Cisco Unified Quick Connect Administration Guide

Release 4.4

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-18495-01

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

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

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

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

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

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

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

Cisco Unified Quick Connect Administration Guide, Release 4.4
© 2009 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface vii

Overview vii

Audience vii

Organization vii

Related Documentation viii

Other Resources ix

Document Conventions ix

Obtaining Documentation and Submitting a Service Request x

Cisco Product Security Overview x

CHAPTER 1 **Introduction to Cisco Unified Quick Connect** 1-1

Overview 1-1

Infrastructure Requirements 1-1

Server Hardware Requirements 1-2

Server Software Requirements for Co-Resident Installation 1-2

Server Software Requirements for Standalone Installation 1-3

Supported Directory Servers 1-3

Salesforce.com Service Requirements 1-4

Supported IP Telephony Systems 1-4

Supported Phones 1-4

CHAPTER 2 **Architecture and Deployment** 2-1

Cisco Unified Quick Connect Modules 2-1

Unified Quick Connect Server Software Integration 2-2

Deploying Cisco Unified Quick Connect 2-4

Deployment Configurations 2-5

Single-Server, Single-Site Configuration 2-5

Multi-Server, Multi-Site Configuration 2-5

Broadcasting Considerations When Using Unicast 2-7

Multi-Server (High-Availability), Multi-Site Configuration 2-7

High-Availability for Cisco Unified Quick Connect 2-7

References 2-8

CHAPTER 3 **Pre-installation Tasks** 3-1

Gathering Installation and Configuration Information 3-1
Starting Windows Services 3-4
Preparing Support for Dual NIC Cards 3-5
Preparing Cisco Unified Application Environment 3-6
Preparing Cisco Unified Communications Manager 3-8
Configuring Directory Services 3-8
If Search is Not Required Before PTT 3-9
Preparing the Enterprise Directory Server 3-10
Binding to Directory Server 3-10
Configuring Directory Server 3-11
Configuring Multiple Directory Servers 3-14
Preparing Salesforce.com 3-15
Providing API Access to Cisco Unified Quick Connect for Developers 3-15
Preparing Microsoft Exchange 3-16
Preparing Unified Quick Connect Server 3-18
Installing Software Prerequisites 3-18
Configuring ASP.NET 3-18
IIS Configuration 3-18
Optional: Installing Active Directory Application Mode 3-19
Configuring a Second Partition and Indexes 3-23
Managing Directory Partitions in Active Directory Application Mode 3-23
Connecting and Binding to ADAM Using Ldp.exe 3-23
Adding Application Directory Partitions 3-24
Creating Indexes 3-25
Installing the ADAM Schema Snap-in 3-25
Adding Indexes Through the ADAM Snap-in 3-26

CHAPTER 4 **Installing Unified Quick Connect Server** 4-1

Requirements for Microsoft SQL Server 2005 4-1
Setting Authentication Parameters 4-2
Requirements for Cisco Unified Application Environment 4-2
Requirement for Dev Tools Installation Based on Installation Environment 4-2
Installing Optional Third Party Software Components 4-3
Running the Setup Wizard 4-3
Completing the Installation 4-8
Installing Cisco Unified Quick Connect Applications in Cisco Unified Application Environment 4-11

Post-Installation Configuration 4-13
Configuring PTT Session Priority 4-13
Configuring the ExitALL Parameter 4-13

CHAPTER 5 **Configuring Cisco Unified Quick Connect Server 5-1**
Required and Optional Configuration Tasks 5-1
Logging In and Out of WebAdmin 5-2
Configuring the Default Web Site Port Number 5-2
Enabling SSL Security for Cisco Unified Quick Connect WebAdmin 5-2
Disabling Anonymous Login to Cisco Unified Quick Connect WebAdmin 5-3
Configuring Servers 5-3
Server Considerations 5-3
Configuring Enterprise Directory Servers 5-3
Directory Server Layout in WebAdmin 5-4
Adding a Directory Server 5-5
Adding Salesforce.com as a Directory Server 5-7
Adding Microsoft Access as a Directory Server 5-8
Configuring Enterprise Policy Servers 5-9
Adding Policy Servers 5-9
Deleting and Editing Policy Servers 5-10
Configuring IP-PBX Servers 5-10
PBX Servers: Using IP-PBX Aliases 5-13
PBX Servers: Associating a Provider with a Directory Group 5-14
PBX Servers: Associating a Service with a Provider 5-15
Using Phone Number Masks 5-16
Matching 5-16
Provider Based Masking 5-16
Directory Server Number is longer than PBX Number 5-16
PBX Number is longer than Directory Server Number 5-17
PBX Number is Formatted Differently than Directory Server Number 5-17
Configuring Unified Quick Connect Locations 5-18
Locations: Associating Providers 5-20
Locations: Associating Directories 5-20
Locations: Associating Broadcasters 5-21
Locations: Associating Policy Servers 5-21
Locations: Device Status 5-22
Configuring Advanced Settings 5-22
Configuring Phone UI Appearance 5-24
Search Settings tab 5-24

Search Results tab 5-25
Phone Softkey Layout tab 5-25
Shortcuts tab 5-26
Other Settings tab 5-27
Phone UI Field Descriptions 5-28
Phone UI: Configuring Phone Softkey Layout 5-29
Adding a Unified Quick Connect Feature SoftKey 5-29
Changing the Order of Soft-Keys 5-30
Configuring Unified Quick Connect Templates 5-31
Plug-ins and Work-flow 5-32
Configuring Directory Mapping Attributes 5-32
Configuring Directory Search Static Filters 5-33
Native Static Filters 5-34
Example Native Static Filter 5-34
Mapped Static Filters 5-34
Example Mapped Static Filter 5-36
Configuring Presence Enabled Broadcasts 5-37
Configuring Policies 5-37
Configuring Access Policies 5-37
Editing Simple Policies 5-37
Adding a New Complex Policy 5-38
Editing Complex Policies 5-42
Centralized Configuration Service 5-43
Modifying Centralized Configuration from WebAdmin 5-44
Modifying Centralized Configuration XML Files 5-44
Access to Centralized Configuration 5-45
Verifying the Installation Using Phones 5-45

CHAPTER 6 **Customizing Cisco Unified Quick Connect** 6-1
Customizing the Template for Push-to-Talk 6-1
Customizing the Push-to-Talk OCM File 6-1
Customizing Presence-related Parameters 6-2
Customizing Media-related Parameters 6-2
Customizing Pre-configured Push-to-Talk Parameters 6-3
Using the Web Service API Programmatically 6-5
Format of the InitializeBCPayload Parameters 6-6
Organizer section 6-8
Invitees Group section 6-8

CHAPTER 7 **Cisco Unified Quick Connect Tools** 7-1

What Tools are Available? 7-1

Synchronizing Unified Quick Connect Servers 7-2

Manually Invoking Synchronization 7-2

Services 7-3

Viewing Status of Services 7-3

Restarting Services 7-4

Provisioning 7-5

Adding a User 7-5

Searching and Querying for Users 7-7

Working with Reports 7-9

Log Files 7-10

Setting Log Levels 7-10

Exporting Logs 7-12

Licenses 7-13

CHAPTER 8 **Troubleshooting** 8-1

Using Unified Configuration Files 8-1

Commonly Found Issues 8-1

Unable to Start Unified Quick Connect PBX Service 8-2

Unable to Access Unified Quick Connect WebAdmin 8-2

Windows Security Updates and ASP.net 8-3

Unable to Push Content on Phone 8-3

CHAPTER 9 **System Maintenance** 9-1

Adding and removing a Directory Server 9-1

Adding and removing a Provider 9-2

Adding and removing a Unified Quick Connect Location or Unified Quick Connect Server 9-3

Adding and removing a Policy Server 9-3

Adding and removing a Unified Quick Connect User 9-3

Associating Devices to the Push User 9-4

Configuring the Directory URL 9-5

Directory URL 9-5

Adding and removing an Access Policy 9-5

Adding and removing a Phone Number Mask for Presence, Matching 9-7

Windows Services Administration 9-7

Starting and Stopping Microsoft Windows Services 9-7

Starting and Stopping Web Services 9-8

APPENDIX A **Cisco Unified Quick Connect Template Files** A-1

List of Template Files A-1

APPENDIX B **Directory Server Parameters** B-1

Directory Server Parameters Mapping Table B-1

APPENDIX C **Cisco Unified Quick Connect Advanced Settings** C-1

Advanced Settings C-1

INDEX

Preface

This preface describes the purpose, audience, organization, and conventions of this guide and provides information on how to obtain additional information.

This section includes these topics:

- Overview, page vii
- Audience, page vii
- Organization, page vii
- Related Documentation, page viii
- Other Resources, page ix
- Document Conventions, page ix
- Obtaining Documentation and Submitting a Service Request, page x

Overview

This document provides information about installing, configuring, and managing Cisco Unified Quick Connect.

Audience

This guide is intended for administrators and who want to install and manage Unified Quick Connect.

Organization

This guide is organized as follows:

Chapter 1, “Introduction to Cisco Unified Quick Connect”	Provides an overview of Cisco Unified Quick Connect and lists hardware and software requirements.
Chapter 2, “Architecture and Deployment”	Describes the architecture and deployment options for Cisco Unified Quick Connect

Chapter 3, “Pre-installation Tasks”	Describes pre-installation tasks for Cisco Unified Quick Connect.
Chapter 4, “Installing Unified Quick Connect Server”	Describes database requirements and how to use the Cisco Unified Quick Connect Setup Wizard to automatically install the Cisco Unified Quick Connect Server components.
Chapter 5, “Configuring Cisco Unified Quick Connect Server”	Describes in detail the configuration tasks that can be performed for Cisco Unified Quick Connect Server.
Chapter 6, “Customizing Cisco Unified Quick Connect”	Describes customizing Cisco Unified Quick Connect.
Chapter 7, “Cisco Unified Quick Connect Tools”	Discusses the tools available to manage Cisco Unified Quick Connect.
Chapter 8, “Troubleshooting”	Discusses troubleshooting resources.
Chapter 9, “System Maintenance”	Discusses common maintenance tasks.
Appendix A, “Cisco Unified Quick Connect Template Files”	Describes the .ocm template files included with Cisco Unified Quick Connect.
Appendix B, “Directory Server Parameters”	Defines the attributes that can be configured in Cisco Unified Quick Connect to support the directory server.
Appendix C, “Cisco Unified Quick Connect Advanced Settings”	Describes the Cisco Unified Quick Connect Server advanced settings that are accessed from Unified Quick Connect Web Admin > Servers > Advanced Settings.

Related Documentation

Table 1provides links to related product documentation.

Table 1 Product Documentation

Related Information	URL
Cisco Unified Quick Connect User Guide, Release 4.4	*http://cisco.com/en/US/products/ps10347/tsd_products_support_series_home.html*
Administration Guide for the Cisco Unified Application Environment, Release 2.5	*http://cisco.com/en/US/products/ps7058/prod_maintenance_guides_list.html*
Cisco Unified Quick Connect Release Notes, Release 4.4	*http://cisco.com/en/US/products/ps10347/tsd_products_support_series_home.html*

Other Resources

The table below lists the additional resources available to developers who want to use the Cisco Unified Application Environment to create and run applications.

Resource Name	Resource Description URL
Cisco Developer Community - Cisco Unified Application Environment home page.	The Cisco Unified Application Environment home page. Contains links to all developer resources, including forums, blogs, our wiki and more. *http://developer.cisco.com/web/cuae/home*
Cisco Unified Application Environment Wiki	Access and contribute to installation instructions, example applications, How-to articles, and more. *http://developer.cisco.com/web/cuae/wikidocs*
Cisco Unified Application Environment Forums	View the latest posts and subscribe to the developer forum, the announcements forum, the beta forum, or the general interest forum. *http://developer.cisco.com/web/cuae/forums*
Developer IRC Channel	Developer chat group. To participate, join our IRC channel, #cuae on Dalnet (irc.dal.net).

Document Conventions

This document uses the following conventions:

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	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`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.

Convention	Description
^	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.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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

Cisco Product Security Overview

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

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html.

If you require further assistance please contact us by sending email to export@cisco.com

CHAPTER 1

Introduction to Cisco Unified Quick Connect

This chapter provides an overview to Cisco Unified Quick Connect. It has the following topics:

- Overview, page 1-1
- Infrastructure Requirements, page 1-1

Overview

Cisco Unified Quick Connect comprises the following components:

- Cisco Unified Quick Connect Server—the Cisco Unified Application Environment solution which enables access to Push-to-Talk capabilities on Cisco IP phones using existing directories.
- Cisco Unified Quick Connect Web Admin—the Cisco Unified Quick Connect Application includes a Web Admin component which allows the administrators to configure, manage, and customize Unified Quick Connect. This includes configuring directory servers and IP-PBX providers, phone number masking, Locations, directory mapping attributes, directory filters, policies, centralized configuration, and phone UI configuration.
- Cisco Unified Quick Connect Phone—the phone UI application that allows users to create Push-to-Talk communications with users and groups from Cisco Unified IP phones.

Infrastructure Requirements

This section gives information on the hardware and software requirements and other service considerations for running Cisco Unified Quick Connect. This section includes:

- Server Hardware Requirements
- Server Software Requirements for Co-Resident Installation
- Server Software Requirements for Standalone Installation
- Supported Directory Servers
- Salesforce.com Service Requirements
- Supported IP Telephony Systems
- Supported Phones

Server Hardware Requirements

Cisco Media Convergence Servers (MCS) (series 7816, 7825, 7835, 7845) with MCS OS 2003, configured with the following minimum hardware requirements:

- Processor: Intel Xeon or higher, dual processor
- Processor clock speed: 2 GHz or higher
- Memory: 2 GB (4 GB based on feature usage)
- Hard disk space: 40 GB
- Network Interface Card (NIC): single-NIC is supported by default. Dual-NIC cards can be supported only by performing the configuration described in Preparing Support for Dual NIC Cards.

Each Cisco Unified Quick Connect server may support up to 5000 devices. The number varies depending on feature usage and Busy Hour Call Attempts (BHCA).

For MCS data sheet, see
http://cisco.com/en/US/products/hw/voiceapp/ps378/products_data_sheets_list.html

Server Software Requirements for Co-Resident Installation

The minimum software requirements for a co-resident installation (where Cisco Unified Quick Connect and Cisco Unified Application Environment are installed on the same machine) are:

- Cisco Operating System image
- Microsoft Windows 2003 Server Standard SP2
- Microsoft SQL Server 2005 Standard SP2
  This is available for purchase from Microsoft. For more information visit,
  http://www.microsoft.com/sqlserver/2005/en/us/Standard.aspx

  Service Pack 2 (SP2) is a free download from Microsoft. For more information visit,
  http://www.microsoft.com/downloads/details.aspx?FamilyId=d07219b2-1e23-49c8-8f0c-63fa18f26d3a&displaylang=en
- Microsoft Internet Information Services 6.0
  This is packaged with the Microsoft Windows Server 2003 operating system.
- Microsoft Exchange Server MAPI Client and Collaboration Data Objects
- Java Media Framework 2.1.1E
- Microsoft .NET Framework 2.0
  This is available as a free download from Microsoft. For more information visit,
  http://www.microsoft.com/downloads/details.aspx?FamilyID=0856EACB-4362-4B0D-8EDD-AAB15C5E04F5&displaylang=en

Note Do not uninstall the Microsoft .NET Framework 3.0 that is installed as part of Cisco Unified Application Environment installation.

- ASP.NET Version 2.0.
- Java Runtime Environment 6.0
  This is available in the support files directory provided with the product.

- Internet Explorer 6.0 SP1 or higher is required for Unified Quick Connect WebAdmin. This is available as a free download from Microsoft. For more information visit, *http://www.microsoft.com/windows/ie/ie6/downloads/critical/ie6sp1/default.mspx*

Server Software Requirements for Standalone Installation

The minimum software requirements for a standalone installation (where Cisco Unified Quick Connect and Cisco Unified Application Environment are installed on separate machines) are:

- Cisco Operating System image
- Microsoft Windows 2003 Server Standard SP2
- Microsoft SQL Server 2005 Standard SP2
- Microsoft Internet Information Services 6.0
- Microsoft Exchange Server MAPI Client and Collaboration Data Objects
- Java Media Framework 2.1.1E
- Microsoft .NET Framework 2.0 and 3.0

Note Microsoft .NET Framework 2.0 is required for the Cisco Unified Quick Connect product, and .NET Framework 3.0 is required for Cisco Unified Application Environment Dev Tools.

- Cisco Unified Application Environment Dev Tools
  This is available at:
  http://developer.cisco.com/web/cuae/downloads

Note .NET Framework 3.0 must be installed before installing Dev Tools.

- ASP.NET Version 2.0.
- Java Runtime Environment 6.0
- Internet Explorer 6.0 SP1 or higher is required for Unified Quick Connect WebAdmin

Supported Directory Servers

The supported directory servers are:

- Microsoft Active Directory with Windows Server 2000 or Windows Server 2003 (ADSI 2.0, 2.5, or 2.6)
- LDAP v2 directories including: Open LDAP v2.3, Cisco DCD.

  SSL for authentication is also supported.
- Microsoft Exchange 2000 or 2003 SP2 (GAL)
- Salesforce.com
- SQL based directory repositories (some customization required)
- Active Directory Application Mode (ADAM)

Salesforce.com Service Requirements

The Salesforce.com account must be an Enterprise Edition or Unlimited Edition account, as these accounts provide access to the Salesforce.com API.

Application developers who use ADN (App-Exchange Developer Network, available at *http://salesforce.com/developer*) are also supported, but additional configuration is required (described in Providing API Access to Cisco Unified Quick Connect for Developers, page 3-15). Any other account types cannot be supported.

A username and password for an administrative account is required. The security token should be reset.

Supported IP Telephony Systems

The Cisco Unified Communications Manager 5.1 and later, with Cisco Unified Application Environment version 2.5 SR2 or later are supported.

Supported Phones

Feature support varies by phone type and display size.

Table 1-1 lists supported phone models and phone loads.

Table 1-1 Supported Phone Models and Phone Loads for Cisco

Vendor	Phone Model	Phone Loads
Cisco	7921	Firmware 1.1(1)
Cisco	7925	7925G-1.3.0.40.LOADS
Cisco	7940	P00308000900
Cisco	7941	SCCP42.8-4-2S SCCP42.8-4-3S
Cisco	7942	SCCP42.8-4-2S SCCP42.8-4-3S
Cisco	7945	SCCP45.8-3-35
Cisco	7960	P00308000800 P00308000900
Cisco	7961	SCCP61.8-4-2S SCCP61.8-4-3S
Cisco	7962	SCCP61.8-4-3S
Cisco	7965	SCCP65.8-4-3S
Cisco	7970	SCCP70.8-4-1SR2 SCCP70.8-4-2S
Cisco	7971	SCCP70.8-2-2SR1S SCCP70.8-3-1S

Table 1-1 Supported Phone Models and Phone Loads for Cisco

Vendor	Phone Model	Phone Loads
Cisco	7975	SCCP70.8-4-3S
Cisco	IP Communicator	2.0 (2.1.3)

CHAPTER 2

Architecture and Deployment

This chapter describes the architecture and deployment options for Cisco Unified Quick Connect. It describes the following topics:

- Cisco Unified Quick Connect Modules, page 2-1
- Deploying Cisco Unified Quick Connect, page 2-4

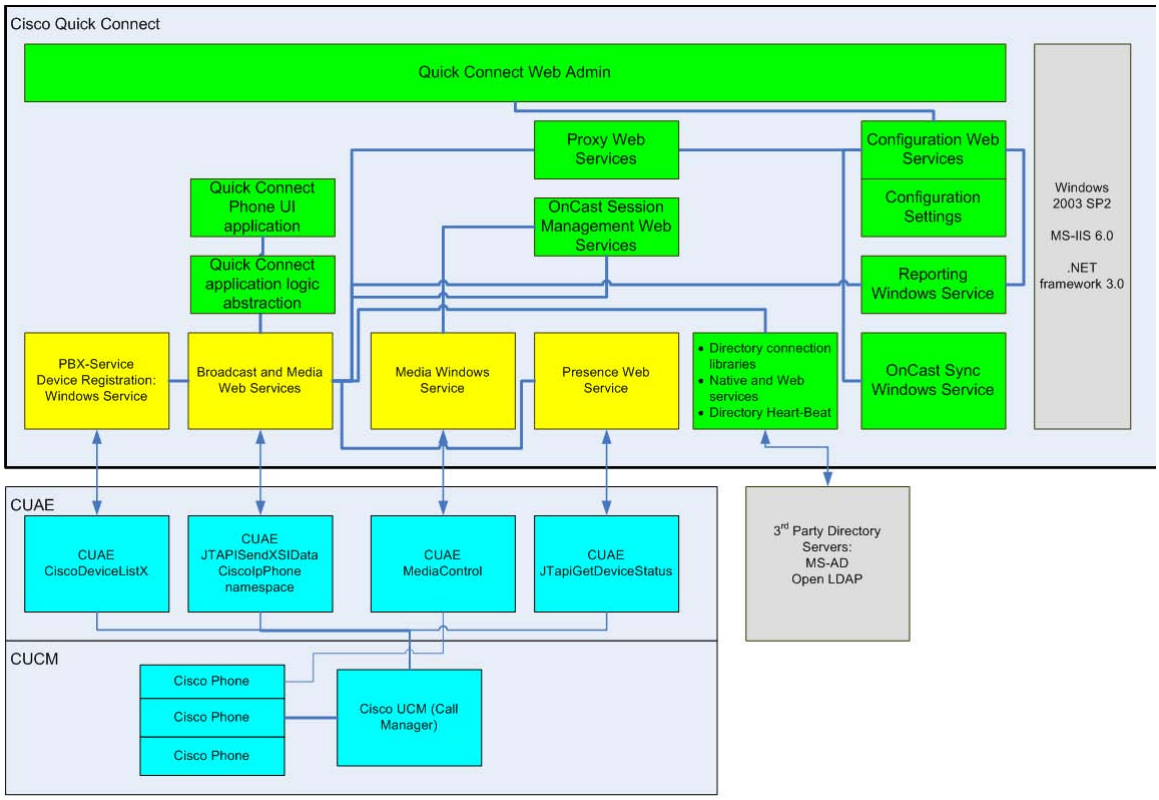
Cisco Unified Quick Connect Modules

Cisco Unified Quick Connect is composed of the modules illustrated in Figure 2-1.

The solution is based on a distributed, service oriented architecture (SOA) and is composed of a collection of Windows services and SOAP-based Web services. The independence of the modules enables administrators to configure and distribute various components independently. This service-based approach provides integration and customization, and simplifies troubleshooting and pinpointing points of failure and bottlenecks.

For integrators, this approach enables developers to leverage the open-standards based Web-services approach and use the components independently and from within their own applications.

Figure 2-1 Unified Quick Connect Modules



Unified Quick Connect Server Software Integration

Table 2-1 outlines the various Unified Quick Connect server components. "Module Name" is the file you will see in Windows Services or IIS. "Diagram Name" is the name shown in Figure 2-1 on the previous page.

Table 2-1 Unified Quick Connect Server Components

Component	Description	Module Name(s)	Diagram Name
Broadcast Service	This component is responsible for orchestrating and delivering all the text/image/audio broadcasts to the IP devices.	WAN Broadcast Web-service in IIS: OnCast Web Service	Broadcast and Media Web Services
Presence Server	This component tracks device presence.	IIS: OnCastPresWebService OnCast Presence Service	Presence Web Services

Table 2-1 Unified Quick Connect Server Components (continued)

Component	Description	Module Name(s)	Diagram Name
PBX Service	This component is responsible for retrieving information from IP-PBX Servers to retrieve extension numbers and device network information. The PBX Service gets all device information from the IP-PBXs and Directory Servers and combines the data into a cached repository which is used by Unified Quick Connect to easily identify users and phones.	OnCastPBXService	PBX Service
Media Server	This component leverages the underlying CUAE media services to perform all handling of media service.	OnCastMediaServer	Media Windows Service
Unified Installer	Deploys application on a server.	Windows application	
Phone UI	These components are responsible for the Phone User Interface including rendering menus and soft-keys, communicating with other components to send the user requests and showing responses on the phone.		Unified Quick Connect Phone UI application
Web Admin: Configuration	These components are responsible for managing and storing all the configurations in a centralized XML depository. With the provided Web user interface, administrators can easily change and set configuration values.	Web application	
Session Service	This component maintains various 'session' information about broadcasts and service invocations in progress. The service also manages media ports and distributes load information among distributed Unified Quick Connect broadcast servers.	IIS: LSSessionServiceWeb	Session Management Web Services
Synchronization Server	Unified Quick Connect Servers in High-availability/distributed environments share data and configuration information that has up-to-date configuration information. This component synchronizes various data and configuration files among Unified Quick Connect servers participating in a server 'cluster'.	IIS: OnCastSyncWebService	Synchronization
Policy Server	This component controls the rights for all the available functions in Unified Quick Connect. Policy Server determines if a user is able to broadcast, make a phone call, group call/conference to other users and groups, or see other users' detail information.	IIS: PolicyService	Policy Web Services

Table 2-1 Unified Quick Connect Server Components (continued)

Component	Description	Module Name(s)	Diagram Name
Directory Connection library	This component handles any communication with the enterprise directory servers. Directory Connector uses ADSI to connect to Microsoft's Active Directory, LDAP to any standard LDAP Server, and MAPI to connect to Microsoft Exchange for users' detail information.	IIS: OnCastDirectoryConnection WebService MAPIConnector Native libraries	Directory Connection
Cache Service	This service copies content from existing systems (such as LDAP or Exchange servers) into a directory that Unified Quick Connect uses to avoid constantly accessing the enterprise systems. This avoids placing excessive loads on the primary servers. Synchronization and refreshing of data can happen as often as desired.	DirectoryCacheService	Cache Service
Centralized Configuration	This service creates and updates system, organization and user personalized options.	Windows service	
Device Status Monitoring	This service monitors the status of phones in real-time, for example, if they are on-hook (idle) or off-hook (in use). This information is also passed to the Presence Server.	OnCast Device Status	Device Status Monitoring
Heartbeat Server	This component maintains a connection between Unified Quick Connect and your specified enterprise directories. Heartbeat clients can register to receive notifications about the following connection statuses: a.When a directory connection is established. b.When a directory connection is established to the Primary Directory server.	DirectorHeartBeatService	Directory Heartbeat
Reporting Service	This component provides reporting information about the progress in various broadcasting service stages (from invocation through completion, per device, per session). The output can be optionally directed to MS-SQL server.	Windows service.	

Deploying Cisco Unified Quick Connect

The deployment configuration that best fits your organization's needs should be determined during the design phase of a Unified Quick Connect deployment.

Deployment Configurations

This section is to be used during the design phase of an implementation and is intended to provide guidelines on how to design a Unified Quick Connect network. The configurations for each scenario will vary significantly based on customer requirements.

The following configurations can be deployed:

- Single-server, single-site
- Multi-server (High-availability), multi-site
- Highly-available multi-site deployment using Microsoft NLB

Single-Server, Single-Site Configuration

Unified Quick Connect can be installed and deployed entirely on a single server. In addition, the Unified Quick Connect Server can co-exist with the underlying enterprise directory server (on the same physical server). One Unified Quick Connect server can service multiple locations. One Cisco Unified Application Environment server is required per Unified Quick Connect server. This can be on the same machine or a separate machine.

Pros:

- Simple installation and configuration.
- Using the pre-installation configuration, the product is up and running out of the box.
- If multicast is enabled across a sufficiently high-network-bandwidth WAN, broadcasts can all be managed from a central and single server location.

Cons:

- Lack of high-availability.
- In WAN based environments, remote devices would increase network traffic. Specifically, for environments where Multi-cast is disabled across the WAN, audio traffic - live or recorded - would have to traverse using Unicast, which can lead to serious network congestion.

Recommended for:

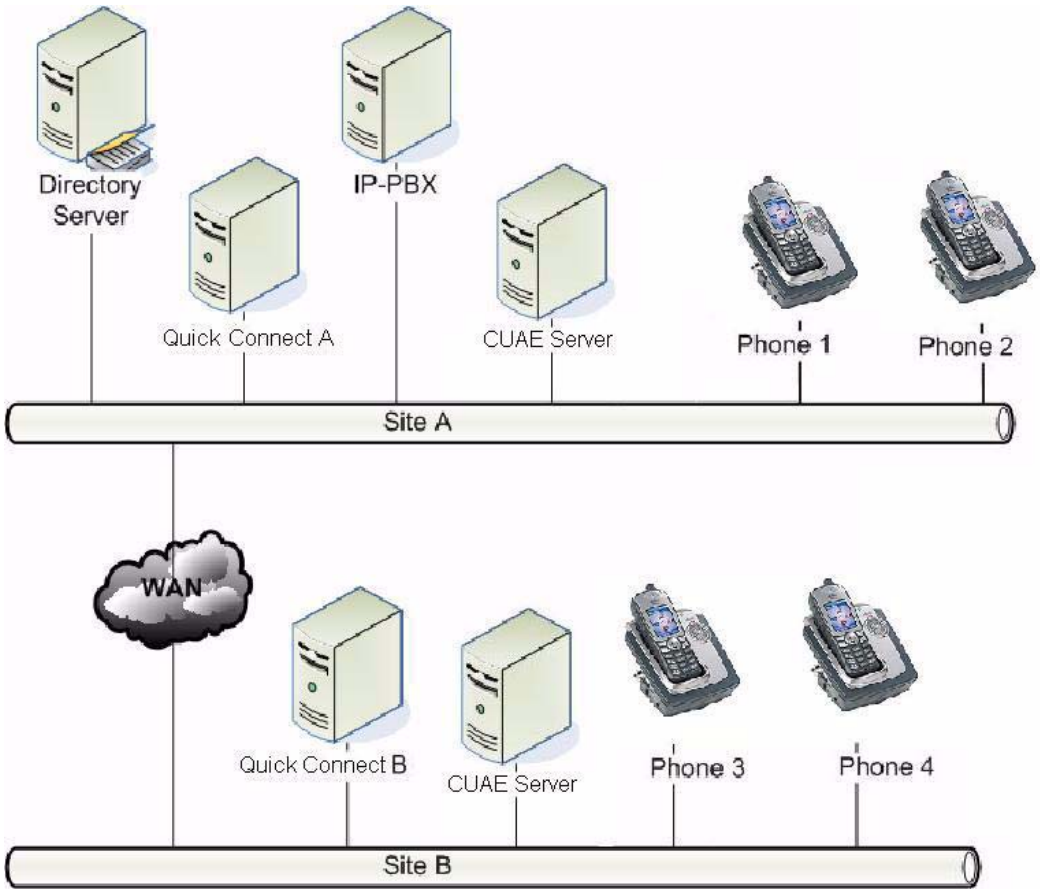
- Environments with smaller than 500 IP device/end-points per site. Limited spanning across high-network-bandwidth WANs with G.729 <-> G.711 trans-coding resources on each side of the WAN to preserve network capacity when reaching remote devices.
- Environments where having a single point of failure is acceptable.
- Environments where the product is used for normal priority paging, not for urgent/emergency notification or day-to-day collaboration automation.

Multi-Server, Multi-Site Configuration

Unified Quick Connect can be installed and deployed on multiple servers across the WAN to minimize the amount of bandwidth utilized for broadcasting (Figure 2-2). This is an important design consideration when using broadcasting across a WAN with, 1) phones that support unicast, or 2) a WAN where IP multicast is disabled. A separate Cisco Unified Application Environment server is required for each Unified Quick Connect server.

In this case, local Unified Quick Connect Servers terminate broadcasts for their own locations regardless of where the broadcasts are initiated. Assume there is a Site A and Site B connected with a WAN. Site A has an IP-PBX, directory server, Unified Quick Connect Server, Cisco Unified Application Environment server, and IP phones. Site B only has a Unified Quick Connect Server, Cisco Unified Application Environment server, and IP phones.

Figure 2-2 Multi-Server, Multi-Site Configuration



Pros:

- Using the pre-installation configuration, the product is up and running out of the box.
- Works fine for Unicast based WANs and IP phones.
- Broadcast load is distributed to local broadcast servers.
- Phones can register with local broadcast servers.
- No single point of failure, highly available and scalable.
- Works well for environments in need of emergency and urgent IP based notification.

Cons:

- Requires additional server administration, monitoring and management.
- Requires detailed network modeling and design.
- Costs more than single server deployments.

Recommended for:

Environments with multiple sites and more than 500 IP device/end-points per site, spanning across high-network-bandwidth WANs with G.729 trans-coding resources on each side of the WAN.

Broadcasting Considerations When Using Unicast

Live voice broadcast from Phone 1 to Phone 2, Phone 3 and Phone 4:

- Unified Quick Connect A sets up a one-way RTP stream from Phone 1 to Phone 2 (on the LAN) and a unicast stream to Unified Quick Connect B. Unified Quick Connect B, in turn, will send a unicast stream to Phone 3 (on the LAN) and Phone 4 (on the LAN). This will utilize four unicast streams (one on Site A's LAN, one on the WAN and two on Site B's LAN).

Pre-recorded audio broadcast from a user in Site 1 (from phone or PC) to Phone 2, Phone 3 and Phone 4:

- The Unified Quick Connect A server transmits a one-way RTP stream to Phone 2 (on the LAN) and a unicast stream to Unified Quick Connect B. Unified Quick Connect B, in turn, will send a unicast stream to Phone 3 (on the LAN) and Phone 4 (on the LAN). This will utilize four unicast streams (one on Site A's LAN, one on the WAN and two on Site B's LAN).

Multi-Server (High-Availability), Multi-Site Configuration

Unified Quick Connect can be installed and deployed on multiple servers at one site to provide scalability and high-availability. One Unified Quick Connect server can service multiple locations. In this mode, each group of servers is grouped using 3rd party network load distribution tools, such as content switches, or using operating system supported network load balancing services, such as Microsoft NLB. Multiple Unified Quick Connect servers can be added at each location. A Cisco Unified Application Environment server is required for each Unified Quick Connect server.

Pros:

- Using the pre-installation configuration, the product is up and running out of the box.
- Works fine for both Multi-cast and Unicast based WANs.
- Broadcast load is distributed to local broadcast servers.
- Phones can register with local broadcast servers.
- No single point of failure, highly available and scalable.
- Works well for environments in need of emergency and urgent IP based notification.

Cons:

- Requires additional server administration, monitoring and management.
- Requires detailed network modeling and design.
- Costs more than single server deployments.

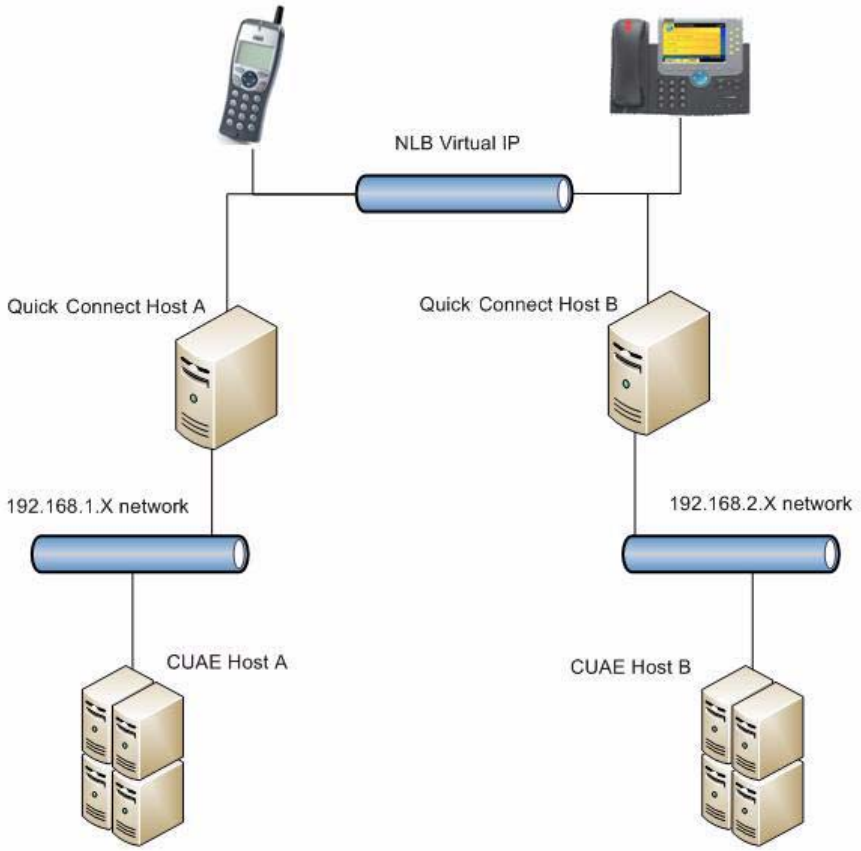
Recommended for:

Environments with multiple sites and more than 500 IP device/end-points per site, spanning across high-network-bandwidth WANs with G.729 trans-coding resources on each side of the WAN.

High-Availability for Cisco Unified Quick Connect

High Availabilitiy for Cisco Unified Quick Connect is provided by having an NLB-based deployment where all phones point to an NLB virtual IP address. All subsequent phones' requests are routed to one of the NLB hosts. The following is a network diagram for the High Availability deployment.

Figure 2-3 High-Availability



Normally, all phones' requests go to one of the NLB hosts, for example, Unified Quick Connect Host A. Unified Quick Connect running on this host communicates with CUAE Host A and processes the requests through this CUAE Host A. If Unified Quick Connect Host A fails then all the subsequent requests are re-directed to Unified Quick Connect Host B. Unified Quick Connect Host B starts processing phones' requests through CUAE Host B.

When Unified Quick Connect Host A comes back up it gets ready for the incoming phones' requests.

References

For more information about using Network load balancing, please use the following references from the Microsoft TechNet site:

NLB Fundamentals

http://technet2.microsoft.com/WindowsServer/en/library/c6c7cd9f-2837-44ab-b7e9-a5ab59bf74931033.mspx?mfr=true

Planning for High Availability and Scalability

http://technet2.microsoft.com/windowsserver/en/library/37b0b6af-c408-4d13-8e73-44a95b92fbac1033.mspx?mfr=true

Improving IIS 6.0 Scalability and Availability with Network Load Balancing

http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/0baca8b73b9-4cd2-ab9c-654d88d05b4f.mspx

Note If the links do not work, search the Microsoft site for the subject listed above the link.

CHAPTER 3

Pre-installation Tasks

This chapter describes pre-installation tasks for Cisco Unified Quick Connect. It describes the following topics:

- Gathering Installation and Configuration Information, page 3-1
- Starting Windows Services, page 3-4
- Preparing Support for Dual NIC Cards, page 3-5
- Preparing Cisco Unified Application Environment, page 3-6
- Preparing Cisco Unified Communications Manager, page 3-8
- Preparing the Enterprise Directory Server, page 3-10
- Preparing Salesforce.com, page 3-15
- Preparing Microsoft Exchange, page 3-16
- Preparing Unified Quick Connect Server, page 3-18

After these tasks are complete, you can install and configure Cisco Unified Quick Connect as described in Chapter 4, “Installing Unified Quick Connect Server”.

Gathering Installation and Configuration Information

The information listed in the following tables is required.

Table 3-1 Pre-installation Checklist: Unified Quick Connect Server Parameters

Required Data	Example or Explanation
IP Address of Unified Quick Connect Server Has port 80 been opened?	Enter an IP address of each IP-PBX node.
Windows Domain Info. Have you inserted the computer into the domain?	Enter the Windows Domain name, if applicable.
Windows Domain User / Password	Enter username as username@domain.com. If not in a domain, enter administrator@hostname, where hostname is the name of a Unified Quick Connect Server.
Unified Quick Connect Directory Configuration Server, if previously created – default is the Unified Quick Connect machine	In most scenarios this is the current Unified Quick Connect Server.

Table 3-1 Pre-installation Checklist: Unified Quick Connect Server Parameters (continued)

Required Data	Example or Explanation
Local broadcast server (should be configured to be the IP address of the Unified Quick Connect machine)	
Load Balancing Server IP address, if any	Typically not applicable.

Table 3-2 Pre-installation Checklist: IP-PBX Parameters

Required Data	Example or Explanation
Type of IP-PBX you will be using	CUAE
PBX version	2.5
Phone vendor models to be used	Refer to "Supported Phones".
Phoneloads for each Phone Type	Refer to list of supported phone loads.
Authorized username and password in the PBX that is allowed to push content to the phones	
Attribute to use in PBX for mapping	Usually the Extension in the IP-PBX, but in some cases may be the User ID configured in the IP-PBX.

Table 3-3 Pre-installation Checklist: Directory Server Parameters

Required Data	Example or Explanation
IP address of your directory server(s)	
Directory ports opened?	Cisco DCD uses 8404; Microsoft Active Directory uses 389; Open LDAP uses 636; Salesforce.com uses port 80.
User Name and password required to access directory servers above	Required if Authentication is enforced. For Microsoft AD, if the Unified Quick Connect Server is in the same domain as the AD server, and the AD server does not require authentication, then username and password is not required. Otherwise, authentication is required. All other directory servers require authentication.
Write access to directory server enabled for user?	Only required if you want to store Complex Access Policies in your directory server. You can also have Complex Access Policies stored in an XML file on the Unified Quick Connect Server.
Hostname or IP address of Microsoft Exchange Server	Required if Personal Address books are to be used
Search Base root directory	

Table 3-3 Pre-installation Checklist: Directory Server Parameters (continued)

Required Data	Example or Explanation
Searchable Attribute: Determines if the Organizational Unit or CN is searchable by Unified Quick Connect. Set to 1000 at the appropriate OU or CN.	Usually set to “flags” or “businessCategory”
Policy Server IP address or file path	IP address for a directory server, or filepath for the Unified Quick Connect Server.

Table 3-4 Pre-installation Checklist: Cisco Parameters

Required Data	Example or Explanation
Version	The Cisco Unified Communications Manager version.
IP Address of Publisher and Subscribers	

- Before you install Unified Quick Connect Server you must obtain environment-specific information. The information depends on the type of Enterprise directory server and IP-PBX being used.
- The directory types listed in Table 3-5 are supported:

Table 3-5 Supported Directory Types

Microsoft Active Directory	SQL Database
Cisco DCD	Open LDAP
LDAP v2	Microsoft Exchange
Salesforce.com	

You will be prompted for connectivity parameters based on the directory server(s) you have selected. These parameters include:

- Host (required): The IP address or name of the Directory server.
- Port (required): Defines which port to use when connecting to LDAP based directory server. This applies to Microsoft Active Directory/DCD/LDAP.

Note If you do not specify the IP address and port, the system performs serverless binding and this applies to Microsoft Active Directory only.

- User name: Defines the user name to be used when connecting. Applies only when Anonymous Binding is unchecked.
- Password: Defines the password to be used when connecting. Applies only when Anonymous Binding is unchecked.
- Anonymous Binding: It is true if the user name and password are specified. Applies to Microsoft Active Directory and Open LDAP.
- Naming Context: Determines the Base DN (distinguished name) of the Directory Server. Applies to DCD/LDAP.

Note This is mandatory for LDAP servers.

- Search Base: Determines the location to begin searches within the directory structure. Applies to Microsoft Active Directory, DCD/LDAP.

Note This is optional.

You will also be prompted for IP-PBX connectivity information:

- PBX User name is the user name of the authorized user used by the Unified Quick Connect Directory product to “push” content to IP phones.
- PBX User password is the password of the authorized user used by the Unified Quick Connect Directory product to push content to IP phones.

Starting Windows Services

Start the Windows Services by performing the following:

Procedure

Step 1 Set the start type to *automatic* and start the following windows services :

- Application Layer Gateway Service
- Network Connections Service
- Network Location Awareness (NLA) Service
- Plug and Play Service
- Remote Access Auto Connection Manager Service
- Remote Access Connection Manager Service
- Remote Procedure Call (RPC) Service
- Telephony Service
- IIS Admin Service
- ASP.Net Status Service
- BITS Services
- HTTP SSL Service
- www Publishing Service

Step 2 For co-resident installations, you must configure the IIS Default Web Site port number to be different from the Cisco Unified Application Environment Web Server port number.

