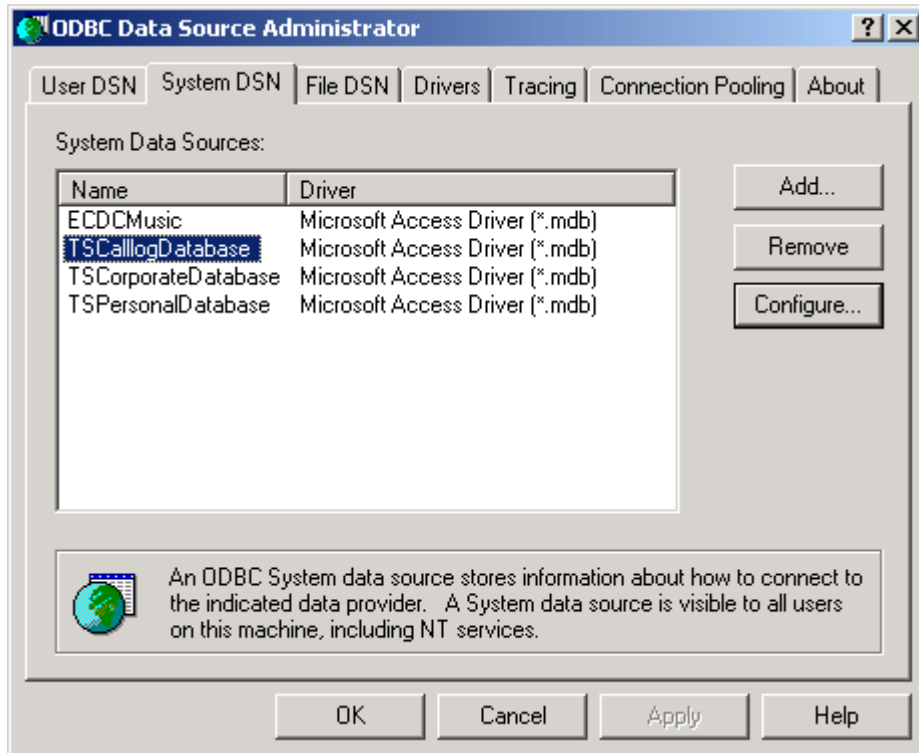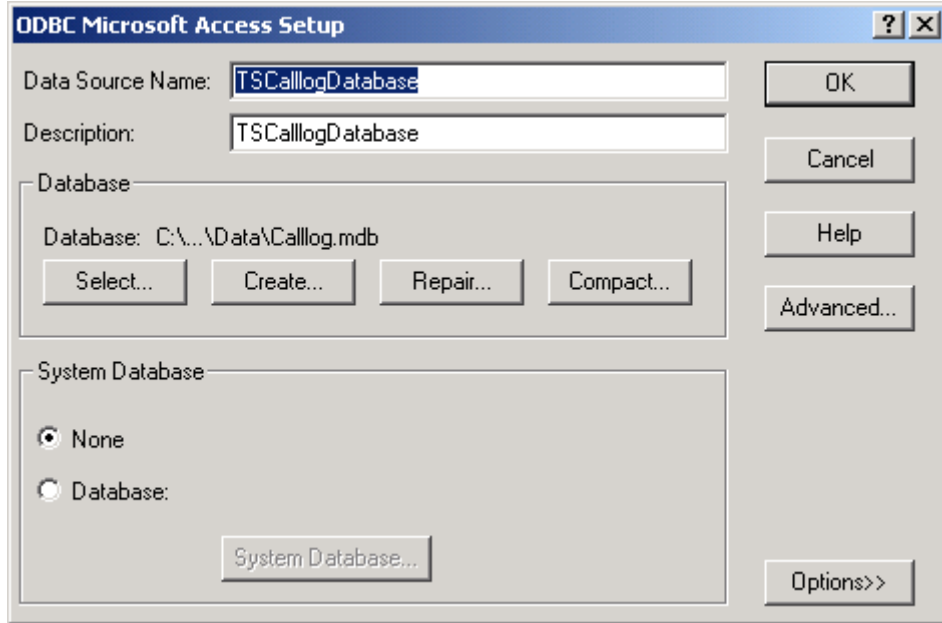
Repairing the Databases

The repair operation rebuilds the indexes that allow a database to quickly search and retrieve data.

To Repair a Database

- Stop the Unified CallConnector Database Server. The server can be stopped from Administrative Tools->Services window.
- Open the Data Sources (ODBC management) window from Administrative Tools-> Data Sources.
- Click on the System DSN tab. The Unified CallConnector databases will be displayed. Select the database that you want to repair and click on Configure button.
- The Configure button will open the ODBC Microsoft Access Setup widow. Verify that the correct database has been selected and click on Repair.

Restart the Unified CallConnector Database Server.

Importing and Exporting Contacts

The Microsoft Access database tools for importing and exporting can be used to populate the corporate directory data. The Corporate Directory database can also be exported.
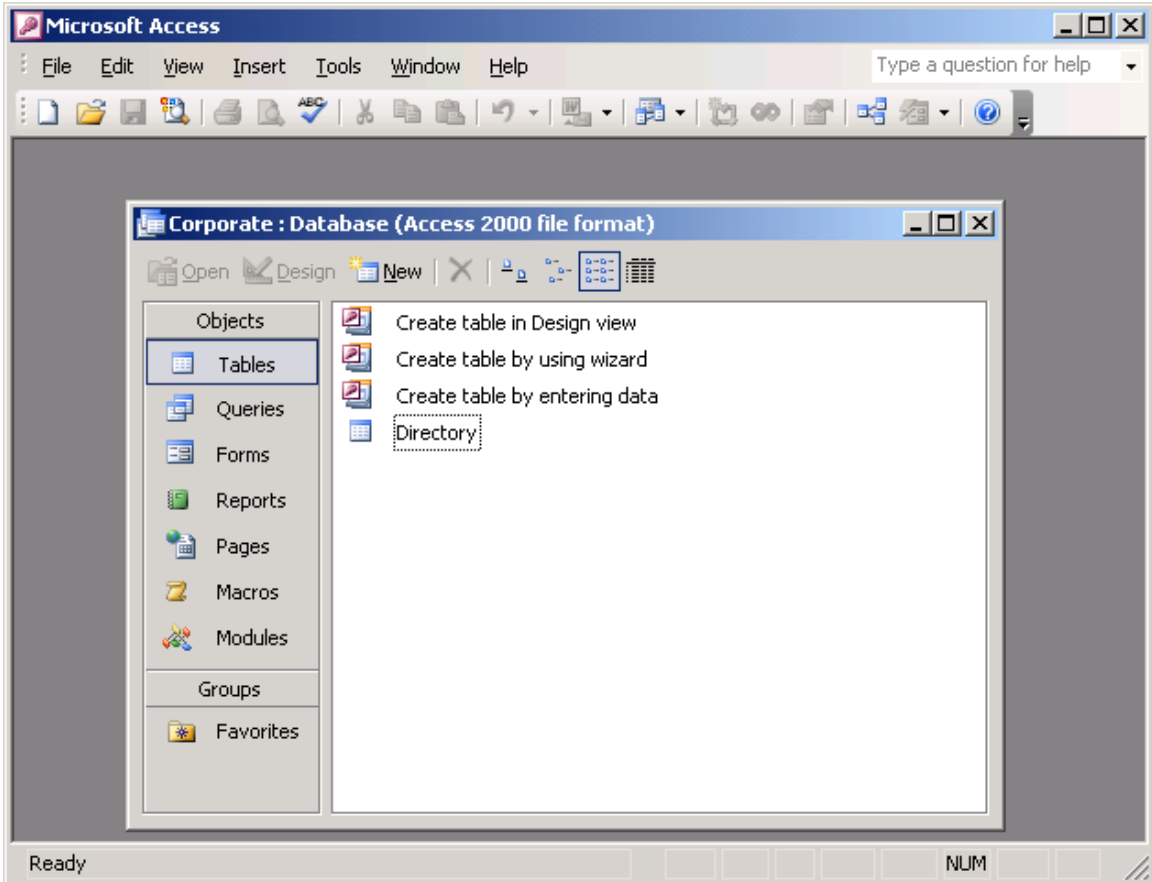
To Import Data to the Directory

- Stop the Unified CallConnector Database Server. The server can be stopped from Administrative Tools->Services window.
- Open the Corporate database from Microsoft Access.
- From the File menu, select Get External Data->Import. The import window will be displayed.
- Select the file and the file type and run through the import wizard.

To Export Data from the Directory

- Stop the Unified CallConnector Database Server. The server can be stopped from Administrative Tools->Services window.
- Open the Corporate database from Microsoft Access. Double-clock on Directory to open the table.
- From the File menu, select Export->Import. The export window will be displayed.
- Select the file and the file type and run through the export wizard.

