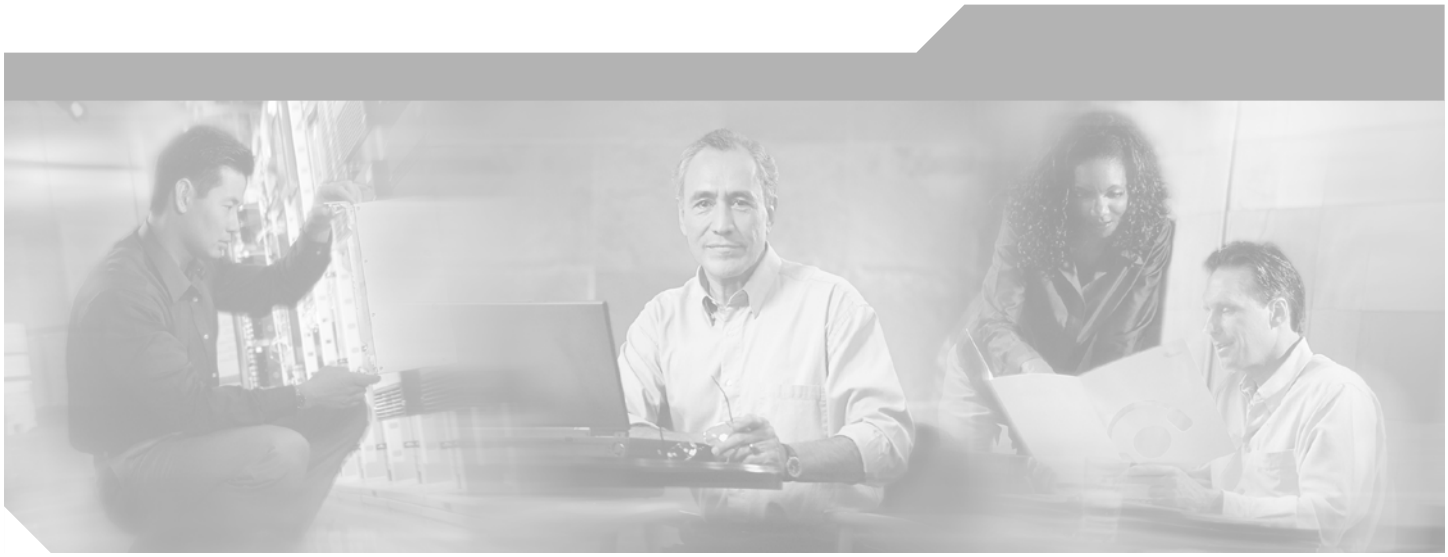


Installation Guide for Cisco Unified Personal Communicator Release 1.1

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

Text Part Number: OL-9190-02

Required notices for open-source software

H.263

UB VIDEO INC. IS THE LICENSOR OF THE UB VIDEO H.263 PROFILE 3 CODEC (ANNEXES I, J, K AND T).

H.264

PORTIONS OF THE H.264 CODEC WERE PROVIDED BY VANGUARD SOFTWARE SOLUTIONS INC 1995-2005 ALL RIGHTS RESERVED

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM

resiprocate, dum - http://www.resiprocate.org

The Vovida Software License v. 1.0

Copyright (c) 2000 Vovida Networks, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The names "VOCAL", "Vovida Open Communication Application Library", and "Vovida Open Communication Application Library (VOCAL)" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact vocal@vovida.org.

4. Products derived from this software may not be called "VOCAL", nor may "VOCAL" appear in their name, without prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NONINFRINGEMENT ARE DISCLAIMED. IN NO EVENT SHALL VOVIDA NETWORKS, INC. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DAMAGES IN EXCESS OF $1,000, NOR FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

ares

Copyright 1998 by the Massachusetts Institute of Technology.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Neon, G.711

neon is an HTTP and WebDAV client library, with a C language API.

Bindings for other languages may also be available, see the web site for more details.

neon is Copyright (C) 1999-2004 Joe Orton <joe@manyfish.co.uk>

Portions are:

Copyright (C) 1999-2000 Tommi Komulainen <Tommi.Komulainen@iki.fi>

Copyright (C) 1999-2000 Peter Boos <pedib@colorfullife.com>

Copyright (C) 1991, 1995, 1996, 1997 Free Software Foundation, Inc.

Copyright (C) 2004 Aleix Conchillo Flaque <aleix@member.fsf.org>

Copyright (C) 2004-2005, Vladimir Berezniker @ http://public.xdi.org/=vmpn

GNU Lesser General Public License (LGPL)

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Library General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library General Public License for more details.

You should have received a copy of the GNU Library General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston,MA 02111-1307, USA

iLBC

Full Copyright Statement

Copyright (C) The Internet Society (2004).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an"AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the IETF's procedures with respect to rights in IETF Documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf- ipr@ietf.org.

AES

Copyright (C) Mok-Kong Shen 2003. mok-kong.shen@t-online.de

Free license:

This work and all modified versions of it may be freely copied, modified, redistributed and used for all legal civilian purposes without formality albeit at licensee's own risk and responsibility, subject to the following conditions:

(1) A copy of this copyright notice with the release history list and the site modification history list must be included in any copy of this work or any modified version of it.

(2) If this work or any modified version of it forms part of a software in object code or binary code, a document for users should accompany the software stating this fact and include this copyright notice as well as an URL of the licensee where the source code of the package in the version actually being used in the software can be found.

(3) Any modification (except dropping of the Supplement) should be appropriately documented in the site modification history list below. The last date of site modification (at the beginning of the package) is to be updated.

(4) In case of non-trivial modifications, i.e. those stemming from efficiency or correctness considerations or from issues of interoperability with other AES implementations, a copy of the modified package is to be immediately sent to the copyright owner at the address above.