For example, typically CUAE Web Server listens on port 80. In IIS, view the properties for the Default Web Site and assign a valid Default Web Site port number other than port 80.

For standalone installations, this step is not required.

Preparing Support for Dual NIC Cards

If your Cisco Unified Quick Connect server is configured with dual NIC cards, you must assign an IP address in Microsoft IIS Manager by performing the following steps:

Procedure

Step 1 Open IIS Manager and select the **Default Web Site**. Right-click to open the **Properties** window.

Step 2 On the Website tab, select the IP address for a NIC card from the *IP address* drop-down menu.

Step 3 Enter a valid TCP port.

Note For standalone this must be port 80. For co-res it must be any port other than port 80.

Step 4 Click **OK** and close IIS Manager.

Step 5 Ensure you have configured one network connection for each NIC card in **Control Panel** > **Network Connections**.

Preparing Cisco Unified Application Environment

To prepare Cisco Unified Application Environment 2.5 SR2:

Note For more information on administering Cisco Unified Application Environment refer to the *Administration Guide for the Cisco Unified Application Environment*.

Note Do not install Cisco Unified Application Environment Dev Tools when installing Cisco Unified Quick Connect and Cisco Unified Application Environment on the same machine.

Procedure

Step 1 Log into Cisco Unified Application Environment at http://<*ip-address*>/cuaeadmin

Step 2 Verify that enough licenses are available in the system.

Step 3 If not present already, populate a Unified Communications Manager Cluster in CUAE. Perform this configuration in **Connections** > **Add Connection**.

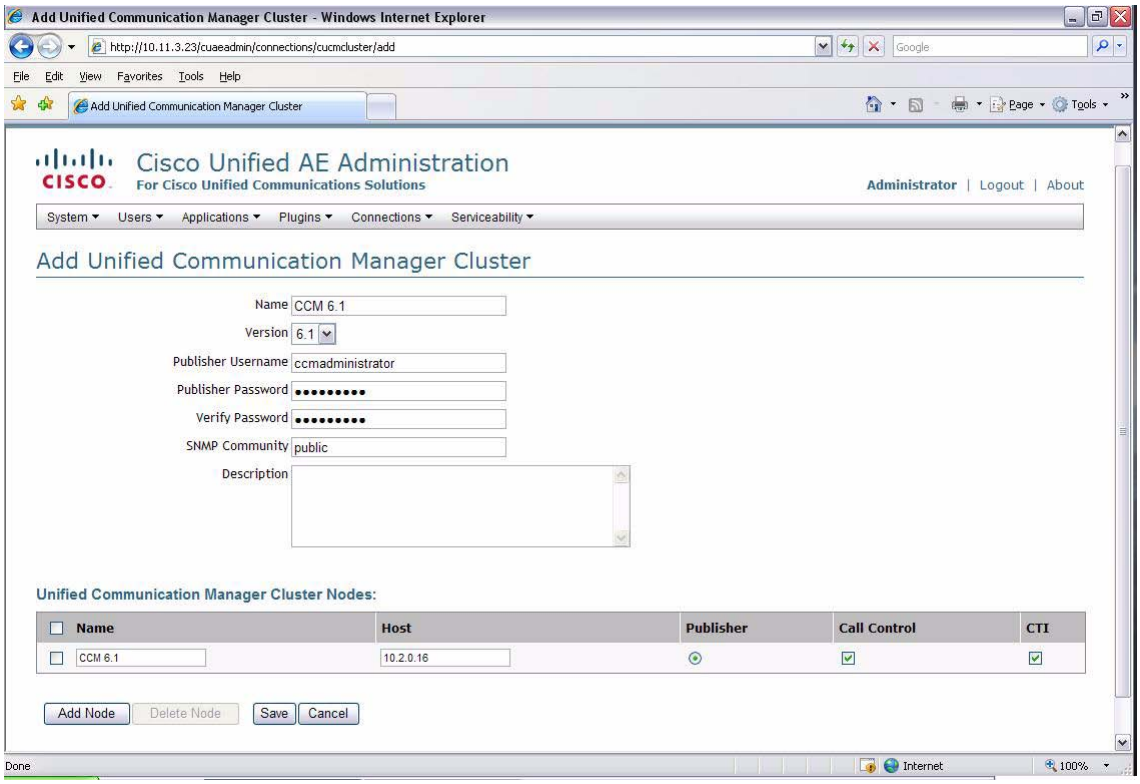
Step 4 Select **Cisco Unified Communication Manager Cluster** and click **Next**.

Step 5 Enter the following information for the cluster (Figure 3-1):

- Name: a descriptive name for the cluster.
- Version: the version of Cisco Call Manager.
- Publisher username: the username for the Publisher.
- Publisher password and Verify password: the password for the Publisher.
- Description (optional): a description of the cluster.
- Unified Communications Manager Cluster Nodes: enter the name and IP address of each Cisco Unified Communications Manager. Check the **Call Control** and **CTI** checkboxes.

Step 6 Click **Add Node**.

Figure 3-1 Adding a Unified Communications Manager Cluster



Step 7 Click **Save**.

Step 8 Create a new Monitored CTI Device Pool and record the name of this device pool. All devices that you intend to monitor must be included in this device pool.

- Select **Monitored CTI Device Pool**. Click **Go**.
- Type a name for the connection,select the Primary and Secondary CTI Manager and enter the credentials of the Telephony Server's application user. Click **Save**.

Step 9 Create a Media Engine connection on CUAE by choosing **Connections** > **Add Connection**.

- Select Media Engine.
- Enter a name for the Media Engine.
- Provide the CUAE IP address.
- Provide the Media Engine password as configured in CUAE.

Note You will enter the value for this device pool's name into the Device Pool Name field in Unified Quick Connect Web Admin when you configure the IP-PBX.

Note The next chapter describes steps to manually install the Cisco Unified Quick Connect applications into Cisco Unified Application Environment.

Preparing Cisco Unified Communications Manager

You must prepare Cisco Unified Communications Manager 6.0, 6.1, or 7.0 by configuring directory services as described next.

Configuring Directory Services

To access Unified Quick Connect from the directory button on a Cisco phone, you must configure the URL Directories field in Cisco Unified Communications Manager. This allows users to 'search' before they start the Unified Quick Connect Push-to-Talk application.

To configure directory services, click **System** > **Enterprise Parameters** > **URL Directories** and set it to the Unified Quick Connect server address (Figure 3-2):

For *standalone* installations, use the following URL:

http://<Unified Quick Connect-Server-IP-Address>/QuickConnect/xmldirectory.aspx

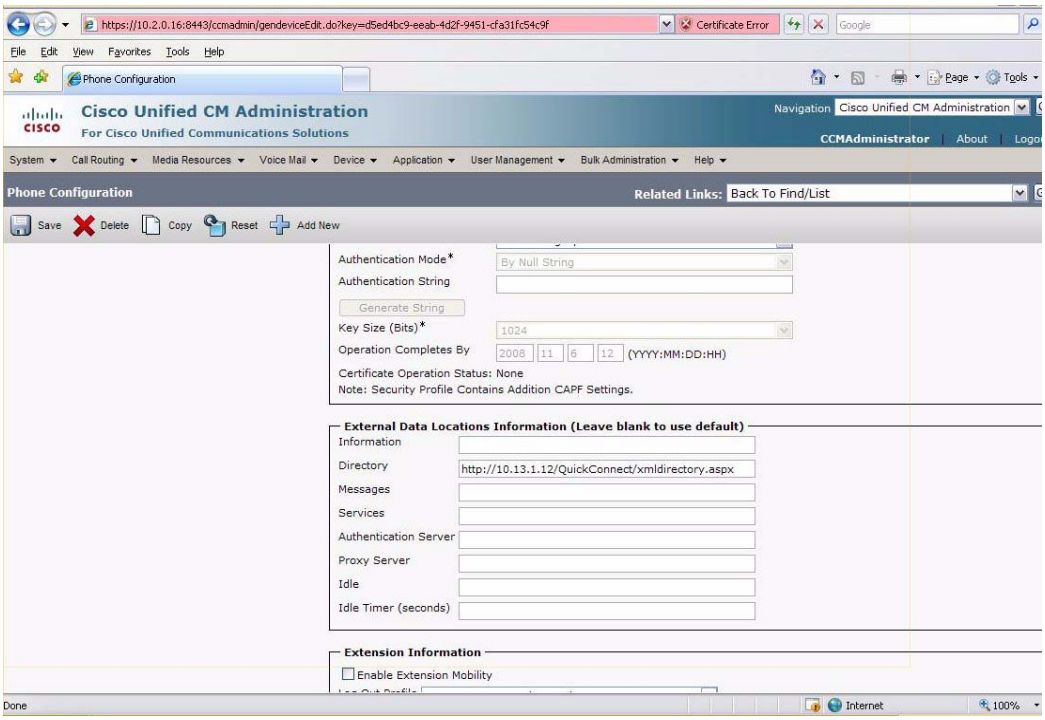
For *co-resident* installations, use the following URL:

http://<Unified Quick Connect-Server-IP-Address>:<port number>/QuickConnect/xmldirectory.aspx

Note Select an available port to configure for the Directories URL. This port must be configured in IIS for use with Cisco Unified Quick Connect, after you have installed it.

Verify that the device is registered with the application user in Cisco Unified Communications Manager.

Figure 3-2 Configuring the Directories URL



If Search is Not Required Before PTT

Any device registered with providers defined within the Unified Quick Connect Location can subscribe to the service (refer to the "Cisco Unified IP Phone Services Configuration" section of the Cisco Unified Communications Manager configuration document for further information on how to configure the devices and providers).

The Cisco service URL would be configured to the following URL:

http://Unified Quick Connect Server Address/OnCastWebService/WalkieTalkie.aspx?id=ptt-grp1&ocm=WalkieTalkiePush.ocm

- Where "id" represents a pre-established group of participants, defined in the following section of the OnCast.Configuration.xml file, to be used for this PTT session. For example:

```
<ShortcutSupportForPTT>True</ShortcutSupportForPTT>
  <Items>
    <Item>
      <Name>ptt-grp1</Name>
      <Params>
      </Params>
      <XmlPayload>
        <LSBC>
          <Organizer>
            <UserID>Q5</UserID>
            <Key>1777</Key>
            <Extension>1777</Extension>
            <MainPhone>1777</MainPhone>
            <IPAddress>10.1.0.208</IPAddress>
            <LDAPDN>Directory Server 1|CN=Q5 Q5,CN=Users,DC=lsqa,DC=local</LDAPDN>
            <ProviderID>IP-PBX 1</ProviderID>
          </Organizer>
          <InviteesGroup>Directory Server
1|CN=group1,CN=Users,DC=lsqa,DC=local</InviteesGroup>
          <Invitees>
            <Invitee>
              <UserID>q1 q1</UserID>
              <Key>1070</Key>
              <Extension>1070</Extension>
              <MainPhone>1070</MainPhone>
              <LDAPDN>Directory Server 1|CN=q1 q1,CN=Users,DC=lsqa,DC=local</LDAPDN>
              <ProviderID />
            </Invitee>
            <Invitee>
              <UserID>Q2 Q2</UserID>
              <Key>1628</Key>
              <Extension>1628</Extension>
              <MainPhone>1628</MainPhone>
              <LDAPDN>Directory Server 1|CN=Q2 Q2,CN=Users,DC=lsqa,DC=local</LDAPDN>
              <ProviderID />
            </Invitee>
            <Invitee>
              <UserID>Q3 Q3</UserID>
              <Key>1021</Key>
              <Extension>1021</Extension>
              <MainPhone>1021</MainPhone>
              <LDAPDN>Directory Server 1|CN=Q3 Q3,CN=Users,DC=sna,DC=local</LDAPDN>
              <ProviderID />
            </Invitee>
            <Invitee>
              <UserID>Q5 Q5</UserID>
              <Key>1577</Key>
              <Extension>1577</Extension>
```

```
                    <MainPhone>1577</MainPhone>
                    <LDAPDN>Directory Server 1|CN=Q5 Q5,CN=Users,DC=sna,DC=local</LDAPDN>
                    <ProviderID />
                  </Invitee>
                  <Invitee>
                    <UserID>QC1 QC1</UserID>
                    <Key>1595</Key>
                    <Extension>1595</MainPhone>
                    <LDAPDN>Directory Server 1|CN=QC1 QC1,CN=Users,DC=sna,
DC=local</LDAPDN>
                    <ProviderID />
                  </Invitee>
                </Invitees>
                <OCMFile>BroadcastTemplates\WalkieTalkiePush.ocm</OCMFile>
                <Conference>
                  <PhoneNumber>918555068850</PhoneNumber>
                  <PassCode>943557</PassCode>
                </Conference>
                <Action>OCM</Action>
                <shortcutURL />
                <Priority>Emergency</Priority>
                <InviteesGroup />
                <UpdateOCM>
                  <updatePay>

<paramtag>OnCastMessage/Workflow/Key/Key[Caption='PushToTalk']/Actions/Action[ID='PushToTa
lk']/Settings/pluginValue/URI</paramtag>
                    <paramvalue>?id=ptt-grp1</paramvalue>
                  </updatePay>
                </UpdateOCM>
              </LSBC>
            </XmlPayload>
          </Item>
```

For information on the input parameters, refer to the *Cisco Unified Quick Connect Administration Guide*. Users can subscribe to multiple PTT services (with different 'id' parameters for different user/groups).

You can also configure the service URL to the URL of a shortcut that you create on the phone. Refer to the *Unified Quick Connect Phone User Guide* for information on creating and managing shortcuts.

Preparing the Enterprise Directory Server

Unified Quick Connect utilizes your existing directory servers as a starting point for collaboration. This has the advantage of:

- Providing you with a single point of administration.
- Minimizing end-user training by re-using existing corporate information for VoIP applications. Unified Quick Connect can connect to multiple directory servers and provide end-users with a single view from their phone.

Binding to Directory Server

Unified Quick Connect must be able to bind to your directory server and retrieve user information. You will need the following information to allow this:

- Directory server type — Options include: Microsoft Active Directory, LDAP v2, Cisco DCD, Salesforce.com, custom SQL, Microsoft Access or Microsoft Exchange.

- Hostname or IP address of your directory server.
- Port — Used to connect to your directory server. Port 8404 must be open for Cisco DCD; 389 must be open for Microsoft Active Directory.
- Credentials — In most cases you will want a username and password to be used by Unified Quick Connect to bind to your directory server. This provides an important level of security for the directory server. If your server is in the same domain as your Microsoft Active Directory, then you may use anonymous binding to not require any credentials.

Configuring Directory Server

Unified Quick Connect requires only two attributes to be modified in your directory server, and you may select which ones to use. The first is called **LSDirKey** within Unified Quick Connect and is used to match a user in the IP-PBX with a user in the directory server. Unified Quick Connect uses this matching to 1) identify the user, and 2) allow the user to access Unified Quick Connect features. The second is called **LSSearchableAttrName** and is used to determine which users, groups and containers in the directory server are searchable within Unified Quick Connect.

You will need to decide the following before configuring your directory server:

- Determine which directory server you will use for storing user information. This is the directory server in the previous section that Unified Quick Connect will be binding to.
- Select which attribute in the directory server will be used for matching to users in the IP-PBX. Make note of the attribute name. In Microsoft Active Directory this is typically the *telephoneNumber* attribute. You may also use a User ID or username attribute.
- Configure the attributes *employeeID* and *extensionAttribute10*. *employeeID* sets the password which the user uses to login to Unified Quick Connect Directory Phone UI.
- *extensionAttribute10* is the name of the PBX (for example, "IP-PBX 1") that the user's phone is associated with.
- Select which attribute in the directory server will be used for searching. Make note of the attribute name. In Microsoft Active Directory this is typically the flags attribute.

To configure your directory server to support Unified Quick Connect you should do the following:

- Configure LSSearchableAttrName — Select which users, containers and groups will be exposed in Unified Quick Connect. For these users, groups and containers you will need to set the flags attribute (or whichever attribute you are using) to 1000.

Note This information is inherited. So if you set this at a top-level container, then all nodes underneath will be searchable in Unified Quick Connect.

- Configure LSDirKey — If you are matching based on telephone number, then the attribute in the directory server associated with LSDirKey (e.g., telephoneNumber) must match the user's extension in the IP-PBX. For example, if a user called Steve Fone has an extension of 20359 in the IP-PBX, then the user Steve Fone in the directory server must have its *telephoneNumber* attribute set to 20359.

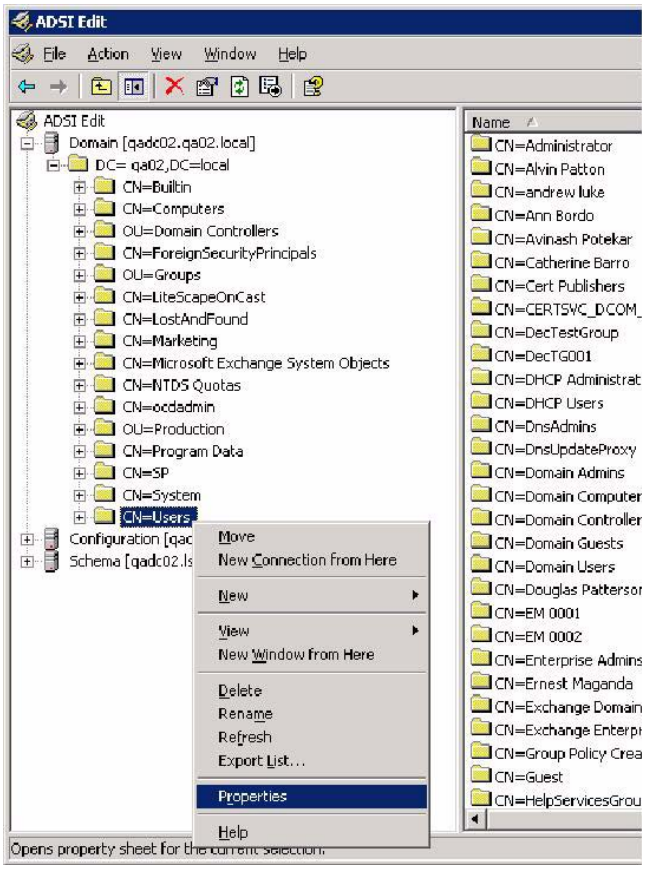
Note You do not need to have an exact match. You may have Steve Fone's telephoneNumber attribute in the directory server set to 650-292-0359 and Unified Quick Connect will be able to remove the first five digits and match him against his extension in the PBX. For information on phone number masking, refer to "Using Phone Number Masks" in Chapter 5, "Configuring Unified Quick Connect Server".

For example, in the directory server below, perform the following steps to make everyone in the Users OU to be searchable by Unified Quick Connect:

Procedure

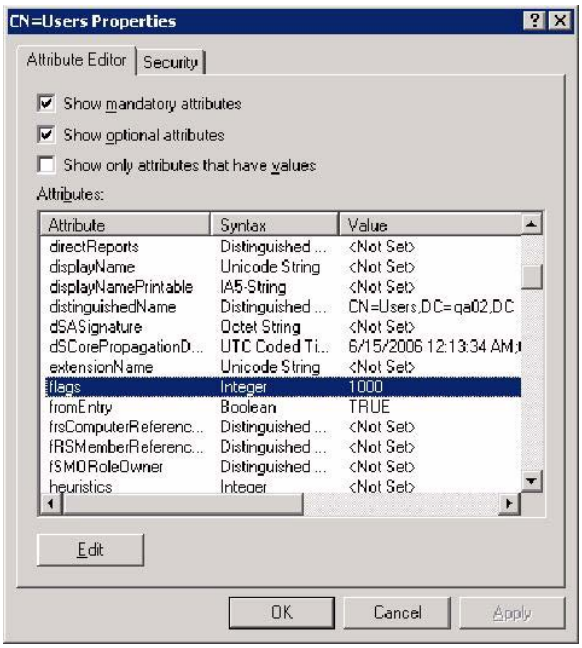
Step 1 Access your Active Directory server using ADSIedit (Figure 3-3). This tool will provide access to hidden attributes (such as flags):

Figure 3-3 Accessing Active Directory Through ADSIedit



Step 2 Find the *flags* attribute and set it to 1000 (Figure 3-4):

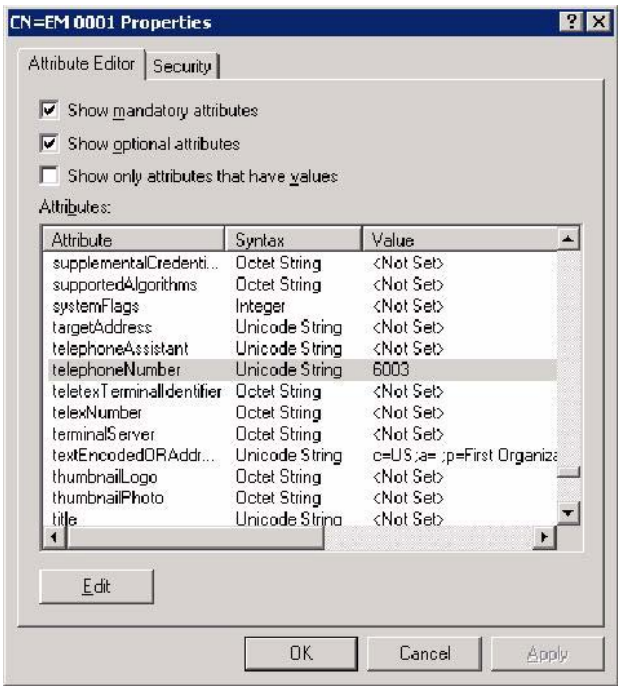
Figure 3-4 Setting the Flags Attribute



You must perform this step for each OU that will be searchable using Unified Quick Connect. All users in this OU will automatically be searchable. If you only want to make some users searchable, then modify the flags attribute for each User or container instead of the OU. This will, however, affect performance.

Step 3 You must now set the attribute in your directory server that will be used to match a user against an extension in your IP-PBX. In Figure 3-5 we use the *telephoneNumber* attribute. Select a user in the above OU and set their *telephoneNumber* attribute to match his extension in the IP-PBX:

Figure 3-5 Setting an Attribute for User to IP-PBX Extension Matching



You must perform this action for each User in your directory server that will be using Unified Quick Connect.

Step 4 Configure the *employeeID* and *extensionAttribute10* attributes:

- *employeeID* sets the password which the user uses to login to Unified Quick Connect Directory Phone UI.
- *extensionAttribute10* is the name of the PBX (for example, "IP-PBX 1") that the user's phone is associated with.

Configuring Multiple Directory Servers

When configuring multiple directory servers it is important to configure the directory servers in the order that they should be processed by Unified Quick Connect, when Unified Quick Connect communicates with a directory server for user information matching. Directories are processed by Unified Quick Connect in the order listed in OnCastConfiguration.xml.

To perform a manual change, you can edit OnCastConfiguration.xml and edit the list of directories to arrange them in the desired order.

Preparing Salesforce.com

Perform the following steps to ensure that Salesforce.com has the correct account type, and that Salesforce.com is setup so that Unified Quick Connect can access your CRM data.

Note Refer to Chapter 1 , section “Salesforce.com Service Requirements”, for requirements for the Salesforce.com service, including supported account types.

Procedure

Step 1 When accessing Salesforce.com from a new network, you need to first log in to Salesforce.com with a user account from the Unified Quick Connect Server.

Step 2 Salesforce.com sends a notification to the administrator’s mailbox.

Step 3 The administrator can authorize the user account in Step 1 by forwarding the activation link email to the person who is configuring Unified Quick Connect to support Salesforce.com (the link needs to be selected from the Unified Quick Connect Server).

Step 4 Log in to Salesforce.com from the Unified Quick Connect server using the user account in Step 1.

This information will be used when you are adding Salesforce.com as a Directory Server in Unified Quick Connect WebAdmin. Refer to “Salesforce.com as a Directory Server.”

Providing API Access to Cisco Unified Quick Connect for Developers

This procedure is only required when you must permit Salesforce.com API access for Unified Quick Connect for application developers who access ADN (App-Exchange Developer Network):

Procedure

Step 1 Make sure your Salesforce.com password is numeric and only 5 digits in length. Alpha-numeric passwords and passwords longer than 5 digits are not supported at this time.

Step 2 In Salesforce.com, log in as the service account user and go to **Setup** > **My Personal information** > **Reset My Security Token**.

Step 3 Salesforce.com will email the new token to the administrator.

Note You only need to complete this procedure once for each service (administrative account being used for Unified Quick Connect access).

Preparing Microsoft Exchange

Microsoft Exchange must be configured to support displaying a user's Personal Address Book and Inbox items from IP phones.

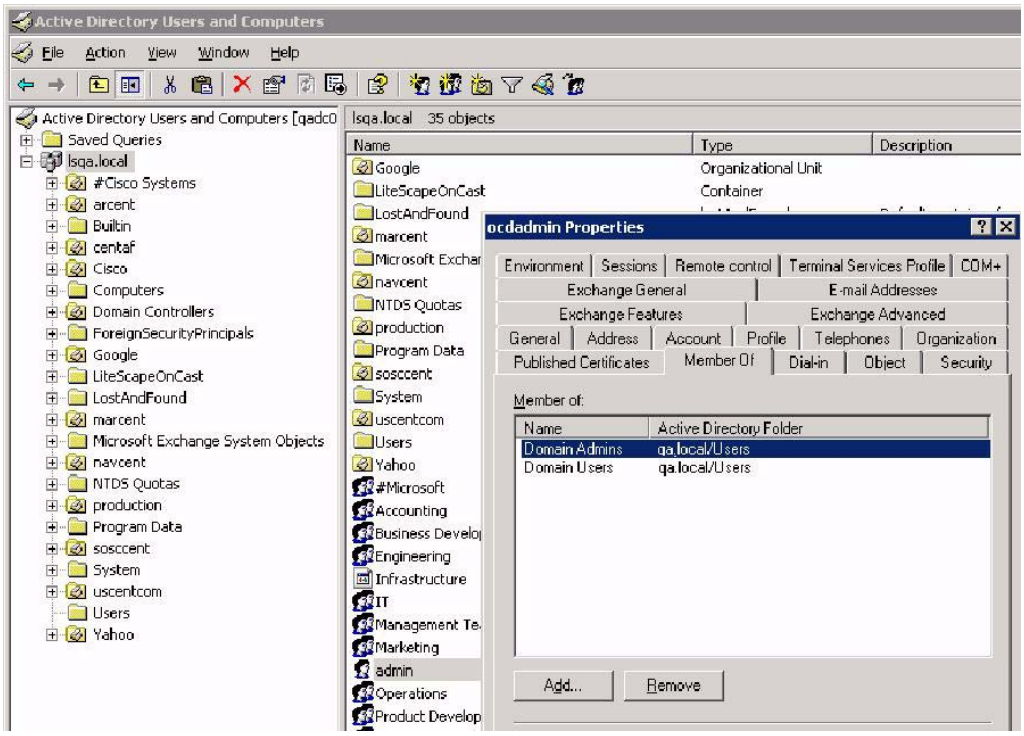
To configure Microsoft Exchange:

Procedure

Step 1 In the Windows domain, create a domain user ("Service Account") with privileges to open user mailbox folders (contact folder). Select a unique user name for this user, for example, Admin.

Step 2 Open Active Directory Users and Computers and verify that the user is to be a member of a group with sufficient read/write privileges into Microsoft Exchange, as shown in Figure 3-6.

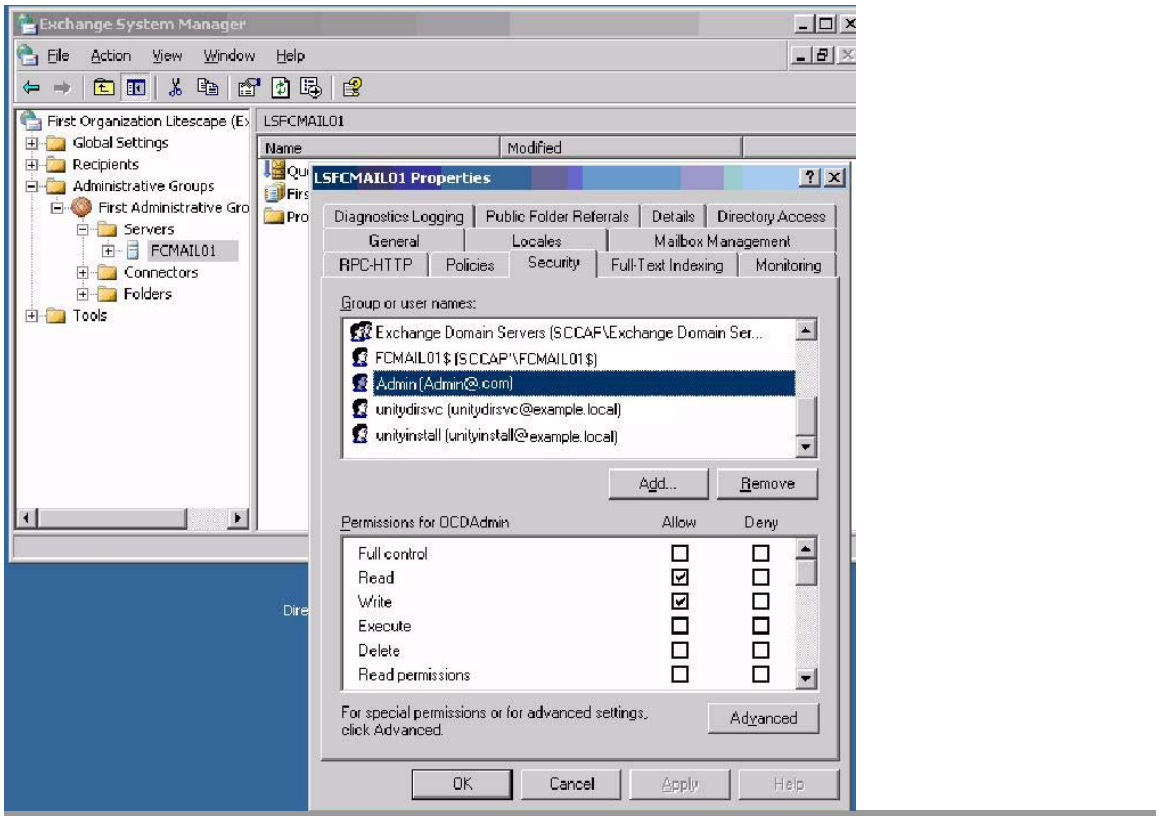
Figure 3-6 Creating a Domain User



Step 3 Using the Microsoft Exchange System Manager, select the **Properties** of the mail server database and click on the **Security** tab.

Step 4 Add the domain user to the list of authorized users to perform specific operations (Figure 3-7). At a minimum, the user should be provided read/write privileges.

Figure 3-7 Adding the Domain User to the List of Authorized Users



Preparing Unified Quick Connect Server

To prepare your server for Unified Quick Connect the following procedures should be performed.

Installing Software Prerequisites

Install the following software on the Unified Quick Connect server:

- Microsoft .NET Framework 2.0 and Microsoft .NET Framework 3.0

Note
- For standalone installation: Install Microsoft .NET Framework 2.0 and 3.0.
- For co-resident installation: Install Microsoft .NET Framework 2.0. Microsoft .NET Framework 3.0 is installed as part of Cisco Unified Application Environment installation.

- Microsoft SQL Server 2005 Standard SP2
- Microsoft Internet Information Services 6.0
- Microsoft Exchange Server MAPI Client and Collaboration Data Objects
- Java Media Framework 2.1.1E
- Cisco Unified Application Environment Dev Tools
  This is required to upload *.MCA files during installation.

Note Cisco Unified Application Environment Dev Tools are required for standalone installations (where Cisco Unified Quick Connect and Cisco Unified Application Environment are installed on separate machines).

Configuring ASP.NET

Perform the following steps to configure ASP.NET:

Procedure

Step 1 On your Unified Quick Connect Server, install Microsoft .Net Framework version 2.0.

Step 2 Open IIS Manager and select the **Default Web Site**. Right-click to open the **Properties** window and click the **ASP.NET** tab. Select **version 2.0** as the default.

Step 3 Click **OK** and close IIS Manager.

IIS Configuration

In IIS Manager, under web service extensions, make sure that ASP.NET v2.0, has status set to “allowed”. Restart IIS if you make changes.

Optional: Installing Active Directory Application Mode

ADAM is designed to provide additional deployment options for Microsoft Active Directory.

ADAM is an optional component for Unified Quick Connect and should only be used to maintain a local cache of directories to improve search performance or provide an additional level of survivability in case the Microsoft Active Directory server is down.

To install ADAM:

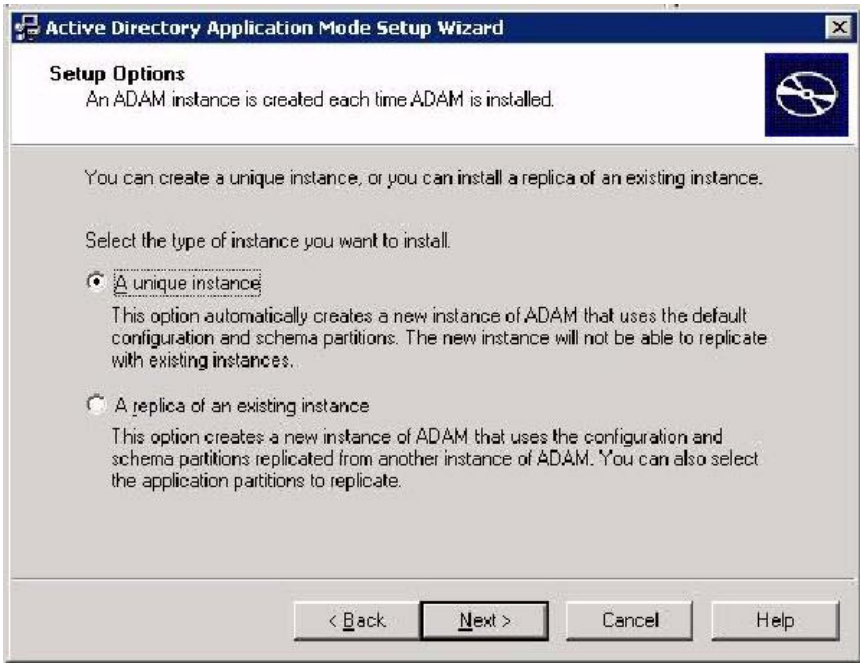
Procedure

Step 1 Start the ADAM installation wizard.

Step 2 Click **Next** to begin the installation.

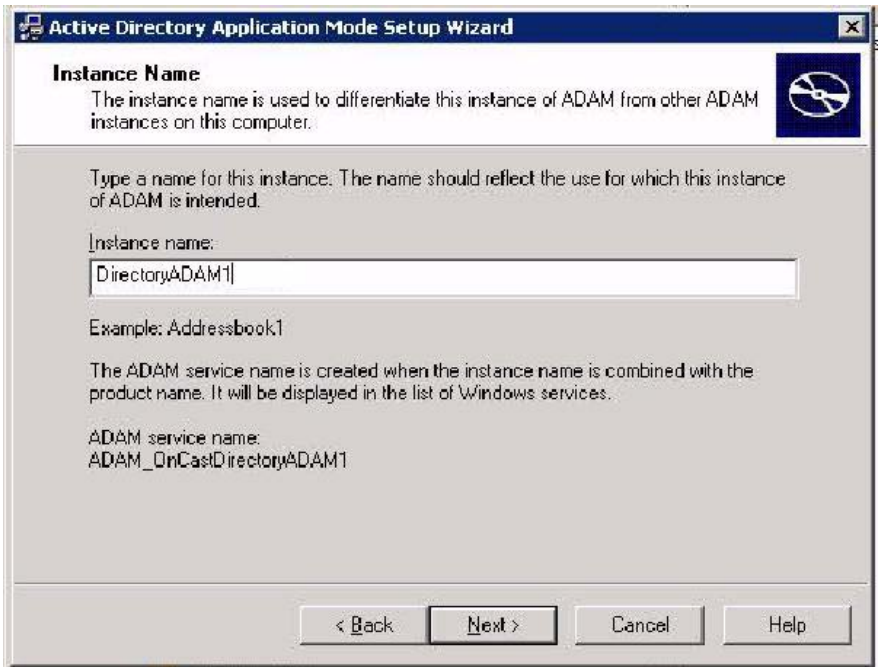
Step 3 Select a unique instance, then click **Next**.

Figure 3-8 Installing ADAM (2 of 9)



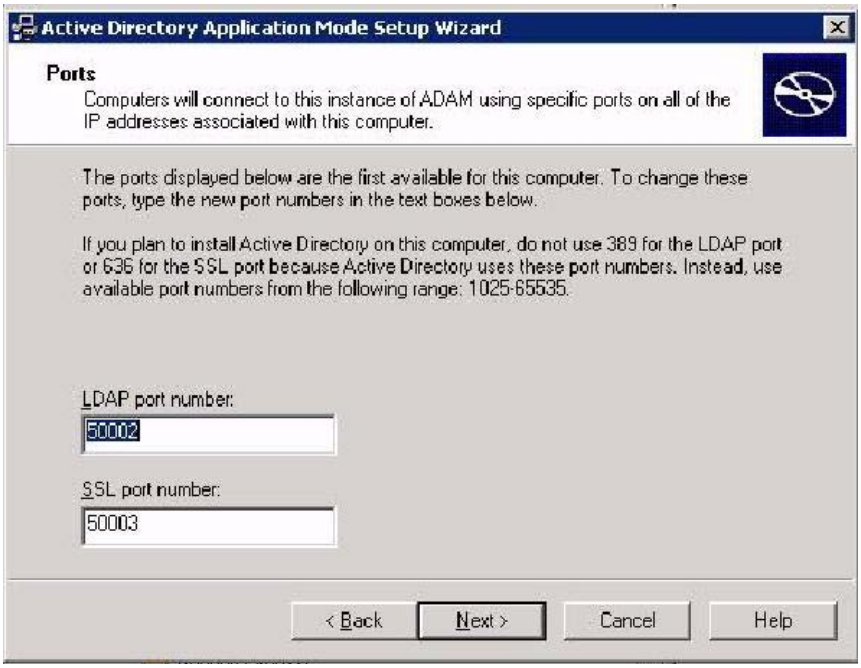
Step 4 Enter a name for the instance, such as *DirectoryADAM*1, then click **Next**.

Figure 3-9 Installing ADAM (3 of 9)



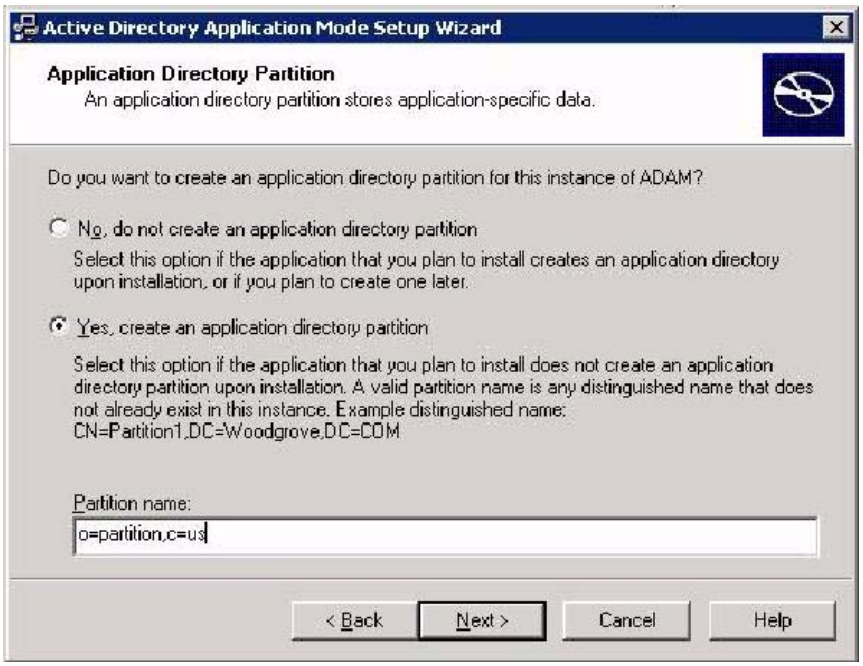
Step 5 Enter the LDAP port number and SSL port number, then click **Next**.

Figure 3-10 Installing ADAM (4 of 9)



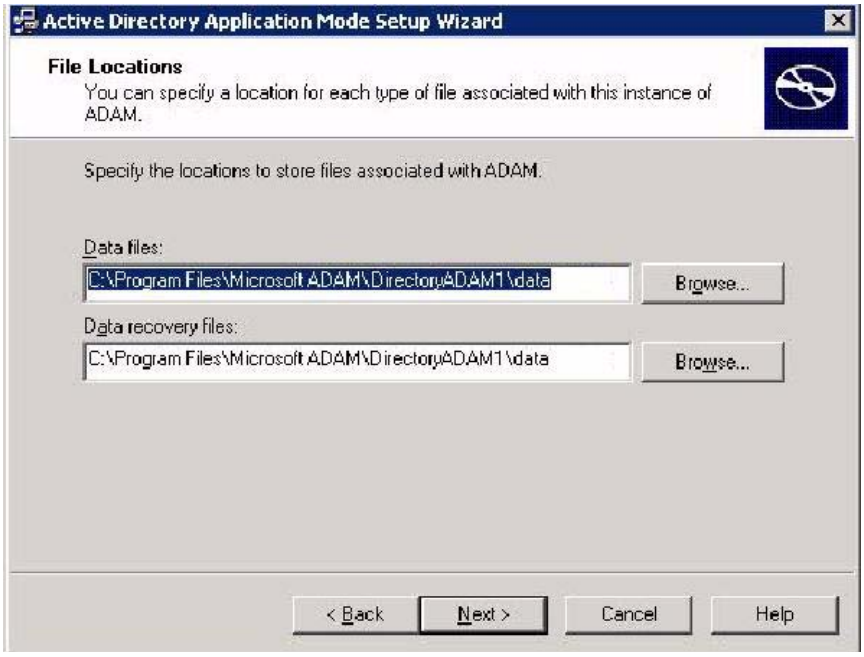
Step 6 Select **Yes**, create an application directory partition, enter the partition name, then click **Next**.

Figure 3-11 Installing ADAM (5 of 9)



Step 7 Accept the default selections or browse for new selections and select them, then click **Next**.

Figure 3-12 Installing ADAM (6 of 9)

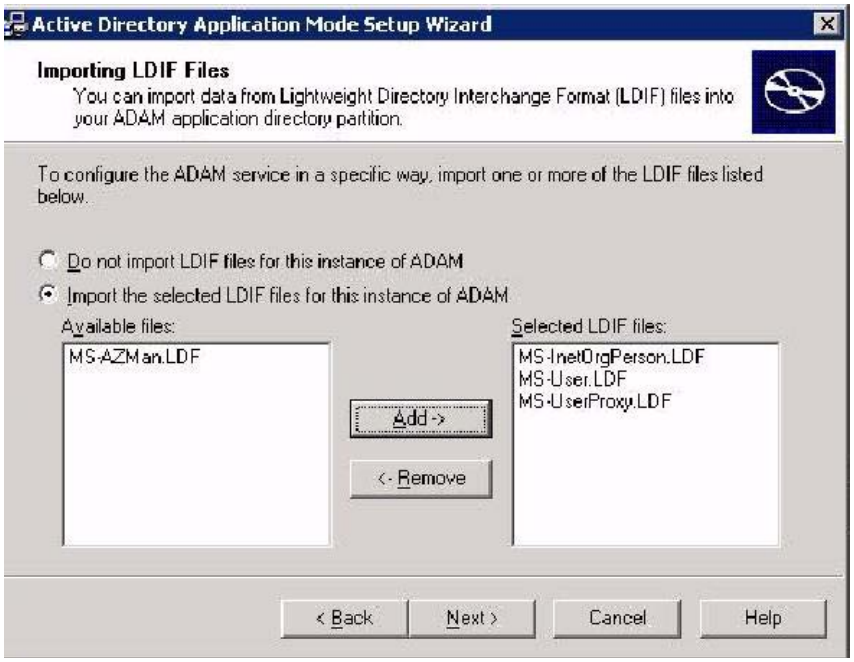


Step 8 Select **This account**, enter the user name and password for the user, then click **Next**.