Maintaining Call Log Data

The CallLog database stores records for the phone calls made through the Cisco Unified CME. These records can accumulate and build up to a large number, increasing the size of the database and impacting the performance when viewing the logs.

The Unified CallConnector Server Wizard provides an option to automatically remove the call log records that are older than the selected date.

To Automatically Purge Call Log Records

- Start the Server Wizard. Click on Database Server or click on Next to move to the Database Server window.
- Select the option 'Remove Call Logs older than (in days)' and from the pull-down list select the number of days of call log data you want to keep in the system.
- Click on Finish to apply the changes.
- Select the file and the file type and run through the export wizard.
- Stop and start the Unified CallConnector Database Server.

CHAPTER

9

Server Diagnostic Tool

The Unified CallConnector Server Diagnostic Tool allows you to view the status of the server applications, configuration information and run diagnostic tests.

This chapter describes the information available from the Diagnostic Tool and provides instructions for running the tests. It includes:

Tool Overview:	Describes the different attributes and functionality available from the Toolbars.
Main Window:	Describes the Diagnostic Tools user interface and the different window sections.
Running Diagnostic Tool:	Describes how to setup an account(s) for use when running the tests
Server Test Suites:	Provides an overview of the Server test cases and description of the information returned when the test is run.
Client Test Suites:	Provides an overview of the client test cases and description of the information returned when the test is run.
Results Discussion:	Describes the implication of the test result success or failure.

Server Diagnostic Tool Overview

The UCC Server Diagnostic tool can be used to isolate problems with the Unified CallConnector Server applications. The Diagnostic Tool can display configuration information, connection status and statistics for the servers. The Tool also contains a suite of diagnostic tests that can be run to determine possible causes for problems experienced when running the UCC clients in the server mode.

The Diagnostic Tool can be run on the Unified CallConnector Server or on the client desktop. Note it the Tool runs only on Windows 2003 or Windows XP systems.

Diagnostic Tool Capabilities

The Unified CallConnector Diagnostic Tool can be used to:

- Run client and server diagnostic test suites:
- Display User, Group, Phone configuration information
- Display Server Status and Statistics
- Display Phone Status and Statistics
- Display Radius Inputs, Call Logs, and Active calls
- Display Registered and Subscribed Users

Diagnostic Tool Main Window

The regions of the Diagnostic Tool window are described below starting from top left and going to bottom right:
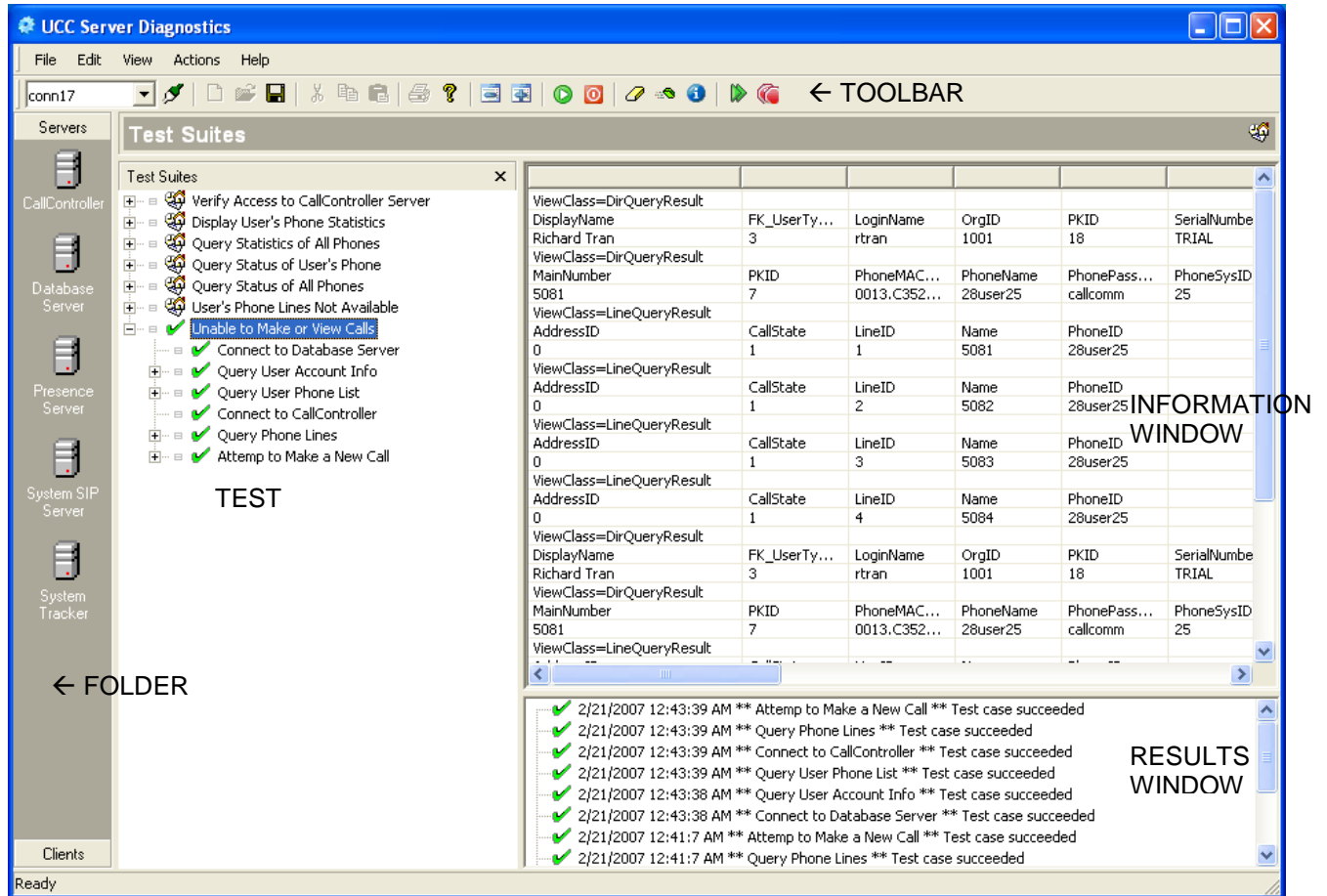
Menu Bar:	The menu provides access to the functions of the diagnostic tool:
Toolbar:	Provides buttons for selecting or setting up the test account and running the tests. These functions include starting and stopping a test suite, saving, printing or clearing the test results and information.
Folders:	The diagnostic tests are organized under server and client folders. Each server application is associated with its own set of test suites.
Test Suites:	A test suite is a collection of unit tests that request information or attempt to isolate a problem.
Information Window:	The Information Window displays the messages received in response to the queries sent by the tool as the tests are executed.
Results Window:	The Results Window displays each test that has been run with an indication of the test result – success or failure.

Menu Bar

File Menu:

Manage Connection - opens the Connections window to setup a user account to run the tests on

Save – allows you to save the contents of the Information and Results windows to a selected a file

Print – prints the contents of the Information and Results Window

View Menu:

Toolbar – displays the toolbar below the menu bar when selected.

Status Bar – displays the status bar at the bottom of the window when selected.

Dialog Test – not currently implemented

Toggle Test Suite Tree – not currently implemented

Actions Menu:

Reload All Test Suites – not currently implemented

Launch Test Suite Builder – not currently implemented

Help Menu:

Help – opens the Diagnostic Tools About dialog window

Toolbar
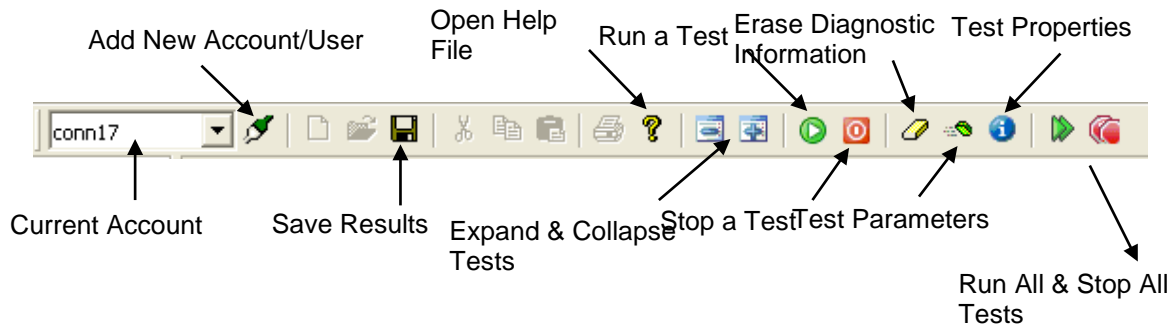
Toolbar Button	Description
Current Test Account	Each test is a Unified CallConnector user account under which it is run. The current account displays the active user account that is be used or will be used by the selected tests. More than one test account can be setup
Add New Accounts	The New Account button allows you to specify a new user account. It opens the New UCC Account window for entering the SIP server address and user login information. You need to specify the account name
Save Results	Opens the 'File Save As' to allow you to specify the file name and location for saving the Information and Results window information.
Save Results	Opens the 'File Save As' to allow you to specify the file name and location for saving the Information and Results window information.
Open Help	Displays the Diagnostics Tool help window.
Expand Tests	The Test Suite is displayed as a hierarchical tree. This button expands the all the Test Suites to display the Unit Tests associated with each suite.
Collapse Tests	Collapses the hierarchy to display only the test suites.
Run a Test	Runs the currently selected test suite or test,
Stop a Test	Stops the currently selected test suite or test,
Erase Diagnostic Information	Clears the data displayed in the Information and Results windows
Display Test Parameters	Open Test Suite Hierarchy to display the parameter field being used for each of the tests
Display Test Properties	Opens the Properties window for the selected item in the test Suite list
Run All Tests	Run all the tests in the selected test suite
Stop All Tests	Stop running all tests