Figure 3-13 Installing ADAM (7 of 9)

Step 9 Select all files in the left pane, click **Add** to add them into the right window, then click **Next**.

Figure 3-14 Installing ADAM (8 of 9)



Step 10 Review the displayed information, then click **Next** to proceed with the installation.

Step 11 Click **Finish** when you are notified that the installation is complete.

Configuring a Second Partition and Indexes

To support caching of directory content for both GAL directory content, Unified Quick Connect supports Microsoft ADAM as a local cached directory repository.

For example:

- o=example,c=us for GAL

The main partition needed for ADAM synchronization is installed automatically during the built in cache server installation. The second partition is added separately. You must create the second ADAM partition and the indexes for search optimization.

Managing Directory Partitions in Active Directory Application Mode

The following exercises help you become familiar with an additional ADAM administration tool, Ldp.exe. Ldp is installed as part of the ADAM administration tool set. In these exercises, you use Ldp to connect and bind to an ADAM instance, and then you use Ldp to manually add and then delete an application directory partition. (Remember, you can also create an application directory partition by using the ADAM setup wizard.)

Connecting and Binding to ADAM Using Ldp.exe

To connect and bind to an ADAM instance using Ldp.exe:

Procedure

Step 1 Click **Start** > **All Programs** > **ADAM** > **ADAM Tools Command Prompt**.

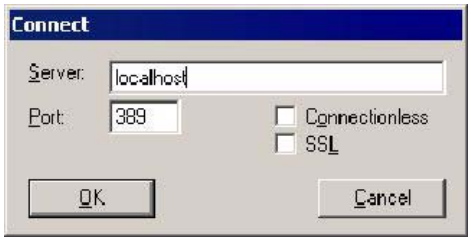
Step 2 At the command prompt, enter ldp, then press **Enter**.

Step 3 Click **Connection** > **Connect**.

Step 4 In Server, enter the host or DNS name of the computer running ADAM. When ADAM is running locally, you can also enter localhost.

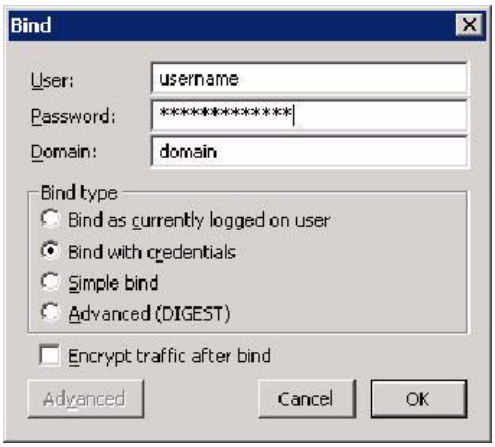
Step 5 In Port, enter the LDAP or SSL communication port number for the ADAM you want to connect to, then click **OK**.

Figure 3-15 Connect Window



Step 6 Set your bind type. Click **Connection** > **Bind** to display the Bind window (Figure 3-16).

Figure 3-16 Bind Window



- To bind using the credentials you used to log in, click **Bind** as currently logged on user.
- To bind using a domain user account, click **Bind** with credentials, enter the user name, password, and domain name (or the computer name, if you are using a local workstation account) of the account you are using, then click **OK**.
- To bind using a user name and password, click **Simple bind**, enter the user name and password of the account that you are using, then click **OK**.
- To bind using an advanced method (NTLM, DPA, negotiate, or digest), click **Advanced (DIGEST)** > **Advanced** in Method, select the method, set other options as needed, then click **OK** twice.

Step 7 Click **OK** to close the Bind window.

Adding Application Directory Partitions

To add an application directory partition:

Procedure

Step 1 Run Ldp.exe.

Step 2 On the Ldp Browse menu, click **Add child**.

Step 3 In Dn, enter o=example2,c=us as the distinguished name for the new application directory partition.

Step 4 Under Edit Entry, enter the following, then click **Enter**:

- In Attribute, enter **ObjectClass**.
- In Values, enter **organization**.

Step 5 Under Edit Entry, enter the following, then click **Enter**:

- In Attribute, enter **InstanceType**.
- In Values, enter **5**.

Step 6 Click **Run**. The application directory partition is added, and the following result appears:

```
***Calling Add...
ldap_add_s(ld, "o=example2,c=us", [2] attrs)
```

```
Added {o=example2,c=us}.
```

Step 7 Click **Close**.

The following attributes on ADAM will be indexed to optimize the search process.

- Description
- adminDescription
- personalTitle
- telephonenumber
- mobile
- homePhone
- givenname
- sn
- displayName
- st
- division

Creating Indexes

There are two methods for creating indexes in ADAM:

- Installing the ADAM schema snap-in.
- Adding indexes through the ADAM snap-in.

Installing the ADAM Schema Snap-in

To install the ADAM Schema snap-in:

Procedure

Step 1 Click **Start** > **Run**, enter mmc /a, then click **OK**.

Step 2 Click **File** > **Add/Remove Snap-in**, then click **Add**.

Step 3 In Available Standalone Snap-ins, click **ADAM Schema** > **Add** > **Close**, then click **OK**.

Step 4 To save this console, click **File** > **Save**.

Step 5 In Save in, point to the %systemroot%\system32 directory.

Step 6 In File name, enter adam_schema_mgmt.msc, then click **Save**.

Step 7 To create a shortcut on your Start menu:

a. Right-click **Start** > **Open All Users**, double-click **Programs** folder, then double-click **ADAM** folder.

b. Click **File** > **New** > **Shortcut**.

c. Enter the location of the item - adam_schema_mgmt.msc - then click **Next**.

d. Enter a name for the shortcut - ADAM Schema - then click **Finish**.

Adding Indexes Through the ADAM Snap-in

To add indexes through the ADAM snap-in, select each of the attributes in the list below, right click the attribute, then click **Properties** > **Index** attribute.

- Description
- adminDescription
- personalTitle
- telephonenumber
- mobile
- homePhone
- givenname
- sn
- displayName
- st
- division

Run the following Perl script.

```
# This Perl code indexes an attribute.
# ------------------------------------------------------------
# Adapted from VBScript code contained in the book:
#      "Active Directory Cookbook" by Robbie Allen
# Publisher: O'Reilly and Associates
# ISBN: 0-596-00466-4
# Book web site: http://rallenhome.com/books/adcookbook/code.html
# ------------------------------------------------------------

# ------ SCRIPT CONFIGURATION ------
# Set to the common name (not LDAP display dame) of the attribute
my $strAttrName = "<AttrCommonName>";   # e.g. rallencorp-LanguagesSpoken
# ------ END CONFIGURATION ---------
use Win32::OLE;
$Win32::OLE::Warn = 3;
my $objRootDSE = Win32::OLE->GetObject("LDAP://RootDSE");
my $objAttr = Win32::OLE->GetObject("LDAP://cn=" . $strAttrName . "," .
                        $objRootDSE->Get("schemaNamingContext"));
$objAttr->Put("searchFlags", 1);
$objAttr->SetInfo;
print "Indexed attribute: $strAttrName\n";
```

After the pre-installation tasks are complete, you can install and configure Unified Quick Connect as described in the following chapters.

CHAPTER 4

Installing Unified Quick Connect Server

This chapter It describes the following topics:

- Requirements for Microsoft SQL Server 2005, page 4-1
- Setting Authentication Parameters, page 4-2
- Requirements for Cisco Unified Application Environment, page 4-2
- Installing Optional Third Party Software Components, page 4-3
- Running the Setup Wizard, page 4-3
- Completing the Installation, page 4-8
- Post-Installation Configuration, page 4-13

Requirements for Microsoft SQL Server 2005

Cisco Unified Quick Connect requires Microsoft SQL Server 2005 to be installed. Refer to Microsoft documentation for the installation procedure, and ensure that you use the values described in Table 4-1 to ensure compatiblity.

Table 4-1 Guidelines for Performing SQL 2005 Installation

Parameter	Required Value
Service Account	"Use the built-in System account" and "Local system"
Authentication	Mixed Mode (Windows Authentication and SQL Server Authentication)
Collation Settings	Verify the SQL collations option has been selected and highlight "Dictionary order, case insensitive, for use with 1252 Character Set."

Setting Authentication Parameters

Perform the following steps to set the authentication parameters used in MS SQL Server Management Studio:

Procedure

Step 1 Open MS SQL Server Management Studio and log in.

Step 2 In the left window (Object Explorer), right-click the hostname of the server and select **Properties**.

Step 3 Navigate to the Security page.

Step 4 In the Server Authentication section, verify that "SQL Server and Windows Authentication Mode" is selected.

Step 5 Click **OK**.

Step 6 In the left window (Object Explorer), choose **Security** > **Logins** > **sa**, right-click and select **Properties**.

Step 7 Change the sa password to a value of your choosing. Record this password for use during the RTCM installation.

Step 8 Restart the SQL Service.

Requirements for Cisco Unified Application Environment

Verify that Cisco Unified Application Environment 2.5 SP2 has been installed. Refer to *Cisco Unified Application Environment Adminstration Guide* for installation procedures. Also refer to Preparing Cisco Unified Application Environment, page 3-6 and Preparing Cisco Unified Communications Manager, page 3-8 for required pre-installation procedures.

Requirement for Dev Tools Installation Based on Installation Environment

The Dev Tools component is only installed in certain environments:

- For co-resident installations (where Cisco Unified Quick Connect and Cisco Unified Application Environment are installed on the same machine): the Dev Tools component must not be installed. In a co-resident installation, Cisco Unified Quick Connect components must manually be installed into Cisco Unified Application Environment, as described in Installing Cisco Unified Quick Connect Applications in Cisco Unified Application Environment, page 4-11.
- For standalone installations (where Cisco Unified Quick Connect and Cisco Unified Application Environment are installed on separate machines): the Dev Tools component must be installed. The installation of Cisco Unified Quick Connect components occurs automatically during installation of Cisco Unified Quick Connect, and no manual steps are requried to install these components into Cisco Unified Application Environment.

Installing Optional Third Party Software Components

To install optional third party software components for use with Cisco Unified Quick Connect:

Procedure

Step 1 You can download the Java Media Framework (JMF) 2.1.1e software from Sun Microsystems at the following URL:

http://java.sun.com/javase/technologies/desktop/media/jmf/2.1.1/download.html

Step 2 You can download Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1 from Microsoft at the following URL:

http://www.microsoft.com/downloads/details.aspx?FamilyID=E17E7F31-079A-43A9-BFF2-0A110307611E&displaylang=en

Running the Setup Wizard

Unified Quick Connect utilizes the Unified Quick Connect Setup Wizard to simplify installation and configuration. The Unified Quick Connect Setup Wizard automatically installs all Unified Quick Connect Server components, provides easy-to-use prompts to automatically create a working configuration, and automatically installs the license file.

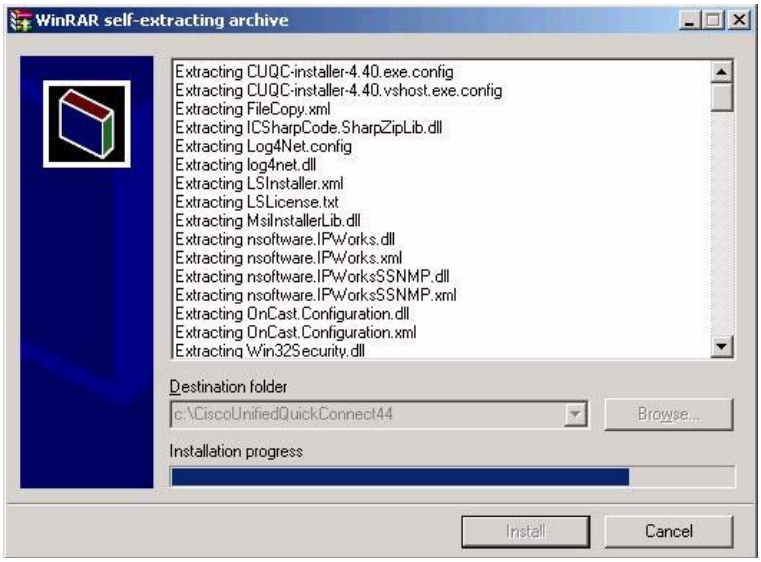
To install Unified Quick Connect Server:

Procedure

Step 1 Insert the DVD-ROM in your DVD-ROM drive.

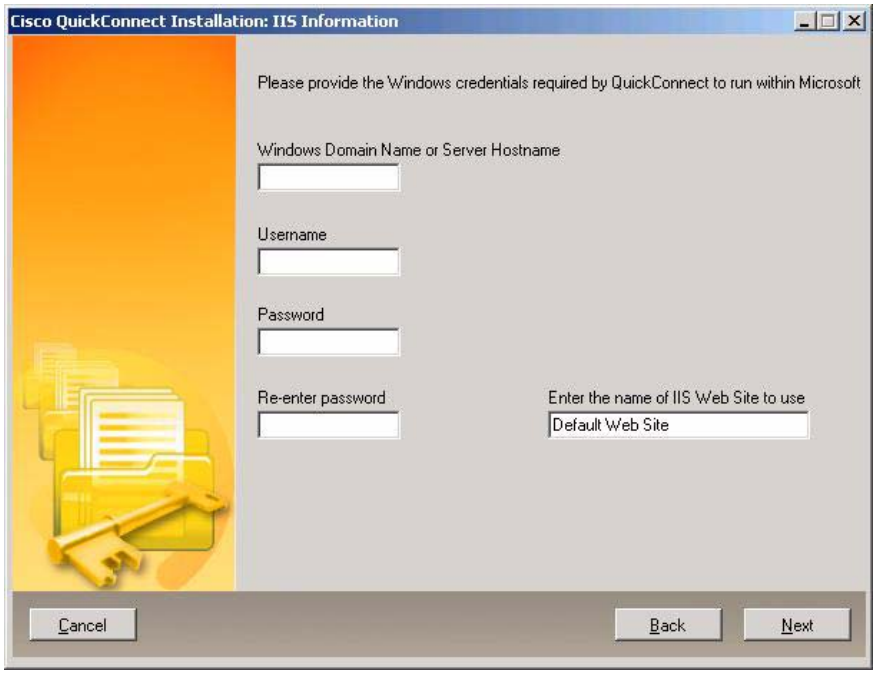
Step 2 Open the self-extracting archive **CUQC-44-package.exe**. Do not change the Destination Folder.

Step 3 Click **Install**. This extracts the package to the specified directory and launches the installation wizard:

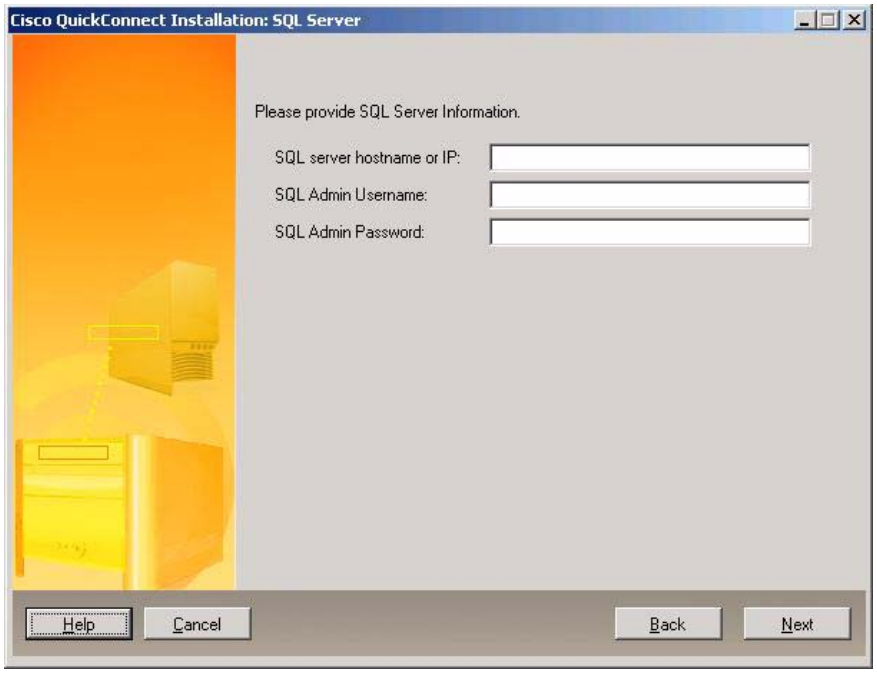


Step 4 You will be prompted with the installer for Unified Quick Connect. Click **Next**.

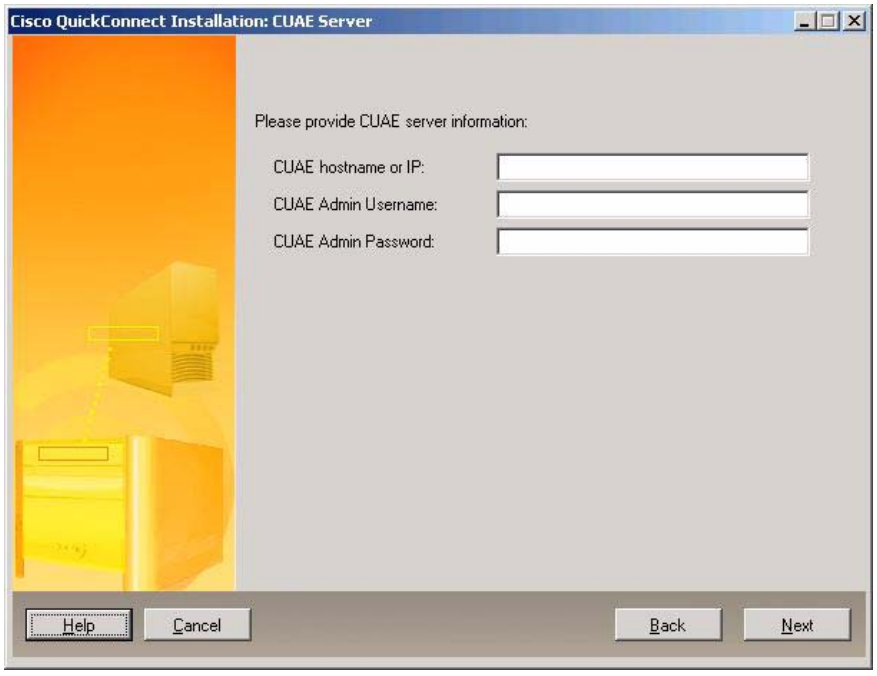
Step 5 Enter the Windows credentials required by Unified Quick Connect to run within Microsoft Windows.



Step 6 Enter the parameters for the SQL Server that will be used with Unified Quick Connect, then click **Next** to continue.



Step 7 Enter the CUAE server parameters, then click **Next** to continue.



Step 8 Enter the IP address of the Unified Quick Connect Configuration server that will handle synchronization, then click **Next** to continue.

Step 9 Enter the IP address of the local broadcast server. This is typically the address of the Unified Quick Connect Server. Click **Next** to continue.

Step 10 Enter the IP address of the Load Balancing server. This is typically the address of the Unified Quick Connect Server. Click **Next** to continue.

Step 11 Click **Next** followed by **Finish** in the last window to start the installation.

A status bar shows the progress of the installation.

Step 12 Close any windows that remain open.

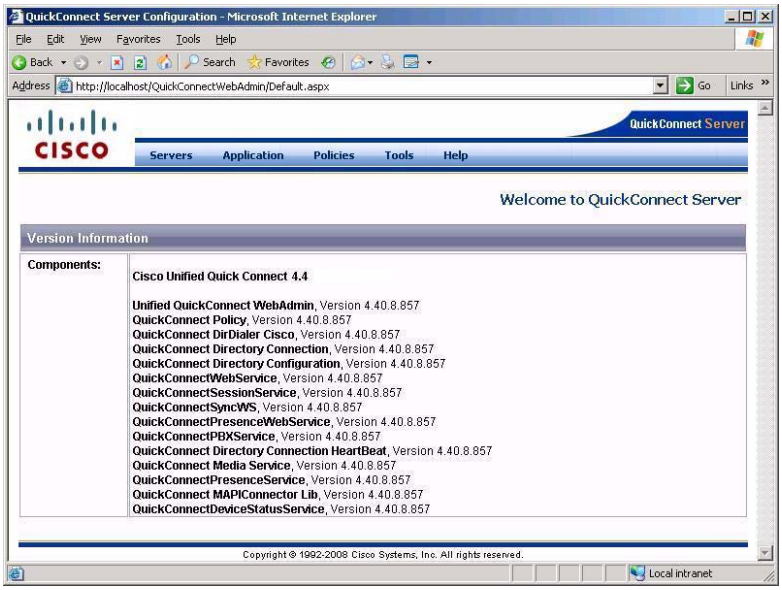
Your installation and configuration are complete.

Step 13 To verify that all of the Unified Quick Connect Server components have been successfully installed, open Unified Quick Connect WebAdmin at:

http://Unified Quick Connect-Server-IP-Address/Unified Quick ConnectWebadmin

Verify that all components show active version numbers and that there are no warnings (Figure 4-5).

Figure 4-1 Verifying Unified Quick Connect Components



Step 14 Java update notification is not required for Unified Quick Connect. If automatic Java update notification is activated, perform the following steps to deactivate it:

- Select **Start** > **Settings** > **Control Panel** > **Java**. The Java(TM) control Panel will display.
- Click on the **Update** tab.
- Uncheck **Check for Updates Automatically**.
- Click **Apply** then close the window.

Step 15 Configure your Directory Server, IP-PBX, and Unified Quick Connect Locations parameters by performing the procedures in subsequent chapters.

Step 16 Restart the Unified Quick Connect Server.

Step 17 By default, all services are set to start automatically, but will not start after installation until you restart the server.

Note If the services do not start after restart (even though they were set to automatic), right click on the service and go to **Properties**. Click on the **Log On** tab and re-enter the credentials.

Step 18 Perform the following steps:

- Verify that LSLicense.txt was copied by the installer during installation to the C:/LiteScape folder.
- Attempt to start MAPEngine.exe through Windows Services. You will receive an error.

Step 19 For standalone installation: in Cisco Unified Application Environment, verify that components for Unified Quick Connect have been populated in the Main Control Panel (Figure 4-6).

For co-resident installation: register each of the applications manually using CUAE Admin.
To add an application:

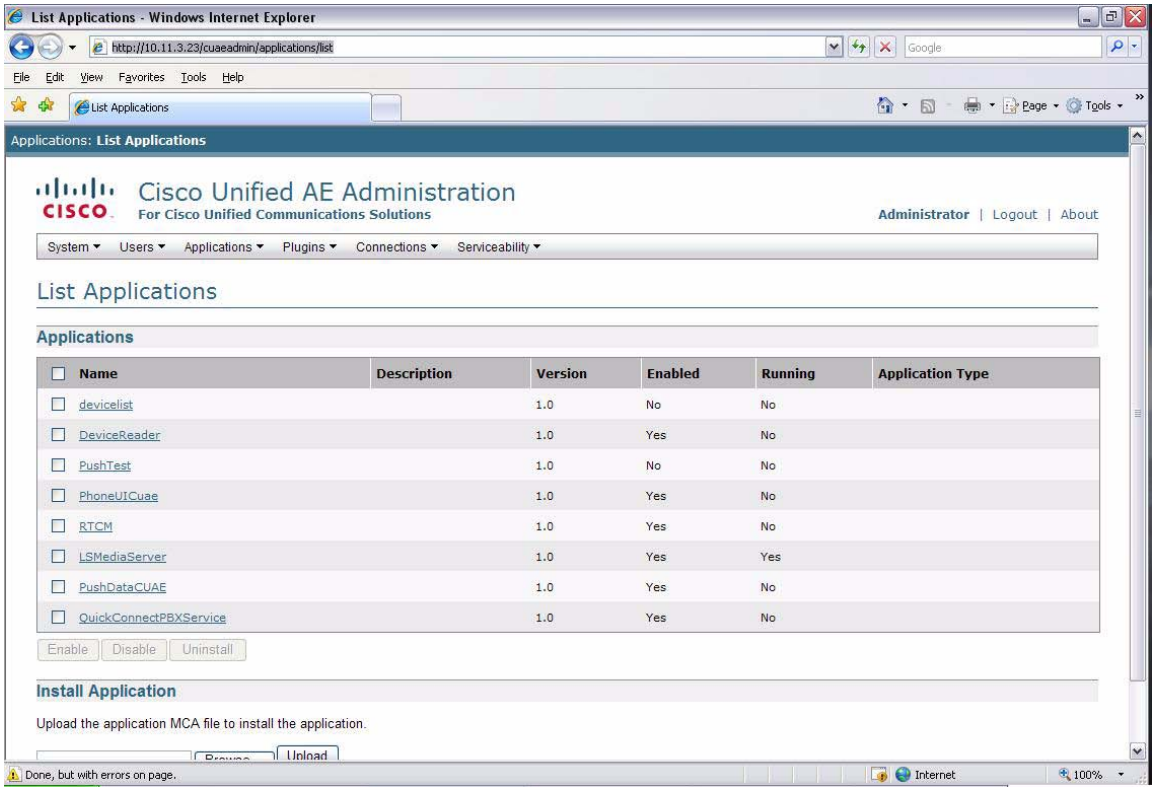
- Login to CUAE Administration window.
- Go to **Applications** > **Add Application**
- Browse and select the respective .mca file located in bin directory of each application

For example, the .mca file for the application called LSMediaServer is located in the following directory:

C:\CiscoUnifiedQuickConnect44\CUAE_Scripts\LSMediaServer\bin

The following components must have been populated: PhoneUICuae, RTCM, LSMediaServer, PushDataCUAE, and QuickConnectPBXService.

Figure 4-2 Main Control Panel in Cisco Unified Application Environment



Completing the Installation

Perform the following steps to complete the installation:

Procedure

Step 1 Ensure to start the following services in Windows Services:

- Application Layer Gateway Service
- Network Connections Service
- Network Location Awareness (NLA) Service
- Plug and Play Service
- Remote Access Auto Connection Manager Service
- Remote Access Connection Manager Service
- Remote Procedure Call (RPC) Service
- Telephony Service
- IIS Admin Service
- HTTP SSL Service
- www Publishing Service

Step 2 Ensure that for *co-resident* installations the IIS Default Web Site port number is different from the Cisco Unified Application Environment Web Server port number.

For example, typically CUAE Web Server listens on port 80. In IIS, view the properties for the Default Web Site and assign a valid Default Web Site port number other than port 80.

For *standalone* installations, this step is not required.

Step 3 In certain cases, the menu items in Unified Quick Connect Web Admin do not get displayed properly. The workaround issued by Microsoft states that this problem can happen as a result of invalid IIS or .net 2.0 installations. Perform the following steps:

a. Go to IIS and view the properties of QuickConnectWebAdmin.

b. Click Configuration in the Virtual Directory Tab.

c. Select the .axd file and click edit.

d. Uncheck ‘Verify that file exists.’

e. Save all settings.

f. Refresh the default application pool.

g. View the Unified Quick Connect application, and verify that menu items appear correctly.

Step 4 Verify that ASP.NET version is set to 2.0.50727 under IIS > Web Sites > ASP.NET.

Step 5 Verify that ASP.NET is not set as Prohibited in Web Service Extensions: in IIS go to Web Service Extensions > ASP.NET Version to 2.0.50727. Click **Allow**.

Step 6 Verify that the Default website is started in IIS.

Step 7 Verify that IIS is not set to run in Isolation mode: in IIS go to the **Web Sites** > **Properties** > **Service** tab. Uncheck isolation mode, click **OK**, and restart IIS.

Step 8 Verify that the IIS Admin, ASP.Net Status Service, and BITS Services are set to start automatically.

Step 9 Install JRE 6.0

Step 10 Start MAPEngine.exe through Windows Services.

Step 11 If the Presence service does not start after restart (even though they were set to automatic), right click on the service and go to Properties. Click on the Log On tab and re-enter the credentials.

Step 12 Ensure the following:

- Stop MAPEngine
- Stop All Oncast Services
- Restart AppServer, Media Engine, and JTAPI Services
- Reset IIS
- Start MAP Engine
- Start Oncast Services

Step 13 Ensure that all devices in the PBXDataCombo.xml file (in C:\Documents and Settings\All Users\Application Data\LiteScape\OnCast\AppData) have valid data.

Step 14 Access Unified Quick Connect WebAdmin as follows:

For For *standalone* installations, use the following URL:

http://<*Unified Quick Connect-Server-IP-Address*>/QuickConnect/xmldirectory.aspx

For *co-resident* installations, use the following URL:

http://<*Unified Quick Connect-Server-IP-Address*>:<*port number*>/QuickConnect/xmldirectory.aspx

Step 15 If you are installing a co-resident installation, you will be prompted to enter the port number. Enter the port number you configured in IIS. You will not be prompted if you are performing a standalone installation.

The menu bar appears (Figure 4-3):

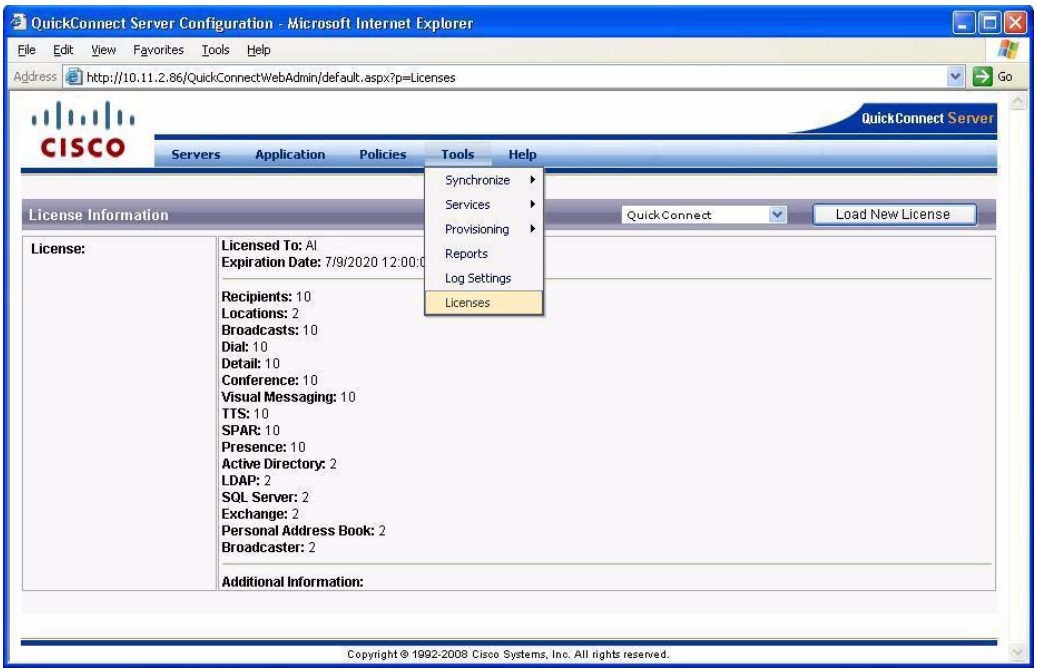
Figure 4-3 Unified Quick Connect Web Admin Menu Bar

Use the navigation bar to access the five main WebAdmin menu options: Servers, Application, Policies, Tools and Help.

Step 16 Perform the following steps to load the WebAdmin license (License.txt) in Unified Quick Connect WebAdmin:

a. Choose **Tools** > **Licenses** (Figure 4-4).

Figure 4-4 Licenses Menu Item



b. Click **Load New License** (Figure 4-4).

c. Click **Browse** and navigate to the license file.

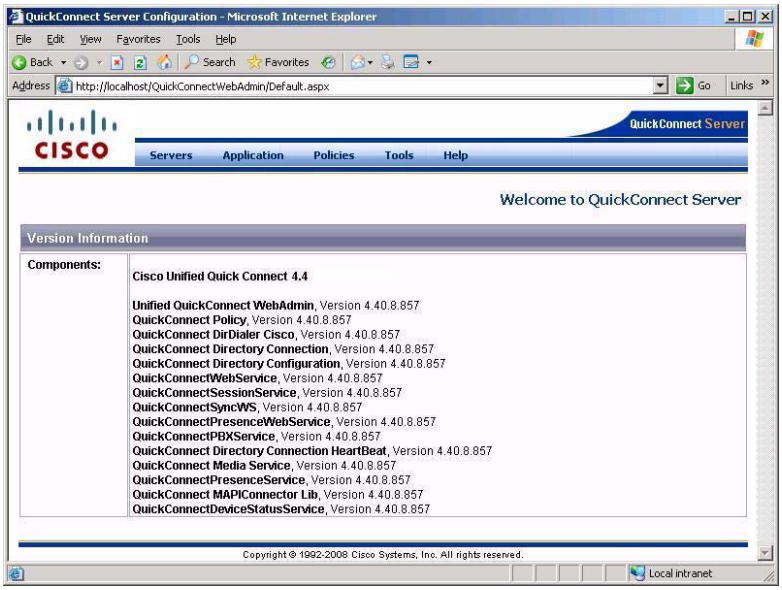
d. Click **Open**.

e. Click **Load**.

The new license is loaded and the license parameters are displayed.

Step 17 Verify that all components show active version numbers and that there are no warnings (Figure 4-5).

Figure 4-5 Verifying Unified Quick Connect Components



Step 18 Java update notification is not required for Unified Quick Connect. If automatic Java update notification is activated, perform the following steps to deactivate it:

- Select **Start** > **Settings** > **Control Panel** > **Java**. The Java(TM) control Panel will display.
- Click on the **Update** tab.
- Uncheck **Check for Updates Automatically**.
- Click **Apply** then close the window.

Step 19 Enter the assigned Default Web Site port number in **Cisco Unified Quick Connect** > **Advanced Settings** > **Web Service URLs**.

Step 20 In the C:\LiteScape\Logs folder, create a new folder called “wrapper.” This allows log files to be created.

Step 21 By default, all services are set to start automatically, but will not start after installation until you restart the server.

Note If the services do not start after restart (even though they were set to automatic), right click on the service and go to **Properties**. Click on the **Log On** tab and re-enter the credentials.

Installing Cisco Unified Quick Connect Applications in Cisco Unified Application Environment

Note This procedure is only required for co-resident installation (where Cisco Unified Quick Connect and Cisco Unified Application Environment were installed on the same machine). Do not perform this procedure if you installed in a standalone installation (where Cisco Unified Quick Connect and Cisco Unified Application Environment were installed on separate machines). Instead, only verify that the components were installed successfully (Step 4).

Perform the following steps to manually install Cisco Unified Quick Connect applications into Cisco Unified Application Environment in a co-resident installation:

Procedure

Step 1 In Cisco Unified Application Environment Web interface, go to **Application** > **Add Applications**.

Step 2 Browse to the following path: `\<IP_address>\<path of installer>\CUAE_Scripts\<name of folder whose script needs to be installed>\bin`. For example, *LSMediaServer\bin*.

Step 3 Find an upload the .mca file, located in the /bin folder, for each of the following components: LSMediaServer, OnCastWebService, PhoneUI, QuickConnectPBXService, and RTCM.

Step 4 In Cisco Unified Application Environment, verify that components for Unified Quick Connect have been populated in the Main Control Panel (Figure 4-6 on page 4-12).

The following components must have been populated: PhoneUICuae, RTCM, LSMediaServer, PushDataCUAE, and QuickConnectPBXService.

Steps 5-8 are required to be performed to refresh the configuration of components on Cisco Unified Application Environment and Cisco Unified Quick Connect:

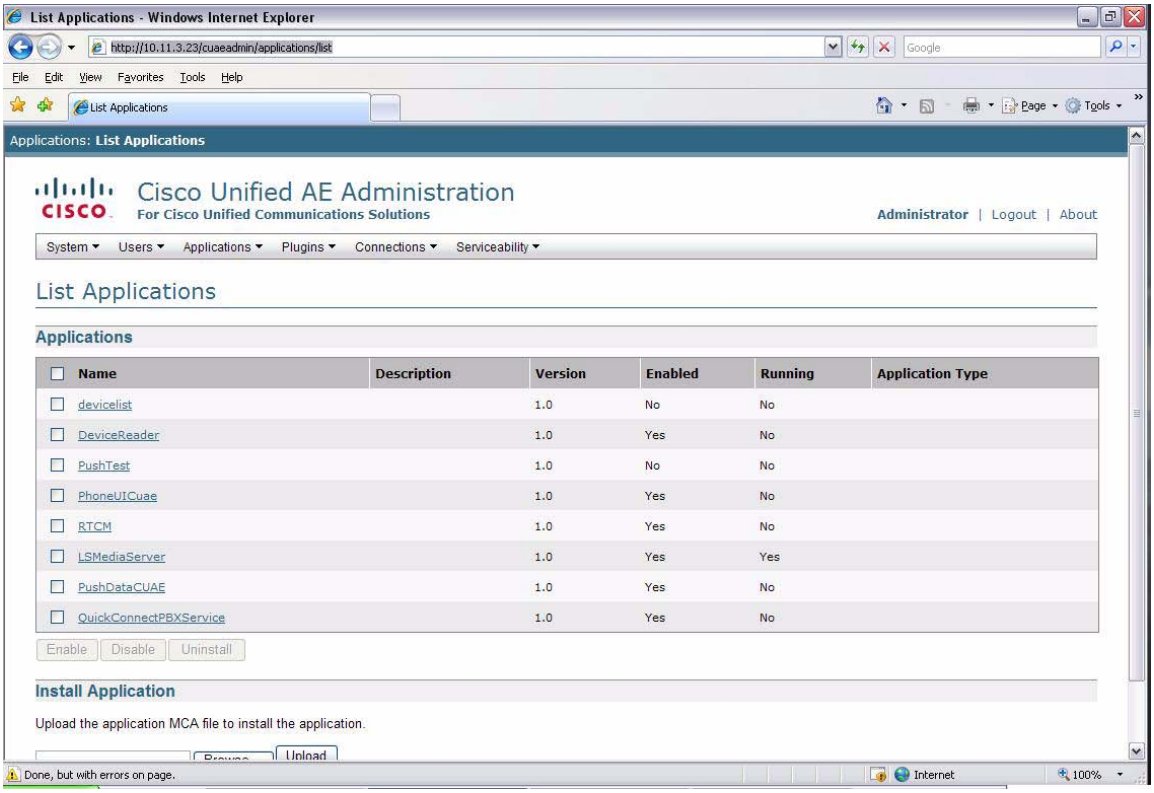
Step 5 Restart the devicelist, Application server, Media server, and JTAPI services.

Step 6 Select **Plugins**> **List plugins** > **CiscoDeviceListXProvider**. Select the **Invoke Extension** button.

Step 7 In Windows Services, restart OnCastPBXService, and OnCastMediaServer.

Step 8 In IIS, restart the default application pool.

Figure 4-6 Main Control Panel in Cisco Unified Application Environment



Post-Installation Configuration

Perform the following post-installation procedures:

- Configuring PTT Session Priority, page 4-13
- Configuring the ExitALL Parameter, page 4-13

Configuring PTT Session Priority

By default, the PTT Session Priority is set to Emergency. In this setting, PTT sessions barge into the recipient's phone calls.

If you want to configure PTT sessions to not barge in on phone calls, you can change the parameter pr=**Normal** in the Oncast.Configuration.xml file (located at C:\Documents and Settings\All Users\Application Data\LiteScape\OnCast\). Perform the following changes to the <WalkieTalkie> section:

```
<WalkieTalkie>
<Item>
          <Name>ptt-def</Name>
<Params>|ocm=BroadcastTemplates\WalkieTalkie.ocm|pr=Normal</Params>
          <XmlPayload>
          </XmlPayload>
 </Item>
```

Configuring the ExitALL Parameter

Configure the ExitALL parameter in Unified Quick Connect WebAdmin as follows:

In WebAdmin select **Advanced Settings** > **Broadcasters** > **ExitALL**.

This parameter is set to false as default, so that an invitee who exits the session does not dissolve the broadcast. The PTT organizer and each recipient must press the Exit key to exit the session. Setting this parameter to true will cause the broadcast to end when an invitee exits the session.

Note Configure your Directory Server, IP-PBX, and Unified Quick Connect Locations parameters by performing the procedures in the subsequent chapter.

CHAPTER 5

Configuring Cisco Unified Quick Connect Server

This chapter describes in detail the configuration tasks that can be performed for Cisco Unified Quick Connect Server. It describes the following topics:

- Required and Optional Configuration Tasks, page 5-1
- Logging In and Out of WebAdmin, page 5-2
- Configuring Servers, page 5-3
- Using Phone Number Masks, page 5-16
- Configuring Unified Quick Connect Locations, page 5-18
- Configuring Advanced Settings, page 5-22
- Configuring Phone UI Appearance, page 5-24
- Configuring Unified Quick Connect Templates, page 5-31
- Configuring Directory Mapping Attributes, page 5-32
- Configuring Directory Search Static Filters, page 5-33
- Configuring Presence Enabled Broadcasts, page 5-37
- Configuring Policies, page 5-37
- Centralized Configuration Service, page 5-43
- Verifying the Installation Using Phones, page 5-45

Note Some sections of Unified Quick Connect Web Admin are not required when configuring Unified Quick Connect Server. The Application > Presence section is no longer used.

Required and Optional Configuration Tasks

The following sections of Unified Quick Connect Web Admin are required to be configured to enable PTT broadcasts:

- Configuring the Directory as described in Configuring Enterprise Directory Servers, page 5-3.
- If Cisco Unified Application Environment and Cisco Unified Quick Connect are installed in the same server, performing the procedure Enabling SSL Security for Cisco Unified Quick Connect WebAdmin, page 5-2.
- Configuring the Provider as described in Configuring IP-PBX Servers, page 5-10.

- Configuring Locations as described in Configuring Unified Quick Connect Locations, page 5-18

The other configuration tasks are optional.

Logging In and Out of WebAdmin

To configure and administer Unified Quick Connect for the first time, you must access the product's Web based administrative interface. Login access to Unified Quick Connect WebAdmin is controlled via domain/local web-server authentication.

Domain and Microsoft IIS administrators can apply the same access control policies they use for other web-based applications to control access to the Unified Quick Connect WebAdmin interface.

Directory security settings for the web-site virtual directory Unified Quick ConnectWebAdmin can be modified to control access to this web-application.

To launch the Unified Quick Connect WebAdmin, open the following URL in your browser:

http://<*Unified Quick Connect-Server-IP-Address*>:<*port number*>/QuickConnectWebAdmin

Configuring the Default Web Site Port Number

If Cisco Unified Application Environment and Cisco Unified Quick Connect are installed in the same server, you must configure the IIS Default Web Site port number to be different from the Cisco Unified Application Environment Web Server port number.

For example, typically CUAE Web Server listens on port 80. You will need to assign a Default Web Site port number different than port 80. The assigned Default Web Site port number must be also entered in **Cisco Unified Quick Connect** > **Advanced Settings** > **Web Service URLs**. See Appendix C, "Cisco Unified Quick Connect Advanced Settings".

Enabling SSL Security for Cisco Unified Quick Connect WebAdmin

Perform the following steps to enable secure SSL access to Unified Quick Connect WebAdmin.

Procedure

Step 1 Open Microsoft IIS Manager.

Step 2 Select **Unified Quick Connect WebAdmin** and right click and select **Properties**.

Step 3 Select the **Directory Security** tab.

Step 4 Click **Edit** under Secure Communication.

Step 5 Configure the following options:

- Check "Require secure channel (SSL)".
- Optionally, check "Require 128-bit encryption".

Step 6 Click **OK**.

Disabling Anonymous Login to Cisco Unified Quick Connect WebAdmin

To improve security by disabling anonymous access to WebAdmin, perform the following steps to require user credentials to be entered:

Procedure

Step 1 Open Microsoft IIS Manager.

Step 2 Select **Unified Quick Connect WebAdmin** and right click and select **Properties**.

Step 3 Select the **Directory Security** tab.

Step 4 In the Authentication and user control section uncheck “Enable anonymous access.”

Step 5 Click **OK**. User credentials are now required for WebAdmin access.

Configuring Servers

Cisco Unified Quick Connect requires at least two, and can use up to four different types of data servers:

- Enterprise Servers
- Directory Servers (required)
- Policy Servers (optional)
- PBX Servers (required)

Server Considerations

At least one Directory Server must be configured in order for Unified Quick Connect Server to find user information. A PBX server is required if users are to control their VoIP phone from Unified Quick Connect.

Configuring Enterprise Directory Servers

Unified Quick Connect utilizes the users and groups in your existing directory servers as a starting point for communications. This greatly minimizes end-user training since the same users and groups they use from within other applications (e.g., e-mail applications) are now available for VoIP communications. It also reduces administrative tasks by providing you with a single point of administration for all users and groups. That is, you can use your directory server(s) as a centralized repository for traditional applications and PC applications.

To use Unified Quick Connect, you must have directory connectivity information available. The information required depends on the type of enterprise directory server being used.

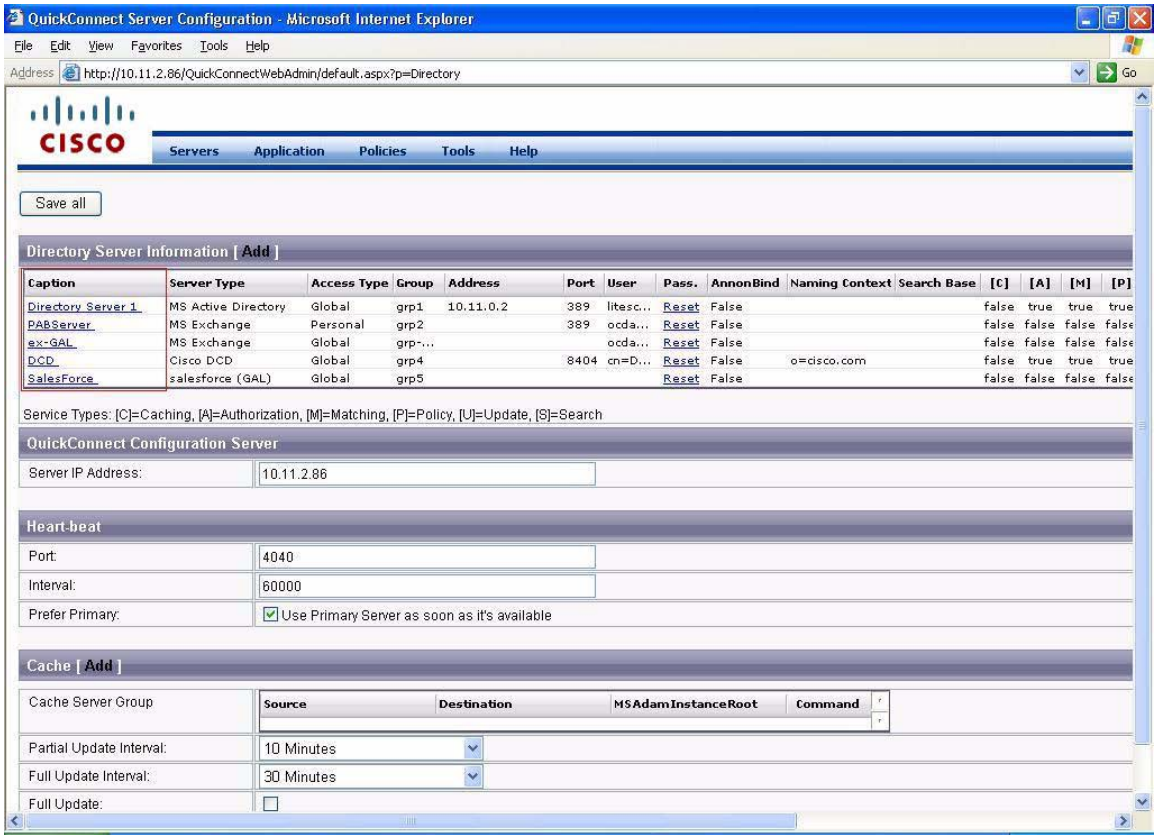
Use Unified Quick Connect WebAdmin to configure access to your directory server(s).

Directory Server Layout in WebAdmin

Select **Servers** > **Enterprise Servers** > **Directory Servers**. This takes you to the default view of the Directory Servers screen (Figure 5-1) where you will see the following sections:

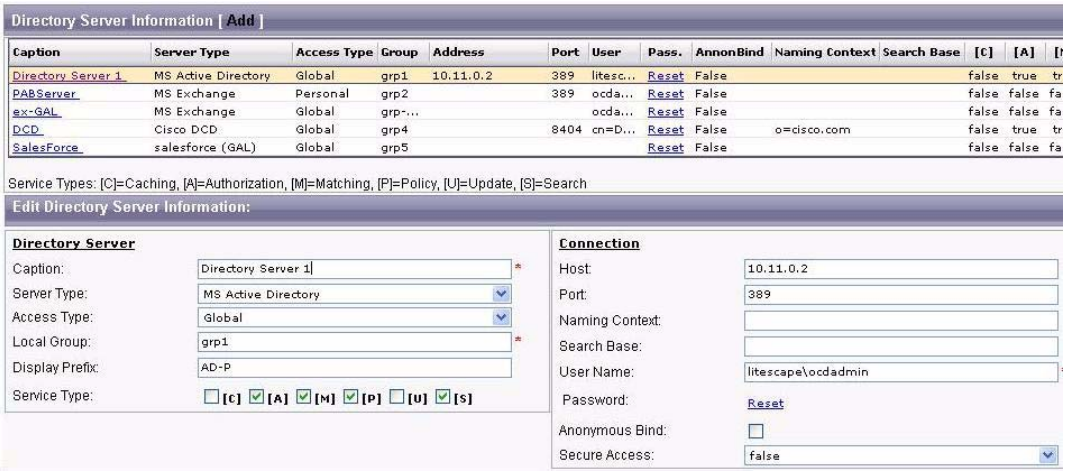
- Directory Server Information: Allows you to define the directory server(s) that Unified Quick Connect might connect to.
- Unified Quick Connect Configuration Server: Defines which Unified Quick Connect server in your environment will act as the configuration server.
- Heartbeat: Configures the keep-alive settings between Unified Quick Connect and the directory servers.
- Cache: Use when you want to cache GAL data on a Unified Quick Connect server.

Figure 5-1 Directory Servers Screen



Click on any of the links for directory servers that are listed in the Caption column to see an expanded view of the Directory Server Information fields (Figure 5-2):

Figure 5-2 Directory Servers Information



Click on any of the links for directory servers that are listed in the Caption column to view and edit its information.

Adding a Directory Server

Click the **Add** link next to Directory Server Information to create a new Enterprise Directory Server. You will see the expanded view for a new directory server, fill in the required information. At the end click the **Save** and **Save All** buttons to save this directory in your Cisco Unified Quick Connect configuration.

Complete the fields in Table 5-1 as required:

Table 5-1 Directory Server Settings

Field Name	Description	Required
Directory Server Information – defines which directories Cisco Unified Quick Connect can connect to.		
Caption	The name of the server within Cisco Unified Quick Connect. This information is only used within the Cisco Unified Quick Connect configuration.	Yes
Server Type	Selects which directory type in your organization will be accessed. The following directory servers are supported. Microsoft Active Directory Open LDAP Cisco DCD Microsoft Exchange SQL Database MS ADAM Salesforce (GAL) – is used for connecting to Salesforce.com	Yes
Access Type	Lists the type of datastore that can be accessed by Cisco Unified Quick Connect. Choose from the following types: Global: Global directory server (for Global Address Book data).	Yes

Table 5-1 Directory Server Settings

Field Name	Description	Required
Local Group	Identifies the group that this directory belongs to. Directories in the same group provide backup and redundancy for one another. These groups are used when configuring Unified Quick Connect Locations.	Yes
Display Prefix	Specifies a server identification tag. The tag you enter will appear before each search result entry that appears on the user's phone screen.	No
Service Type	Specifies the directory server's purpose. Select from the following options: [S]: is for Search, specifies if this directory server is used for searching capabilities. [C]: is for Caching, specifies if the directory server is used as a replica of the existing enterprise directory. [A]: is for Authorization, specifies if the directory server is used to find and authenticate user identify. [M]: is for Matching, specifies if the directory server is used to match an attribute against the IP-PBX. [P]: is for Policy, specifies if the directory server will store Unified Quick Connect policies. When choosing more than one service type, only the following combinations are recommended: "S A", "M A", "S M", "S A M" & "S C A M P"	At least one must be selected
Connection – records the information for connecting to the directory server.		
Host	Specifies host IP address or name for directory server.	Yes
Port	Defines which port to use when connecting to the directory server	No
Naming Context	Determine which credentials to use when connecting to the directory server. Unified Quick Connect will use this setting if it is populated. If left blank, Unified Quick Connect will use server-less binding to connect to the configured directory servers. Important: Mandatory for LDAP and MS Exchange. For example, o=cisco.com	No
Search Base	Defines where in the target directory server that Unified Quick Connect will begin searching. If blank, Unified Quick Connect will begin searching at the root.	No
User Name	Specifies the username to be used to access the directory server. The domain name must be included as part of the user name. For example, cisco\admin. If specifying an anoymous connection using Anonymous Bind, user credentials are not required.	No
Password	Specifies the user password to be used to access the directory server. This is only required if you are not using Anonymous Bind (see below).	No
Anonymous Bind	Important: If checked, Unified Quick Connect binds to the underlying directory using anonymous credentials.	No

Table 5-1 Directory Server Settings

Field Name	Description	Required
Secure Access	This can be set to True or False. This should be set to True if the directory server requires SSL for secure connectivity. If set to True, your directory server is required to support SSL DS binding and you must set the proper port (port 636 is standard).	No
Unified Quick Connect Configuration Server		
Server IP Address	Records which Unified Quick Connect server in the entire network will act as the configuration server.	No
Heartbeat – configures the keep-alive settings between Unified Quick Connect and the directory servers.		
Port	Defines which port to use when checking availability of directory server.	No
Interval	Defines in milliseconds, how often to query the main directory server to verify its availability.	No
Prefer Primary	Configures Unified Quick Connect to switch to the primary directory server once it is available.	No
Cache – use when you want to cache data on the Unified Quick Connect server.		
Cache Server Group	Records information about the caching server and its source directory server. You may include the following fields: Source – the directory server being used as the source for the cached data. Destinations – records where the information will be cached. MSADAMInstanceRoot – the directory where Microsoft Active Directory Application Mode resides	No

To delete a server, scroll to the far right side of the Directory Server Information table and click the **Del** link for the server. You will be asked to confirm the removal of the record from the system; click **OK**.

Adding Salesforce.com as a Directory Server

With Unified Quick Connect you may extend access of your Salesforce.com directory to IP phones. For example, users not licensed to use Salesforce.com from the web can still look up customer information from an IP phone and communicate with them.

To allow Unified Quick Connect to access Salesforce.com from IP phones, add a directory as specified above. Only the following information is required (Figure 5-3):

- Caption – can be any name.
- Server Type – select **salesforce (GAL)**.
- Access Type – select **Global**.
- Local Group – can be any name.
- Display Prefix – this will be listed next to any Salesforce.com entries that are displayed in Unified Quick Connect Phone. Due to phone screen sizes, it is recommended that this be no more than four characters.
- Service Type – *only* check **[S]** for Search.

- User Name – this should be the username for a valid Salesforce.com user within your organization. Unified Quick Connect will use this user's credentials to connect to Salesforce.com and read information from it.
- Password – the password consists of a Salesforce.com password appended by a security token provided to the administrator.

For example, if your SFDC password is 12345, and the token issued is *qweouqweoiqwr*, then enter the following for the Salesforce.com password: ***12345qweouqweoiqwr***

Figure 5-3 Adding SalesForce.com as a Directory Server

To complete the addition, restart MAPI Connector in Windows Services.

Adding Microsoft Access as a Directory Server

You may expose a customer Microsoft Access data repository to be displayed within Unified Quick Connect. For example, you may have a custom list of users and phone numbers that is stored in Microsoft Access. You may allow Unified Quick Connect users to access this data repository from Unified Quick Connect for any supported features.

To allow Unified Quick Connect to access Microsoft Access from IP phones, add a directory as specified above. Only the following information is required:

- Caption – can be any name.
- Server Type – select **MS-Access**.
- Access Type – select **Personal**.
- Local Group – can be any name.
- Display Prefix – this will be listed next to any Salesforce.com entries that are displayed in Unified Quick Connect Phone. Due to phone screen sizes, it is recommended that this be no more than four characters.
- Service Type –check **[S]** for Search and **[A]** for Authorization.
- Host – should be the local path were the Microsoft Access database (.mdb file) is located.

  You must manually map attributes in Microsoft Access to attributes in Unified Quick Connect. To do this:
- Open OnCast.Configuration.xml
- Go to the section under <Mapping/Default>
- For each ID, map it to the appropriate attribute in your Microsoft Access database. For example:

```
<Field>
    <ID>LSDisplayName</ID>
    <Attribute>Ofc_sym</Attribute>
    <Category>3</Category>
```

```
</Field>
```

- Configure the LSDisplayName, and any other Unified Quick Connect attributes in **Unified Quick Connect WebAdmin** > **Phone UI** > **Search Settings** to enable searching your Microsoft Access database.

Configuring Enterprise Policy Servers

Simple policies are stored in the OnCast.Configuration.xml file, so no Policy Server definition is needed. However, complex policies can be stored on the network directory servers or on the Unified Quick Connect server, so their place of residence must be defined. When you have multiple Unified Quick Connect servers, you can define which is used for storing and fetching policies for a specified Unified Quick Connect location (See "Locations: Associating Policy Servers" later in this chapter).

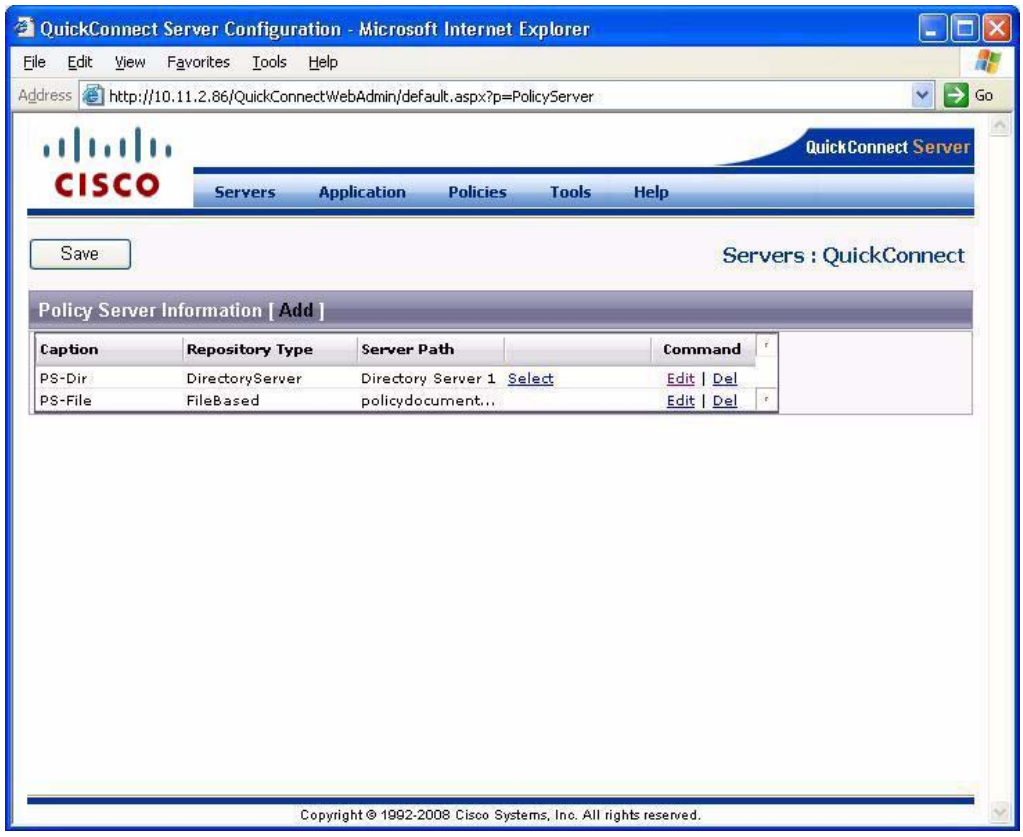
Adding Policy Servers

To configure a policy server for a complex policy:

Procedure

Step 1 Select **Servers** > **Enterprise Servers** > **Policy Servers**. This takes you to the Policy Server Information screen (Figure 5-4).

Figure 5-4 Policy Server Information



Step 2 Click **Add** to create a new policy server configuration.

Step 3 Type a name for the server in the Caption field.

Step 4 In the Repository Type field, do one of the following:

- Select **DirectoryServer** if you want to store the policy on an existing server.
- Select **FileBased** if you want to store the policy in a folder on a local server.

Step 5 To enter a Server Path, click the **Select** link.

- If you selected **DirectoryServer** in Step 4, type in the IP address of the server, or click **OK** then click **Select** to select a server that will store the policies.
- If you selected **FileBased** in Step 4, type or paste in the path to the selected drive and folder.

Step 6 Make your selection and click **OK** to reset the screen.

Step 7 Click **Save** to save and implement your changes.

Deleting and Editing Policy Servers

You can edit or delete policy servers.

To delete a policy server:

Procedure

Step 1 From the Servers: Unified Quick Connect screen, click the **Del** link for the server you want to delete.

Step 2 Click **OK** on the confirmation window to complete the deletion.

To edit a policy server:

Procedure

Step 1 From the Servers: Unified Quick Connect screen, click the **Edit** link for the server you want to edit.

Step 2 You can change the Caption, Repository Type, or Server Path fields as needed.

Step 3 Click **OK** to save your changes.

Configuring IP-PBX Servers

Unified Quick Connect reads device information your IP-PBX and uses this information to deliver applications to the IP phone. Have your Pre-Installation Checklist available when configuring this section of WebAdmin.

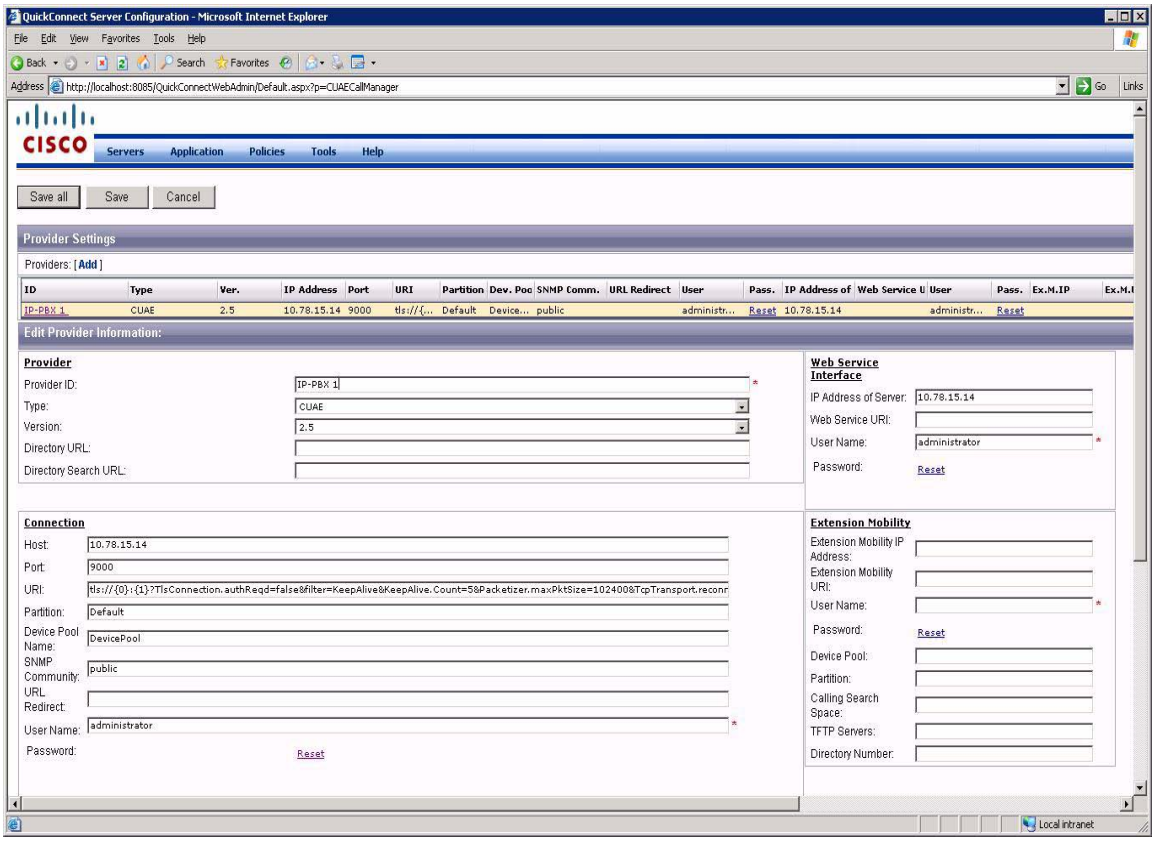
To configure IP-PBX servers:

Procedure

Step 1 Select **Servers** > **IP-PBX (Providers)** > **PBX Servers**. This opens the Provider Settings screen (Figure 5-5). Click the link in the ID column to display an expanded view of the IP-PBX settings.

The fields displayed in the expanded view below are the same as those that run from left to right in the default view. Only the display is different.

Figure 5-5 Provider Settings Screen



Change the settings in Table 5-2 as required:

Table 5-2 IP-PBX Settings

Field Name	Description	Required
Provider Information		
Provider ID*	Select a unique name for this provider (strings allowed).	Yes
Type*	Select CUAE (Cisco Unified Application Environment)	Yes
Version*	Select 2.5 for the version of software the IP-PBX uses.	Yes
Directory URL	End-users not authorized for Unified Quick Connect are redirected to this URL when accessing Directories from a phone.	No
Directory Search URL	Users not authorized to search Unified Quick Connect are redirected to this URL when attempting to gain access to the search criteria screen.	No

Table 5-2 IP-PBX Settings

Field Name	Description	Required
Connection		
Host*	Enter a comma delimited IP address for all nodes in the IP-PBX cluster.	Yes
Port*	Enter the provider port. Should be configured to 9000.	Yes
URI	This is populated automatically from the OnCastConfiguration.xml file.	Yes
Partition	Enter the name of the partition created in CUAE. The default is "default".	Yes
Device Pool Name	Enter the name of the device pool created in CUAE.	Yes
URL Redirect	Push requests from unauthenticated users are redirected to this URL.	No
Username*	Specify the user ID to be used to push content to IP phones.	Yes
Password*	Specify and confirm the user password to be used to push content to IP phones. After the initial setting of the password, these fields are hidden behind a password Reset link.	Yes
Web Service Interface		
IP Address of Server	Specify the IP Address of the CUAE server.	Yes
Web Service URI	Specifies the Web service URI to use. Must be set to: /Soap/risport.dll	Yes
User Name*	Specifies the IP-PBX provider user-ID that has permission to make Web service calls.	Yes
Password*	Specify and confirm the password of the IP-PBX provider user ID that has permission to make Web service calls. After the initial setting of the password, these fields are hidden behind a password Reset link.	Yes
Extension Mobility		
Ex. M. URI	Specifies the CallManager URL to use when invoking extension mobility. For most CallManager versions this should be: Ex. M URL: should be /emservice/EMServiceServlet	Yes

Step 2 To support Extension Mobility, configure the *Ex. M. URI* field only.

Step 3 Click **Save** when you have finished entering the data.

PBX Servers: Using IP-PBX Aliases

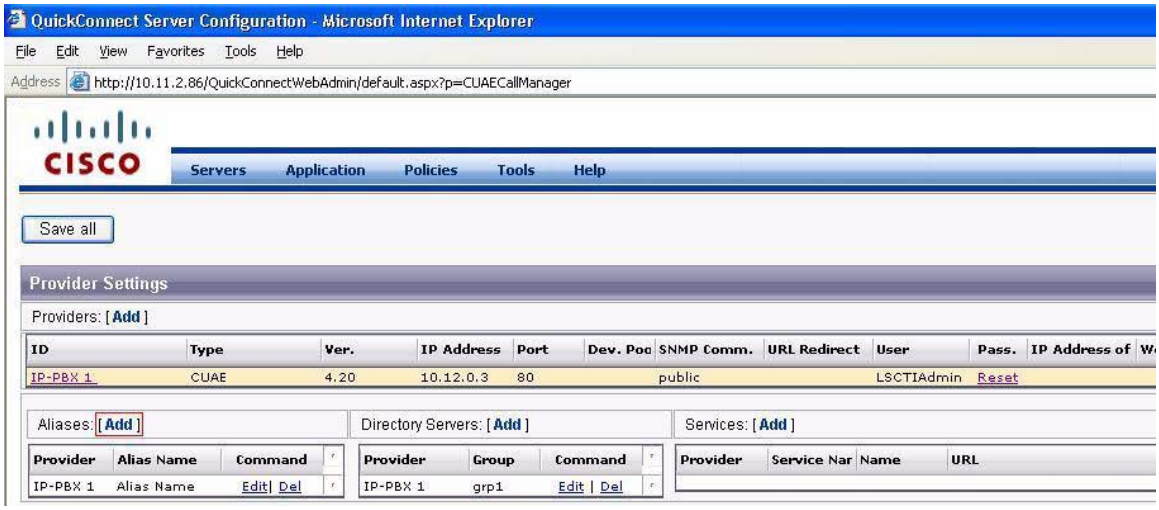
This feature is useful in IP-PBX environments with multiple directory number plans for each site. Examples include multi-extension environments where one site has multiple dialing prefixes from the outside, and sites where some devices on one IP-PBX have five digit extensions and others have six digit extensions.

To configure a provider with an alias:

Procedure

Step 1 Choose **WebAdmin** > **Servers** > **IP-PBX (Providers)** > **PBX Servers**. In the Providers section (Figure 5-6), click on the provider you would like to add an alias to.

Figure 5-6 Associating a Provider with an Alias



Step 2 In the Aliases section (Figure 5-7), click [**Add**]. This creates a new blank row in the Aliases section.

Figure 5-7 Aliases Section

Step 3 Enter the Alias Name.

Step 4 Click **OK**.

Step 5 Click **Save** at the top of the page.

Step 6 Click **Save All**.

PBX Servers: Associating a Provider with a Directory Group

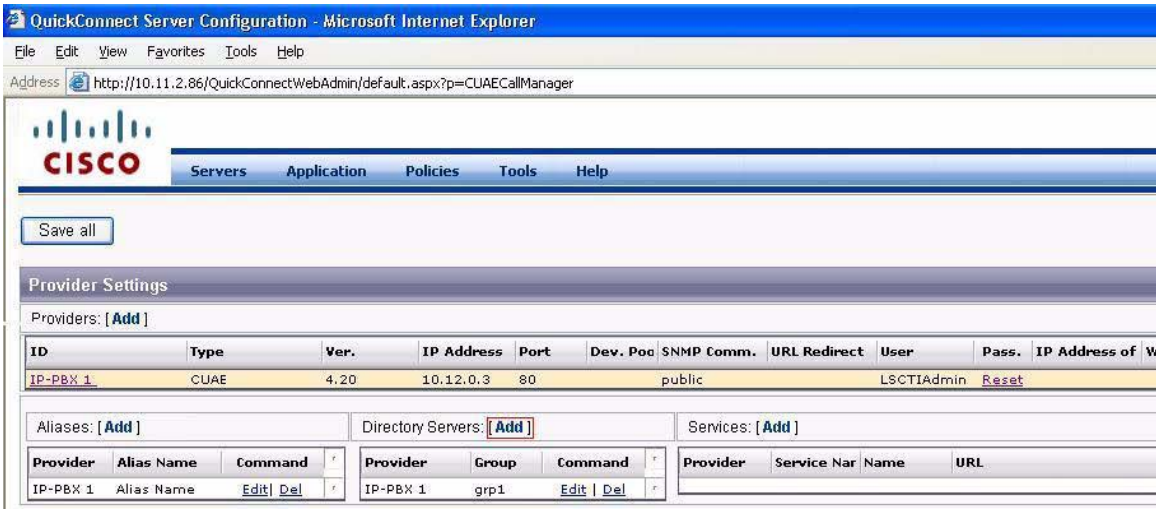
Unified Quick Connect allows you to associate a provider with a directory group. Use this feature when you want all the phones registered with that provider to only have access to the servers in that group. For more information about defining a local directory group, see the "Directory Server Configuration Options" section above.

To associate a provider with a directory group:

Procedure

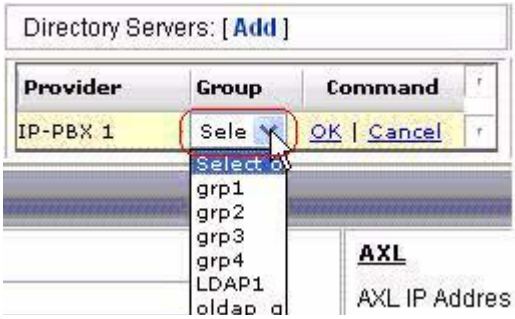
Step 1 Choose **WebAdmin** > **Servers** > **IP-PBX (Providers)** > **PBX Servers**. In the Providers section, click on the provider you would like to add an alias to (Figure 5-8).

Figure 5-8 Associating a Provider with a Directory Group



Step 2 In the Directory Servers section (Figure 5-9), click [**Add**]. This creates a new blank row in the Directory Servers section.

Figure 5-9 Directory Servers Section



Step 3 From the dropdown list in the Group field, select the group you want to associate with the provider.

Step 4 Click **OK** to make the association.

Step 5 Click **Save** at the top of the screen to save it.

Step 6 Click **Save All**.

PBX Servers: Associating a Service with a Provider

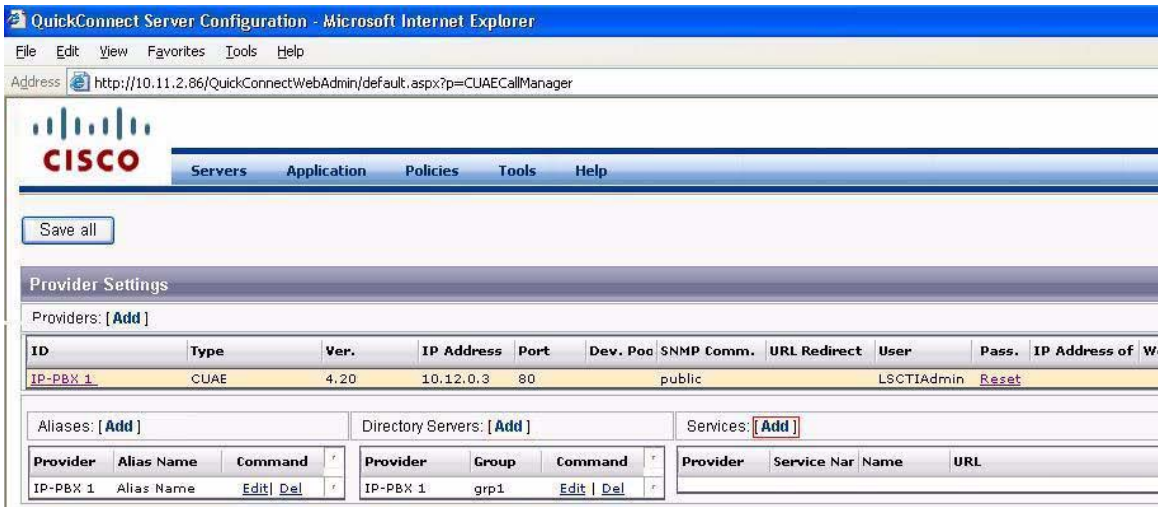
Unified Quick Connect allows you to configure all of the phones registered with a provider to allow access to an IP phone service or application. Users can then access the service or application button from their IP phone.

To associate a service with a Provider:

Procedure

Step 1 Choose **WebAdmin** > **Servers** > **IP-PBX (Providers)** > **PBX Servers**. In the Providers section, click on the provider you would like to add a service to (Figure 5-10).

Figure 5-10 Associating a Provider with a Service



Step 2 In the Services section (Figure 5-11), click [**Add**]. This creates a new blank row in the Services section.

Figure 5-11 Services Section

Step 3 In the Service Name field, type the name of the service or application.

Step 4 In the Name field, type the service or application name as you want users to see it on their phone screens.

Step 5 In the URL field, enter the web location of (or path to) the service or application. When users select the service or application, they'll automatically be taken to this page.

Step 6 Click **OK** to make the association.

Step 7 Click **Save** at the top of the screen to save the new service.

Step 8 Click **Save All**.

Using Phone Number Masks

Unified Quick Connect provides you with the flexibility to have varying formats for phone numbers in your PBX and directory. With the Phone Number Mask feature you can configure Unified Quick Connect to handle matching and presence.

Note You will typically have many phone number masks configured to account for the dialing plan in your PBX. Unified Quick Connect analyzes phone number mask rules from the top to the bottom and stops when it finds the first rule that applies.

Matching

There may be instances when a telephone number in the directory server does not match what is in the IP-PBX. As a result, you can set up a masking rule to match extensions. You will always use a "M" at the beginning of the rule to indicate that this rule is to be used for matching.

Provider Based Masking

When creating a masking rule, you specify whether the rule applies to All Providers or to only a specific provider.

Directory Server Number is longer than PBX Number

There may be cases where a user's number is stored as an extension in the PBX and a full phone number in the directory server. For example, if a number is configured in your PBX as "2366" and "1-650-292-2366" in your directory server.

To create a masking rule for this scenario in Unified Quick Connect WebAdmin:

Procedure

Step 1 Choose **WebAdmin** > **Servers** > **IP-PBX (Providers)** > **Phone Number Masks**.

Step 2 Click the **Add** button.

Step 3 In the Provider column, select All Providers or select a specific IP-PBX provider from the list.

Step 4 In the Mask column, enter **M|A1A-A6A5A0A-A2A9A2A-####**.

a. "M|" — Indicates that this rules is for matching.

b. "A1A-A6A5A0A-A2A9A2A-" — Unified Quick Connect takes the phone extension in the PBX and, with masking, it adds digits to and removes digits from the PBX extension to find the identical telephone number match in the directory server.

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

Step 6 Repeat these steps, substituting "P|" for "M|". This allows the OnCast Presence server to provide presence indications.

In the example, Unified Quick Connect will take PBX extension 2366 and find a match using the first masking rule that applies. Unified Quick Connect will find the match (a user) in the directory server and allow the user to use Unified Quick Connect further on the phone.

PBX Number is longer than Directory Server Number

There may be cases where the phone number in the PBX is longer or formatted differently than how the number is stored in the directory server (e.g., if a number is configured in your PBX as “16502920359” and “650-292-0359” in your directory server).

To create a masking rule for this scenario in Unified Quick Connect WebAdmin:

Procedure

Step 1 Choose **WebAdmin** > **Servers** > **IP-PBX (Providers)** > **Phone Number Masks**.

Step 2 Click the **Add** button.

Step 3 In the Provider column, select All Providers or select a specific IP-PBX provider from the list.

Step 4 In the Mask column, enter **M|R1###A-###A-####**. This will do the following:

- **a.** “M|” — Indicates that this rules is for matching.
- **b.** “R” — Will remove the first character from the PBX number, so it will be transformed from “16502920359” to “6502920359”
- **c.** “###” — Skip the next three digits in the PBX number
- **d.** “A-” — Will add a “-“, so the PBX number will be transformed from “6502920359” to “650-2920359”
- **e.** “###” — Skip the next three digits in the PBX number
- **f.** “A-” — Will add a “-“, so the PBX number will be transformed from “650-2920359” to “650-292-0359”
- **g.** “####” — Skip the next four digits in the PBX number.
- **h.** Unified Quick Connect has thus taken the PBX number and transformed it to match the number in the directory server.

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

PBX Number is Formatted Differently than Directory Server Number

In another example, if a number is configured in your PBX as “16502920359” and “(650) 292-0359” in your directory server, you must configure Unified Quick Connect to account for this difference in format.

To create a masking rule for this scenario in Unified Quick Connect WebAdmin:

Procedure

Step 1 Choose **WebAdmin** > **Servers** > **IP-PBX (Providers)** > **Phone Number Masks**.

Step 2 Click the **Add** button.

Step 3 In the Provider column, select All Providers or select a specific IP-PBX provider from the list.

Step 4 In the Mask column, enter **M|RA(###A)A ###A-####**. This will do the following:

a. "M|" — Indicates that this rules is for matching.

b. "R" — Will remove the first character from the PBX number, so it will be transformed from "16502920359" to "6502920359"

c. "A(" — Will add a "(", so the PBX number will be transformed from "6502920359" to "(6502920359"

d. "###" — Skip the next three digits in the PBX number

e. "A)" — Will add a ")", so the PBX number will be transformed from "(6502920359" to "(650)2920359"

f. "A" — Will add a space, so the PBX number will be transformed from "(650)2920359" to "(650) 2920359".

Note The extra space has been added after the closed parenthesis.

g. "###" — Skip the next three digits in the PBX number

h. "A-" — Will add a "-", so the PBX number will be transformed from "(650) 2920359" to "(650) 292-0359"

i. "####" — Skip the next four digits in the PBX number.

j. Unified Quick Connect has thus taken the PBX number and transformed it to match the number in the directory server.

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

Configuring Unified Quick Connect Locations

A Unified Quick Connect Location is used for segmenting users, locations or groups and assigning them with the following:

- Providers — The IP-PBXs used by the Unified Quick Connect Location.
- Directories — The directory server(s) used by the Unified Quick Connect Location.
- Broadcasters — Indicates which Unified Quick Connect Server on the network should be used for broadcasting at this Unified Quick Connect Location.
- Policy Servers — Where to find the Unified Quick Connect policies to be used by the Unified Quick Connect Location.

Locations are created automatically when a new Unified Quick Connect Server initializes itself using a Unified Quick Connect Configuration Server. In the WebAdmin interface, you can associate a location with providers, directories, broadcasters, and policy servers.

To edit location information:

Procedure

Step 1 Choose **Unified Quick Connect WebAdmin** > **Servers** > **Unified Quick Connect Locations**.

Step 2 Choose **All Locations** in the tree browser, then click **Edit**.

Step 3 Edit the Location's information as described in Table 5-3:

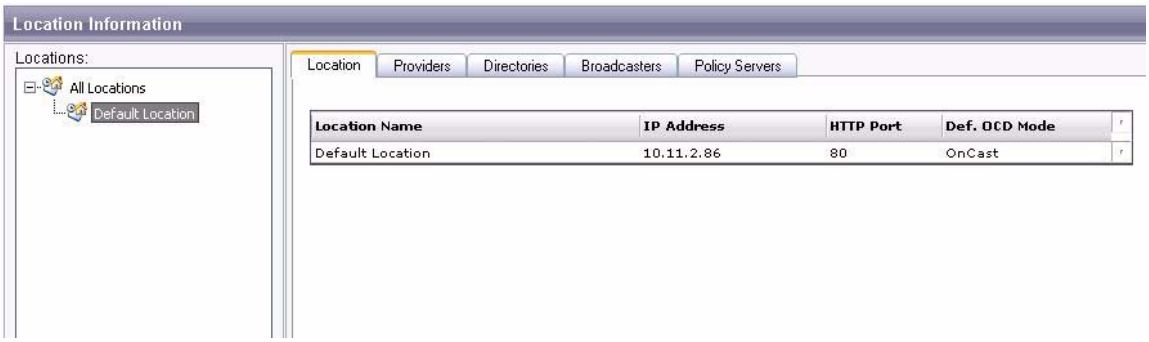
Table 5-3 Editing Location Information

Field	Description	Required
Location Name	Specifies the name of the location within the Unified Quick Connect configuration.	Yes
IP Address	In a single server deployment, the IP address is the IP address of the Unified Quick Connect server. In a high-availability/redundant deployment, the IP address is the IP address of the network load balancing server for this cluster or content switch behind which the Unified Quick Connect server is located.	Yes
HTTP Port	Leave this field blank if Unified Quick Connect and Cisco Unified Applications Environment are co-resident on the same server. Otherwise, configure an HTTP port.	Yes
Default OCD Mode	Defines the default behavior of all Unified Quick Connect users within this location. Select either Active Dial or QuickConnect from the dropdown menu. Active indicates that the Active Dial feature will be used by default for all users. With Active Dial, a user will perform a search and can easily dial by simply highlighting an entry from the search results screen and picking up the handset. Predictive Search cannot be used together with Active Dial mode, due to phone API limitations.	Yes
Current checkbox	Indicates if this location is the current location for this server.	No

Step 4 Click **OK**, then click **Save**.

Each Unified Quick Connect Server has a local identity. In a single server deployment, the location created above would match the local identity of the server. In a multi-server/site deployment, one of the locations created would have to match the local identity of this specific server. Figure 5-12 shows the Location Information screen.

Figure 5-12 Location Information



Locations: Associating Providers

Each Unified Quick Connect location is paired with an IP-PBX provider. This defines which IP-PBXs will read user and device information from this Unified Quick Connect location.

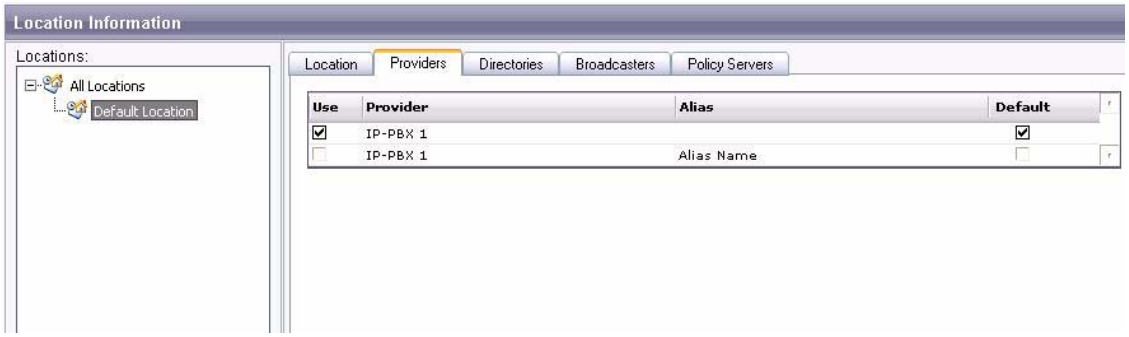
To associate locations with providers:

Procedure

Step 1 Choose **WebAdmin** > **Servers** > **Unified Quick Connect Locations** and click the **Providers** tab.

Step 2 Put a check next to which Providers this location will be associated with (Figure 5-13). Make sure you select providers which have been defined in WebAdmin > IP-PBX (Providers).

Figure 5-13 Associating Locations to Providers



Step 3 You should also check one Provider as the default for this location. Make sure you insert the Alias for the providers to be associated with this location.

Locations: Associating Directories

Each Unified Quick Connect location can access multiple directories.

To associate locations with directories:

Procedure

Step 1 Choose **WebAdmin** > **Servers** > **Unified Quick Connect Locations** and go to the Directories section.

Step 2 Select which directory servers this location should be associated with. Make sure you associate directories which have been defined in WebAdmin > Servers > Enterprise Servers > Directory Servers.