Folders
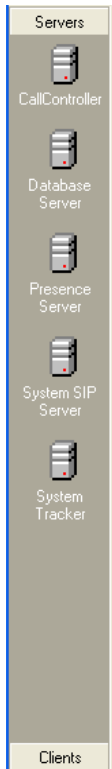
Folders provide access to the test suites. The diagnostic tests are organized in test suites which are associated with items in the folders.

There are two folders – Server and Client.

The server folder has an entry for each of the Unified CallController server applications. Example of these are the CallController or Presence Server. When you select an entry in the folder, the test suites associated with that entry are displayed in the Test Suites window. There may one or more test suites associated with each entry.

The Client Folder has one entry for all the client test suites.

To View Available Test Suites

Select the Folder by clicking on Servers or Clients.
Select the Folder Entry by clicking on the item.
The list of available test suites for the entry will be displayed in the Test Suites window.

Test Suites

A Test Suite is the problem that you want to diagnose or the type of information that you want to view from the server.
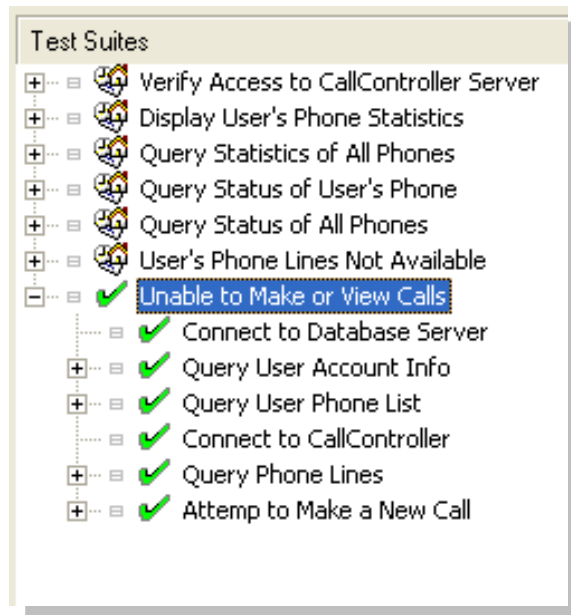
Each test suite can be comprised of a number of individual tests. Test Suite attempts to isolate the problem by validating each of the requirements for that function.

In the example above, to determine why the use is unable to make calls, the following steps have to be validated.

- Login to the UCC system using the account of the user that is experiencing the problem.
- Connect to the Database Server. If this fails then the user account cannot be accessed as there is a problem connecting to the Database Server.
- Obtain the user' account information. This is to verify that the user has an account on the server
- Obtain the user's phone information. If no phones are configured then this will fail.
- Verify that the phone is connected to the Unified CallConnector and is available.
- And finally an attempt is made to place the call.

Diagnostic Information Window

ViewClass=DirQueryResult					
DisplayName	FK_UserTy…	LoginName	OrgID	PKID	SerialNumbe
Richard Tran	3	rtran	1001	18	TRIAL
ViewClass=DirQueryResult					
MainNumber	PKID	PhoneMAC…	PhoneName	PhonePass…	PhoneSysID
5081	7	0013.C352…	28user25	callcomm	25
ViewClass=LineQueryResult					
AddressID	CallState	LineID	Name	PhoneID	
0	1	1	5081	28user25	
ViewClass=LineQueryResult					
AddressID	CallState	LineID	Name	PhoneID	
0	1	2	5082	28user25	

The Information window displays the results from the individual test that is run. A test may return a single line of result or many responses.

Each of the responses is displayed in three lines.
ViewClass: The first line is the message type. This is the beginning of a response entry.
Parameter - Line After ViewClass: List of the parameters or the fields that are send in the message. Each ViewClass messages has its own list of fields.
Value – Value of parameters listed in the previous line. The value for each of the fields or parameters returned in the response message is listed below its Parameter or Field name.

For Example in the display above:
ViewClass=DirQueryResult. This message returns information from the database.

The fields returned include the Display Name, User Type Login Name etc.
The value of these fields is in the next line, respectively Richard Tran, 3, rtran etc.

Test Results

The Results window indicated is the particular test was a success or failure. For each test run there will be a corresponding result status.
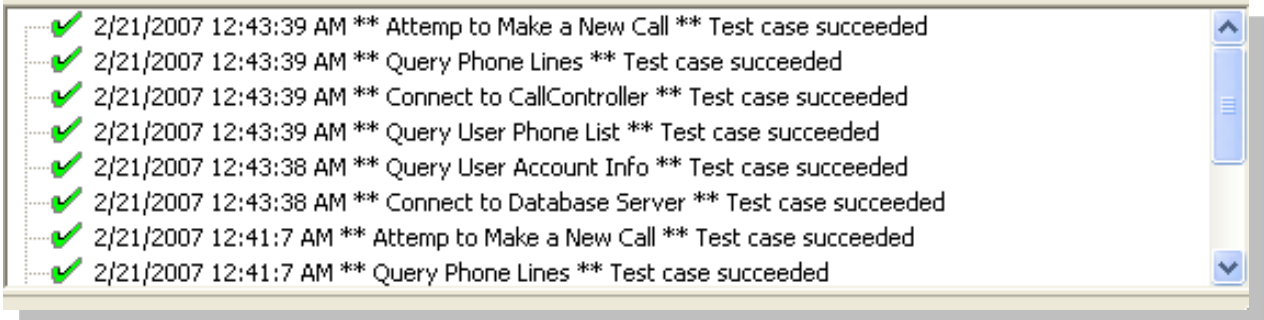
Test Parameters
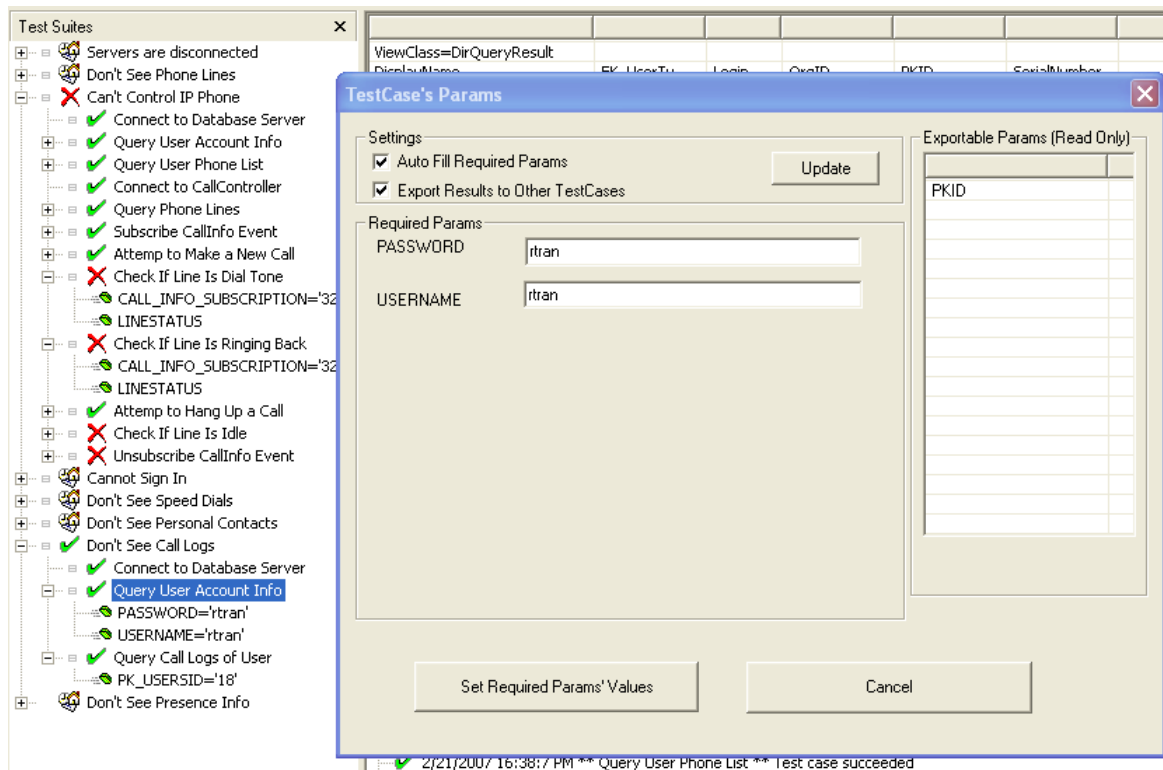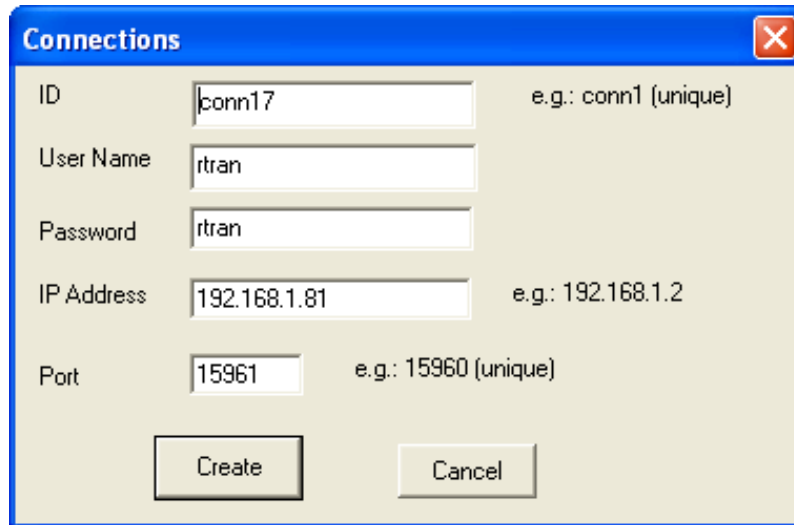
The parameters required in each of the tests are displayed in the parameter list. The parameters can be displayed by highlighting the test and clicking on the toolbar button – Display Test Parameters or by double clicking on a test entry. Each test can inherit the results from the prior test(s) in the test suite. You can right-click to open the properties window and change the inheritance rules or enter a specific For example in the Make a Call test, the telephone number to be dialed can be entered as a parameter.