Step 3 Click **Save**.

Locations: Associating Broadcasters

Broadcast servers (Broadcasters) are associated with locations and are responsible for delivering content and services to endpoints. There can be many broadcast servers for each location. At each location, any number of broadcast servers can be deployed for high-availability, redundancy or load distribution purposes.

To associate locations with broadcasters:

Procedure

Step 1 Choose **WebAdmin** > **Servers** > **Unified Quick Connect Locations**, click the **Broadcasters** tab and click [**Add**].

In the IP field, enter the IP address of the broadcast server, in the HTTP Port section leave this field blank if Unified Quick Connect and Cisco Unified Applications Environment are co-resident on the same server. Otherwise, configure an HTTP port.

Step 2 In the Audio Port section enter 5055.

Step 3 In the Broadcasters section, provide the actual IP address of the Broadcast Server for this location.

- In single and multi-server deployments, this matches the server's internal IP address (not the NLB/virtual IP address).

Step 4 Click **OK**, then **Save**.

Locations: Associating Policy Servers

If you have created multiple policy servers, you can associate each server with a different location. Each Unified Quick Connect server delivers policies for all Unified Quick Connect users within its location.

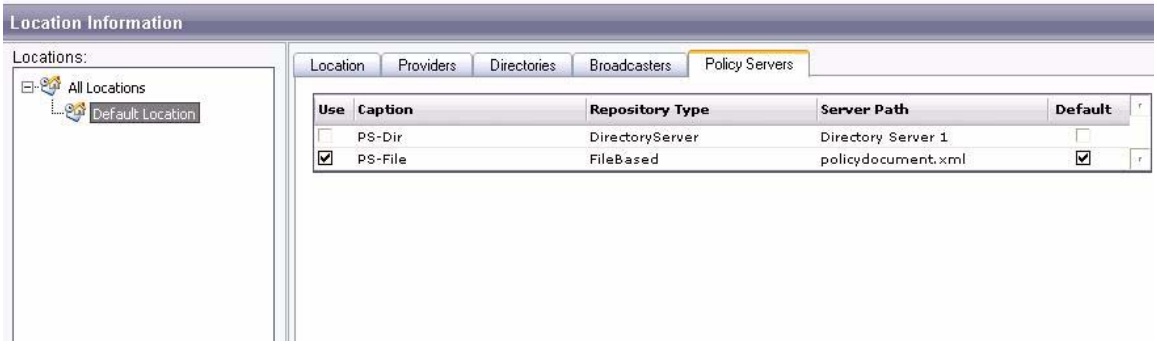
To associate a policy server with a location:

Procedure

Step 1 Choose **Unified Quick Connect Locations** from the **Servers** menu. This takes you to the Servers: Locations screen.

Step 2 Click on the **Policy Servers** tab, which lists all of the policy servers you've configured (Figure 5-14).

Figure 5-14 Policy Servers Tab



Step 3 You can configure the following options on this page:

- You can designate a server as both the Use (as in In-Use) server and the Default server.
- You can designate one server as the Use (for example, “In-Use”) and leave another as the Default.

When different servers are identified as in-use and default servers, Unified Quick Connect uses the default server as a backup if the in-use server becomes unavailable.

Step 4 Click **Save** when you have completed your selections.

Locations: Device Status

To verify Device Status configuration:

Procedure

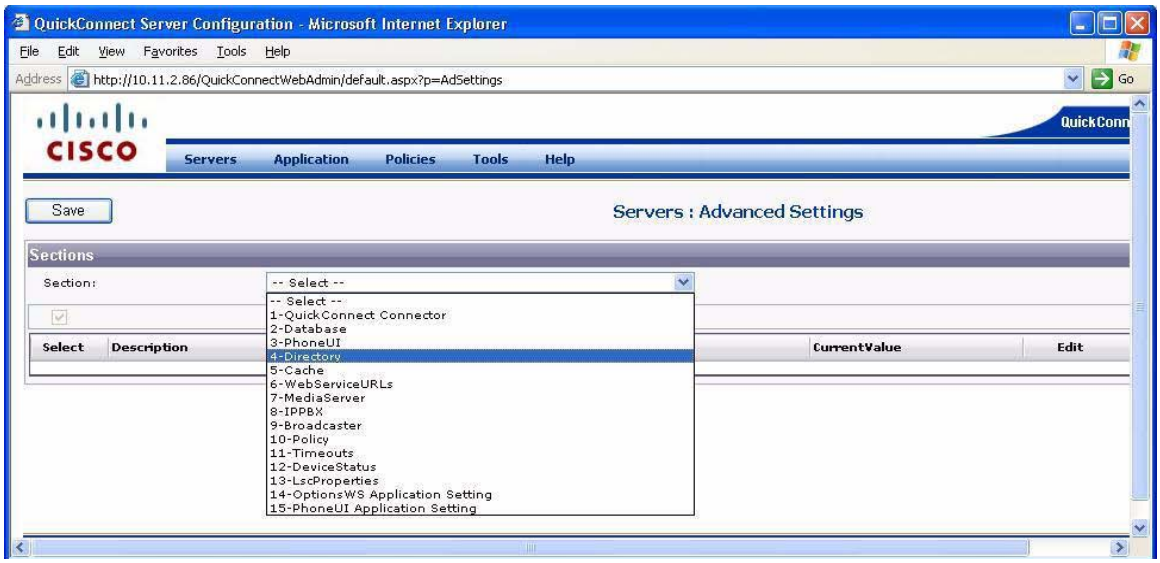
Step 1 On the **Device Status** tab, and verify that the MAP IP parameter is configured to the IP address of the local server.

Configuring Advanced Settings

Unified Quick Connect WebAdmin allows you to make changes to advanced settings in the system configuration file from within WebAdmin. These settings will typically not need to be changed unless your environment requires some level of custom configuration.

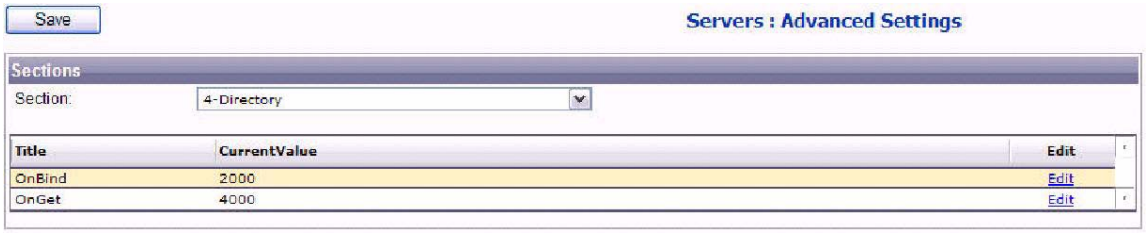
To make changes, go to **Servers** > **Advanced Settings** (Figure 5-15). From the Section: field, click the drop-down box and select which part of the OnCast.Configuration.xml file you would like to customize. For a detailed look at this file, see the separate OnCastConfiguration.xml document.

Figure 5-15 Advanced Settings



Upon selecting one of the sections, you will see a list of parameters for that section that can be configured (Figure 5-16).

Figure 5-16 Advanced Settings



You can select or deselect parameters using the checkboxes in the Select column. You can also select or deselect all of the listed parameters by using the checkbox above the list of parameters.

You can make changes to any of these parameters, and click **Save** in the upper-left hand corner to apply the change. In some cases you may have to restart Microsoft IIS on the Unified Quick Connect Server for the change to take effect.

Configuring Phone UI Appearance

The Unified Quick Connect user interface that appears on user VoIP phones is highly configurable. The following pages illustrate the Unified Quick Connect Phone User Interface (UI) configuration options and describe how to use each one.

To access Unified Quick Connect UI options:

Procedure

Step 1 Select **Phone UI** from the Application menu.

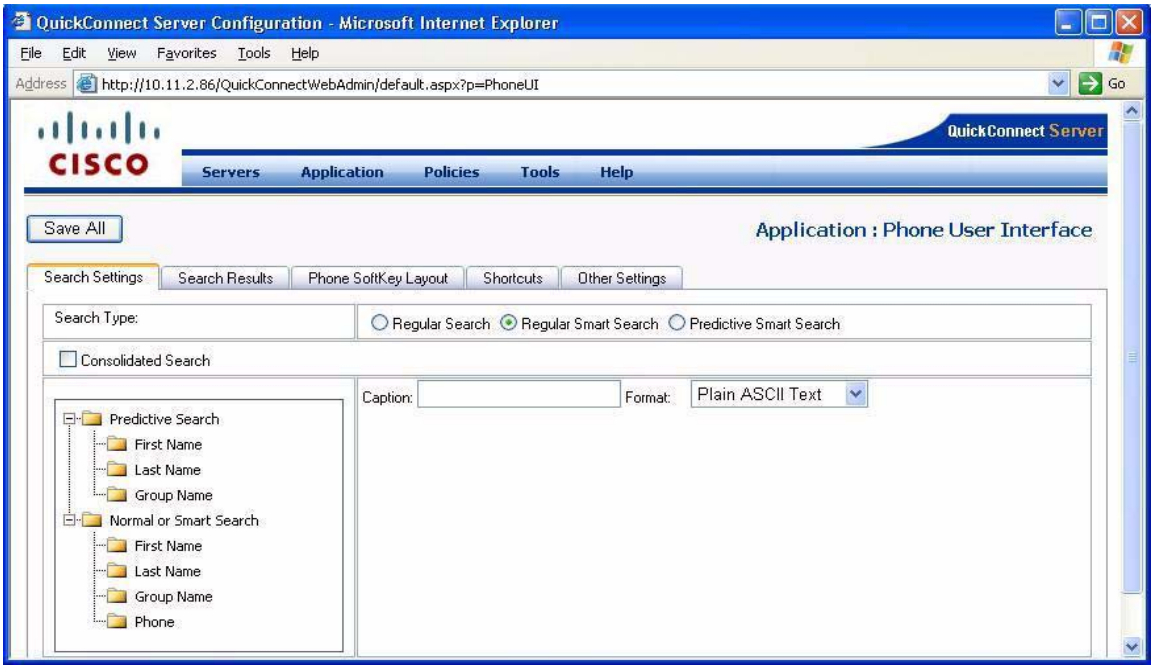
Step 2 Create or edit the entries needed in each of the tabs to set up or change the UI, as described in the following sections.

Step 3 Click **OK** and **Save** to save and implement your changes.

Search Settings tab

The Search Settings tab (Figure 5-17) allows you to specify the default search type used by Unified Quick Connect. Use the Search Type radio buttons to specify the default search type.

Figure 5-17 Search Settings Tab

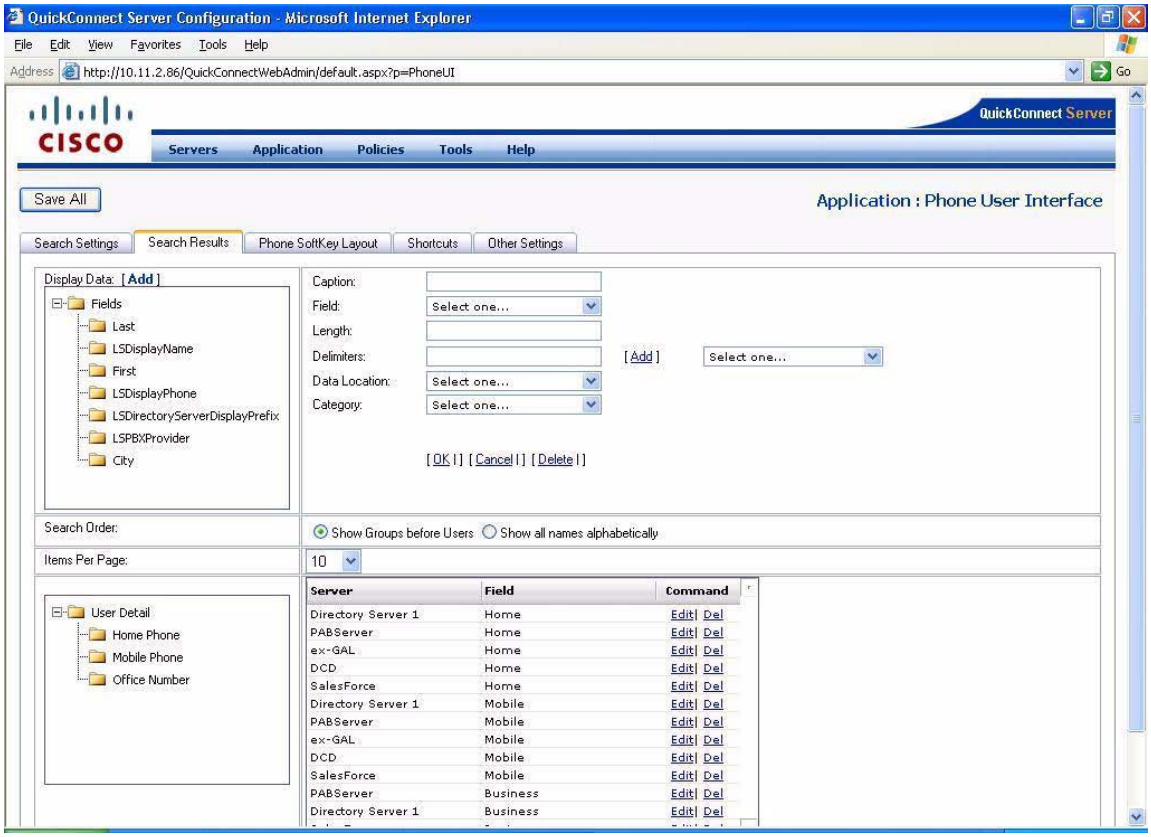


Refer to the Search Settings section of the *Phone UI Tabs: Field Descriptions* table for more information.

Search Results tab

The Search Results tab (Figure 5-18) allows you to define fields for use in the display of search results. Use the Add and Delete buttons to create or remove fields that are used for displaying search results.

Figure 5-18 Search Results Tab

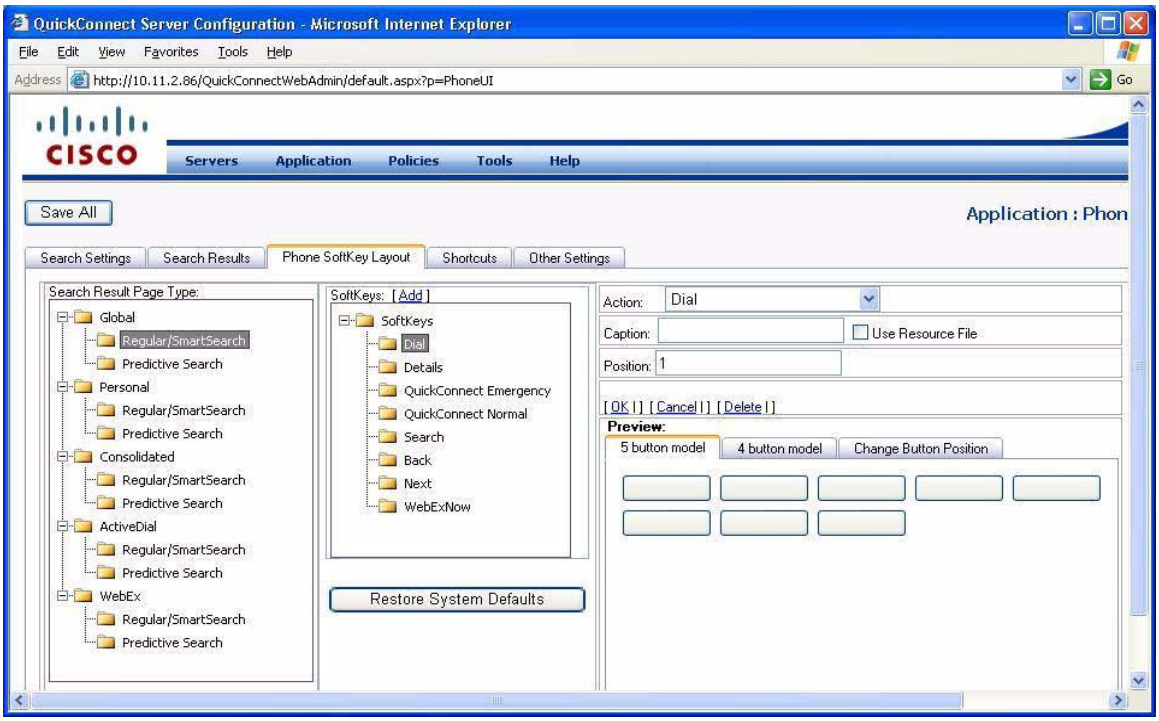


Refer to the Search Results section of the *Phone UI Tabs: Field Descriptions* table for more information.

Phone Softkey Layout tab

The Phone SoftKey Layout tab (Figure 5-19) allows you to configure which Unified Quick Connect features are shown to end-users on their IP phone and also how these features are presented.

Figure 5-19 Phone Softkey Layout Tab



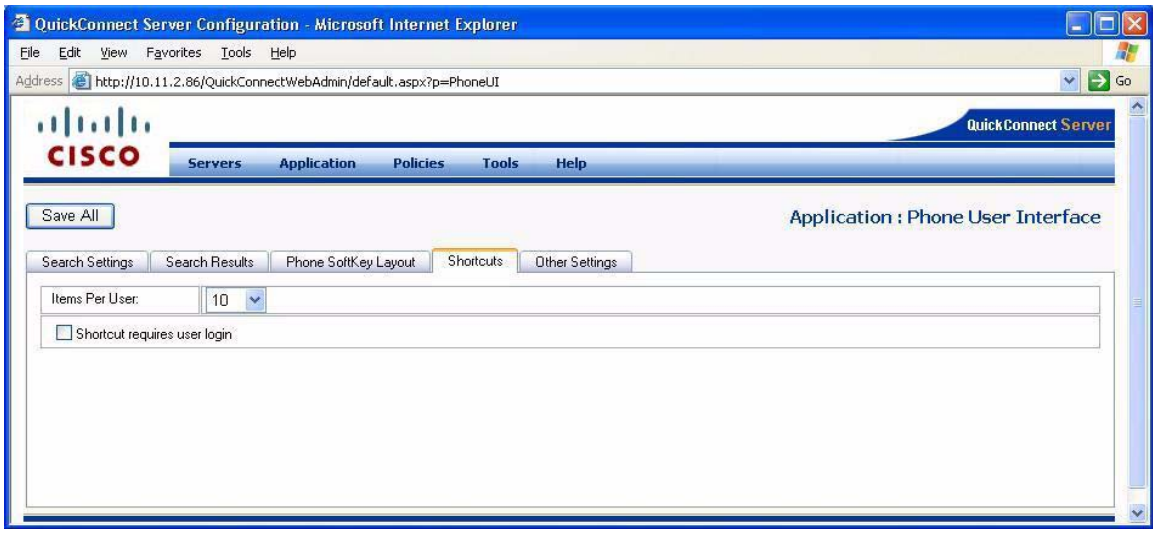
Refer to the Phone Softkey Layout section of the *Phone UI Tabs: Field Descriptions* table, and the section “Phone UI: Configuring Phone Softkey Layout” for more information

Shortcuts tab

The Shortcuts tab (Figure 5-20) allows you to specify the number of shortcuts the user can use on his or her phone. You can also specify whether or not shortcut use requires login.

Use the “Items Per User” dropdown menu to indicate the number of shortcuts the user can use on his or her phone. Check the “Shortcut requires user login” box to require a login to use shortcuts.

Figure 5-20 Shortcuts Tab



Refer to the Shortcuts section of the *Phone UI Tabs: Field Descriptions* table for more information.

Other Settings tab

The settings on this tab are not currently used for Cisco Unified Quick Connect.

Phone UI Field Descriptions

Table 5-4 lists descriptions for parameters in all the Phone UI tabs.

Table 5-4 Phone UI Screen: Field Descriptions

Field	Description	Required
Search Settings		
Search Type	**Regular Search**: Select this checkbox to activate regular search, which is typically used as the default mode. This mode is active until users turn on one of the other modes (Smart, or Predictive). Compared to the other modes, this mode is the most "manual." For example, to search for names beginning with "B," users need to press the 2 key twice. To perform the same search in Smart mode, users can enter the 2 key once to have Unified Quick Connect return results for all of the letters associated with that key.	Yes
	Regular Smart Search: Select this checkbox to allow users to press a single button on the phone keypad to search for all characters associated with that button. For example, if users press 2 on the phone keypad in Smart Search mode, Unified Quick Connect displays all the contacts in the user's address book that begin with A, B or C.	
	Predictive Smart Search: Select this checkbox to return search results as users type search criteria. For example, if users press the 4 key, Unified Quick Connect will immediately start listing entries that start with the letters G,H, I, and with the number 4. This is useful for large directories where users want to receive immediate results and modify search criteria upon seeing results. Includes smart search capability. Predictive Search cannot be used together with Active Dial mode due to phone API limitations.	
Search Items	For each search item, you can specify which Directory Server(s) will be searched for that field. IMPORTANT: In the Format dropdown, select Plain ASCII Text for each field to make searching easy for your users.	
Search Results		
Display Data	Use the fields in this section to specify how search results are displayed on the phone screen. You can configure which fields to display for each user and group in the search results screen. For example, you can display Last Name, followed by First name, followed by Phone number, followed by Location. You can add or remove data display fields as needed. To add a field: give the field a name (e.g. Caption). Select the type of data you want to display in the field (use the down arrow in the Field field). These are fields in the Directory Mapping section and map to attributes in your directory servers. Specify the maximum Length of the field in characters. This is useful to prevent long fields from utilizing too much screen space. Use the Delimiters and Add links fields to add delimiters to help separate search results. Identify the Location from which the search data is retrieved. Select the display results Category (users and groups, just groups, just users).	Yes

Table 5-4 Phone UI Screen: Field Descriptions

Field	Description	Required
Search Order	Determines order of search results, (i.e. show groups first or alphabetically sort all results).	Yes
Items Per Page	Specifies the total search results displayed per page.	Yes
User Details (GAL)	Note: This feature is not currently supported in Cisco Unified Quick Connect.	Yes
Shortcuts		
Items Per User	Use these fields to specify the number of shortcuts that are allowed on each user phone.	Yes
Shortcut requires user login	Select this field if users must log in before using a shortcut.	No
Other Settings		
TTS Voice	Note: This feature is not currently supported in Cisco Unified Quick Connect.	Yes
Start Screen	Specify the destination page when the user invokes the Back or Exit buttons on the phone keypad. You can send the user to the Directories or the Services screen on the phone.	Yes

Phone UI: Configuring Phone Softkey Layout

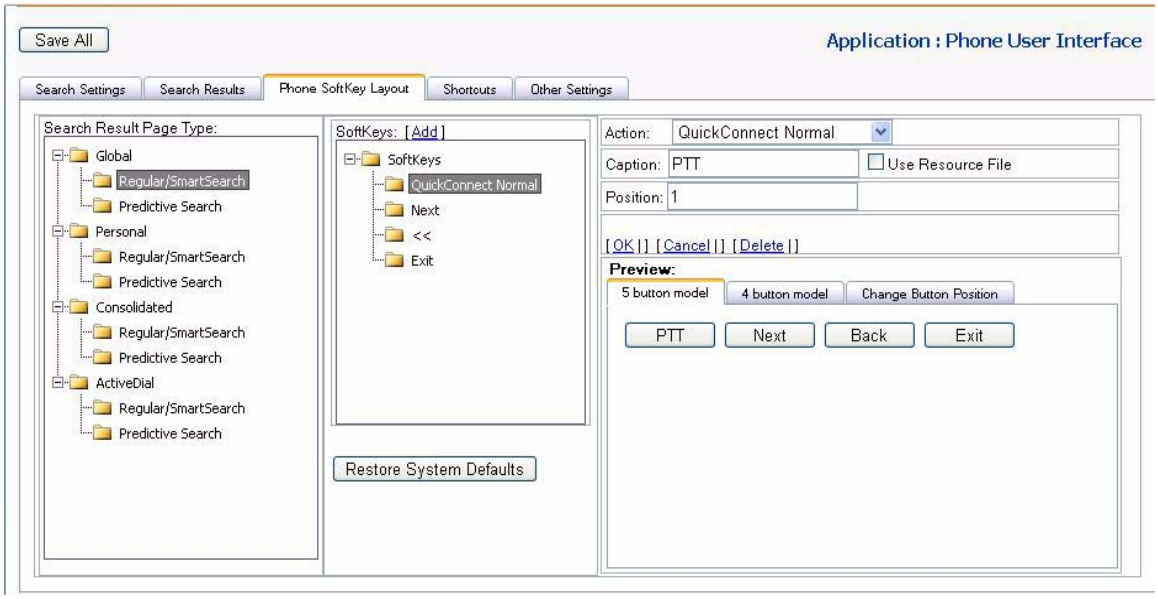
This section allows you to configure which Unified Quick Connect features are shown to end-users on their IP phone and also how these features are presented. You may also configure the soft-key layout based on the search type utilized by the users.

Adding a Unified Quick Connect Feature SoftKey

To customize the soft-key layout, first select the type of format used in the Search Results page in the phone user interface. In Figure 5-21, the soft-keys will only be modified.

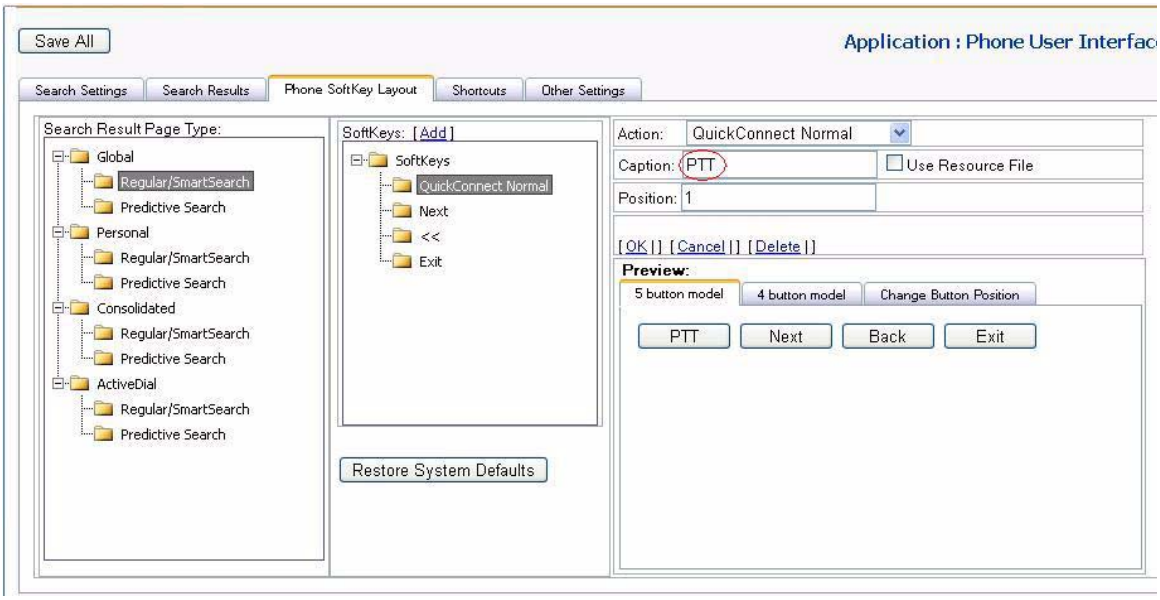
Next, you may select which Unified Quick Connect feature to add or modify by selecting the appropriate folder under SoftKeys (Figure 5-22). You can select the action this soft-key will invoke by selecting the drop-down box in the Action: field.

Figure 5-21 Customizing Softkey Layout - 2 of 4



You can determine what the feature is called when displayed on the phone UI and also which physical button it will be associated with (Figure 5-22).

Figure 5-22 Customizing Softkey Layout - 3 of 4



Once done, click [**OK**]. Make sure to click **Save** in the upper left hand corner of WebAdmin.

Changing the Order of Soft-Keys

You can also change the order of existing soft-keys in the phone user interface. From the Phone SoftKey Layout section in Unified Quick Connect WebAdmin, click the **Change Button Position** tab.

You can highlight the appropriate feature and click **Move Up** or **Move Down** to place the soft-key in the appropriate section in the phone user interface.

Once done, click [**OK**]. Make sure to click **Save** in the upper left hand corner of WebAdmin.

Configuring Unified Quick Connect Templates

The work flow and *look and feel* of Unified Quick Connect broadcasts are controlled by a set of programmable templates. Templates enable the delivery of text, images, pre-recorded audio, real-time voice streams and text-to-speech content to IP end points. The templates also control the functional appearance of soft keys on IP phones along with the processes they invoke when pressed.

The Unified Quick Connect template framework supports the following content-types:

- Primary content types
  - Text
  - Images
  - Audio files

Unified Quick Connect provides support for the following types of templates:

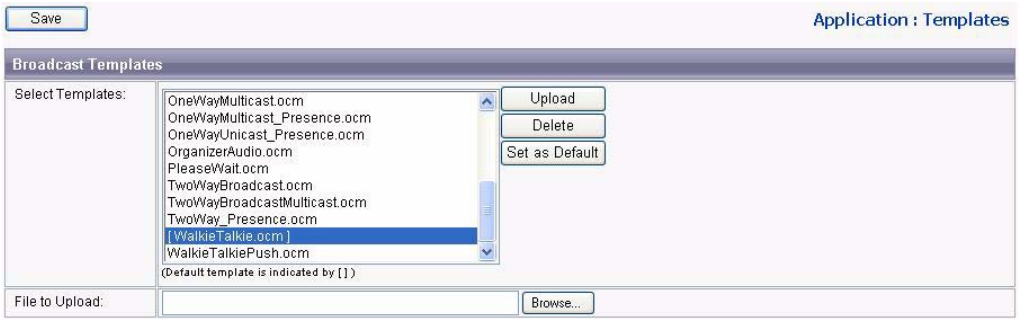
- Templates for one-way audio broadcast

To configure templates in Unified Quick Connect:

Procedure

Step 1 Choose **WebAdmin** > **Application** > **Templates** to open the Application: Templates screen (Figure 5-23).

Figure 5-23 Application:Templates Screen



Step 2 Unified Quick Connect template files can be loaded from anywhere in your network. Click the **Browse** button to locate the template file. All template files use the .ocm file extension.

Step 3 Click **Upload**, then click **Save**.

Each type of template - Broadcast, Meet-me conference and 3rd party conference - can have multiple templates for users to select. Templates are global; once a template is loaded into Unified Quick Connect, all users can start using it instantly. Loading templates does not require any service restart.

Each Template type should have one default template. To set a template as default:

Procedure

Step 1 Select the template in the list. For Unified Quick Connect, the most appropriate default template is WalkieTalkiePush.ocm.

Step 2 Click the **Set as Default** button.

Step 3 Click **Save** at the top of the page.

Step 4 Click **Save All**.

Plug-ins and Work-flow

Unified Quick Connect templates can internally invoke each other. In addition, the product provides an extendable framework, so that templates can call external plug-ins - composite business objects that perform specific tasks.

Unified Quick Connect includes a group of templates and plug-ins for common workflows.

Configuring Directory Mapping Attributes

Unified Quick Connect uses existing attributes in your enterprise directory. You may customize which attributes are used for each Unified Quick Connect feature. The matching criteria between your directory server and IP-PBX are configurable. For more information about configuring directory server settings, see "Configuring Enterprise Directory Servers".

To configure Unified Quick Connect for directory mapping:

Procedure

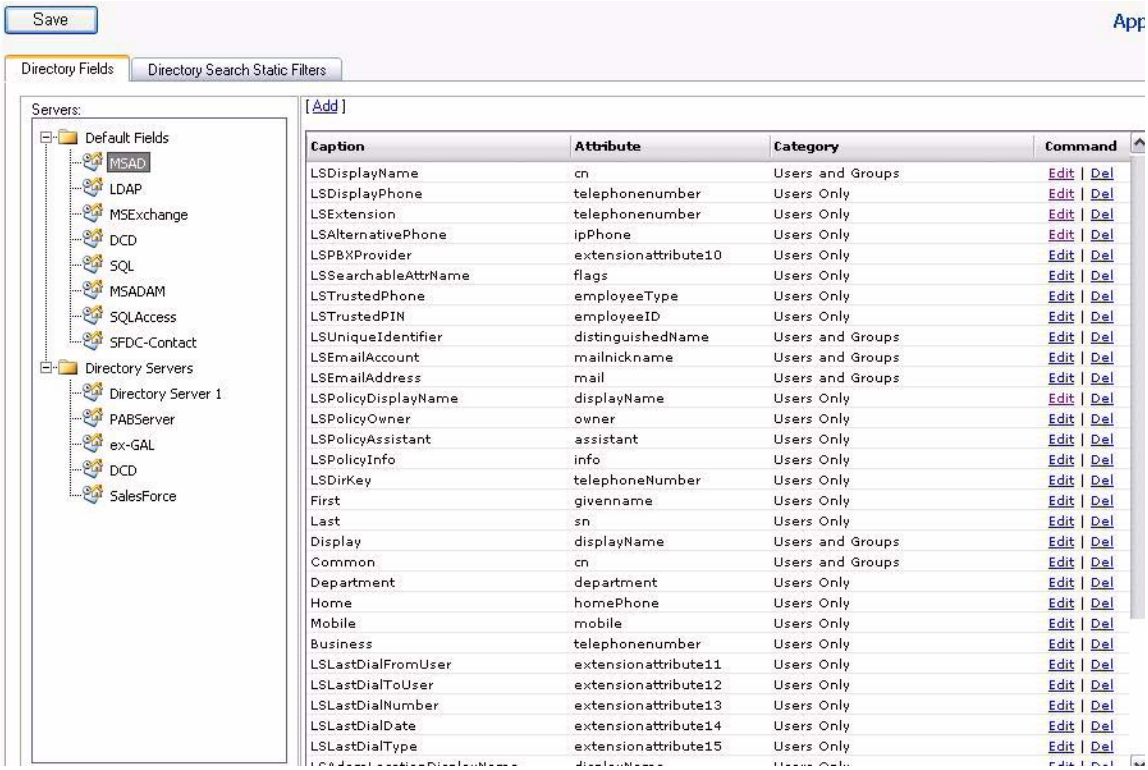
Step 1 Choose **WebAdmin** > **Application** > **Directory Mapping** > **LSDirKey** where LSDirKey may be an attribute in the directory server, such as telephoneNumber. If you are matching based on telephone number, then the attribute in the directory server associated with LSDirKey (e.g., telephoneNumber) must match the user's extension in the IP-PBX. For example, if a user called Steve Fone has an extension of 20359 in the IP-PBX, then the user Steve Fone in the directory server must have its *telephoneNumber* attribute set to 20359.

Step 2 Choose **WebAdmin** > **Servers** > **Advanced Settings > LSSNMPkey**. You may change this to be *extension* if you will be matching based on a telephone number in your directory server. You may change this to *username* if you will be matching based on UID in your directory server.

a. The user PIN is stored in an encrypted format in the directory server using SHA-1 or MD5.

b. Wildcard for access policy allowed in the FROM: and/or TO: field.

Figure 5-24 Application:Directory Mapping Screen



Step 3 Use the descriptions in Appendix B, "Directory Server Parameters" to help determine how to configure mapping parameters and attributes.

Step 4 Click **Save** to save your changes.

Configuring Directory Search Static Filters

Static filters can be configured for each directory server type. Each directory server type can have multiple filters of each type. They all will be appended to the main search queries with the operator AND. Changes for filters are done by directly editing the OnCast.Configuration.xml file, or through Unified Quick Connect Web Admin.

By default, the following search result filters exist:

- Groups with no display name (LSDisplayName).
- Users with no extension (LSExtension).

The following are Unified Quick Connect attributes that must be populated if used in a filter.The mapping between directory server attributes and Unified Quick Connect attributes is described in Configuring Directory Mapping Attributes, page 5-32.

- LSDisplayName
- LSExtension
- LSTrustedPIN
- LSTrustedPhone

Native Static Filters

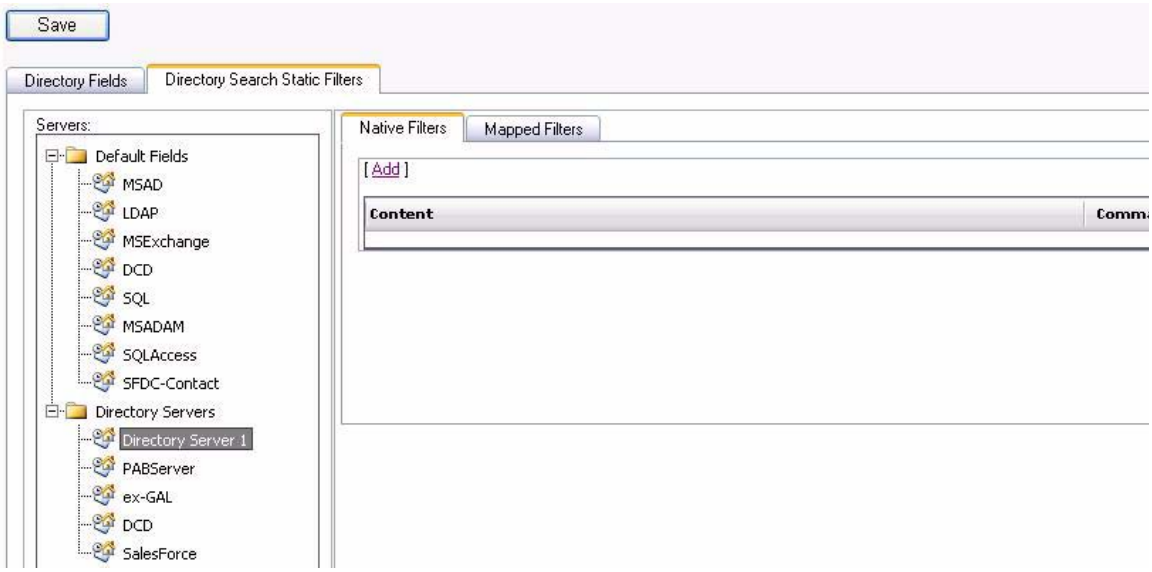
Native static filters contain queries which are constructed in the native syntax of the specified directory server type and will be appended "as-is" to the main search queries with the operator AND. The directory connection library does not analyze the content of the native static filters.

To configure a native static filter:

Procedure

Step 1 Choose**WebAdmin** > **Application** > **Directory Mapping**, and select the **Directory Search Static Filters tab** (Figure 5-25).

Figure 5-25 Directory Search Static Filters Tab



Step 2 Select a default field or directory server and click **Add** in the **Native Filters tab**.

Step 3 Add content to the Content field and click **OK**.

Step 4 Click **Save** to save the filter.

Example Native Static Filter

The following is an example of a native static filter. This filters any object which has a name and telephone number, *or* is a group and has a name.

(|(&(cn=*)(telephonenumber=*))(&(objectCategory=Group)(cn=*)))

Mapped Static Filters

Mapped static filters can contain multiple conditions (criteria). Conditions can be combined into groups. Conditions inside one group are processed with AND operation; groups are processed with OR operation.

Each condition has three components:

- Caption (Unified Quick Connect Parameter Name)
- Operation,
- Value

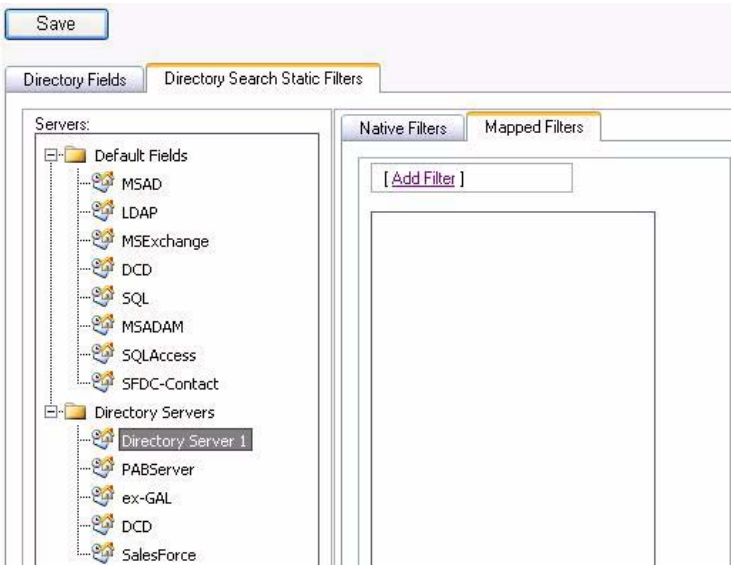
To configure a mapped static filter:

Procedure

Step 1 Choose **WebAdmin** > **Application** > **Directory Mapping**, and select the **Directory Search Static Filters tab**.

Step 2 Select the **Mapped Filters tab** (Figure 5-26).

Figure 5-26 Mapped Filters Tab



Step 3 Select a default field or directory server.

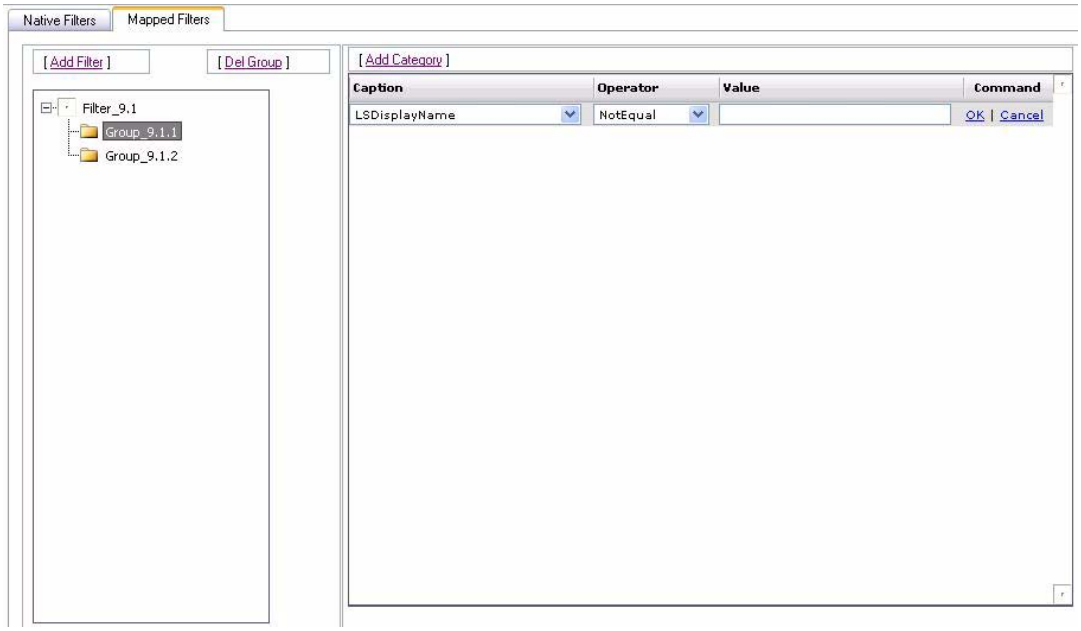
Step 4 Click **Add Filters** in the Mapped Filters tab.

Step 5 Click **Add Group** to add a group within the filter.

Step 6 Expand the filter to view all the groups contained in it.

Step 7 Click **Add Category** to add a category (a condition) to a group (Figure 5-27).

Figure 5-27 Adding a Category (Condition) to a Group



Step 8 Enter following parameters for the static filter conditions:

- Caption: select the Unified Quick Connect Parameter Name from the drop-down list. For definitions of the parameters, see Appendix B, "Directory Server Parameters".
- Operator: select one of the following supported operators: Equal, NotEqual, OR from the drop-down list.
- Value: enter the value of the Unified Quick Connect parameter.

Example Mapped Static Filter

For example, here is a set of static filter conditions:

Table 5-5 Static Filter Conditions

Caption	Operation	Value
1 LSDisplayName	<>	<Empty string>
2. LSExtension	=	20*

Step 9 Add content in the Content field and click **OK**.