Running the Diagnostic Tool

- Copy the ccUCCDiagnostic.exe and UCCDiagnostic.xml file to the tools folder of the UCC client.
- Diagnostic Tool can also be run from a shared drive or on the CallConnector server.
- The computer where it is run needs to have the UCC client or server installed. Ports setup for the Tool must not be blocked. The Diagnostic tool is not compatible with Windows 2000.
- Double Click on ccUCCDiagnostic.exe. The UCC Server Diagnostic Tool will run.
- Setup or select the account you want to use for the tests.
- Click on the Server or Client Folder button and select the folder by clicking on the icon.
- Click on the Test Suite that you want to run.
- To execute the test, click on the Run button.
- You can also right-click and select Run Test Suite
- The tests will run and display the information in the Information Window and success/failure in the Results Window.

Creating a New Account

- Click on the Create New Account button on the top left hand corner on the toolbar (next to Accounts dropdown menu).
- It will bring up a window where you can create a new Account. Enter the following information in the New Accounts window:
- The ID you would like to give to this account (to distinguish between other accounts)
- The username and password of an account on the Unified CallConnector Server you are currently troubleshooting.
- The IP address of the Unified CallConnector Server you are currently connecting to.
- The port where you will use to access the UCC Server.
- When you are finished, click on Create to create this account. You can create new accounts. However, you cannot edit any existing accounts.

Selecting a Client Test Suite

- On the left hand side of the Diagnostic Tool window, from the Folder menu click on the Client Test Suites button. By default, the Server button is open when you first open the Diagnostic Tool. The Client Test Group button is at the bottom of the folder menu.
- Click on the All Clients button. A list of the client test suites will be displayed in the Test Suites window to the right.
- Click on the plus sign of any test suite to expand and show a list of different tests under the test suite.

Selecting a Server Test Suite

- On the left hand side of the Diagnostic Tool window, from the Folder menu click on the Server button. By default, the Server button is open when you first open the Diagnostic Tool. The Server button is at the top of the folder menu.
- A list of folders representing a group of tests for each Unified CallConnector Server components is displayed. This allows the you to test each component individually. Note however that some components are dependent on other components in order to work.
- The Server folders listed are CallController Server, Database Server, Presence Server, System SIP Server, and System Tracker. Click one of these icons to select that group of tests.
- A list of the test suites for that server component will be displayed in the Test Suites window to the right.
- Click on the plus sign of any test suite to expand and show a list of different tests under the test suite.

Starting and Stopping a Test

- After you have selected a test suite to run, expand the test suite by clicking on the plus button next to it.
- It will display a list of tests that must pass in order for this functionality to work.
- Because each test suite is associated with its own individual account, please be sure to select the correct account that you would like to use from the Account Dropdown menu. You may select an account from the drop down menu, or create a new one by clicking on the marker button next to it. If you do not select the correct account, you may be running these tests on a UCC Server account you were not intending to troubleshoot.
- Some tests (one level under test suites) will require parameters to be filled in. If there is a tiny box icon next to a test, this means that it will automatically fill this parameter and you needn't worry about it. But if it does not have a box icon next to it, you may need to fill in this parameter.
- Right click on the test suite and click on the Run Test Suite option to start the test suite.
- You may also start a test suite by selecting a test suite and then clicking the green play button from the menu at the top of the screen.
- After the test is finished it will stop automatically.
- If you would like to stop the test at any time while it is running, you may right click on the test suite and select the Stop Test suite option. You may also click on the Stop

Button from the menu at the top of the screen. This will also stop the current selected test from running.

Start and Stop All Tests

- You may run through all the tests by clicking on the Run All Test Suites button located on the toolbar menu at the top of the screen.
- You may stop these tests from running by clicking on the Stop All Tests button.

Interpreting the Test Results

- After running a Test suite, the tool will display a green check mark to all tests that have passed and a red **X** mark to all tests that have failed.
- In the Results window, it will also display the results (pass or fail) of each test case.
- If the result of a particular test has failed, you can find the list of possible causes of this failure in the Test Results Appendix in this Help File.

To Clear the Information and Results Window

- To clear the Tests Results (success and error messages) and Information Data (data messages received from Servers), click on the **Erase** button located on the top toolbar menu.
- Clicking this will erase all data and result messages.

Saving Test Results a File

- Click on the floppy disk icon located on the top toolbar menu.
- This will bring up a prompt to save the Information Data. If you do not want to save the Information data, click cancel to continue to saving the Test Results.
- After you are finished saving the Information Data, you will be prompted to save the Test Results. If you do not want to save the Test Results, then please click cancel.

Clearing Test Status

- After running through test suites, you may notice that the status check marks are not removed from the test suites and tests.
- It will remain there for your own convenience and will not be erased until you exit the Diagnostic Tool application or hit the Stop Test button or Stop all Tests button.
- To clear the status check marks from a particular test suite, select the test suite and click on the Stop Test button on the toolbar menu located at the top of the screen.
- To clear all the status check marks from all tests suites in the Test suite Menu, simply click on the Stop All Tests button on the toolbar menu located at the top of the screen.

To View the Test Parameters

- To view parameters used in a test, expand the test suite and right click on a test. Then select the properties option.
- It will show the parameters being used by this particular test.
- Parameter Settings:
- If the Auto-fill check box is checked, it will automatically fill these parameters upon running it. If Auto-fill it is unchecked, then you may check it to have it automatically fill in parameters or you may fill in these parameters manually.
- You may have the test suite stop execution upon test failure by checking the Stop Execution upon Any Test Failure box. If it is not checked it will continue execution if any test fails.
- It is recommended that you have the Auto-Export setting checked. This will automatically export all test results to the rest of the tests so that the Auto-fill feature will work.

To Displaying the Tests in a Test Suite

- When you first open a Client or Server Test Group, it will show you a collapsed list of Test suites.
- To expand a specific Test suite, click on the Expand button located to the left of the Test suite.
- You may also expand a specific test suite by clicking on the plus button next to the left of the test suite.
- You can expand all sub directories of the test suites (showing tests and their parameters) by clicking on the Expand All button located on the toolbar menu at the top of the screen.

To Hide the Tests in a Test suite

- When you first open a Client or Server Test Group, it displays a collapsed list of test suites.
- If you happen to have any of these test suites expanded you can collapse one test suite by selecting it. Then select the Collapse button located to the left of the test suite to hide all the tests under the test.
- You may also collapse a test suite by clicking on the test suite and clicking on the Collapse button on the toolbar menu at the top of the screen.
- You can hide all sub directories of the test suites (hiding tests and their parameters) by clicking on the Collapse All button located on the toolbar menu at the top of the screen.

Test Results Discussion

This section describes possible problems related to the failed tests. This should be helpful in troubleshooting UCC problems.

Server Tests

CallController Server

Verify Access to CallController Server: Checks to see if a connection can be established with the CallController Server.

> Success: The CallController Server is online, running, and connection can be established with it.

> Failure: The CallController Server is offline, not running, or connection cannot be established with it (possible firewall issues).

Display User's Phone Statistics: Returns statistics of the user's phone.

> Success: Statistics of User's phone which includes: Number of times disconnected, number of errors, number of incoming calls, number of outgoing calls, ID of the phone, number of times phone reconnected from failure, number of times the phone was reset, the status of the phone, and the total number of calls (incoming/outgoing).

> Failure: Cannot Contact CallController Server or there is no phone associated with this user.

Query Statistics of All Phones: Returns statistics of all phones associated with this UCC Server.

> Success: Statistics of all phones associated with this UCC Server, which includes: Number of times disconnected, number of errors, number of incoming calls, number of outgoing calls, ID of the phone, number of times phone reconnected from failure, number of times the phone was reset, the status of the phone, and the total number of calls (incoming/outgoing). (It will show list of statistics for all phones, differentiated by Phone ID)

> Failure: Cannot Contact CallController Server or there are no phones associated with this UCC Server.

Query Status of User's Phone: Checks the status of the user's phone: The main phone number, the phone ID, and the phone's status.

> Success: It returns the status of the user's phone (Idle/Busy/Disconnected).

> Failure: The CallController Server is offline or the user is not associated with a phone.

Query Status of All Phones: Checks the status of the all phones connected to this UCC Server: The main phone number, the phone ID, and the phone's status.

> Success: It returns the status of the user's phone (Idle/Busy/Disconnected).

> Failure: The CallController Server is offline or the user is not associated with a phone.

Phone Lines Not Available: Checks to see if the user can obtain phone lines.

Success: It returns a list of the user's phone lines (phone DN's).

Failure: The CallController Server is offline, the user is not associated with a phone, or the user's phone is disconnected.

Unable to Make or View Calls: Checks to see if the user can obtain phone lines.

Success: It makes an outgoing phone call.

Failure: The Client is unable to contact the CallController Server, the user is not associated with a phone, or the user's phone is disconnected.

Database Server

Verify Access to Database Server: Checks to see if a connection can be established with the Database Server.

Success: The Database Server is online, running, and connection can be established with it.

Failure: The Database Server is offline, not running, or connection cannot be established with it (possible firewall issues).

Unable to Login: Checks the Database for your account username and password.

Success: The Database is running and is able to verify correct username and password.

Failure: The Database Server is not running, or the account information used is incorrect.

Speed Dial Numbers are Not Displayed: Requests a list of Speed dial entries for this user from the Database Server.

Success: The Database Server was able to return all speed dial results.

Failure: The Database Server is either not running or speed dials may have not been created yet.

Display All User Accounts: Checks the Database for all user accounts.

Success: The Database is running and returns all user account information.

Failure: The Database Server is not running, or there are currently no user accounts on this UCC Server.

Display All Phones: Displays a list of all phones associated with this UCC Server.

Success: The Database is running and returns all phones connected to this UCC Server.

Failure: The Database Server is not running, or there are currently no phones controlled by this Server.

Personal Contacts are Not Displayed: Requests a list of all Personal Directory Contacts from the Database Server.

> Success: The Database Server was able to return all Personal Directory Contacts.

> Failure: The Database Server returned nothing. The Database Server may be offline or something could be blocking the query from being received by the Database Server. It's possible that the user may not have any Personal Directory Contacts.

Call Logs are Not Displayed: Requests a list of all Call Logs from the Database Server.

> Success: The Database Server was able to return all Call Log results.

> Failure: The Database Server returned nothing. The Database Server may be offline or something could be blocking the query from being received by the Database Server. It's possible that the user has no call logs.

Display Latest Call Logs in Database: Requests a list of all Call Logs from the Database Server.

> Success: The Database Server was able to return the 10 most recent call logs written to the Database.

> Failure: The Database Server returned nothing. The Database Server may be offline or something could be blocking the query from being received by the Database Server. It's possible that the user has no call logs.

System SIP Server

Display Registered Servers and Users: Displays the current list of registered users and servers.

> Success: Returns a list of registered users and Servers.

> Failure: The System SIP Server is offline, or none of the other services are running.

Presence Server

Verify Connection to the Presence Server: Checks to see if a connection can be established with Presence Server.

> Success: The Presence Server is online, running, and connection can be established with it.

> Failure: The Presence Server is offline, not running, or connection cannot be established with it.

Display All Groups: Requests a list of all user groups from the Presence Server.

> Success: Returns a full list of all user groups.

> Failure: The Presence Server is down, or unable to populate its list of groups and users. It's possible that the Database Server was down when the Presence Server was started so it wasn't able to obtain the information it needs to run properly.

Presence Status is Not Displayed: Requests the status of the user from the Presence Server.

>Success: The Presence Server is online and returns the user's status.

>Failure: The Presence Server is offline or is not ready. It's possible that the Database Server was down when the Presence Server was started so it wasn't able to obtain the information it needs to run properly.

Query Presence Server's Latest Call Logs: Requests a list of the last 10 call logs that were written by the Presence Server.

>Success: Returns the last 10 call logs written by the Presence Server.

>Failure: No call logs are returned. The Presence Server is either offline, is not ready, or the Radius Packets are not being sent to this UCC Server. If radius has not been configured, then it's not possible to see Call Logs being written.

Display Current Subscribers to the Presence Groups: Requests the list of currently subscribed users of the Presence Server.

>Success: Returns the list of subscribed users.

>Failure: The Presence Server is offline, not ready, or there are no subscribed users.

Display Current Active Calls: Requests the list of current active calls being made.

>Success: Radius packets are being sent to this UCC Server. Returns the list of active calls.

>Failure: The Presence Server is offline, not ready, or there are no active calls.

System Tracker

Display Server Connection Statistics: Attempts to establish a connection with the System Tracker.

>Success: The System Tracker is online, running, and connection can be established with it. Also returns the connection status of all Servers.

>Failure: The System Tracker is offline, not running, or connection cannot be established
>with it.
>Server Statistics:
>SIP Server:
>Current state of this server.
>Number of times this server went offline.
>Current running duration of uptime.
>CallController Server:
>Current state of this server.
>Number of times this server went offline.
>Current running duration of uptime.
>Database Server:
>Current state of this server.
>Number of times this server went offline.
>Current running duration of uptime.
>Presence Server:
>Current state of this server.
>Number of times this server went offline.

Current running duration of uptime.

Client Tests

Servers are Disconnected: This tells if you can or cannot connect to all servers.

Success: All services: System SIP Server, CallController Server, Database Server, Presence Server, and System Tracker are all running.

Failure: One or more of the servers are not running.

Don't See Phone Line: Checks to see if the you can make a phone call.

Success: It is able to make a phone call correctly.

Failure: The CallController Server is offline, the user is not associated with a phone, or the user's phone is disconnected.

Can't Control IP Phone: Checks to see if the user can obtain phone lines.

Success: It returns a list of the user's phone lines (phone DN's).

Failure: The CallController Server is offline, the user is not associated with a phone, or the user's phone is disconnected.

Cannot Sign In: Checks the Database for your account username and password.

Success: The Database is running and is able to verify correct username and password.

Failure: The Database Server is not running, or the account information used is incorrect.

Don't See Speed Dial Numbers: Requests a list of Speed dial entries for this user from the Database Server.

Success: The Database Server was able to return all speed dial results.

Failure: The Database Server is either not running or speed dials may have not been created yet.

Don't See Personal Contacts: Requests a list of all Personal Directory Contacts from the Database Server.

Success: The Database Server was able to return all Personal Directory Contacts.

Failure: The Database Server returned nothing. The Database Server may be offline or something could be blocking the query from being received by the Database Server. It's possible that the user may not have any Personal Directory Contacts.

Don't See Call Logs: Requests a list of all Call Logs from the Database Server.

Success: The Database Server was able to return all Call Log results.