Step 10 Click **Save** to save the filter.

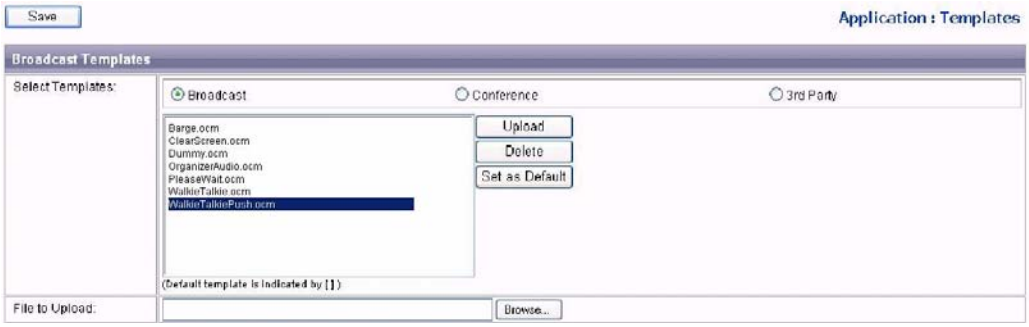
Note The current version of Directory connection library only supports static filters for LDAP-based directory servers (MS AD, MS ADAM, OpenLDAP).

Configuring Presence Enabled Broadcasts

Unified Quick Connect allows you to control the conditions in which a normal priority broadcast is sent to recipients. This functionality is pre-configured; you should not have to change anything in this screen. For example, you can specify that recipients in an active call do not receive a normal priority broadcast or an invitation.

To set presence-enabled broadcasts as a default, open the **WebAdmin** > **Application** > **Templates** screen (Figure 5-28). Highlight a template from the list, as shown below, then click **Save as Default**.

Figure 5-28 Application:Templates Screen



Configuring Policies

Access policies control user access to the following Unified Quick Connect functions:

- Broadcast allows users to send multimedia broadcasts using Unified Quick Connect.
- Get Config and Set Config are used by the centralized configuration service. They determine if a user or group can get or set another user or group's Unified Quick Connect capabilities.

Configuring Access Policies

Unified Quick Connect policies provide two levels of control over access to features:

- Simple: A simple policy provides access to the same Unified Quick Connect functions to all Unified Quick Connect users and groups within the system. Simple policies are stored in the OnCast.Configuration.xml file. This is the default choice for Unified Quick Connect.
- Complex: Complex policies allow you to restrict access by user, group, and function. Complex Policies can be stored in an XML file on the Unified Quick Connect Server or in the directory server(s).

Editing Simple Policies

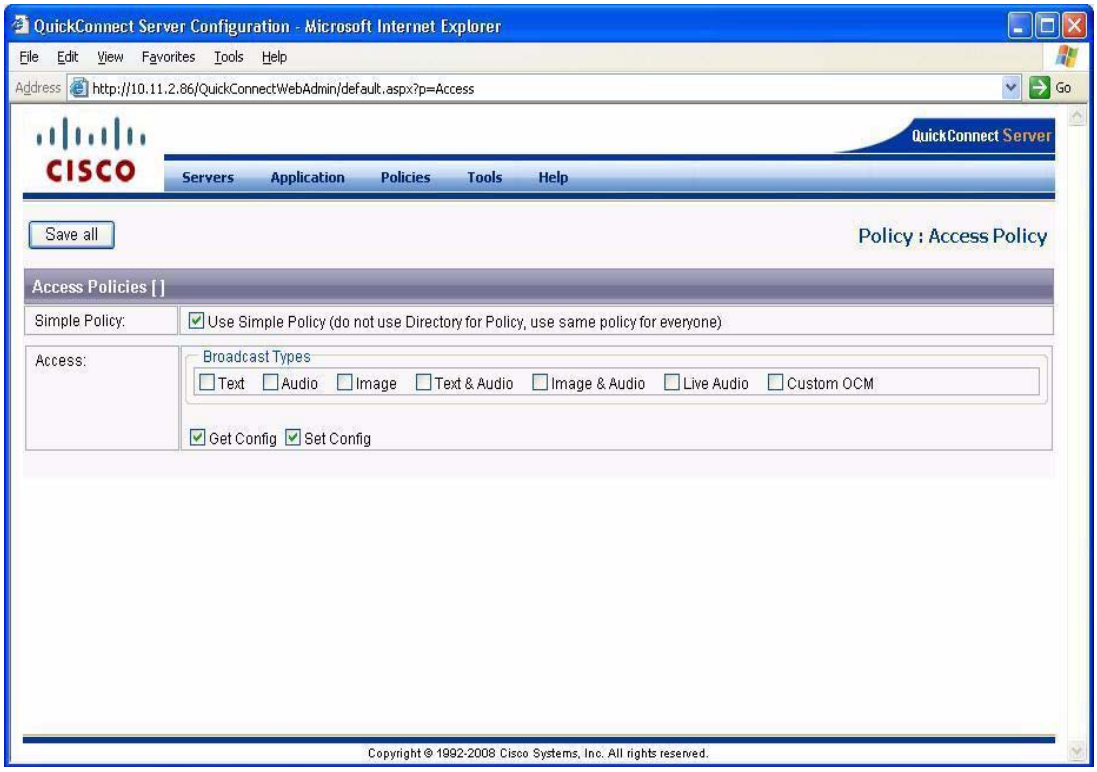
If you choose to implement a simple policy, a set policy will be applied globally. You can edit a simple policy at any time; changes will take effect immediately.

To edit the simple policy:

Procedure

Step 1 Select **Access Policy** from the Policies menu. This takes you to the Policy: Access Policy screen (Figure 5-29), which displays simple policy parameters.

Figure 5-29 Policy:Access Policy Screen



Unified Quick Connect functions are listed in the Access section. By default, access is provided to the Get Config and Set Config functions. By default, all Broadcast Types are allowed.

Step 2 To remove access to a function, click the checkbox in front of the function name. This unchecks the box. To add access, click the blank checkbox in front of the function name.

Step 3 To remove access to a Broadcast Type, uncheck the associated checkbox. To add access, click the blank checkbox in front of the function name.

Step 4 Click **Save** to save and implement your selections. Changes will be immediate for any new sessions that are created after you save.

Adding a New Complex Policy

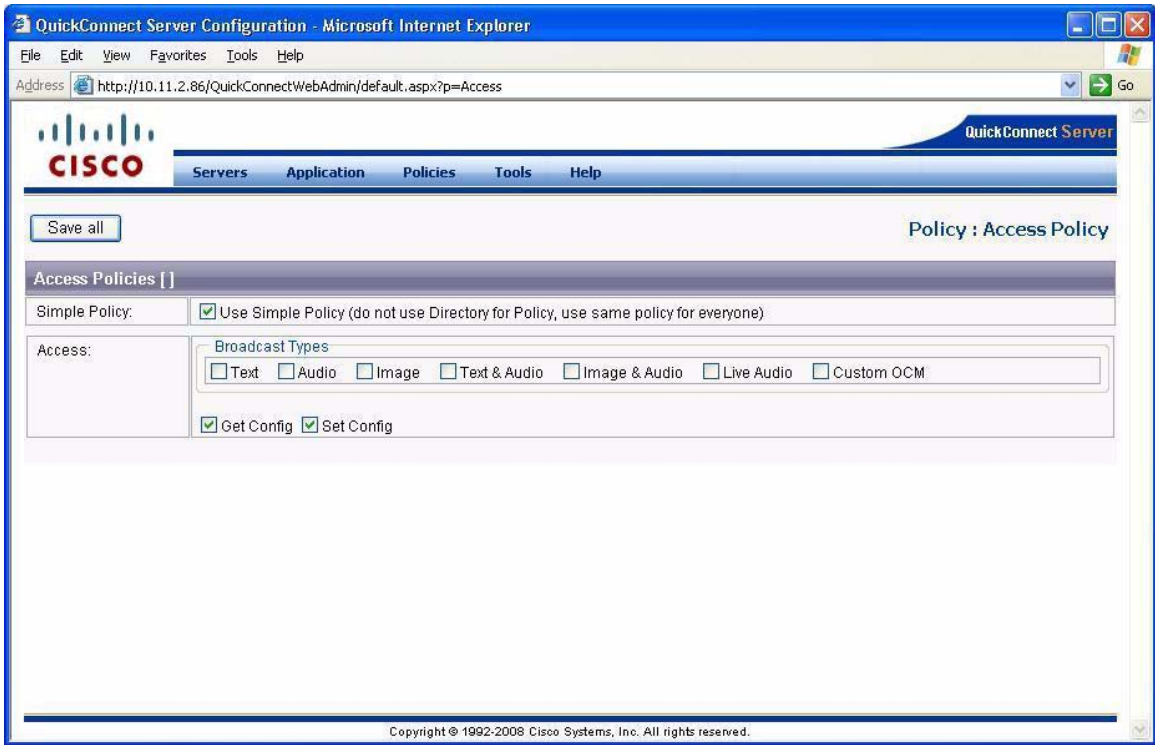
Note You must have defined a Policy Server before you can implement Complex Policies.

To add a new complex policy:

Procedure

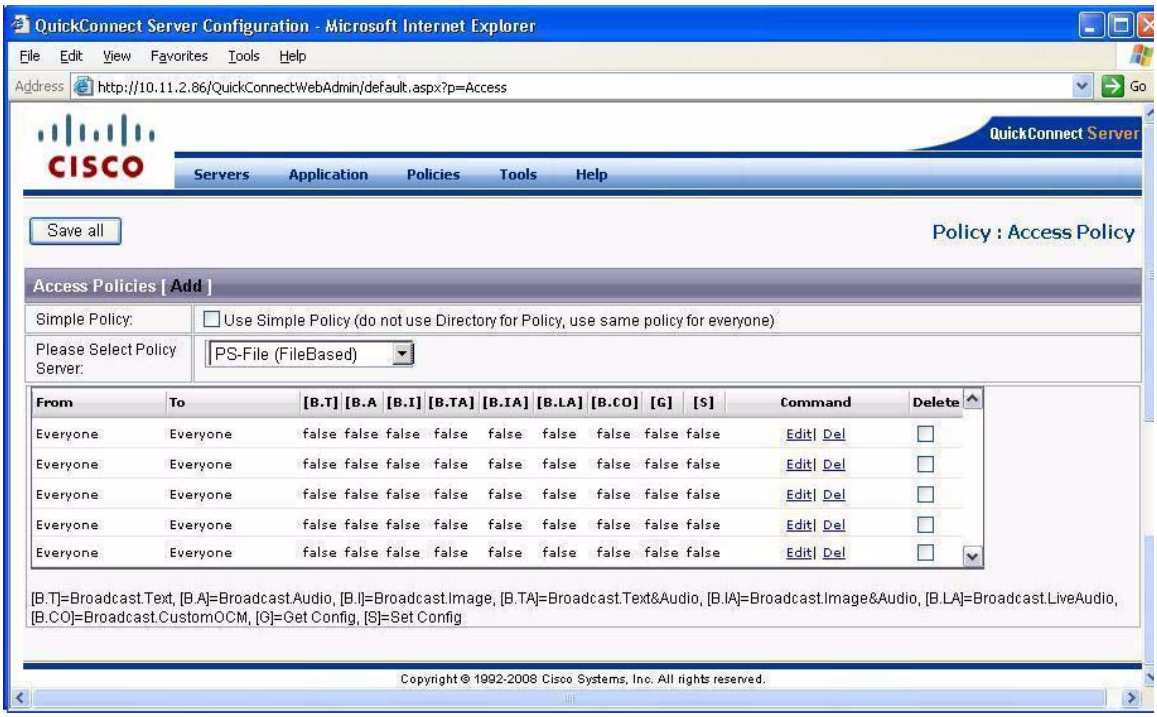
Step 1 Select **Access Policy** from the Policies menu. This takes you to the main Policy: Access Policy screen (Figure 5-30), which displays simple policy parameters if you have not yet configured any policies.

Figure 5-30 Policy:Access Policy Screen



Step 2 Uncheck the **Use Simple Policy** checkbox to display a list of all the complex policies that have been configured to date (if any), as shown in Figure 5-31.

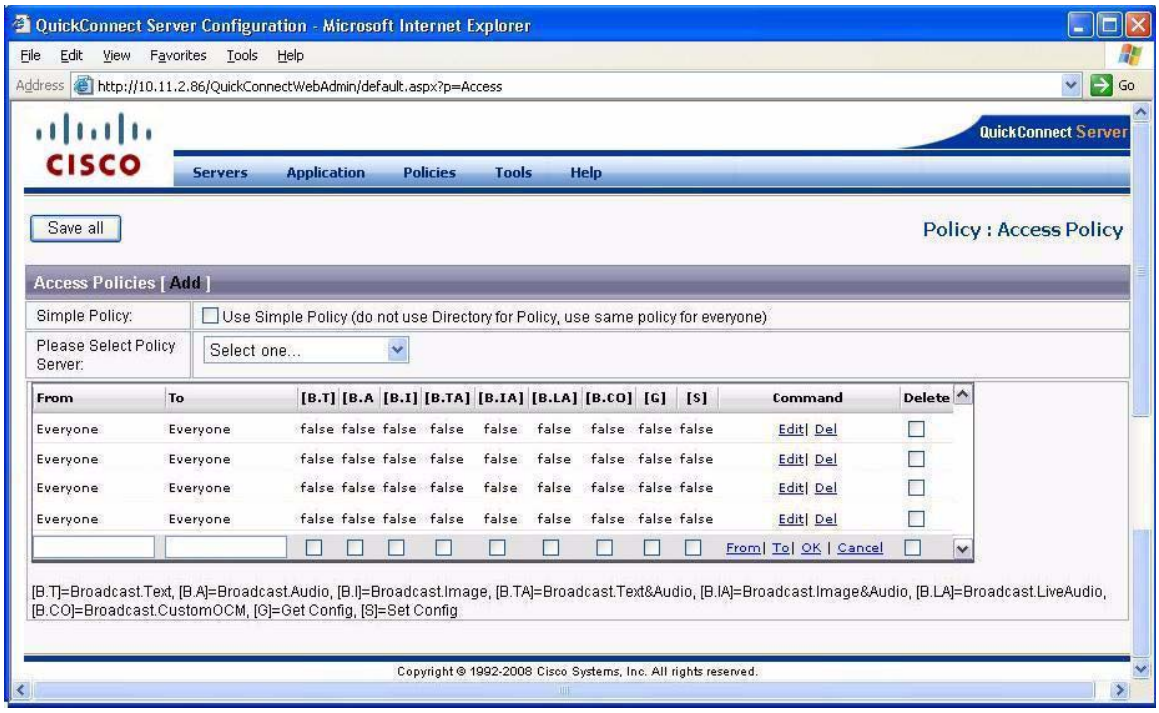
Figure 5-31 Complex Policies



Step 3 On the Policy: Access Policy screen, click the **Add** link to display blank fields to populate (Figure 5-32).

Note Unified Quick Connect evaluates access policies from top to bottom in the table for every call. The first 'matching' policy that includes the sender/recipient is processed. In the screenshot below, no one can do anything because the top (first) policy in the list has every function marked as false (i.e., inactive).

Figure 5-32 Selecting Add to Populate the Policy



Step 4 In the From field, type the name or number to which you are providing the access by function.

Note The entry in the From field should match the attribute assigned to the LSDisplayName on the Application>Directory Mapping screen. You can use “Everyone” (with a capital ‘E’) or “everyone” (with a lower-case ‘e’) interchangeably.

Clicking the **From** link allows you to search for defined Groups.

Step 5 In the To field, type the name or number the From user can contact using the functions s/he is given access to.

Note The entry in the To field should match the attribute assigned to the LSDisplayName on the Application>Directory Mapping screen. Clicking the **To** link will open a popup window in which you can search for defined groups.

Step 6 Change the function access fields (Table 5-6) to true to provide access or false to restrict access to each function. A checkmark in the field makes the function “true” (access granted).

Table 5-6 Function Access Fields

Function Name	Description
B.T=Broadcast Text	Allows users to create text broadcast messages.
B.A=Broadcast Audio	Allows users to create audio broadcast messages.
B.I=Broadcast Image	Allows users to create image broadcast messages.
B.TA=Broadcast Text and Audio	Allows users to create text and audio broadcast messages.

Table 5-6 Function Access Fields

Function Name	Description
B.IA=Broadcast Image and Audio	Allows users to create image and audio broadcast messages.
B.LA=Broadcast Live Audio	Allows users to create live audio broadcast messages.
B.CO=Broadcast Custom OCM	Allows users to create broadcasts of custom broadcast templates.

Step 7 Click **OK** to return to the previous screen.

Step 8 Click **Save** to save and implement your changes.

Editing Complex Policies

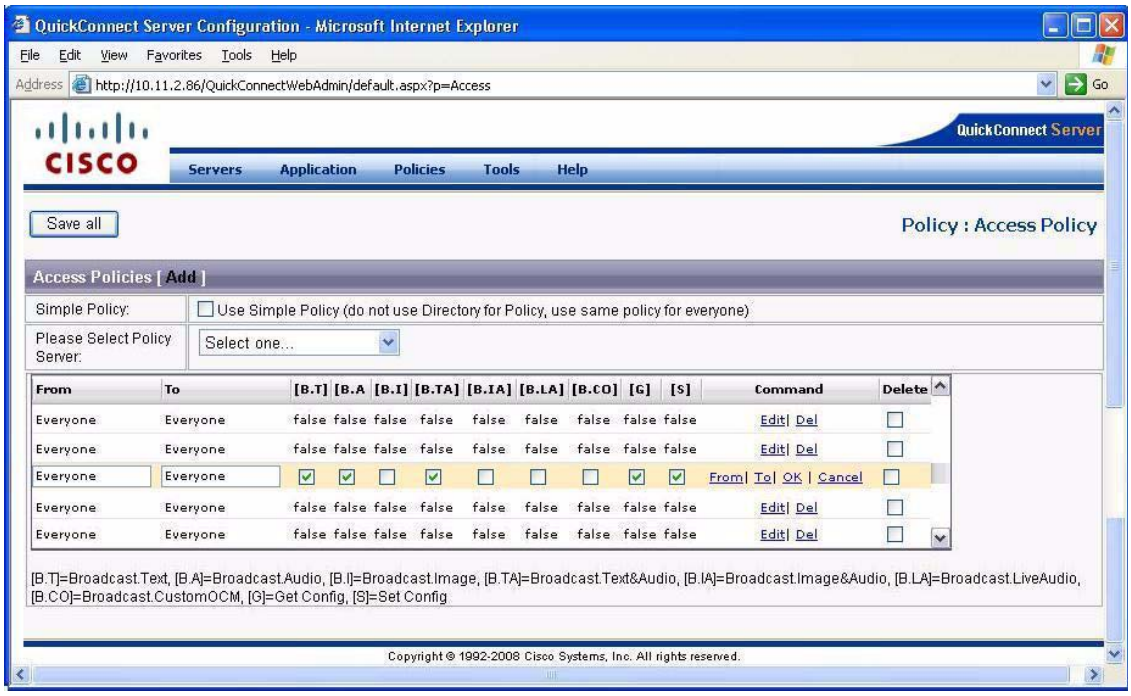
To edit a complex policy:

Procedure

Step 1 Select **Access Policy** from the Policies menu. This takes you to the main Policy: Access Policy screen, which displays a list of all the complex policies that have been configured to date.

Step 2 To edit a policy, click the **Edit** link for the policy you want to edit. This makes the policy's fields editable (Figure 5-33).

Figure 5-33 Editing a Complex Policy



Step 3 Change the following fields as needed:

The entry in the From or To fields should match the attribute assigned to the LSDisplayName on the Application>Directory Mapping screen.

Change the function access fields to true to provide access or false to restrict access to each function. A checkmark in the field makes the function “true” (access granted).

Step 4 Click **OK** to return to the display view.

To delete a policy, click the **Del** link for the policy you want to delete. A confirmation window appears. Click **OK** to perform the deletion. The policy will no longer appear on this screen.

Step 5 Click **Save** to save your changes.

Centralized Configuration Service

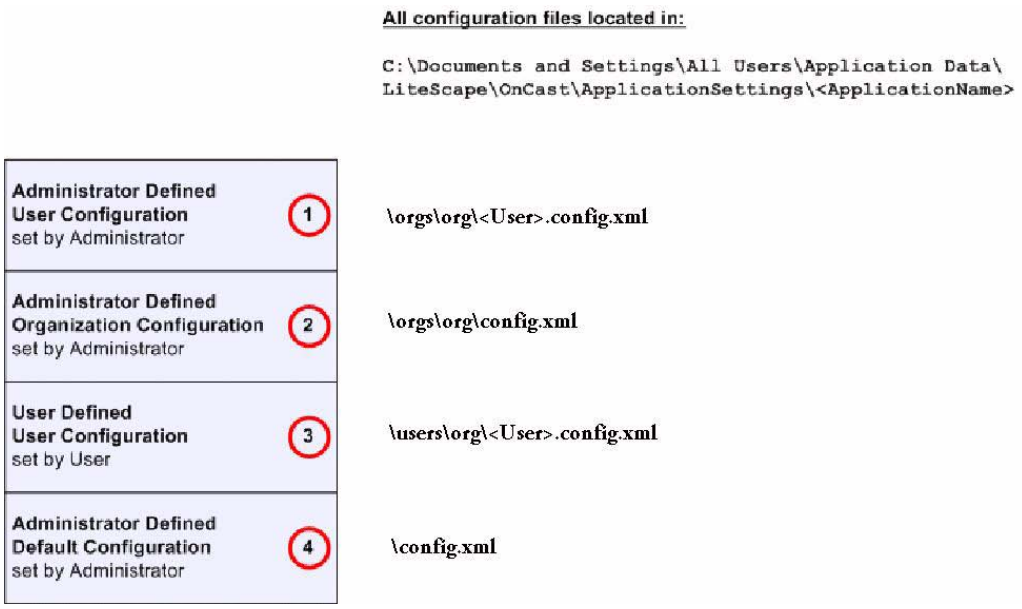
The Centralized Configuration Service allows administrators to control which features and capabilities are exposed to end-users and groups. Upon login, a Unified Quick Connect application will query the Centralized Configuration Service, which will in turn collect all the relevant configuration files for that user and his/her groups and return which features the user has permissions to access with this Unified Quick Connect application.

There are four levels of configuration parameters that Centralized Configuration Service checks, in order of increasing priority:

- Administrator Defined Default Configuration – this is the default configuration for all users who access this application. This is the baseline amount of functionality exposed to all users.
- Administrator Defined Organization Configuration – the administrator can define settings for a group of users. Conflicting settings here supersede what is available in the configuration files above.
- User Defined User Configuration – this determines which settings the end-user can modify themselves. Conflicting settings here supersede what is available in the configuration file above.
- Administrator Defined User Configuration – the administrator can define settings for a specific user. Conflicting settings here supersede what is available in the configuration files above.

The architecture of the centralized installation is shown in Figure 5-34:

Figure 5-34 Unified Quick Connect Centralized Configuration



Modifying Centralized Configuration from WebAdmin

You may of course change configuration settings directly in each XML file. The preferred method, however, is to access and modify user and group settings from Unified Quick Connect WebAdmin. You can do this by going to **Servers** > **Advanced Settings** and selecting which service settings to set user and group configuration settings for.

Note Refer to Appendix C, "Cisco Unified Quick Connect Advanced Settings", for information on the advanced settings that you can configure.

To modify the configuration for each, first select which service settings you would like to customize in the Section: drop-down. Next select if you want to modify this interface at the Default level (item 4 in the diagram above), Organization level (item 2 in the diagram above) or User level (item 1 in the diagram above).

You will see a list of possible fields that can be modified. The Description column describes the setting you can modify, the Parameter column displays the XML tag and CurrentValue displays what this setting is currently configured for. This table will vary dependent on which Section you are configuring (for example, Unified Quick Connect Phone UI).

Modifying Centralized Configuration XML Files

The typical, and recommended, way to make changes to Unified Quick Connect parameters is through Unified Quick Connect WebAdmin. However, there also exists the facility to make changes to Centralized Configuration using the various XML configuration files listed in the diagram above. This method may be useful when making a large number of changes.

Access to Centralized Configuration

Unified Quick Connect centralized configuration service also integrates with Policy Service to determine which applications can set and read configuration for users or groups. You can configure this by going to **Unified Quick Connect WebAdmin** > **Policies** > **Access Policies**. You will see two options: [G] Get Config and [S] Set Config that can be set using the same methodology Unified Quick Connect Policy Service supports.

Verifying the Installation Using Phones

Perform the following steps to verify the installation with supported phones:

Procedure

Step 1 On the phone, select the Directories URL. Verify that Global directories are displayed.

Step 2 Search for a particular user, and verify that the user's presence information is appearing correctly.

(You can perform this test by changing the status of that user by having them start and end a call). If not, restart *OncastDeviceStatusService* to be able to see the correct information on device presence.

Step 3 Select the **PTT** softkey and select **PTT** to start the PTT session.

Step 4 Stop the PTT session by pressing **Exit**. Verify that the PTT priority is working as expected.

CHAPTER 6

Customizing Cisco Unified Quick Connect

The administrator can create Cisco Unified Quick Connect customizations that are described in the following sections:

- Customizing the Template for Push-to-Talk, page 6-1
- Customizing the Push-to-Talk OCM File, page 6-1
  - Customizing Presence-related Parameters, page 6-2
- Customizing Media-related Parameters, page 6-2
- Customizing Pre-configured Push-to-Talk Parameters, page 6-3
- Using the Web Service API Programmatically, page 6-5

Note Refer to Chapter 5, "Configuring Cisco Unified Quick Connect Server" for information on customizing the Directory Search criteria, Directory Search results, and softkey layout.

Customizing the Template for Push-to-Talk

You can customize the template (OCM file) to use for the Push-to-talk product.

By default, the users will use the pre-configured 'WalkieTalkiePush.ocm' template. The template can be selected in Unified Quick Connect WebAdmin at the following URL:

http://Unified Quick ConnectServerAddress/Unified Quick ConnectWebAdmin/?p=Templates

Customizing the Push-to-Talk OCM File

The Push-to-Talk OCM file can be configured to control the following characteristics of the broadcast:

- Ring tone (audible) to be used to indicate the start and stop of the audio session. The file names reference any ring tone file available on the Cisco Unified Call Manager system.

The ring-tone is determined using the <Header><EmergencyRingTone> parameter in the OCM payload document (.pay file). See PTT OCM Customization steps for more details.

- The text appearing on the screen of the phones
- Whether 'Exit' closes the application for ALL users or just the user who pushed the button

To customize the Push-toTalk OCM file, administrators can edit the contents of the following files:

- WalkieTalkiePush.pay file (included in the BroadcastTemplates\WalkieTalkiePush.OCM file):

```
<Header>
    <Type>AUDIO</Type>
    <Priority>NORMAL</Priority>
    <Sender> </Sender>
    <ExitKey>False</ExitKey>
    <UseMainDN>True</UseMainDN>
    <UsePresence>True</UsePresence>
    <PresenceUnknownPushOkay>true</PresenceUnknownPushOkay>
    <SendInvitation>False</SendInvitation>
    <ExitKeyPosition>3</ExitKeyPosition>
    <Recipients />
  </Header>
  <Message>
    <Prompt>Powered by Unified Quick Connect</Prompt>
    <Subject>Audio Push-To-Talk</Subject>
    <Body>Press "Push" button and release to start speaking when the audible sound is
heard. Push again to STOP. "Talk-back" creates a one-to-one session with the
originator. "Call Me" calls the originator</Body>
  </Message>
```

- WalkieTalkie.pay file (included in the BroadcastTemplates\WalkieTalkie.OCM file):

```
<EmergencyRingTone>Chime.raw</EmergencyRingTone>
```

Customizing Presence-related Parameters

If the <UsePresence> parameter in the WalkieTalkie.pay payload document is set to true, a phone call will not barge into users who are on the phone (they will not hear any audio from their phones)

If the <PresenceUnknownPushOkay> is set to true, the PTT application will allow a phone call to barge-in to devices for which it cannot determine the presence status.

Customizing Media-related Parameters

The PTT application uses the RTP streaming capabilities of the Cisco IP phone to transmit and receive the voice content of the users to each other. Cisco Unified Application Environment provides a Media server. To provide such functionality, the PTT application can either instruct the transmitting device to send RTP streams to a Multi-cast address or to a specific UniCast address/port.

This information is part of the template parameters:

```
<Audio>
  <Type>BROADCAST</Type>
  <Streaming>MULTICAST</Streaming> //Could be changed to Unicast
</Audio>
```

By default, when Multicast is selected, the PTT application sends ‘control’ commands to the IP phones. In this case, the Unified Quick Connect Media server is not part of the audio transmission process..

In certain environments, this is not a desired outcome. For example, if the devices are not within the same LAN, Multicast transmission may be blocked through the WAN (by the routers).

To change this behavior for the PTT application, Unified Quick Connect can be configured to act as a media proxy between the devices. To enable this, the following parameter needs to be set in OnCastConfiguration.xml:

```
<Broadcaster> <UseMediaForLiveMultiCast>true</UseMediaForLiveMultiCast>
```

In this case, a Unicast RTP stream from the originating IP device is first sent to the Unified Quick Connect Media server (provided by Cisco Unified Application Environment), then the media server uses the <Streaming> parameter mentioned above to determine how to route the traffic to various devices.

For devices which are within the same 'location' as the media server, a Multicast broadcast is relayed as follows:

Device_1 > Unicast > Unified Quick Connect Media server > Multicast > Other devices

For devices which are not within the same 'location' as the media server, the server can either Unicast the content to each of the devices:

Unified Quick Connect Media server > Unicast > Other devices

Or, the server can use a Unified Quick Connect Media server at the other 'location'. Once the Second server receives the audio transmission from the first media server, it will then be able to transmit the audio using Multicast to the devices:

Media server at location 1 > Unicast > Media server at location 2 > Multicast > Devices at location 2

Unified Quick Connect at location 1

Media server 1 (CUAE)
PBX 1
Devices with alias location 1

Unified Quick Connect at location 2

Media server 2 (CUAE)
PBX 2
Devices with alias of location 2

The message flow is as follows:

1. The Unified Quick Connect Server receives a request from a user to start a Push-to-Talk session with users spread over two locations..
2. The Unified Quick Connect Server at location 1 instructs phone at location 1 (organizer) to transmit to media server 1.
3. The Unified Quick Connect Server at location 1 instructs media server 1 to send audio to media server 2.
4. The Unified Quick Connect Server at location 1 instructs media server 2 to listen to audio from media server 1.
5. The Unified Quick Connect Server instructs devices at location 2 to listen for a multicast at location 2.
6. The Unified Quick Connect Server instructs devices at location 1 to listen to a different multicast at location 1.

Customizing Pre-configured Push-to-Talk Parameters

A pre-built shortcut allows a user to have a service URL setup on their phone pointing to invoke a PTT session with a pre-defined group. The following section of OnCast.Configuration.xml manages the configuration of the pre-built Push-to-Talk shortcuts:

```
<BroadCaster>
    <WalkieTalkie>
//Determines if a user pressing "Exit" will end the PTT application for ALL users.
```

```
    <ExitALL>false</ExitALL>
      <Items>
        <Item>
          <Name>ptt-grp2</Name>
          <Params></Params>
          <XmlPayload>
            <LSBC>
              <Organizer>
                <UserID />
                <IPAddress>
                </IPAddress>
                <Extension>20444</Extension>
                <MainPhone />
                <LDAPDN />
                <ServerLDAPID />
                <ProviderID>
                </ProviderID>
                <ProviderSource>
                </ProviderSource>
                <OnCastBCLocationName>Default Location</OnCastBCLocationName>
                <Prefix />
              </Organizer>
              <Invitees>
              </Invitees>
              <OCMFile>BroadcastTemplates\WalkieTalkiePush.ocm</OCMFile>
              <Conference>
                <PhoneNumber>918665068850</PhoneNumber>
                <PassCode>943037</PassCode>
              </Conference>
              <Action>OCM</Action>
              <shortcutURL />
              <Priority>Emergency</Priority>
              <InviteesGroup>PTTG1</InviteesGroup>
              <UpdateOCM>
                <updatePay>

<paramtag>OnCastMessage/Workflow/Key/Key[Caption='PushToTalk']/Actions/Action[ID='PushToTa
lk']/Settings/pluginValue/URI</paramtag>
                  <paramvalue>?id=ptt-grp1</paramvalue>
                </updatePay>
              </UpdateOCM>
            </LSBC>
          </XmlPayload>
        </Item>
        <Item>
          <Name>ptt-grp1</Name>
          <Params>grp=PTTG1|ocm=BroadcastTemplates\WalkieTalkie.ocm|pr=Emergency</Params>
          <XmlPayload></XmlPayload>
          </Item>
          <!--4.3.5 MR12 4.4 MR6: addition of default PTT group -->
          <!--group name will be added dynamically -->
      <Item>
        <Name>ptt-def</Name>
        <Params>|ocm=BroadcastTemplates\WalkieTalkie.ocm|pr=Emergency</Params>
        <XmlPayload>
        </XmlPayload>
      </Item>
      <Item>
        <Name>ptt-defe</Name>

<Params>|ocm=BroadcastTemplates\ClearScreen.ocm|pr=Emergency|pttgrp=ptt-def</Params>
        <XmlPayload>
        </XmlPayload>
      </Item>
```

```
    </Items>
    <DummyResponse>
      <CiscoIPPhoneExecute>
        <ExecuteItem URL="Hello World" />
      </CiscoIPPhoneExecute>
    </DummyResponse>
  </WalkieTalkie>
```

Using the Web Service API Programmatically

Other third-party applications can leverage the Web Service interface to invoke and initiate the Push-to-Talk application.

For example, the following message shows the xml message used in invoking the InitializeBCPayload interface of the WAN Broadcast Web service (from OnCast Web Service).

In this example, the user with userid = ‘pttuser1’ will receive the “Push to Talk start” screen on their IP phone (extension 20444).

When this user presses the PTT button, all the recipients identified in the <Invitees> section of the message will see the same “Push to Talk start” screen on their phones as well and can start using the Unified Quick Connect PTT product.

```
<LSBC>
  <Organizer>
    <UserID>pttuser1</UserID>
    <Key>20444</Key>
    <Extension>20444</Extension>
    <MainPhone>20444</MainPhone>
    <IPAddress>10.11.2.38</IPAddress>
    <LDAPDN>AD|CN=PTT User1,OU=Test Accounts, DC=example, DC=local</LDAPDN>
    <ProviderID>IP-PBX 1</ProviderID>
  </Organizer>
  <InviteesGroup />
  <Invitees>
    <Invitee>
      <UserID>PTT User4</UserID>
      <Key>20447</Key>
      <Extension>20447</Extension>
      <MainPhone>20447</MainPhone>
      <LDAPDN>AD|CN=PTT User4,OU=Test Accounts,DC=example,DC=local</LDAPDN>
      <ProviderID />
    </Invitee>
  </Invitees>
  <Action>OCM</Action>
  <Priority>Emergency</Priority>
  <OCMFile>c:\Documents and Settings\All Users\Application
Data\LiteScape\OnCast\BroadcastTemplates\WalkieTalkiePush.ocm</OCMFile>
  <Conference>
    <PhoneNumber />
  </Conference>
<shortcutURL>http://10.11.2.72/DirDialer/Options/createShortcut.aspx?key=20444&amp;session
id=894b332e-391e-4226-90b3-34de0c82d5c6</shortcutURL>
</LSBC>
```

Format of the InitializeBCPayload Parameters

XMLData: the format of XMLData must adhere to the BCPayload.LoadXML.xsd schema.

```
<xs:element name="LSBC">
  <xs:annotation>
    <xs:documentation>Comment describing your root element</xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:sequence>
      <xs:element name="OCMFile" type="xs:string">
        <xs:annotation>
          <xs:documentation>BCPayload.LoadXML + processOCM</xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element name="SetFileName" type="xs:string">
        <xs:annotation>
          <xs:documentation>BCPayload.LoadXML</xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element name="FilmSessionID" type="xs:string">
        <xs:annotation>
          <xs:documentation>BCPayload.LoadXML</xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element name="URLOCMFile" type="xs:string">
        <xs:annotation>
          <xs:documentation>BCPayload.processOCM</xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element name="SessionID" type="xs:string">
        <xs:annotation>
          <xs:documentation>BCPayload.processOCM</xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element name="CreateOCM">
        <xs:annotation>
          <xs:documentation>BCPayload.createOCM</xs:documentation>
        </xs:annotation>
        <xs:complexType>
          <xs:sequence>
            <xs:element name="OnCastMessage" type="xs:string">
              <xs:annotation>
                <xs:documentation>BCPlayoad.createOCM + these methods only look at the
node but not inner text</xs:documentation>
              </xs:annotation>
            </xs:element>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="AttachFileOCM">
        <xs:annotation>
          <xs:documentation>BCPayload.createOCM</xs:documentation>
        </xs:annotation>
        <xs:complexType>
          <xs:sequence>
            <xs:element name="Files" maxOccurs="unbounded">
              <xs:annotation>
                <xs:documentation>BCPayload.createOCM</xs:documentation>
              </xs:annotation>
              <xs:complexType>
                <xs:sequence>
                  <xs:element name="Url" type="xs:string">
```

```
                    <xs:annotation>
                      <xs:documentation>BCPayload.createOCM</xs:documentation>
                    </xs:annotation>
                  </xs:element>
                  <xs:element name="FileName" type="xs:string">
                    <xs:annotation>
                      <xs:documentation>BCPayload.createOCM</xs:documentation>
                    </xs:annotation>
                  </xs:element>
                </xs:sequence>
              </xs:complexType>
            </xs:element>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="UpdateOCM">
        <xs:annotation>
          <xs:documentation>BCPayload.processOCM</xs:documentation>
        </xs:annotation>
        <xs:complexType>
          <xs:sequence>
            <xs:element name="updatePay" minOccurs="0" maxOccurs="unbounded">
              <xs:annotation>
                <xs:documentation>BCPayload.processChangePayload +
BCPayload.processUpdatePayload</xs:documentation>
              </xs:annotation>
              <xs:complexType>
                <xs:sequence>
                  <xs:element name="paramtag" type="xs:string" minOccurs="0">
                    <xs:annotation>
                      <xs:documentation>BCPayload.processUpdatePayload + Code use this
value to find a child node of UpdateOCM</xs:documentation>
                    </xs:annotation>
                  </xs:element>
                  <xs:element name="formatvalue" type="xs:string" minOccurs="0"
maxOccurs="unbounded">
                    <xs:annotation>
                      <xs:documentation>BCPayload.processUpdatePayload</xs:documentation>
                    </xs:annotation>
                  </xs:element>
                  <xs:element name="paramvalue" type="xs:string" minOccurs="0"
maxOccurs="unbounded">
                    <xs:annotation>
                      <xs:documentation>BCPayload.processUpdatePayload</xs:documentation>
                    </xs:annotation>
                  </xs:element>
                </xs:sequence>
              </xs:complexType>
            </xs:element>
            <xs:element name="addPay" minOccurs="0" maxOccurs="unbounded">
              <xs:annotation>
                <xs:documentation>BCPayload.processChangePayload +
BCPayload.procesAddPayload</xs:documentation>
              </xs:annotation>
              <xs:complexType>
                <xs:sequence>
                  <xs:element name="paramtag" type="xs:string">
                    <xs:annotation>
                      <xs:documentation>BCPayload.procesAddPayload</xs:documentation>
                    </xs:annotation>
                  </xs:element>
                  <xs:element name="paramvalue" type="xs:string">
                    <xs:annotation>
                      <xs:documentation>BCPayload.procesAddPayload</xs:documentation>
```

```
                    </xs:annotation>
                  </xs:element>
                </xs:sequence>
              </xs:complexType>
            </xs:element>
            <xs:element name="deletePay" type="xs:string" minOccurs="0"
maxOccurs="unbounded">
              <xs:annotation>
                <xs:documentation>BCPayload.processChangePayload</xs:documentation>
              </xs:annotation>
            </xs:element>
            <xs:element name="AttachFileOCM" minOccurs="0" maxOccurs="unbounded">
              <xs:annotation>
                <xs:documentation>BCPayload.processChangePayload</xs:documentation>
              </xs:annotation>
              <xs:complexType>
                <xs:sequence>
                  <xs:element name="Files" maxOccurs="unbounded">
                    <xs:complexType>
                      <xs:sequence>
                        <xs:element name="Url" type="xs:string"/>
                        <xs:element name="FileType" type="xs:string"/>
                        <xs:element name="FileName" type="xs:string"/>
                      </xs:sequence>
                    </xs:complexType>
                  </xs:element>
                </xs:sequence>
              </xs:complexType>
            </xs:element>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
```

Organizer section

The Organizer section provides information about the sender of the broadcast (From). The section is Required.

- UserID: User ID as represented in the relative directory server. The tag is Required.
- Extension: The phone extension of the organizer (sender). The tag is Required.
- IPAddress: IP address of the device of the sender. If omitted, OnCast will select the default device automatically. Optional parameter.
- LDAPDN: LDAP Distinguished Name of the Organizer. Optional parameter.
- Provider ID: Associated IP-PBX for the organizer's device. This parameter is used to resolve conflicts when duplicate user accounts are found across multi-PBX environments. Optional parameter.

Invitees Group section

The Invitees Group section is used to identify distribution groups from the underlying directory servers. Optional parameter.

Invitees section: The Invitees section provides the list of recipients (To) of the broadcast. The section is required.

- Invitee: one section is required per individual Invitee. Provides information about the recipients (To) of the broadcast. At least one recipient is required.
- User ID: User ID as represented in the relative directory server. The tag is Optional.
- Extension: The phone extension of the recipient (To). The tag is Required.
- LDAPDN: LDAP Distinguished Name of the Recipient. Optional parameter.
- Provider ID: Associated IP-PBX for the recipient's device. This parameter is used to resolve conflicts when duplicate user accounts are found across multi-PBX environments. Optional parameter.
- Action: The action to be taken by the broadcast service. Supported actions are: OCM, Dial. Parameter is Required.
- Priority: Delivery priority. Supported: Normal, Emergency. Normal broadcasts require recipients to accept the broadcast before receiving it (screened). Emergency broadcasts barge-in. Parameter is Required.
- OCMFile: The path to the broadcast OCM template file. This can be either a relative path (a path relative to the OnCast folder on the deployment server) or a full path.
- shortcutURL: If the organizer presses the Shortcut soft-key, the broadcast will be saved as a user-level shortcut for future usage. Optional parameter.
- Override OCM: This is the override of the OCM File. Any and all parameters in the document will replace the OCM predefined settings. The entire section is Optional.
- AttachFile: The override of the OCM image file. The reference to the Old File and new file can either be file UNC paths or URL references to the location of the New File. The entire section is Optional.
- CreateOCM: This section is for on-the-fly (ad-hoc) creation of new OCM files. The format of the section follows the OnCast Payload format, published and documented separately. Section is Optional.

CHAPTER 7

Cisco Unified Quick Connect Tools

This chapter discusses the tools available to manage Cisco Unified Quick Connect, and contains the following sections:

- What Tools are Available?, page 7-1
- Synchronizing Unified Quick Connect Servers, page 7-2
- Services, page 7-3
- Provisioning, page 7-5
- Working with Reports, page 7-9
- Log Files, page 7-10
- Licenses, page 7-13

What Tools are Available?

The Tools menu (Figure 7-1) allows you to access five different system maintenance features:

Figure 7-1 Tools Menu

Table 7-1 describes the Tools menu items:

Table 7-1 Tools Menu Items

Tool Menu Item	Description
Synchronize	On-demand synchronization of clustered Unified Quick Connect servers.
Services	Restarts the Windows Services used by Unified Quick Connect.
Provisioning	Assign licenses to users.
Reports	View the number of providers.
Log Settings	Set activity recording levels for Unified Quick Connect System logs and export log files.
Licenses	Displays information on the current Unified Quick Connect license, and allows you to upload a new license.