Failure: The Database Server returned nothing. The Database Server may be offline or something could be blocking the query from being received by the Database Server. It's possible that the user has no call logs.

Don't See Presence Info: Requests a group list and user list from the Presence Server.

Success: Returns a full list of all user groups and users in those groups.

Failure: The Presence Server is down, or unable to populate its list of groups and users. It's possible that the Database Server was down when the Presence Server was started so it wasn't able to obtain the information it needs to run properly.

CHAPTER

10

Server Troubleshooting

This chapter describes the common error conditions that occur with the Unified CallConnector Server and steps to solving these problems. The following are the areas of possible error conditions what will be covered:

Cannot Register (TSP Mode) with the IP Phone

Activation Fails with Timeout

Phone Lines are Not Shown or Cannot Dial

Call Logs Not Showing

Parts of the Toolbar are grayed out

Presence Buttons are Grayed Out

Popup System Tray Icon Becomes Gray

Cannot Login

Can not view the Logs Window (in TAPI Mode)

Can not view the Contacts Window (in TAPI Mode)

Can not view the Shortcuts Window (in TAPI Mode)

UCC Server Troubleshooting

While using the Unified CallConnector, users may experience some common problems. This chapter focuses on troubleshooting these common problems. The troubleshooting information contains information on the nature of the problems and steps to solving these problems.

The Unified CallConnector system consists of multiple interacting components. These components are shown below with a summary of the impact of a failure in a component and the appropriate debugging tool.
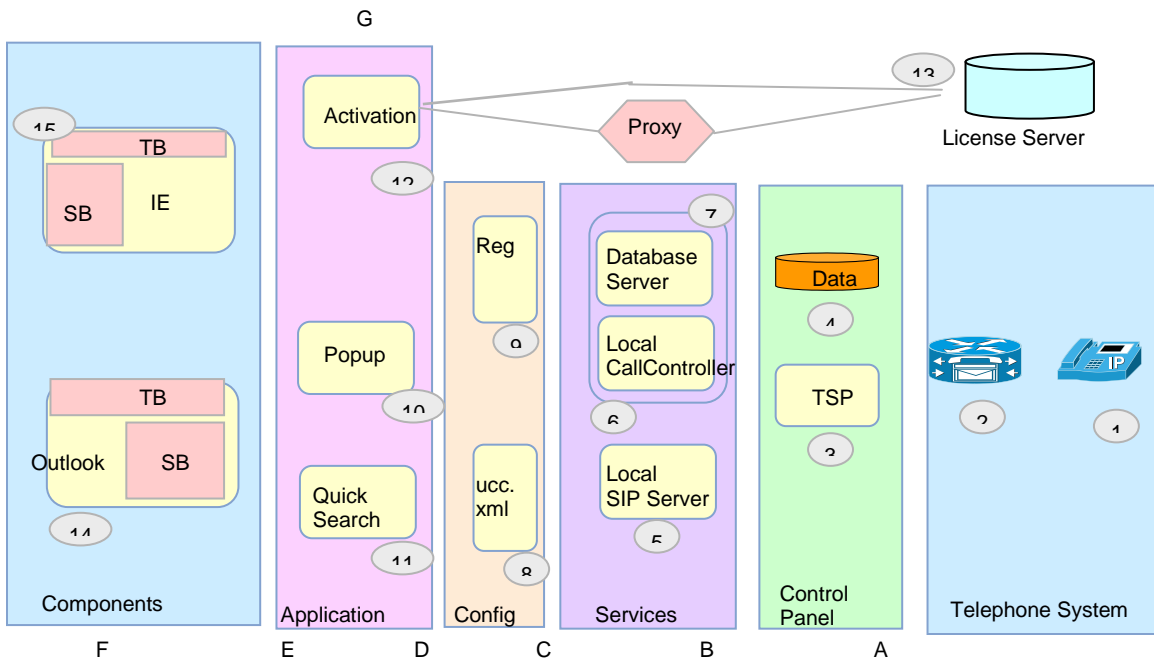
Summary of Component Failure and Possible Failure Symptoms

- IP Phone Not Registered; Cannot/Lost Connection to CME Router:
- Cannot Register, Cannot Access/Corrupted Database: From Control   Panel open Phone & Modems; Admin Tools ->ODBC ->System DSN
- GUI Gray; Unable to Connect/Login: Connectivity Status; Windows Services ->Stop/Start
- Reset Activation, Change Configuration: Windows Registry; UCC.XML in System32
- Cannot View Information (caller id, search results): Popup Options; UCC Debug Logs
- Toolbar Not Showing, IE/Outlook Crash: Unregister/Register.bat files
- Activation Timeout: Check firewall and IE settings

Cannot Register (TSP Mode) with the IP Phone

Description

The Cisco Unified CME router can be successfully pinged, but the Wizard or TSP cannot register to CME.

Possible Causes

- Invalid user name and password have been entered.
- Another TSP is running and using the same IP-Phone.
- Ephone has not been configured with the User Name and Password.
- Firewall blocking Local SIP Server and Popup.
- The CMCE User Name and Password are too long (if more than 15 characters)

Procedures

Step 1: Verify that the account information has been entered correctly. Enable CME Debug for IP Phone Registration

Step 2: Re-enter the information and verify connectivity using the Wizard.

Step 3: If the Wizard still displays the error, then contact your system administrator or service provider.

Activation Fails with Timeout

Description

When Activating Serial Number, the progress bar run through three times and posts an error message.

Possible Causes

- No access to the Internet from this PC
- Access to the UnifiedCallConnector.com site is not resolved/available.
- Firewalls may be blocking Popup access to internet.
- Password access proxy

Procedures

Step 1: Verify that there is access to Internet. Browse to www.cisco.com.

Step 2: Verify proxy settings on Internet Explorer, if proxy is in use.

Step 3: Verify that the firewalls on the PC allow Popup external access

Step 4: Verify that there is access to the License Server site. Browse to www.unifiedcallconnector.com.

Step 5: If the Activation still displays the error, then contact your system administrator or service provider.

Phone Lines are Not Shown or Cannot Dial

Description

When trying to select a phone line from the Popup menu, the phone lines are not shown. Or attempting to dial, but the call is not being dialed out.

Possible Causes

- Client is not logged in.
- CallController Server is stopped or session to CME dropped.
- IP Phone or IP Communicator have been disconnected or not in service.
- IP Phone has not been configured with the CME.
- All lines are in use.
- Dial plan is not properly configured

Procedures

Step 1: Check whether logged in or logged out.

Step 2: If IE or Outlook open, click on Cisco button in UCC Toolbar and check on servers in Connectivity.

Step 3: Right-click on the red Popup system tray icon, select Options and Click on the Server tab.

Step 4: If Server Tab displays the Logout button, then logged in. If it shows a Login and Reset button, then logged out.

Step 5: If you are logged out, then type your Login name and password and click on the Login button. If not using UCC Server, uncheck/check 'Use Local TAPI Driver' to reset user-name and password.

Step 6: Check whether or not the CallController Server is down from Option-Server or Toolbar->Cisco->Connectivity.

Step 7: If in TAPI mode, check in Services to see if the ccCallController service is stopped. If it has stopped, then select the service and click the "play" icon on the top to start the service.

Step 8: If in Server mode, check the CallController Server on the Server machine to see if it has stopped. If it has stopped, then start the service from the Services menu.

Step 9: Verify that IP Phone is operating properly and all lines are visible.

Step 10: If TAPI mode, use TAPITest tool to verify phone operation.

Step 11: If Server mode, use the sharpshooter to isolate problems. If problem persists, collect debug and report the problem.

Step 12: Check if your Windows dialing plan is set up correctly. You can access it either from the control panel or from Popup Options > Dial tab > click on **Windows Dialing Rules**.

Call Logs Not Showing

Description

When you click on the Logs, none of the Call Logs are shown.

Possible Causes

- No Calls have been made.
- Presence Server is not writing Call Logs because it is stopped.
- Presence Server not receiving messages from the Radius Server.
- Your Login name isn't associated with a contact entry.
- Your contact's business phone number hasn't been filled in.
- DB server is not running

Procedures

Step 1: Verify that Call Logs are not being shown. Make a phone call to any number and hang up. Open the Call Logs Window in Internet Explorer. Right-click on the menu and click refresh. If nothing is shown, proceed with the next step.

Step 2: Check if the Presence Server on the Server Machine is stopped. On the Server Machine open the Services menu and hit the refresh button. If the Presence Service has failed

Step 3: Check whether the Database Server has stopped running. In order for the user to be logged in the System SIP Server (Server mode) or CallController (TAPI mode) needs to be able to access the database to authenticate the user.

Parts of the Toolbar are grayed out

Description

Some parts of the toolbar such as the presence status buttons and the QuickSearch box maybe grayed out. Ask customer which parts of toolbar are grayed to determine area of need.

Possible Causes

- Auto Recovery has not been turned on (by default this is enabled).
- Some services stopped working, need to determine cause (and restart service)

Procedures

Step 1: Determine which servers are stopped using Toolbar->Cisco->Connectivity.

Step 2: Enable Auto Recovery if disabled from toolbar or in UCC.XML file

Step 3: Restart Internet Explorer or Outlook for auto-recovery to be enabled.

Step 4: If Servers are stopped, restart the servers using Windows-Services or Popup-Services.
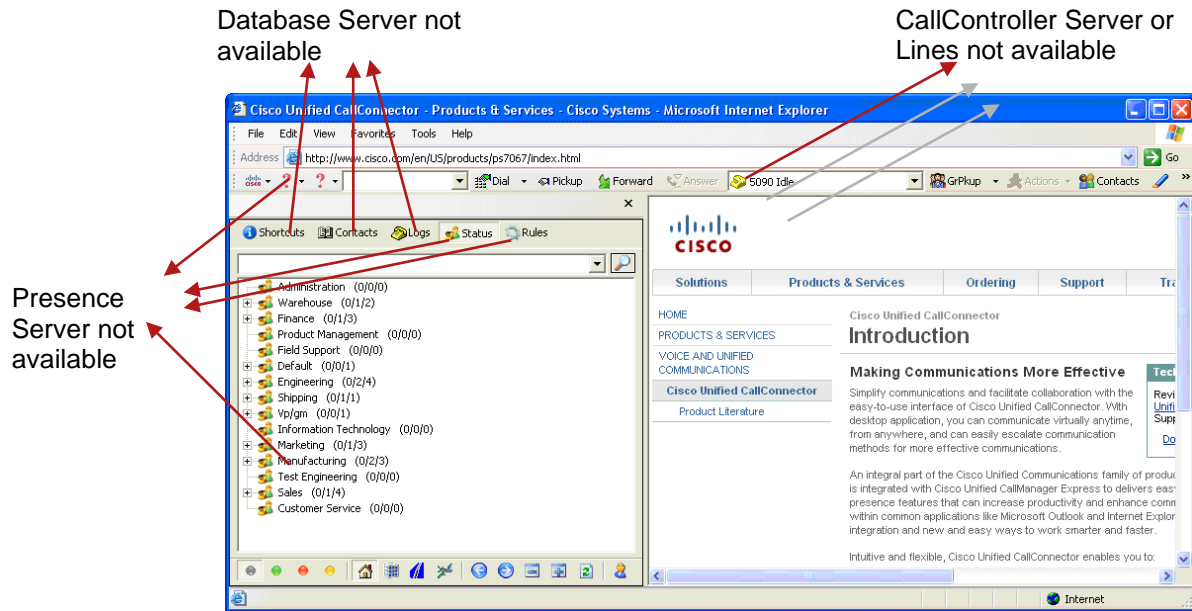
1. Local SIP Server not Available – All Objects Grayed Out
2. CallController Server Not Available – Line Display show " No Phone Lines Available"
3. Presence Server Not Available – Status Window Grayed Out
4. Database Server Not Available – Shortcuts, Contacts, Logs Grayed Out

Presence Buttons are Grayed Out

Description

The Presence buttons on the toolbar are grayed out and cannot be used.

Possible Causes

- Presence Server on UCC Server is stopped.
- Auto recovery is off.
- The Client is running in Personal mode

Procedures

Step 1: View Services status using CTI Services Manager

Step 2: Restart the Presence Server. On the Server machine, open the Services menu from Administrative tools in the Control Panel.

Step 3: Select the ccPresenceServer item and press the play button at the top to start the service.

Step 4: Click on the Cisco help button in the toolbar and make sure the Auto Recover is **On**.

Step 5: You may have to restart the application that you are running (Internet Explorer or Outlook) because the Presence buttons may not refresh when you change your availability and location.

Popup System Tray Icon Becomes Gray

Description

The red Popup icon in the System Tray becomes grayed out.

Possible Causes

- The Local SIP Server has stopped.
- The System SIP Server has stopped.
- The Local CallController has stopped. (TAPPI Mode)
- The CallController Server has stopped and you cannot get phone lines.
- The CME became unavailable.
- The IP Phone or the IP Communicator has stopped.

Procedures

Step 1: Check to see whether the Local SIP Server has stopped.

Step 2: Right-click on the Popup system tray icon.

Step 3: Then move the mouse over the Services menu item. A menu showing the status of the local services will appear.

Step 4: If the Local SIP Server is stopped, then please start the service by clicking on Start All Services.

Step 5: Check to see whether the System SIP Server has stopped. You can check this on the server machine that it is running from. In Control Panel\Administrative Tools\Services, you can verify if the System SIP Server has stopped.

Step 6: If it has stopped, right-click on the service and select start.

Step 7: Check to see whether the CallController Server has stopped. If you are in TAPI mode, open Control Panel\Administrative Tools\Services. Check whether ccCallController service has stopped. If it stopped, right-click on the service and select start to restart the service.

Step 8: If you are in Server mode, check to make sure whether the CallController Server has stopped on the Server machine. You can check that from the Services menu. Find the service called CallController Server and see if it is started or stopped. If it stopped, right-click on the service and select start to restart the service.

Cannot Login

Description

You cannot login.

Possible Causes

- Wrong User information.
- Local SIP Server stopped (TAPI Mode).
- System SIP Server stopped (Server Mode).
- Database Server has stopped.
- The firewall is blocking the Local SIP Server and the Popup.
- The wrong Network adapter is chosen.

Procedures

Step 1: Check whether you typed in the wrong user information.

Step 2: The login information for TAPI mode and Server mode are completely different.

Step 3: If you are unsure about what your username and password are for either modes or you don't have a username and password, talk to your system administrator or service provider for assistance.

Step 4: Check whether the Local SIP Server has stopped. If it is stopped, there is no way for your client to communicate with the System SIP Server or Local CallController to log in.

Step 5: On your machine, check in Services to see if the ccLocalSIPServer service is stopped. If it has stopped, then select the service and click the "play" icon on the top to start the service.

Step 6: Check whether the System SIP Server has stopped. If you are logging in, in Server mode, the System SIP Server must be running to authenticate the user.

Step 7: On the Server machine, check in Services to see if the ccSystemSIPServer service is stopped. If it has stopped, then select the service and click the "play" icon on the top to start the service.

Step 8: Check whether the Database Server has stopped running. In order for the user to be logged in the System SIP Server (Server mode) or CallController (TAPI mode) needs to be able to access the database to authenticate the user.

Can not view the Shortcuts Window (in TAPI Mode)

Description

You can not view the Shortcuts window.

Possible Causes

- The Local CallController has stopped.
- The Client is not logged in.

Procedures

Step 1: Check to see whether the CallController Server has stopped. If you are in TAPI mode, open Control Panel\Administrative Tools\Services. Check whether ccCallController service has stopped. If it stopped right-click on the service and select start to restart the service.

Step 2: Restart Popup to log in.

Can not view the Contacts Window (in TAPI Mode)

Description

You can not view the Contacts window.

Possible Causes

2. The Local CallController has stopped.
3. The Client is not logged in.

Procedures

Step 1: Check to see whether the CallController Server has stopped. If you are in TAPI mode, open Control Panel\Administrative Tools\Services. Check whether ccCallController service has stopped. If it stopped right-click on the service and select start to restart the service.

Step 2: Restart Popup to log in.

Can not view the Logs Window (in TAPI Mode)

Description

You can not view the Logs window.

Possible Causes

4. The Local CallController has stopped.
5. The Client is not logged in.

Procedures

Step 1: Check to see whether the CallController Server has stopped. If you are in TAPI mode, open Control Panel\Administrative Tools\Services. Check whether ccCallController service has stopped. If it stopped right-click on the service and select start to restart the service.

Step 2: Restart Popup to log in.

Can not view the Status and the Rules Windows (in TAPI Mode)

Description
You can not view the Status and the Rules window.