Synchronizing Unified Quick Connect Servers

Unified Quick Connect Servers participating in a distributed cluster (at one location or at multiple locations) can share configuration information.

This enables each node to be independently managed in the case of server/network failures. In addition, this enables intelligent selection of local vs. remote access to data files and configuration documents. Data files that change infrequently are published to each server node, enabling local access to such information. Frequently changing and accessed data files can be retrieved from the central configuration server, while cached copies of such data files are made available for local usage in the event of network/configuration server failures.

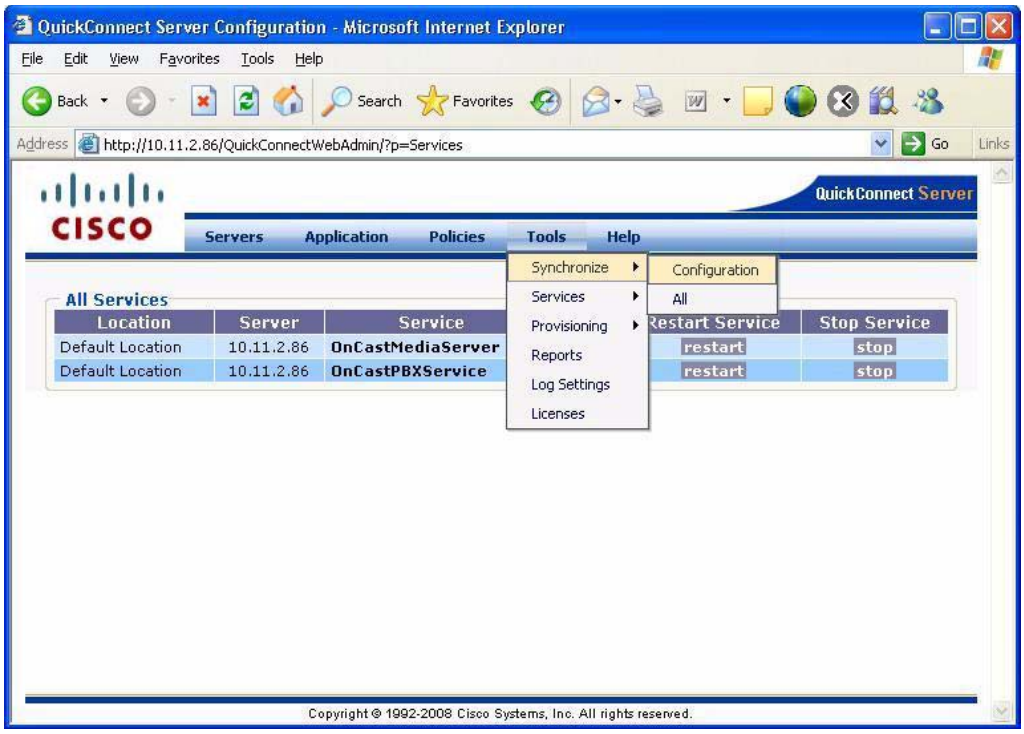
The synchronization service ensures that all Unified Quick Connect Servers have access to up-to-date configuration information. Synchronization occurs on an automatic basis; however, the service can also be invoked manually.

Manually Invoking Synchronization

To invoke synchronization manually, select **Tools** > **Synchronize**. (Figure 7-2).

You can either synchronize all configuration and data files (by selecting **All**) or just the configuration documents (by selecting **Configuration**).

Figure 7-2 Synchronization Menu Items



Once synchronization is invoked, a Synchronization Result text box displays the results.

Services

You can use Unified Quick Connect Web Admin to view the status of services, or to restart local services or all services.

Viewing Status of Services

To view the status of services:

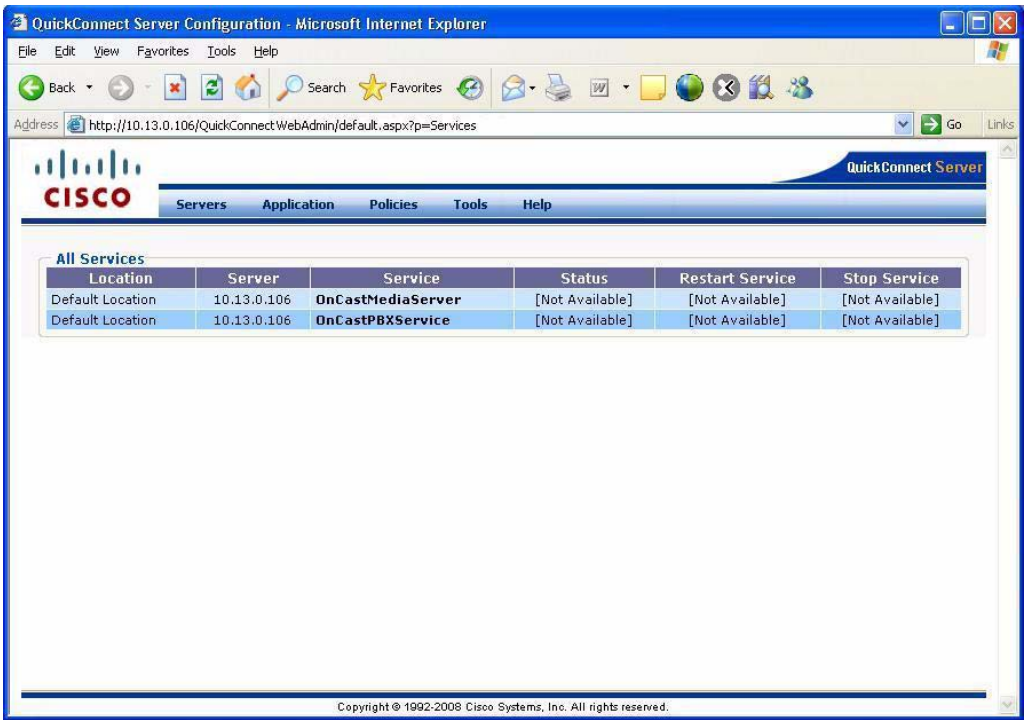
Procedure

Step 1 Choose **Tools** > **Services** > **Status**.

The following information will be displayed for each service (Figure 7-3):

- Location: the Location where the service is running.
- Server: the IP address of the Unified Quick Connect server.
- Service: the name of the service.
- Status: the status of the service (Running, Stopped).
- Restart Service: selecting this button restarts the associated service.
- Stop Service: selecting this button stops the associated service.

Figure 7-3 Viewing Status of Services



Restarting Services

To restart local services:

Procedure

Step 1 Choose **Tools** > **Services** > **Restart** > **Local Services** (Figure 7-4).

You will see the message “Windows services on local service restarted.”

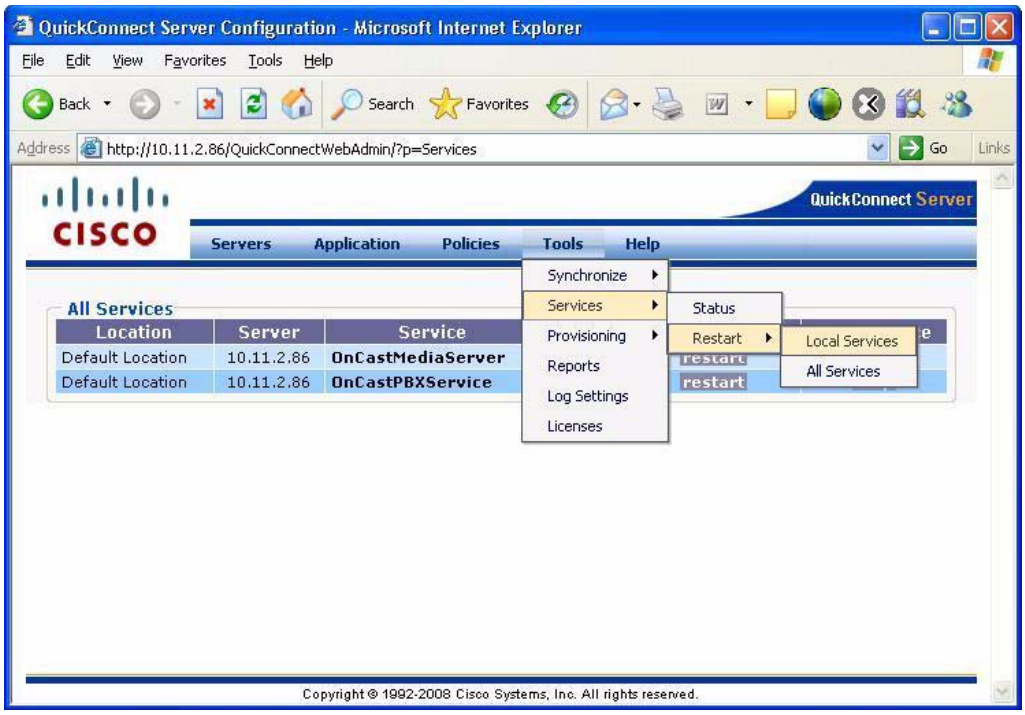
To restart all services:

Procedure

Step 1 Choose **Tools** > **Services** > **Restart** > **All Services**.

You will see the message “Windows services on all machines restarted.”

Figure 7-4 Restarting Services



Provisioning

Provisioning is the act of manually adding Users into Unified Quick Connect directly rather than relying on directory servers to forward their information. You can also search for a particular user.

Adding a User

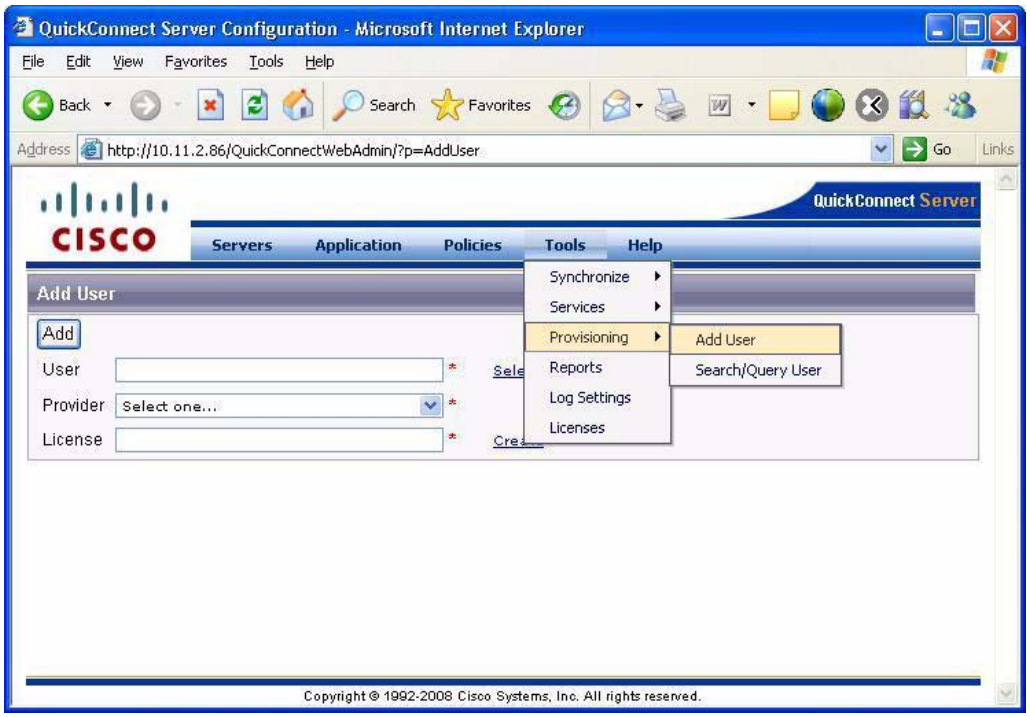
When you add a user, you are assigning them a Unified Quick Connect license for the server you associate them with.

To add a User:

Procedure

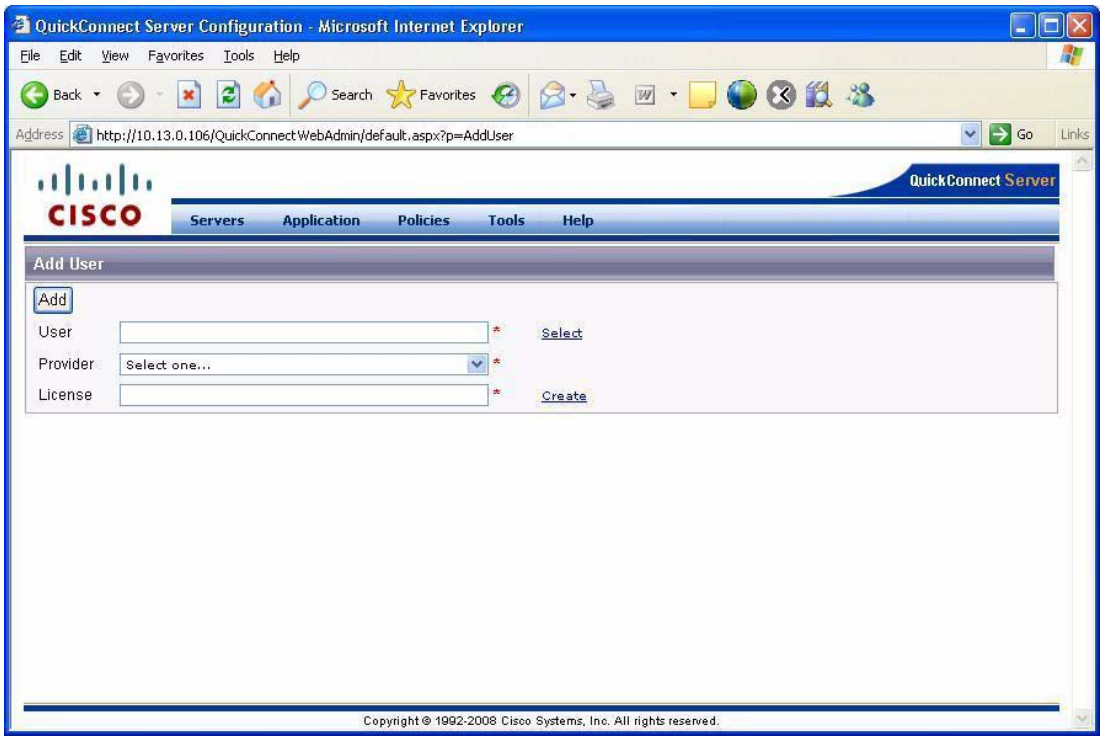
Step 1 Choose **Tools** > **Provisioning** > **Add User** (Figure 7-5).

Figure 7-5 Adding a User (1 of 2)



Step 2 Enter the username (or search for it using the Select dialog) (Figure 7-6).

Figure 7-6 Adding a User (2 of 2)



Step 3 Select the Provider you wish to associate them with.

Step 4 Click **Create** to generate their license.

Step 5 Click **Add** to enter the user and license in the database.

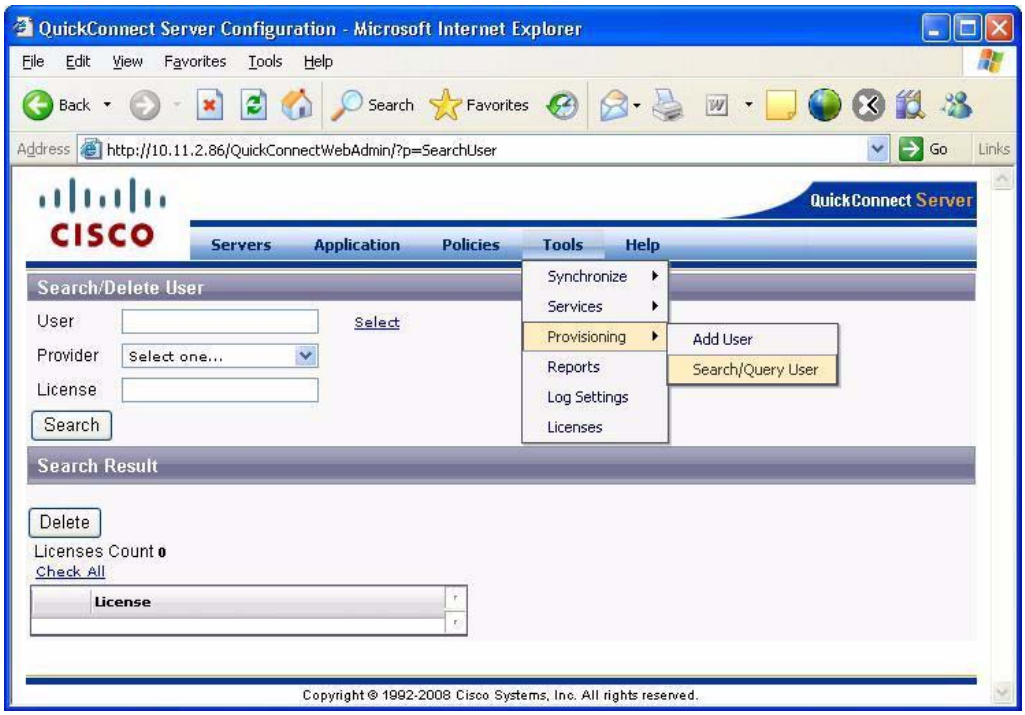
Searching and Querying for Users

To search for a user:

Procedure

Step 1 Choose **Tools** > **Provisioning** > **Search/Query User** (Figure 7-7).

Figure 7-7 Searching and Querying for Users



Step 2 Enter the username (or search for it using the Select dialog as shown in Figure 7-8 and Figure 7-9).

Figure 7-8 Entering Search Information

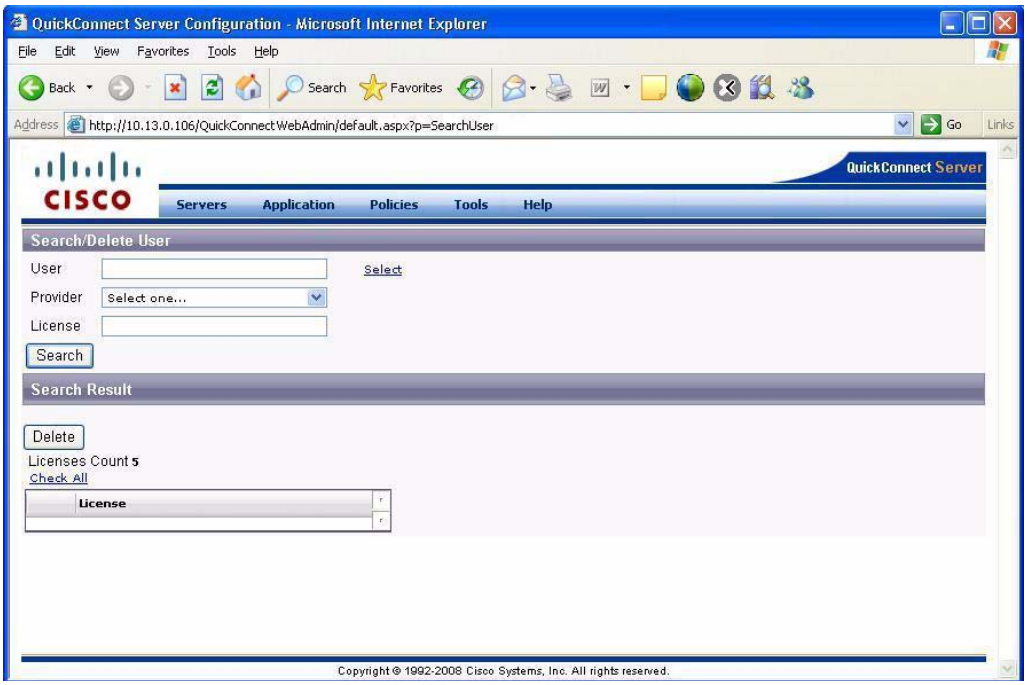
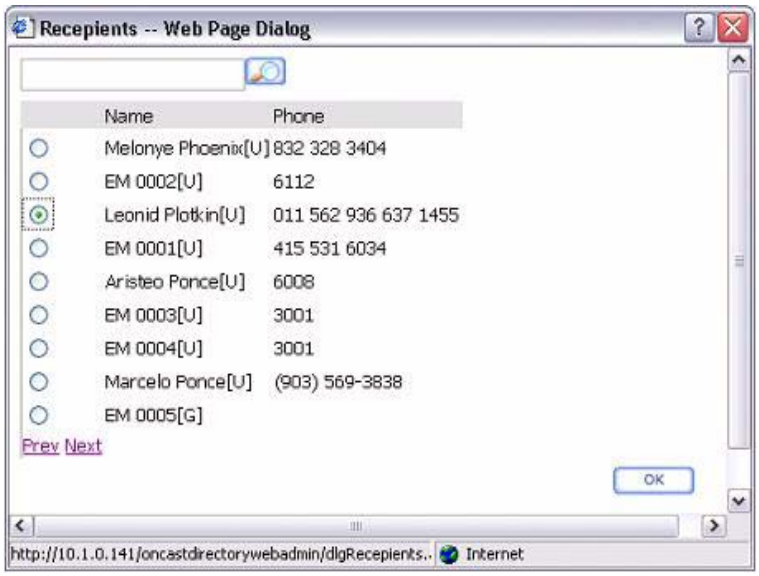


Figure 7-9 Selecting a User Name



Step 3 Select a Provider, then click **Search**. The user's license number will be displayed.

Working with Reports

The Reports menu item (Figure 7-10) generates a report showing the number of Providers configured in the Unified Quick Connect system (Figure 7-11).

Figure 7-10 Reports Menu Item

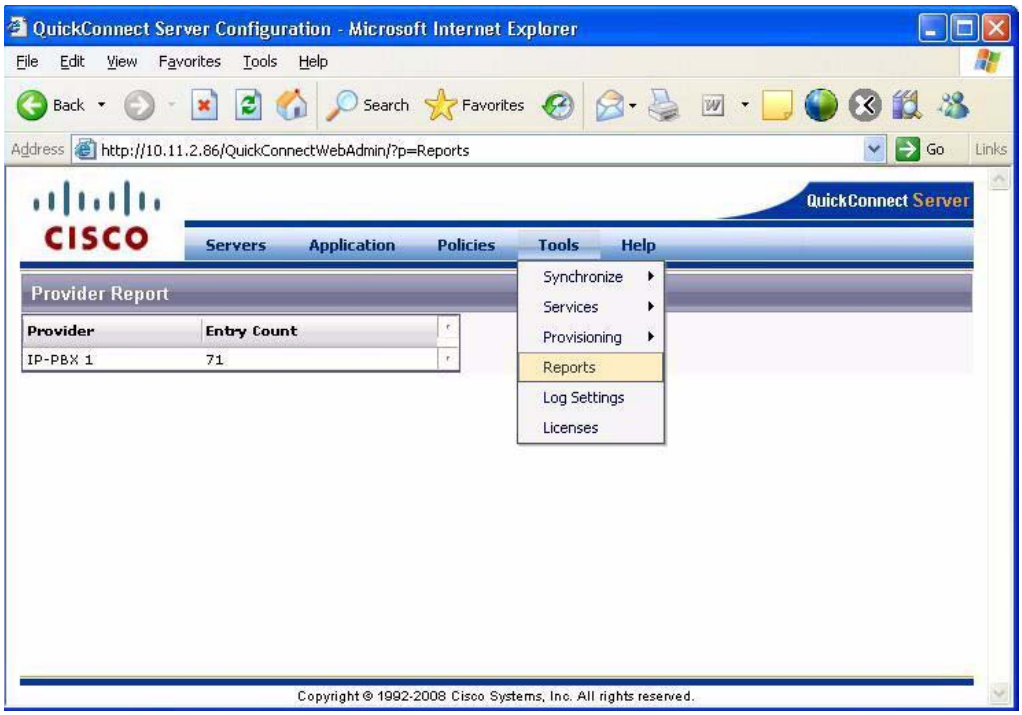


Figure 7-11 Report on Number of Providers Configured in Unified Quick Connect

Log Files

Setting Log Levels

Each and every Unified Quick Connect service component creates log files. The log level can be changed to determine the level of information detail in the log files. In general, logging should be set at the level which provides the least amount of information in order to maintain system throughput at acceptable levels.

You can find the log files in the following location:

C:\Documents and Settings\All Users\Application Data\LiteScape\OnCast\Logs

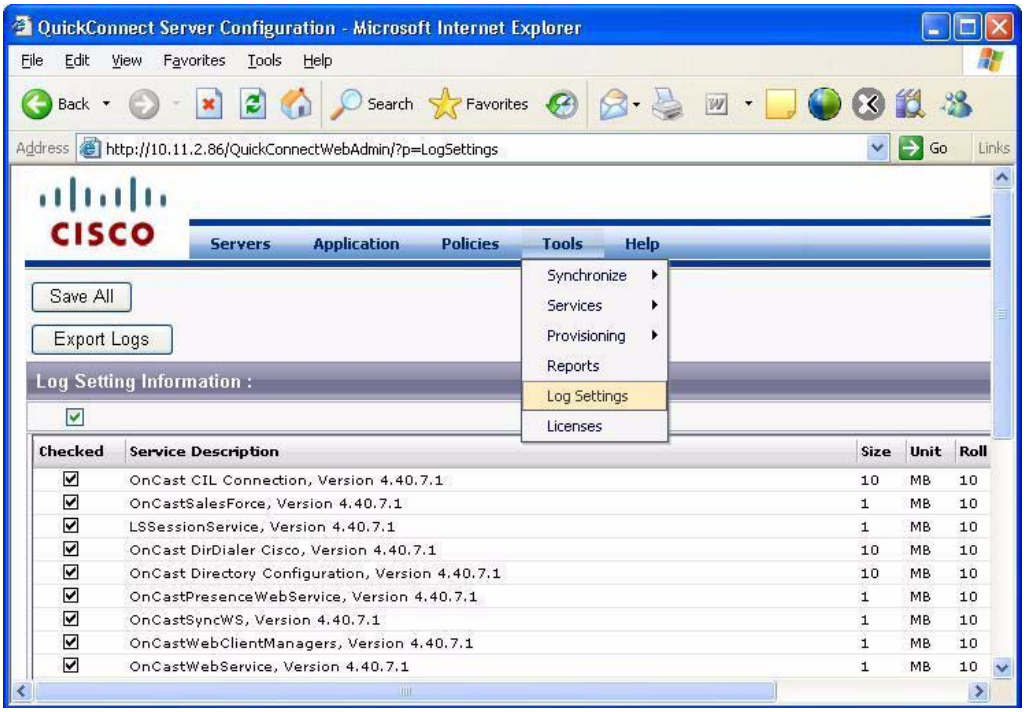
Log files rotate on a frequency and size basis.

To set Log Levels in WebAdmin:

Procedure

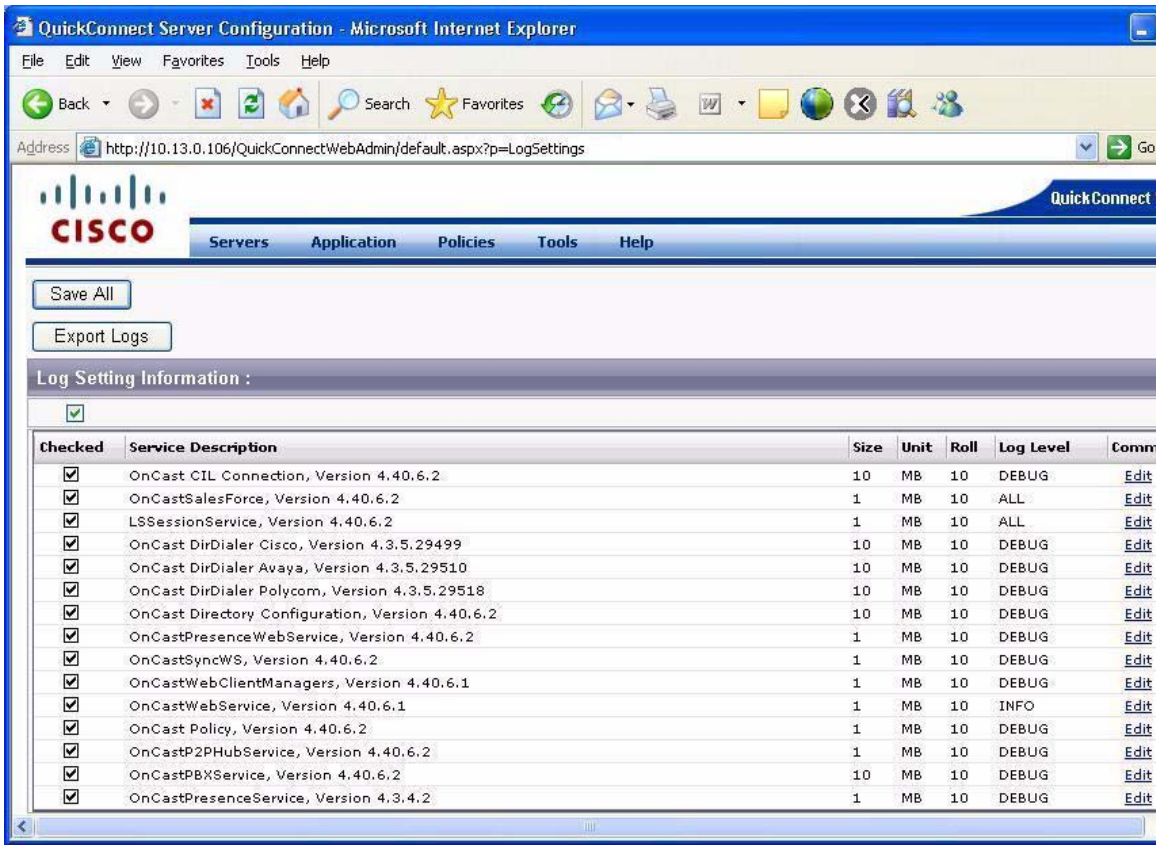
Step 1 Choose **Tools** > **Log Settings** (Figure 7-12).

Figure 7-12 Log Settings Menu Item



The Log Settings screen will open (Figure 7-13). If you wish to enable or disable logging for all services, click the checkbox below Log Setting Information.

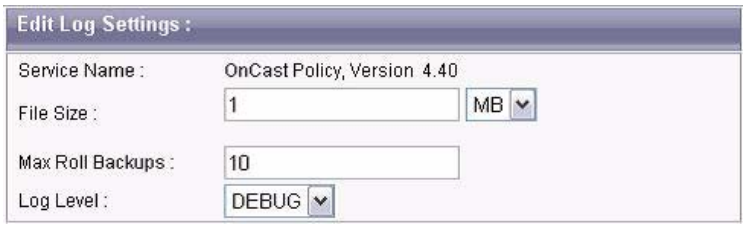
Figure 7-13 Log Settings Screen



Step 2 Click **Edit** in the line for the Service you wish to set logging for.

Step 3 In the Edit Log Settings area, set the maximum file size for the log and the number of rolling backup logs to keep.

Figure 7-14 Edit Log Settings



Also select the Log Level (listed from least info to most info). Table 7-2 describes the levels and the information recorded for each.

Table 7-2 Log Levels

Log Level	Information Recorded
INFO	Informational messages about the progress of the service at a coarse-grained level.
ERROR	Only non-fatal error conditions are recorded.

Table 7-2 Log Levels

Log Level	Information Recorded
DEBUG	Fine-grained informational events useful to debug an application are recorded.
ALL	All transactions and operations performed by the service are recorded.
OFF	Nothing is recorded for this service.

Step 4 Click **Save**.

Note The <FileLogLevel> parameter in the configuration file has nothing to do with Unified Quick Connect; it is related to the Java-based Media Server. Do not change this parameter.

Exporting Logs

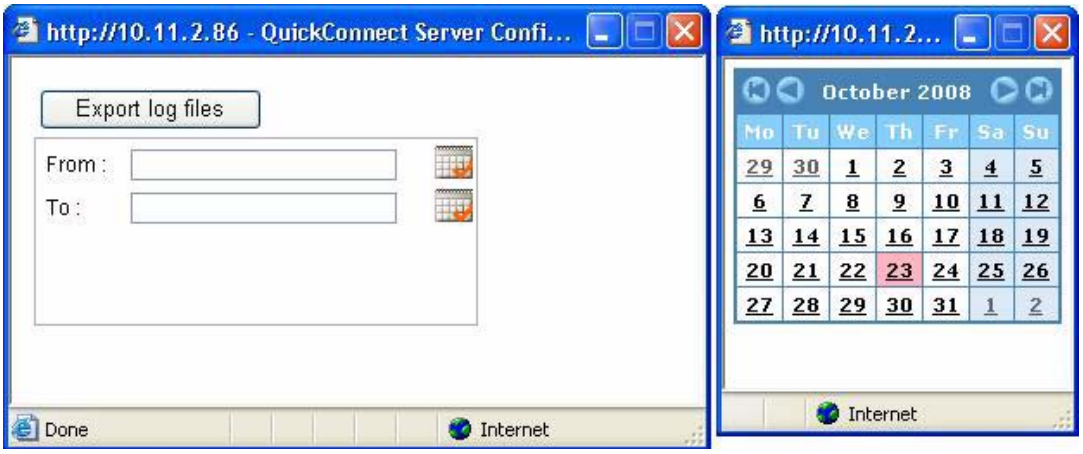
If you are asked to submit logs by the Customer Support group, this function will allow you to export the logs. This is performed in the Log Settings screen.

Procedure

Step 1 In the Log Settings screen, click **Export Logs**.

Step 2 Click **Edit** in the line for the Service you wish to set logging for.

The Date Selector window will pop up:



Step 3 Type in From and To dates or use the calendar pop-up to select dates.

Step 4 When you have entered the To date, press **Enter** and the files will be created and made available to download using a standard File Download dialog box.

Licenses

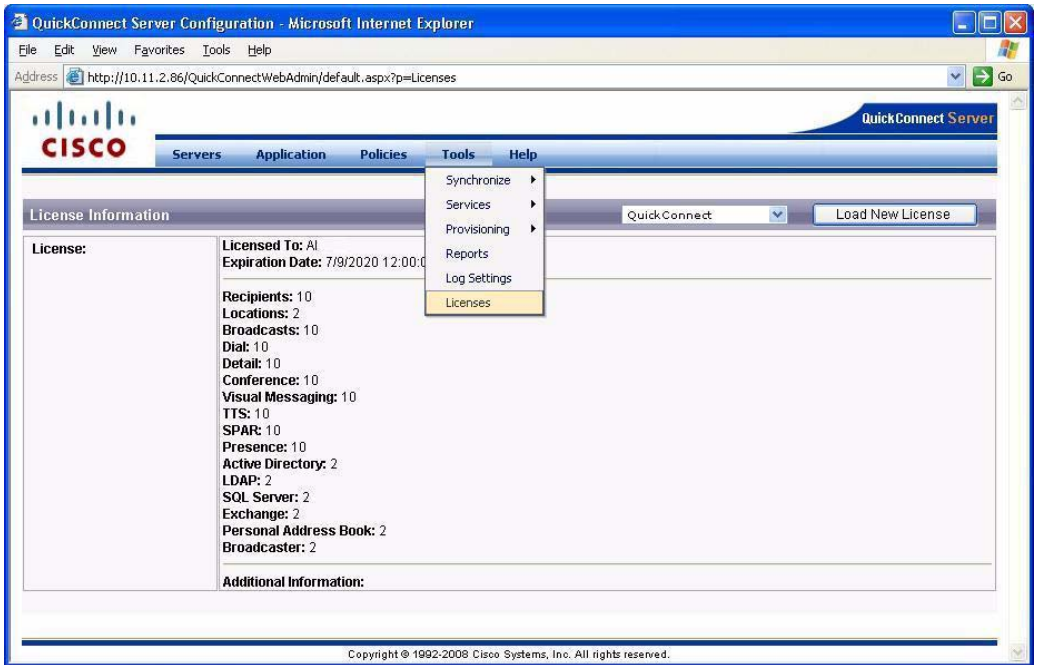
The Licenses menu item displays information on the current Unified Quick Connect license, and allows you to upload a new license.

To view the Licenses page in WebAdmin:

Procedure

Step 1 Choose **Tools** > **Licenses** (Figure 7-15).

Figure 7-15 Licenses Menu Item



To load a new license:

Step 1 Click **Load New License** (Figure 7-15).

Step 2 Click **Browse** and navigate to the license file.

Step 3 Click **Open**.

Step 4 Click **Load**.

The new license is loaded and the license parameters are displayed.

CHAPTER 8

Troubleshooting

This chapter discusses the following troubleshooting resources:

- Using Unified Configuration Files, page 8-1
- Commonly Found Issues, page 8-1

Using Unified Configuration Files

Note It is recommended that you do not access or modify the unified configuration file.

Unified Quick Connect Server configuration information is stored in XML format as part of a unified configuration file, which you can find in the following location:

C:\Documents and Settings\All Users\ApplicationData\LiteScape\OnCast\ OnCast.Configuration.xml

The file contains information about all the services used in Unified Quick Connect. You can find a copy of the file in Appendix A.

Each server also holds one additional identity document that is not replicated to other servers and nodes, which you can find in the following location:

\\Deployment Server Address\Documents and Settings\All Users\Application Data\LiteScape\OnCast\OnCast.Configuration.Local.xml

Although Unified Quick Connect should be configured using the WebAdmin interface, the contents of both files can be modified using a Microsoft Windows Notepad or an XML editor.

Commonly Found Issues

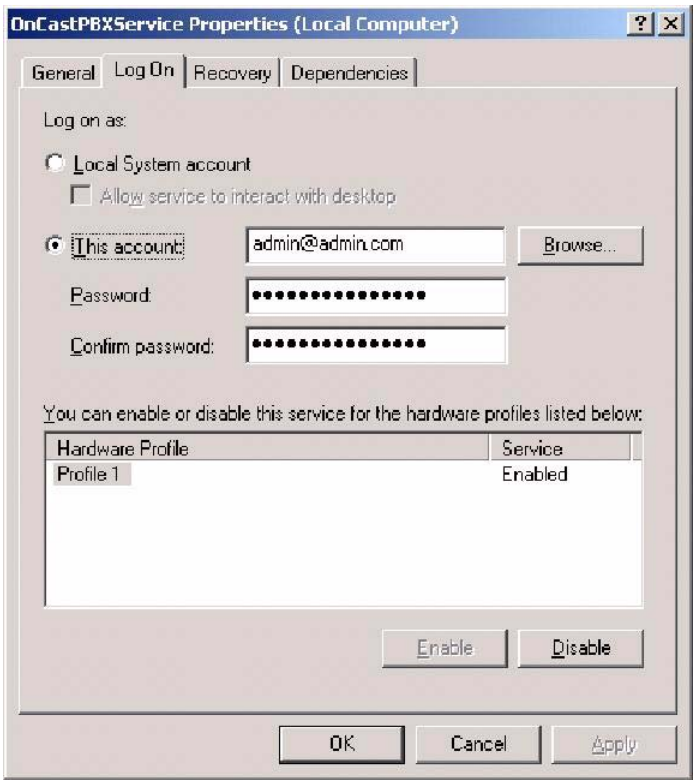
Issues that you can commonly encounter include:

- Unable to Start Unified Quick Connect PBX Service, page 8-2
- Unable to Access Unified Quick Connect WebAdmin, page 8-2
- Windows Security Updates and ASP.net, page 8-3
- Unable to Push Content on Phone, page 8-3

Unable to Start Unified Quick Connect PBX Service

You must verify that the OnCastMediaServer and OnCastPBXService services have the proper permissions. Right-click each, select **Properties**, and then click the **Log On** tab (Figure 8-1).

Figure 8-1 Log On Tab in OnCastPBXService Properties



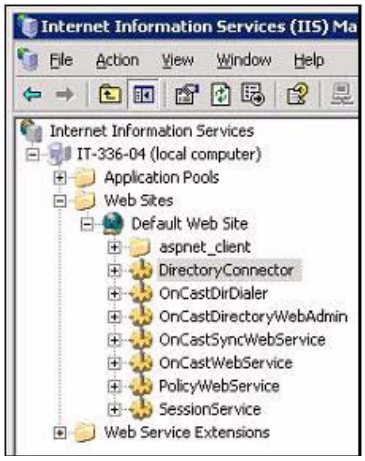
Unable to Access Unified Quick Connect WebAdmin

If you are having trouble accessing the Unified Quick Connect WebAdmin page:

Procedure

Step 1 Verify that Microsoft IIS has been properly configured. Go to Microsoft IIS Manager and ensure that Default Web Site is populated:

Figure 8-2 Microsoft IIS Manager



Step 2 Open the Directory Security tab and verify that the Windows Domain username and password you entered during the installation has been properly populated for each Microsoft IIS virtual directory.

a. Click **Edit**, then **Browse**.

b. Provide a user who has sufficient rights to run the application, for example, domain administrator.

Step 3 Click **OK**.

Windows Security Updates and ASP.net

Some Windows Updates will disable or prohibit the use of ASP.net, so you will need to allow its use in order for Unified Quick Connect to work properly. If the Web Admin page is not viewable (Error 404 in IE) after you have updated Windows Server with patches or update files, check the status of ASP.NET on the machine.

Unable to Push Content on Phone

You may encounter the following issue:

- Unable to receive or initiate broadcasts on the IP phone

This is most likely due to the phone not being associated with the trusted user or authenticated. You should troubleshoot the phone with the following steps.

Use the following Cisco command to test if your phone is properly setup:

Procedure

Step 1 From Internet Explorer, enter the following URL: http://<IP-address-phone>/CGI/Execute (case sensitive URL)

Step 2 You will be prompted with a dialog box

Step 3 Enter the Push username and password as authentication in the dialog box.

Step 4 This will be followed by 1 of 4 responses:

- "CiscoIPPhoneError Number="0"": This implies your phone can accept content
- "CiscoIPPhoneError Number="4"": This implies your phone cannot accept content so either you did not enter the correct username/password or the phone is not associated with that Push user.
- "CiscoIPPhoneError Number="6"": This implies your phone cannot accept content and means that the phone should be given a hard-reset and tried again.
- Page not found: This error is typically because port 80 is blocked and it most likely means the phone is configured properly.

CHAPTER 9

System Maintenance

This chapter discusses the following common maintenance tasks or topics:

- Adding and removing a Directory Server, page 9-1
- Adding and removing a Provider, page 9-2
- Adding and removing a Unified Quick Connect Location or Unified Quick Connect Server, page 9-3
- Adding and removing a Policy Server, page 9-3
- Adding and removing a Unified Quick Connect User, page 9-3
- Associating Devices to the Push User, page 9-4
- Configuring the Directory URL, page 9-5
- Adding and removing an Access Policy, page 9-5
- Adding and removing a Phone Number Mask for Presence, Matching, page 9-7
- Windows Services Administration, page 9-7

Adding and removing a Directory Server

In many cases you will need to access additional directory servers from Unified Quick Connect. For example, you may expand Unified Quick Connect to support a new site that has its own corporate directory server.

Procedure

Step 1 Select **Servers** > **Enterprise Servers** > **Directory Servers**. This takes you to the default view of the Directory Servers screen.

Step 2 Click **Add** to create a new Enterprise Directory Server, and fill in the required information.

Step 3 Click **Save** when you have finished entering the data, then click **Save All**.

Step 4 Select **Servers** > **Locations**. Click on your currently configured location.

Step 5 Select the **Directories** tab. You should see the newly configured directory server you configured in step 2.

Step 6 Check the USE and DEFAULT checkboxes.

Step 7 Click **Save**.

Step 8 Restart IIS.

You may also want to not have a directory available in Unified Quick Connect. For example, you will be performing maintenance on your server and do not want it accessed. To remove a directory server from being displayed in Unified Quick Connect, but still maintain its configuration in Unified Quick Connect Server, do the following:

Procedure

Step 1 Go to **Servers** > **Locations**.

Step 2 Select the **Directories** tab.

Step 3 Un-check the USE and DEFAULT checkboxes.

Step 4 Click **Save**.

Step 5 Restart IIS.