Possible Causes
The Status and the Rules are not available in the TAPI mode

CHAPTER 11

Mobility Troubleshooting

This chapter describes the common error conditions that occur with the Unified CallConnector Mobility Service and the steps to resolve them. The following are the areas of possible error conditions that will be covered:

Single Number Reach doesn't work properly:

The SNR Works intermittently:

The Mid-Call Features doesn't work:

The MNR does not work properly:
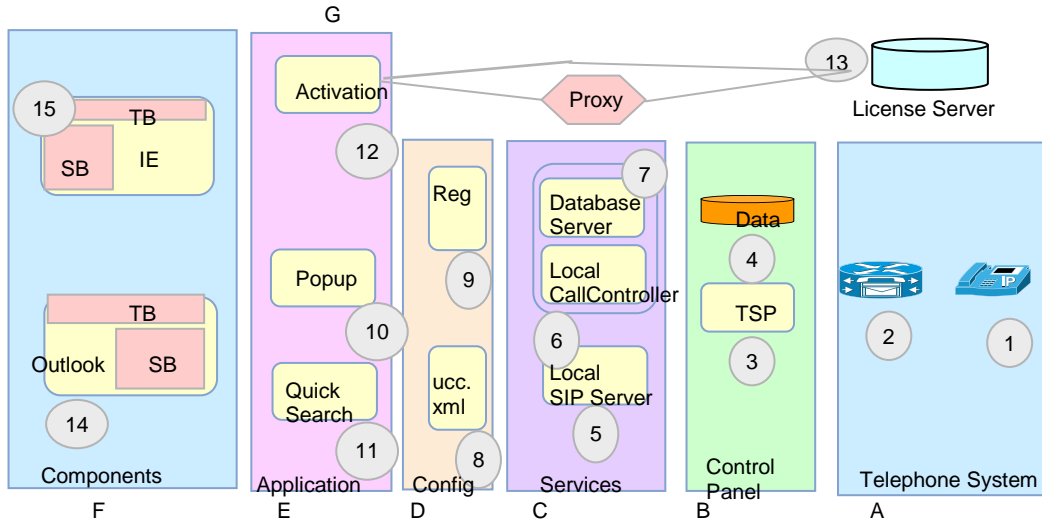
The reached call gets dropped when the user answers it:

The Dial-in System Access doesn't work properly:

The Mobility Service doesn't play custom recorded voice prompt:

UCC Mobility Troubleshooting

While using the Unified CallConnector, users may experience some common problems. This chapter focuses on troubleshooting these common problems. The troubleshooting information contains information on the nature of the problems and steps to solving these problems.

The Unified CallConnector system consists of multiple interacting components. These components are shown below with a summary of the impact of a failure in a component and the appropriate debugging tool.

Summary of Component Failure and Possible Failure Symptoms

    a.   IP Phone Not Registered; Cannot/Lost Connection to CME Router:

    b.   Cannot Register, Cannot Access/Corrupted Database: From Control   Panel open Phone & Modems; Admin Tools ->ODBC ->System DSN

    c.   GUI Gray; Unable to Connect/Login: Connectivity Status; Windows Services ->Stop/Start

    d.   Reset Activation, Change Configuration: Windows Registry; UCC.XML in System32

    e.   Cannot View Information (caller id, search results): Popup Options; UCC Debug Logs

    f.   Toolbar Not Showing, IE/Outlook Crash: Unregister/Register.bat files

    g.   Activation Timeout: Check firewall and IE settings

This chapter describes the common error conditions that occur with the Unified CallConnector Mobility Service and steps to solving these problems.

Mobility Features Troubleshooting

Single Number Reach doesn't work properly:

Description	The SNR does not launch after a personal routing policy is created.
Possible Causes	Automation server is not running CallConnector fails to acquire ephone. The ephones in CME are not available The personal routing policy is not setup correctly SNR session or softphones exhausted. Not enough PSTNs to serve SNR.
Procedures	Launch the CTIServer Server Manager to check the automation server status making sure it is "Started". If not, click Stop and wait until all servers are stopped then click Start. Launch the CTIServer Server Manager to check the CallConnector server status making sure it is "Started". If not, click Stop and wait until all servers are stopped then click Start. Launch the Cisco CallConnector Server Wizard and go to the Automation Ephone Pool setup page to verify the ephone pool setup making sure the ephones are assigned correctly. Also, it is required to assign SNR application to at least one ephone pool. Check the personal routing policy's condition checks, making sure all the enabled conditions are matched. Add more softphones and increase SNR sessions.

Description	SNR does not call my PSTN reach #
Possible Causes	Not enough PSTN The Dial plan not setup correctly The Timeout is too short
Procedures	Configure your phone dialing rules correctly from your Windows 'Phone and Modem Options' From the server Wizard, increase the Timeout period

Description	Cannot create/edit rules
Possible Causes	Automation Server is not running Client is not in Server/Client mode Client is not connecting to the Server or is not running
Procedures	Launch the CTIServer Server Manager to check the automation server status making sure it is "Started". If not, click Stop and wait until all servers are stopped then click Start. Change Client to run in Server/client mode. Start the Client.

Description	SNR does not show the Caller ID
Possible Causes	Caller ID forward is disabled The Analog line does not transmit Caller ID
Procedures	Run the Server Wizard to enable the Caller ID forwarding Note: Mobility server cannot publish the Caller ID through Analog lines which are not configured to show the Caller ID information.

Description	SNR cannot authorize me to pick up and routed phone call
Possible Causes	Using the DISA password instead of the Tel password
Procedures	Please use the Tel password which is set up in the client Popup options

The SNR Works intermittently:

Description	Sometimes SNR does not launch even tough the servers have enough ephones, softphones and SNR sessions.
Possible Causes	Ephones/Softphones are not returned to their pools.
Procedures	Please wait and try again later. When the call terminates, the mobility does some cleanup procedures then returns the softphones and SNR sessions to their pool.

The Mid-Call Features doesn't work:

Description	The Mid-Call Features doesn't respond to the user's input once an SNR session is established.
Possible Causes	Mid-Call Features is not enabled Hardware Conferencing is not enabled One of the participants pressed '##' (this will terminate the Mid-Ca;; features or Dial-in Access sessions)
Procedures	Launch the Cisco CallConnector Server Wizard and go to the Automation Mobility Service setup page. Check the "Allow mid-call to access features" option is enabled in the Single Number Reach Options section. Go to the Settings to Access CME/US500 Features setup page making sure that the option "Use Hardware conferencing" is checked. In the case of one of the participants pressing '##', please hang-up and reestablish the connection.

Description	DISA show my home phone in the Caller ID instead of my office phone.
Possible Causes	'Hide User Phone Number' is disabled
Procedures	Run the server wizard and make sure the 'Hide User Phone Number' is enabled.

The MNR does not work properly:

Description	MNR does not ring all reach phone numbers
Possible Causes	Not enough softphones
Procedures	To use the MNR, you need "X+1" softphones available. X is the number of simultaneous reach numbers you would like to have. Note: When you pick up the call from one of your reach numbers all X softphones are returned to the pool and you are only occupying 1 softphone.

The reached call gets dropped when the user answers it:

Description	When the mobility service gets the incoming call and tries to route the call to the user, the reached call gets dropped too fast.
Possible Causes	Timeout for user answer setting might be too short One of the reach calls has been successfully established
Procedures	Launch the Cisco CallConnector Server Wizard and go to the Automation Mobility Service setup page to increase the Timeout for user answer value.

The Dial-in System Access doesn't work properly:

Description	The Dial-in System Access doesn't work when the user calls the DISA pilot number.
Possible Causes	Automation server is not running DISA features is not enabled No pilot number or ephone assigned for DISA pilot number configuration The hunt-group number is being used as a DISA number
Procedures	Launch the CTIServer Server Manager to check the automation server status making sure it is "Started". If not, click Stop and wait until all servers are stopped then click Start. Launch the Cisco CallConnector Server Wizard and go to the Automation Mobility Service setup page making sure that the option Allow Dial-in access is checked. Check the DNs list box in the Dial-in Access Options section making sure the DISA pilot number that the user called is in the list. If the pilot number you intend to use is not in the list, then you need to assign an ephone that has the pilot number to an ephone pool set to be dedicated and assign the DISA application to the ephone pool.

Description	The outside access code have to be entered while setting up the rule
Possible Causes	The Dial plan is not properly configured.
Procedures	Configure the client's Dial plan

Description	Everyone has access to my DISA server or no one has access to my DISA server
Possible Causes	The 'Authentication Type' is incorrect
Procedures	Run the server wizard and select the appropriate Authentication Type Run the Client to rest the DISA password (from the Popup, Options window, Contact tab). Enter the new password and click **update**.

The Mobility Service doesn't play custom recorded voice prompt:

Description	
	The mobility service doesn't play custom voice prompt that users recorded.
Possible Causes	Language setting is incorrect Location or Name of the prompt files are invalid Audio format of the prompt files are invalid
Procedures	Launch the Cisco CallConnector Server Wizard and make sure the language setting on the first setup page is selected as "Custom" The location of the prompt files must be the Cisco Unified CallConnector Server installation path\Wave\Custom directory. The required audio format criteria for custom recorded voice prompt are: Bit Rate: 128kbps Audio Sample Size: 16bit Channels: 1(mono) Audio Sample Rate: 8bit Audio Format: PCM