The next time you access Unified Quick Connect, you will not be able to search this directory.

To delete a server, scroll to the far right side of the Directory Server Information table and click the **Del** link for the server. You will be asked to confirm the removal of the record from the system; click **OK**, then click **Save**.

Adding and removing a Provider

You can add a second provider in a Unified Quick Connect server when the server is a Configuration Server and there is another Unified Quick Connect server configured for use at a different location. To configure a provider for that server:

Procedure

Step 1 Select **Servers** > **IP-PBX (Providers)** > **PBX Servers**. This opens the Provider Settings screen.

Step 2 Click **Add** to create a new PBX Server, and fill in the required information.

Step 3 Click **Save** when you have finished entering the data.

Step 4 Select **Servers** > **Locations**. Click on your currently configured location.

Step 5 Select the **Providers** tab. You should see the newly configured provider you configured in step 2.

Step 6 Check the USE and DEFAULT checkboxes.

Step 7 Click **Save**.

To delete a server, scroll to the far right side of the PBX Server Information table and click the **Del** link for the server. You will be asked to confirm the removal of the record from the system; click **OK** then click **Save All**.

Adding and removing a Unified Quick Connect Location or Unified Quick Connect Server

After you create an IP-PBX (provider) and directory server on your configuration server, you must add a location under Locations and associate the newly-configured provider and directory server to that Location. Once you have completed those steps, you can then install the new Unified Quick Connect server.

Having multiple Locations also allows you to associate specific resources with a particular Location.

Adding and removing a Policy Server

You may want to store your Unified Quick Connect Access policies in a new Unified Quick Connect Server. This might be required if you want to improve reliability by distributing the functionality of your Unified Quick Connect Server across multiple physical servers. To add a new Policy Server:

Procedure

Step 1 Select **Servers** > **Enterprise Servers** > **Policy Servers** from the **Servers** > **Enterprise Servers** menu. This takes you to the Policy Server Information screen.

Step 2 Click **Add** to create a new policy server.

Step 3 Type a name for the server in the Caption field.

Step 4 In the Repository Type field, do one of the following:

- Select DirectoryServer if you want to store the policy on an existing server.
- Select FileBased if you want to store the policy in a folder on a local server.

Step 5 To enter a Server Path, click the **Select** link.

- If you selected DirectoryServer in Step 4, type in the IP address of the server, or click OK then click Select to select a server that will store the policies.
- If you selected FileBased in Step 4, type or paste in the path to the selected drive and folder.

Step 6 Make your selection and click **OK** to reset the screen.

Step 7 Click **Save** to save and implement your changes.

Step 8 To delete a policy server, click the **Del** link for the server you want to delete. Click **OK** in the confirmation window to complete the deletion.

Adding and removing a Unified Quick Connect User

Provisioning is the act of manually adding Users into Unified Quick Connect directly rather than relying on directory servers to forward their information.

Perform the following steps in your Directory Server:

Procedure

Step 1 Find the new user in your directory server.

Step 2 If the entire directory server has not been configured as searchable, make sure the Organizational Unit or Container the user is in has the flags attribute set to 1000.

Step 3 Ensure the matching attribute (e.g., telephoneNumber) is populated and matches the extension of the user in the IP-PBX.

Step 4 If all users are not configured as trusted, ensure that the LSTrustedPhone attribute (e.g., employeeType) field is populated so that the user can access Unified Quick Connect.

Step 5 In your Cisco CallManager, associate the user's extension and device with the push user, as detailed in the section Associating Devices to the Push User, page 9-4.

Step 6 Find the user's extension in the IP-PBX.

Step 7 Make sure their extension matches the attribute in step 3 above.

Step 8 Make sure the URL Directories attribute is populated for this user or for the entire IP-PBX, as detailed in the section Configuring the Directory URL, page 9-5.

Step 9 Restart the user's phone.

This user should now be able to access Unified Quick Connect.

Associating Devices to the Push User

When you add new phones to your Cisco Unified Communications Manager, they must be associated with the push user in Unified Communications Manager.

Perform the following steps to associate a new phone with the push user:

Procedure

Step 1 Log in to Unified Communications Manager and navigate to the Application User Configuration screen. Create the Unified Quick Connect administrator user in Unified Communications Manager as an Application User

Step 2 In the Device Information section, click **Find More Phones** to locate the phones to associate.

Step 3 Use the up and down arrows to associate the phones by moving them from the bottom box to the top "Available Devices" box.

Step 4 Click the diskette icon at the top of the screen to save your user and the associated phones.

Configuring the Directory URL

If you ever change the IP address or hostname of your Unified Quick Connect Server through the **Change IP Address** button in the installer, then you must also change how it is configured in Unified Communications Manager. Specifically, you will need to change the following:

- Directory URL – this is the page end-users first see when accessing Unified Quick Connect.

Perform the following steps to configure and test the Directory URL:

Procedure

Step 1 Log in the Cisco Call Manager with administrative privileges

Step 2 Select **System** > **Enterprise Parameters**.

Step 3 Set the Service Provisioning parameter to “Both”.

Step 4 Save Settings.

Step 5 Reset all devices.

Step 6 Go to a registered phone.

Step 7 Select the directories Icon on the first screen.

Step 8 Select **Directory Services**.

Step 9 Select **Global directory**.

Step 10 Search for a phone or a user by First/last name and select the **PTT** softkey.

Step 11 The originator and the recipient will get a PTT screen pushed to their phones.

Step 12 The originator presses the PTT button again and the PTT session between the originator and recipient starts.

Note Changing this parameter will require a reboot of any phones that will be using Unified Quick Connect.

Directory URL

In the Unified Communications Manager administrative interface, choose **System** > **Enterprise Parameters** > **URL Directories** and set it to the Unified Quick Connect Directory server address:

http://Unified Quick Connect-Server-IP-Address/Unified Quick Connect/xmldirectory.aspx

Adding and removing an Access Policy

As you continue to use Unified Quick Connect, you may want to modify which users and groups have access to certain functionality. For example, you may soon realize that a specific department has the need to start broadcasting only within their department, but not to the entire organization.

Note You must have defined a Policy Server before you can implement Complex Policies.

To create a Unified Quick Connect Access Policy to enable this functionality for that department:

Procedure

Step 1 Select **Access Policy** from the Policies menu. This takes you to the main Access Policy screen, which displays simple policy parameters if you have not yet configured any policies.

Step 2 Uncheck the Use Simple Policy checkbox to display a list of all the complex policies that have been configured to date (if any).

Step 3 In the Access Policy screen, click the **Add** link to display a new blank record.

Step 4 In the From field, type the name or number to which you are providing the access by function.

Note The entry in the From field should match the attribute assigned to the LSDisplayName on the Application>Directory Mapping screen. You can use “Everyone” (with a capital ‘E’) or “everyone” (with a lower-case ‘e’) interchangeably.

Clicking the From link will open a pop-up window in which you can search for Groups.

Step 5 In the To field, type the name or number the From user can contact using the functions s/he is given access to.

Note The entry in the To field should match the attribute assigned to the LSDisplayName on the Application > Directory Mapping screen. Clicking the To link will open a popup window in which you can search for defined groups.

Step 6 Change the function access fields (Table 9-1) to true to provide access or false to restrict access to each function. A checkmark in the field makes the function “true” (access granted).

Table 9-1 Function Access Fields

Function Name	Description
B.T=Broadcast Text	Allows users to create text broadcast messages.
B.A=Broadcast Audio	Allows users to create audio broadcast messages.
B.I=Broadcast Image	Allows users to create image broadcast messages.
B.TA=Broadcast Text and Audio	Allows users to create text and audio broadcast messages.
B.IA=Broadcast Image and Audio	Allows users to create image and audio broadcast messages.
B.LA=Broadcast Live Audio	Allows users to create live audio broadcast messages.
B.CO=Broadcast Custom OCM	Allows users to create broadcasts of custom broadcast templates.
G=Get Config	Used by Centralized Configuration Service to provide the ability to retrieve another user’s or group’s configuration.
S=Set Config	Used by Centralized Configuration Service to provide the ability to set another user or groups configuration.

Step 7 Click **OK** to return to the previous screen, then click **Save** to save your new policy.

To delete a policy, click the **Del** link for the policy you want to delete. Click **OK** in the confirmation window to complete the deletion.

Adding and removing a Phone Number Mask for Presence, Matching

There may be instances when an extension in the directory server does not match what is in the IP-PBX. As a result, you can set up a masking rule to match extensions and you can also prepend a PSTN access code.

To create phone number masks:

Procedure

Step 1 Select **Servers** > **IP-PBX (Providers)** > **Phone Number Masks**. The Phone Number Masks screen will open.

Step 2 Click **Add** to create a new record.

Step 3 Select the IP-PBX that will use this mask, then enter the mask itself.

When entering the mask, Use P for a Presence-related mask, and M for a number matching mask.

Step 4 Click **OK**, then **Save**.

Windows Services Administration

Service administration consists of the following procedures:

- "Starting and Stopping Microsoft Windows Services"
- "Starting and Stopping Web Services"

Starting and Stopping Microsoft Windows Services

The Unified Quick Connect product includes the following Microsoft Windows services:

- QuickConnectMediaServer
- QuickConnectPBXService
- DirectoryHeartBeatService – this service runs permanently.

After the installation, add the administrator user to these services in Windows. Verify that the C:\Documents and Settings\All Users\Application data\Litescape folder has a Network service user associated with full rights to write.

These services should then start automatically on systems start-up and do not require user or system log in. If they do not start automatically, the system administrator needs to review the logs and determine possible reason for service failure. For more information on the logs, review the section Troubleshooting

Starting and Stopping Web Services

Unified Quick Connect includes the following Microsoft Windows Web services:

- Unified Quick Connect WebAdmin
- CILConnection Web Service
- CalendarWebService
- CILWebService
- Device Status
- DirectoryCacheService
- DirectoryConnection WebService
- DirectoryHeartbeat Service
- DnD
- MAPIConnector
- OnCastPBXService
- PresWebService
- SyncWebService
- PolicyWebService
- SessionService

Other than Unified Quick Connect WebAdmin (a Web-based application interface), the components are Microsoft IIS Web Services that start automatically on system start-up. If they do not start automatically, the system administrator should follow these steps:

Procedure

Step 1 Verify that the Microsoft Windows IIS service is running

Step 2 Verify that the Microsoft World Wide Web Publishing Service is running

Step 3 Verify that each Unified Quick Connect Web service is running and responding properly.

a. In Microsoft IIS, expand each service and locate the Web service invocation (.asmx) document, right click the document and select **Browse**.

b. Verify that the invocation methods for each web-service show up properly.

Step 4 To verify the DirectoryConnectionService is working properly - click the DirectoryConnectionService.asmx link in Microsoft IIS to expose the SOAP based methods of the web service.

a. Invoke the getGroupMembersUsers.

b. Enter true for the showDisplayName field shown below.

c. Click **Invoke**.

d. You can see the results of the directory search appear on the browser screen in XML format.

Step 5 Verify the PolicyWebService is working properly - click the **OnCast.Policy.asmx** link in Microsoft IIS to expose the SOAP based methods of the web service.

Step 6 Invoke getPermission.

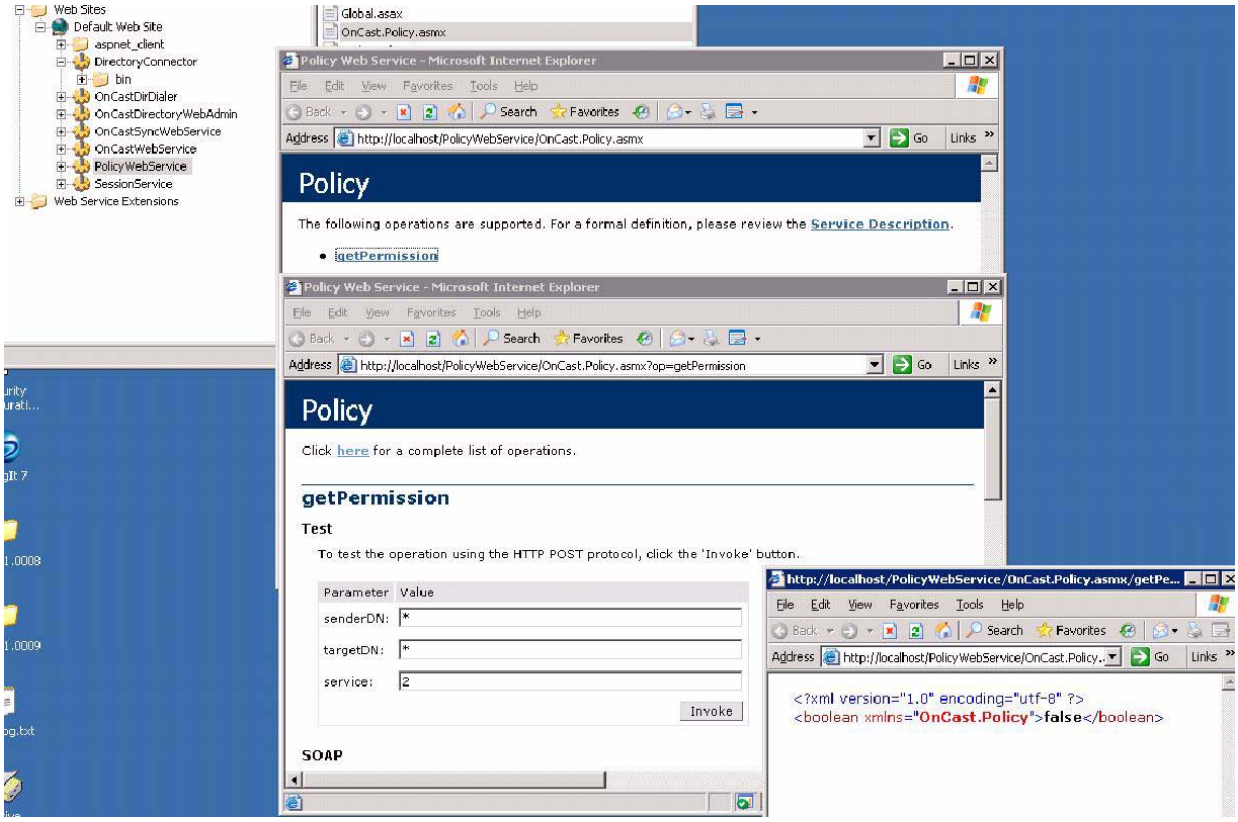
Step 7 Type a senderDN and targetDN (where DN is the distinguished name in a directory server). Service can be:

- 0: Broadcast

Step 8 Click **Invoke**.

Step 9 You can see the results of the policy check appear on the browser screen in XML format (Figure 9-1).

Figure 9-1 Result of the Policy Check in XML Format



Step 10 To verify the QuickConnectWebService is working properly, click the **WANBroadcast.asmx** link in Microsoft IIS to expose the SOAP-based methods of the Web service.

Step 11 Invoke the InitializeBCPayload service.

Step 12 Paste an XML message into the Value field and click **Invoke** to test the service. Use the following XML message as a sample starting point and update to match your environment settings:

```
<LSBC>
  <Organizer>
    <UserID>pttuser1</UserID>
    <Key>20444</Key>
    <Extension>20444</Extension>
    <MainPhone>20444</MainPhone>
    <IPAddress>10.11.2.38</IPAddress>
    <LDAPDN>AD|CN=PTT User1,OU=Test Accounts, DC=example, DC=local</LDAPDN>
    <ProviderID>IP-PBX 1</ProviderID>
```

```
  </Organizer>
  <InviteesGroup />
  <Invitees>
    <Invitee>
      <UserID>PTT User4</UserID>
      <Key>20447</Key>
      <Extension>20447</Extension>
      <MainPhone>20447</MainPhone>
      <LDAPDN>AD|CN=PTT User4,OU=Test Accounts,DC=example,DC=local</LDAPDN>
      <ProviderID />
    </Invitee>
  </Invitees>
  <Action>OCM</Action>
  <Priority>Emergency</Priority>
  <OCMFile>c:\Documents and Settings\All Users\Application
Data\LiteScape\OnCast\BroadcastTemplates\WalkieTalkiePush.ocm</OCMFile>
  <Conference>
    <PhoneNumber />
  </Conference>
<shortcutURL>http://10.11.2.72/DirDialer/Options/createShortcut.aspx?key=20444&amp;session
id=894b332e-391e-4226-90b3-34de0c82d5c6</shortcutURL>
</LSBC>
```

For information on the input parameters, see Format of the InitializeBCPayload Parameters in Chapter 6, “Customizing Cisco Unified Quick Connect”.

Step 13 Review your application logs and determine the reason for web-service failure. For more information on the logs, see Chapter 8, “Troubleshooting”.

APPENDIX A

Cisco Unified Quick Connect Template Files

This appendix describes the .ocm template files included with Cisco Unified Quick Connect, and contains the following topics:

- List of Template Files, page A-1

List of Template Files

The broadcast templates are used for sending unicast or multicast broadcast to one or more phones. Templates marked as required should not be deleted.

Table A-1 Unified Quick Connect Template Files

Template File	Description
Barge.ocm **(required)**	This template allows for barge-in broadcasts on IP phones.
ClearScreen.ocm **(required)**	This template clears the IP phone screen.
Dummy.ocm **(required)**	This template controls invitations to broadcasts.
OrganizerAudio.ocm (**required)**	This template control audio broadcast.
PleaseWait.ocm (**required)**	This template is used when a screen is being loaded.
WalkieTalkie.ocm (**required)**	This template is for internal use.
WalkieTalkiePush.ocm (**required)**	This template enables the push-to-talk feature (one-to-many or one-to-one) between IP phones. It can be configured for 1-button invocation, and a Talkback feature allows a recipient to have a private conversation with the sender.

APPENDIX B

Directory Server Parameters

This appendix defines the attributes that can be configured in Cisco Unified Quick Connect to support the directory server, and contains the following topics:

- Directory Server Parameters Mapping Table, page B-1

For more information about configuring directory server settings, see the "Configuring Enterprise Directory Servers" and "Configuring Directory Mapping Attributes" sections in Chapter 5, "Configuring Cisco Unified Quick Connect Server".

Directory Server Parameters Mapping Table

Gather the data for each parameter before beginning the installation so you have it available when it is required.

Note The directory server attributes used here are customizable and can be configured to match what your enterprise directory supports.

Table B-1 Directory Server Parameters Mapping

Unified Quick Connect Parameter Name	Default Directory Attribute	Data Type	Level	Function	Servers
LSDisplayPhone	telephoneNumber	Unicode string, expects Numeric	User	Defines which phone is displayed by default when viewing search results.	MS-AD, LDAP, MS Exchange, Salesforce.com
LSDisplayName	Cn	Unicode string	User	Defines which name is displayed by default when viewing search results.	MS Active Directory, LDAP, MS Exchange, Salesforce.com
LSDirKey	telephoneNumber	Unicode string, expects Numeric	User	Defines the unique key that must match an attribute in the IP-PBX.	MS-AD, LDAP, MS Exchange, Salesforce.com

Table B-1 Directory Server Parameters Mapping (continued)

Unified Quick Connect Parameter Name	Default Directory Attribute	Data Type	Level	Function	Servers
LSExtension	telephoneNumber	Unicode string, expects Numeric	User	Define the primary Directory Number (extension) for a specific user.	MS-AD, LDAP, MS Exchange, Salesforce.com
LSPBXProvider	extension10	Unicode string	User, Group	Unified Quick Connect uses this field to determine the Provider-ID for the user. The Provider represents various IP-PBX aliases. The IP-PBX aliases are selected in the product's web-based administrative interface.	MS-AD, LDAP, MS Exchange, Salesforce.com
LSSearchableAttr Name	Flags	Numeric, expects Numeric	Organizational Unit or Container	Determines whether to use/hide an OU or CN from filter/search results. Acceptable values: 1000 Searchable Anything else, including <not set>, is not searchable.	MS-AD, LDAP, MS Exchange
LSTrustedPhone	employeeType	Unicode string, expects Numeric	User	Acceptable values: 0 – Global Address Book is trusted. Applies to: Global.	MS-AD, LDAP, MS Exchange, Salesforce.com

Table B-1 Directory Server Parameters Mapping (continued)

Unified Quick Connect Parameter Name	Default Directory Attribute	Data Type	Level	Function	Servers
LSTrustedPIN	employeeID	Unicode string, expects Numeric	User	Determines password to be used for user access to Unified Quick Connect Phone. This PIN must be entered by a user if their phone is non-trusted. Applies to: Global Address Book, Options, Shortcuts (if configured to be covered with Log In).	MS-AD, LDAP, MS Exchange, Salesforce.com
LSUniqueIdentifier	distinguishedName	Unicode string	User, Group	Defines which attributes uniquely identifies the CN or OU within the directory server.	MS-AD, LDAP, MS Exchange, Salesforce.com
LSEmailAccount	mailNickname	Unicode string	User, Group	Defines the user ID for accessing personalized features. Applies to: Global Address Book, Options, Shortcuts (if configured to be covered with Log In).	MS-AD, LDAP, MS Exchange, Salesforce.com
LSSNMPKey	Extension	Unicode string	User, Group	Matches value declared in LSDirKey.	MS-AD, LDAP, MS Exchange, Salesforce.com
LSPolicyDisplayName	displayName	Unicode string	User	Policy unique object name for ID.	MS-AD, LDAP, MS Exchange
LSPolicyOwner	Owner	Unicode string	User	Policy name of policy owner.	MS-AD, LDAP, MS Exchange
LSPolicyAssistant	assistant	Unicode string	User	Policy name of policy receiver.	MS-AD, LDAP, MS Exchange
LSPolicyInfo	Info	Unicode string	User	Policy information.	MS-AD, LDAP, MS Exchange

Table B-1 Directory Server Parameters Mapping (continued)

Unified Quick Connect Parameter Name	Default Directory Attribute	Data Type	Level	Function	Servers
First	Givenname	Unicode string	User	Defines which attribute to use when searching by first name.	MS-AD, LDAP, MS Exchange, Salesforce.com
Last	sn	Unicode string	User	Defines which attribute to use when searching by last name.	MS-AD, LDAP, MS Exchange, Salesforce.com
Display	displayName	Unicode string	User, Group	Defines which attribute to use when searching by displayed name.	MS-AD, LDAP, MS Exchange, Salesforce.com
Common	cn	Unicode string	User, Container or Organizational Unit	Defines which attribute to use when searching by common name.	MS-AD, LDAP, Salesforce.com
Department	Department	Unicode string	User	Defines which attribute to use when searching by department.	MS-AD, LDAP, Salesforce.com
LSEmailAddress	mail	Unicode string	User, Group		MS-AD, LDAP, MS Exchange, Salesforce.com
LSDisplayType	objectClass	Unicode string	User, Group		MS-AD, LDAP, MS Exchange, Salesforce.com
LSAlternativePhone	homePhone, ipPhone	Numeric	User		MS-AD, LDAP, MS Exchange, Salesforce.com
LSSortBy	cn	Unicode string	User		MS-AD, LDAP, MS Exchange, Salesforce.com
Company	company		User, Group		MS Exchange
LSAdamContactDefaultPhone	telephoneNumber or mobile		User		MS-AD
LSAdamContactDisplayName	displayName		User		MS-AD
LSAdamContactID	Description		User		MS-AD
LSAdamGALObjectID	adminDescription		User, Group		MS-AD

Table B-1 Directory Server Parameters Mapping (continued)

Unified Quick Connect Parameter Name	Default Directory Attribute	Data Type	Level	Function	Servers
LSAdamLocation DisplayName	displayName		User		MS-AD
LSAdamLocationIP	description		User		MS-AD
LSCity			User, Group		MS-AD
LSLastDialDate	extensionattribute14		User		MS-AD, LDAP, MS Exchange
LSLastDialFromUser	extensionattribute11		User		MS-AD, LDAP, MS Exchange
LSLastDialNumber	extensionattribute13		User		MS-AD, LDAP, MS Exchange
LSLastDialToUser	extensionattribute12		User		MS-AD, LDAP, MS Exchange
LSLastDialType	extensionattribute15		User		MS-AD, LDAP, MS Exchange
LSLastModified			User		MS Exchange
LSMessageID			User, Group		MS Exchange
LSSpeakerMacAdd	extensionattribute15		User		MS-AD

APPENDIX C

Cisco Unified Quick Connect Advanced Settings

This appendix describes the Cisco Unified Quick Connect Server advanced settings that are accessed from Unified Quick Connect Web Admin > Servers > Advanced Settings, and contains the following topics:

- Advanced Settings, page C-1

For information on Centralized Configuration, refer to Chapter 5, "Configuring Cisco Unified Quick Connect Server".

Advanced Settings

Table C-1 describes the advanced settings for Unified Quick Connect Connector.

Table C-1 Unified Quick Connect Connector Advanced Settings

Parameter	Description	Allowed or Default Values
HostIP	IP address for the Unified Quick Connect server used for MAPI Windows service (for connectivity to MS Exchange, MS Access, and Salesforce.com). For example 10.11.2.1.	An IP address.
HostPort	Port used for MAPI Windows service.	1025-65536. Default is 6962.
UseCompression	Uses compression when connecting to MAPI Windows service.	True or False. Default is False.

Table C-2 describes the advanced settings for Database.

Table C-2 Database Advanced Settings

Parameter	Description	Allowed or Default Values
ImpType	The configured database type. For example, MSSQL.	MSSQL, ORACLE, or MYSQL. Default is MSSQL.

Table C-3 describes the advanced settings for the Phone UI.

Table C-3 Phone UI Advanced Settings

Parameter	Description	Allowed or Default Values
MaxFilterLength	Maximum number of letters searched per field in Unified Quick Connect Smart Search.	1-10. Default is 6.
MaxRemoteFilterLength	This parameter is not currently used.	
OnCastNormal	Caption for the Normal broadcast softkey on the phone. Obsolete since Unified Quick Connect introduced the softkey layout feature.	
OnCastEmergency	Caption for the Emergency broadcast softkey on the phone. Obsolete since Unified Quick Connect introduced the softkey layout feature.	
LocalDirectory	Displays the local directory in Unified Quick Connect Phone.	True or False. Default is False.
VisualMessaging	This parameter is not currently used.	True or False. Default is False.
MyBroadcasts	Displays MyBroadcasts in Unified Quick Connect Phone.	True or False. Default is False.
WebEx	This parameter is not currently used.	True or False. Default is False.
Options	Displays Options in Unified Quick Connect Phone.	True or False. Default is False.
Shortcuts	Displays Shortcuts in Unified Quick Connect Phone.	True or False. Default is False.
AllUsersTrusted	Makes all the phones accessing Unified Quick Connect trusted. That is, no username or password is required. This is a system wide feature and affects all phones that are configured to use Unified Quick Connect. If set to False, you have to configure a Unified Quick Connect password in the customer directory server (AD: employeeID).	True or False. Default is False.
CheckStatus	Indicates whether Unified Quick Connect Phone UI will retrieve and display contact presence information (for search results).	True or False. Default is False.
IdlePageTimeout	The time in seconds for any page to dissolve once idle.	
MaxFilterItemsPerRequest	The maximum number of queries sent simultaneously to the directory server. Certain directory servers have limitations on maximum queries.	
LastSearchResult	Displays the "Last Search Result" option in Unified Quick Connect Phone.	True or False. Default is False.

Table C-4 describes the advanced settings for the directory.

Table C-4 DirectoryAdvanced Settings

Parameter	Description	Allowed or Default Values
OnBind	Timeout value that directory connection library waits to establish a connection to the directory server.	Default is 10000
OnGet	Timeout value for search requests.	Default is 20000

Table C-4 DirectoryAdvanced Settings (continued)

Parameter	Description	Allowed or Default Values
MaxFilterLength	Maximum number of letters searched per field in Unified Quick Connect Smart Search.	1-5. Default is 5.
MaxTotalRecordsTo Request	Maximum number of records returned to Directory search queries for wild card searches.	100-12000. Default is 1000.
MaxRecordsToFetch	Maximum number of records returned to Directory search queries from Phone interface applications.	1-100. Default is 100.
OnSleep	Idle period in milliseconds between extensive search processes. Helps avoid CPU spikes resulting from extensive searches.	5-100. Default is 10.
OnSleepIterations	Number of iterations to process before going idle for OnSleep period. Helps avoid CPU spikes resulting from extensive searches.	1-100. Default is 10.

Table C-5 describes the advanced settings for the caching service.

Table C-5 Cache Advanced Settings

Parameter	Description	Allowed or Default Values
Threads	The number of threads that run simulaneously in the thread pool created by the caching service. No more than 32 threads are recommended.	For example, 15.
ThreadPoolTimeOut	How long the thread pool will wait in milliseconds for the thread to respond.	For example, 600000.

Table C-6 describes the advanced settings for Web service URLs.

Table C-6 Web Service URLs Advanced Settings

Parameter	Description	Allowed or Default Values
WebServiceURLPort	If Unified Quick Connect and Cisco Unified Applications Environment are co-resident on the same server, you must assign a port number that is the same port number configured in the Default Web Site in IIS. If you assign a port number, that number is prepended to each Web service path in the /WebServiceURLs section in OnCast.Configuration.xml . If you assign a value of 0, all prepended port numbers are removed from the Web services paths.	0-65536. Default value is 80.
Timeout	Timeout value for calling WebServices when requests are synchronous.	10-100000. Default is 30000.
ASyncWaitTimeout	When requests are asynchronous, when the requesting entity establishes a callback mechanism for processing responses from the underlying Web service.	10-100000. Default is 15000.

Table C-7 describes the advanced settings for the Media Server.

Table C-7 Media ServerAdvanced Settings

Parameter	Description	Allowed or Default Values
MediaServerPort	Port of the media server.	1025-65536. Default is 5055.
FileLogLevel	File log level from 1 to 8.	1-10. Default is 10.
ConsoleLogLevel	Console log level from 1 to 8.	1-10. Default is 10.
MaxNumberofLogFiles	The maximum number of log files.	1-10. Default is 10.
MaxSizeofLogFile	The maximum size of the log file in kilobytes.	1-10. Default is 10.
CheckPortsInterval	Specifies the time interval, in minutes, for checking the ports xml file.	1-10. Default is 10.
SessionTimeOutMin	The Broadcast server checks for the start date of the session created and if it has expired after the specified number of minutes, the server removes it.	1-10. Default is 10.

Table C-8 describes the advanced settings for the IP-PBX.

Table C-8 IP-PBX Advanced Settings

Parameter	Description	Allowed or Default Values
RefreshTime	The time interval, in minutes, used by PBXService to Refresh its data. How often PBXService polls the IP-PBX to get devices (in minutes).	1-10. Default is 10.
SNMPTimeout	The time interval, in seconds, used by PBXService to connect and wait before throwing an exception.	1-100. Default is 10.
Threads	Specifies the number of threads to run simultaneously. The rest of the threads are queued.	1-100. Default is 10.
WaitBetweenThreads	This value (in milliseconds) determines the amount of time the PBX Service will sleep in between each thread invocation. This will provide processing time back to the server, preventing CPU starvation.	1-100. Default is 10.
OCCSPort	Collaboration server Port.	1025-65536. Default is 5055.
PBXMaxAXLThreads	If PBX Service is connecting to Cisco AXL for information retrieval, this parameter is used to determine the maximum number of AXL threads created at any given time	1-10. Default is 5.
PBXAXLTimeout	If PBX Service is connecting to Cisco AXL for information retrieval, this parameter is used to determine the connectivity time-out in milliseconds.	1-10. Default is 5.
PBXAXLRetry	If PBX Service is connecting to Cisco AXL for information retrieval, this parameter is used to how may times to retry connecting to AXL in the event of a connection failure	1-10. Default is 5.
PBXDODirectory	Determines whether or not the PBX Service will reconcile PBX information with directory information. If the setting is False, all LDAP related attributes in the PBXData xml files will be left empty.	True or False. Default is False.

Table C-8 IP-PBX Advanced Settings (continued)

Parameter	Description	Allowed or Default Values
PBXRemoveOIDFiles	Determines whether or not the PBX Service will remove temprary OID translation files when processing device retreival related information. Used for troubleshooting information retrieval issues to pinpoint the components that are returning corrupted information	True or False. Default is False.
UsePBXPolling	If true, PBXService will poll configured IP-PBX (frequency = RefreshTime) and re-write PBXDataCombo.xml. If false, PBXService will not poll IP-PBX for new devices and will instead use existing devices in PBXDataCombo.xml.	True or False. Default is False.
PBXDirectoryThreadCount	Specifies the number of threads to run simultaneously. The rest of the threads are queued.	1-50. Default is 5.
PBXUseBulkRequest	Use Bulk request to query for providers. Default value is true.	True or False. Default is False.
PBXUseSQLDB	Use SQL Database to populate the MAP database. PBX Service will populate devices in litescapedb40 (which is used by RTCM for device presence). The database gets populated at the end of PBXService either, 1) restarting, or 2) during regular polling period.	True or False. Default is False.
PBXSQLPartition	When creating extensions in the SQL database there is a column called partition. "1" is the default value.	1-10. Default is 5.
PBXUseSPMSQLDB	This parameter is not used.	N/A
PBXSaveTimeInterval	Specifies the time interval, in seconds, when the PBXDataCombo.xml file is saved.	0-100. Default is 60.

Table C-9 describes the advanced settings for the broadcasters.

Table C-9 Broadcaster Advanced Settings

Parameter	Description	Allowed or Default Values
UseMediaForLive MultiCast	Indicates whether to use the Media Server for live multicast. This parameter should be set to true.	True or false. Default is true.
ExitALL	If true, and the invitee in a broadcast session presses the Exit key, the invitee and all participants will be exited from the session.	True or false.
CollaborationWaitTime Sleep	Determines the wait time between consecutive broadcasts to the same device from the same application.	1-100. Default is 10.
DeviceType	A string of allowable device types.	
TimeToWaitBefore EnteringPasscode	Time Quick Connect Waits Before Entering user Passcode (used for various applications such as conference automation).	10-10000. Default is 4000.

Table C-9 Broadcaster Advanced Settings (continued)

Parameter	Description	Allowed or Default Values
AmountOfKeysToExecute	Number of key strokes To broadcast to an IP device at once. For example, if the number to send is 123456 and AmountOfKeypsToExecute=3, Unified Quick Connect will send the data in 2 separate broadcasts (123, then 456). This is help to prevent overloading IP devices with consecutive broadcasts.	10-10000. Default is 10.
MeetMeSoftkeyPosition	The position of the MeetMe softkey.	1-20. Default is 7.
MeetMeWaitTime	Amount of time to wait before entering MeetMe telephone number	10-10000. Default is 2000.
ConfPasscodeWait	Amount of time to wait before entering MeetMe conference password (for Meetme conferences)	1-10. Default is 3.
MaxSoftKey	Number of soft-keys assumed during a broadcast to an IP device (per screen)	1-10. Default is 3.
Name	The phone type name defined in /Broadcaster/SupportedPhones/PhoneTypes/PhoneType /Name. For example CP-7970G-GE or CP-7960G-GE.	PhoneType/Name
Value	The phone type value defined in /Broadcaster/SupportedPhones/PhoneTypes/PhoneType /Value. For example, Cisco 7970, Cisco 7971, Cisco 7960, Cisco 7961.	PhoneType/Value
RTPPortStart	This start of the port range used for the Media Server (only for Cisco CallManager). The minimum value is 20480.	20480-65536. Default is 26384.
RTPPortEnd	This end of the port range used for the Media Server (only for Cisco CallManager).	1025-32768. Default is 26384.
TimeoutForPhonePush	How long to wait, in seconds, for a response from a phone device when a push has been sent.	10-100. Default is 10.
ClearscreenTimeOut	Specifies the time, in seconds, before the screen is automatically cleared if the broadcast has no audio and the screen is left on the phone.	10-100. Default is 10.
RetrySleepTime	Specifies the time, in milliseconds, to wait for each retry before trying again.	10-100. Default is 10.
SleepTime	Specifies the time, in milliseconds, to wait for each retry before simultanous broadcast threads	0-100. Default is 10.
WaitBeforeBroadcasting	How long to wait, in milliseconds, before RunBCPayload is called by InitializeBCPayload.	0-100. Default is 60.
HowLongToWaitFor Broadcast	How long to wait, in milliseconds, before we send out the broadcast for the organizer. Usually this is used for Audio broadcasts in Emergency mode.	0-100. Default is 60.

Table C-10 describes the advanced settings for policies.

Table C-10 Policy Advanced Settings

Parameter	Description	Allowed or Default Values
UseDefaultRights	Use the default rights in this policy.	

Table C-11 describes the advanced settings for timeouts.

Table C-11 Timeouts Advanced Settings

Parameter	Description	Allowed or Default Values
IdlePageTimeout	The time in seconds for any page to dissolve once idle.	
LastSearchResultTimeout	The time in minutes the application keeps information in memory about your last search.	
SessionTimeoutCisco	How long the session will last on your Cisco IP phone.	

Table C-12 describes the advanced settings for device status.

Table C-12 Device Status Advanced Settings

Parameter	Description	Allowed or Default Values
MAPIP	IP Address of MAP server that the Unified Quick Connect server will be connecting to (presence, device information).	
MAPPORT	Port of MAP server that the Unified Quick Connect server will be connecting to (presence, device information).	1025-65536. Default is 5555.
TimeIntervalForProcess	Time Interval For Processing device status information.	0-60000. Default is 1000.
ThreadCountForPbxService	Thread Count For sending device status updates to the PBX Service.	1-10. Default is 6.

Table C-13 describes the advanced settings from the LscProperties file (RTCM).

Table C-13 LscProperties Advanced Settings

Parameter	Description	Allowed or Default Values
intlKeepAliveMsec	Specifies the interval in milliseconds used to check the health of the RTCM message queue.	1-10000. Default is 10000.
intlKeepAliveCount	Specifies the number of non-responded keep-alive messages before RTCM's message queue is restarted.	1-10000. Default is 2.
fixedRateDelayMsec	Specifies a delay in milliseconds before the keep-alive timer task will be run for the first time after the timer was engaged.	1-10000. Default is 1000.
serverBindAddress	Network interface address to listen on for incoming TCP/IP client connections.	
serverSocketType	Specifies the SOCKET protocol.	socket or socket2. Default is socket.
deviceInfoSource	Specifies the source of device info	Default is database.

Table C-13 LscProperties Advanced Settings (continued)

Parameter	Description	Allowed or Default Values
DevListIntervalMin	Time interval in minutes between pollings of device information.	Default is 5.
jdbc.url	Specifies the path to the database.	Default is jdbc:jtds:sqlserver://localhost:1433/ litescapedb40.
user	User name for the Unified QuickConnect database.	
password	Password for the Unified QuickConnect database.	
loggerParamUpdate IntervalMsec	Time interval in milliseconds shows how often RTCM checks logger's logging level.	Default is 120000.
cuaeAppName	RTCM's application name presented in CUAE.	Default is RTCM.

Table C-14 describes the advanced settings for Options WS Application Settings.

Table C-14 Options WS Advanced Settings

Parameter	Description	Allowed or Default Values
Predictive	If CurrentValue = True, then predictive search will be enabled.	True or False. Default is False.
Smart	If CurrentValue = True, then smart search will be enabled.	True or False. Default is True.
BroadcastOptions	CurrentValue should equal the server file location of the default broadcast to be used by Unified Quick Connect.	C:\Documents and Settings\All Users\Application Data\LiteScape\OnCast\Broadcast Templates\WalkieTalkiePush.ocm
Type	CurrentValue should equal the default conference type to use. The options include Meet Me (CallManager conference resource) or 3rd Party.	MeetMe or 3rd Party. Default is MeetMe.
DialingMode	If CurrentValue = OnCast, then QuickConnect mode will be used. If CurrentValue = Active, then Active mode will be used.	QuickConnect or Active. Default is QuickConnect.

Table C-15 describes the advanced settings for Phone UI Application Settings.

Table C-15 Phone UI Advanced Settings

Parameter	Description	Allowed or Default Values
Predictive	If CurrentValue = True, then predictive search will be enabled.	True or False. Default is False.
Home	If CurrentValue = Directories, then Unified Quick Connect Phone should be started using the Directories button on a Cisco phone. If CurrentValue = Services, then Unified Quick Connect Phone should be started using the Services button on a Cisco phone.	Default is Directories.
Landing Page	The landing page.	Default is GAL.
Result Per Page	CurrentValue should equal how many entries to show on each Search Results page on the phone UI.	Default is 10.
Show Groups First	If CurrentValue = True, then Unified Quick Connect Phone will show all groups before users in the Search Results page.	True or False. Default is True
Shortcut Per User	CurrentValue should equal the number of shortcuts that can be configured per user.	Default is 10.
Shortcut Login	If CurrentValue = True, the Unified Quick Connect Phone will require a Unified Quick Connect username/password to access Unified Quick Connect Shortcuts.	True or False. Default is False.
Shortcut ID Start Index	CurrentValue should equal the index record for starting Unified Quick Connect Shortcuts.	Default is 12.
Shortcut ID End Index	CurrentValue should equal the index record for ending Unified Quick Connect Shortcuts.	Default is 99.
Show Default Phone	Whether to display the directory attribute defined by Default Phone in the Unified Quick Connect Search Results page for each user.	True or False. Default is True.
Default Phone	CurrentValue should equal with directory attribute should be displayed by default in the Unified Quick Connect Search Results page for each user. This is only valid if Show Default Phone = True.	Default is Home Phone.
All Users Trusted	If CurrentValue = True, then all Unified Quick Connect users will be trusted by default and will not have to enter a username and password to access Unified Quick Connect.	True or False. Default is False.
Provider Directory URL	The URL used to access Unified Quick Connect Directory on the provider.	None.
Provider Directory Search URL	The URL used to access Unified Quick Connect search on the provider.	None.

Table C-15 Phone UI Advanced Settings (continued)

Parameter	Description	Allowed or Default Values
Show Icons	If CurrentValue = True, the Unified Quick Connect Phone will show icons for users and groups in the Search Results page.	True or False. Default is True
Idle Page Timeout	CurrentValue should equal the idle time for the Unified Quick Connect page before timeout. This is in seconds.	Default is 180 seconds.

INDEX

A

about Microsoft NLB 2-8
ADAM, creating indexes 3-26
ADAM, directory partitions in, managing 3-23
ADAM, installing 3-19
ADAM schema snap-in, installing 3-25
adding Application Directory partitions 3-24
Application Directory partitions, adding 3-24

B

binding to ADAM using Ldp.exe 3-23

C

CallManager, preparing 3-8
configuring ASP.NET 3-18
configuring directory server 3-11
configuring multiple directory servers 3-14
configuring PTT session priority 4-13
connecting to ADAM using Ldp.exe 3-23
creating indexes in ADAM 3-26

D

deployment, highly available multi-site using Microsoft NLB 2-7
deployment, multi-server multi-site 2-5, 2-7
deployment, single-server single-site 2-5
deployment configurations 2-5
directory services 3-8

E

enabling secure SSL access 5-2
ExitALL parameter 4-13

H

highly available multi-site deployments using Microsoft NLB 2-7

I

IIS configuration 3-18
indexes in ADAM, creating 3-26
installing ADAM 3-19
installing ADAM schema snap-in 3-25

L

Ldp.exe 3-23

M

managing directory partitions in ADAM 3-23
Microsoft Exchange, preparing 3-16
Microsoft NLB references 2-8
multi-server multi-site deployments 2-5

N

navigation bar 4-9

P

post-installation procedures 4-13
preparing CallManager 3-8
preparing Cisco Unified Communications Manager 3-8
preparing Enterprise Directory Server 3-10
preparing Microsoft Exchange 3-16
preparing Salesforce.com 3-15
prerequisites 3-18

R

references, Microsoft NLB 2-8

S

Salesforce.com
    ADN 3-15
    preparing 3-15
second partition and indexes, configuring 3-23
setting authentication parameters 4-2
single-server single-site deployments 2-5
support for dual NIC 3-5

V

verifying installation using phones 5-45