(5) Eventual negative or unfavourable consequences and losses or damages of any form to any persons in connection with the use of this work or its modified versions do not constitute any liabilities on the part of the copyright owner.

This free license is unlimited in time [1]. Any attempt of non-compliance with the above terms or any occurence of // their practical unsatisfiability due to whatever reasons, however, automatically terminates the license. Such termination does not affect other licensees who have previously obtained materials from the person with the terminated license but who continue to comply with the above terms.

Other licenses:

Any usages of the contents of the package that don't qualify for a free license as stated in the above require explicit // specific licenses from the copyright owner.

[1] Since copyright grants could be revoked after 35 years (see http://www.copyright.gov/title17/92chap2.html#203), it // could be argued that this license is not timeless for sure On the other hand, the lifespan of AES itself isn't likely to exceed that period. So the issue is not practically relevant in our context.

DES - (http://www.itl.nist.gov/fipspubs/fip46-2.htm)

Cryptographic devices implementing this standard may be covered by U.S. and foreign patents issued to the International Business Machines Corporation. However, IBM has granted nonexclusive, royalty-free licenses under the patents to make, use and sell apparatus which complies with the standard. The terms, conditions and scope of the licenses are set out in notices published in the May 13, 1975 and August 31, 1976 issues of the Official Gazette of the United States Patent and Trademark Office (934 O.G. 452 and 949 O.G. 1717).

MD5

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

SHA1

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns. This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OpenSSL

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.

Libxml2

Except where otherwise noted in the source code (e.g. the files hash.c, list.c and the trio files, which are covered by a similar licence but with different Copyright notices) all the files are:

Copyright (C) 1998-2003 Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights

to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE DANIEL VEILLARD BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of Daniel Veillard shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from him.

NTP

This document and the NTPTime program and source code are all Copyright (c) Tom Horsley, 1997-2004. All rights reserved. The right to unlimited distribution and use of this program is granted to anyone who agrees to keep the copyright notice intact and not alter the program.

Translation: You want changes in the program, make 'em yourself, but don't go distributing the new version with my name on it (or with your name on it either, since you didn't write most of it :-). If there are changes you would like to see distributed, by all means send 'em in to me, and if I like 'em I'll incorporate them in the next version.

expat

The MIT License

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

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.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0601R)

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.

Installation Guide for Cisco Unified Personal Communicator

CONTENTS

Preface

Purpose

This guide describes the installation and configuration tasks on supporting servers that must be completed by a system administrator before deploying the Cisco Unified Personal Communicator application on a Voice-over-IP (VoIP) network.

This guide does not describe how to use the application; see the *User Guide for Cisco Unified Personal Communicator* for this information.

Audience

This guide is intended for the system administrator who is responsible for deploying the application. The administrator should have a thorough understanding of voice and data networking terminology and concepts. This guide is *not* for end users.

Because of the close interaction of this application with Cisco Unified CallManager, Cisco Unified Presence Server, Cisco Unity Connection, and Cisco Unified MeetingPlace Express, many of the tasks in this guide require familiarity with these products.

For changes that occurred to this product after the publication date of this guide, see the release notes at this URL:

http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

The release notes include important information about system requirements, product limitations, restrictions, caveats, and documentation updates.

Organization

Table 1 provides the organization of this guide.

Table 1 Document Organization

Chapter and Title	Description
Chapter 1, "About Cisco Unified Personal Communicator"	Describes the key features of the application and how the application fits into your network.
Chapter 2, "Preparing to Deploy Cisco Unified Personal Communicator"	Describes how to prepare your network before deploying the application.
Chapter 3, "Deploying Cisco Unified Personal Communicator"	Describes how to deploy the application and prepare users for application use.
Chapter 4, "Adding a New User After the Initial Deployment"	Lists the required configuration steps to add a new user with full functionality in Cisco Unified Personal Communicator after the initial deployment of the application

Conventions

Notes, cautions, and timesavers use these conventions and symbols:

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

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

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

Tip Means *the information contains useful tips*.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

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

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

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

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

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

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

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

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.

Reporting Security Problems in Cisco Products

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

- For emergencies only—security-alert@cisco.com

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

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

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

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

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

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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

http://tools.cisco.com/RPF/register/register.do

Note Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting

show command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

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

http://www.cisco.com/techsupport/servicerequest

http://www.cisco.com/techsupport/servicerequest

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

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

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

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

About Cisco Unified Personal Communicator

Cisco Unified Personal Communicator is a desktop application that provides quick access to frequently used communication tools. These communication tools include voice, video, web conferencing, call management, directory access, and presence (knowing that another person is currently online and available for a conversation with other Cisco Unified Personal Communicator users). Cisco Unified Personal Communicator allows users to communicate more effectively, to streamline communications, to increase productivity, and to enhance collaboration.

Topics in this section include:

Features and Benefits

Cisco Unified Personal Communicator integrates a wide set of communication functionality and enables users to:

Communicate more effectively:

- Check the availability of contacts before trying to reach them, thereby reducing the incidence of “phone tag” and improving productivity. Availability information in the application is automatically updated through dynamic presence information from the Cisco Unified Presence Server.
- Set personal reachability information (such as available, busy, away) and preferred method of contact (voice, video, e-mail).
- Search the corporate directory to locate important contacts and to initiate communications.
- Use video and web conferencing to exchange ideas face-to-face, to share content and presentations, and to collaborate more effectively with colleagues. The web portion of the meeting is supported through integration with Cisco Unified MeetingPlace Express. The audio and video portions are supported by Cisco Unified CallManager and Cisco Unified Videoconferencing.
- Play back, view, sort, and delete voice-mail messages in the Cisco Unified Personal Communicator interface through integration with Cisco Unity Connection.
- Exchange ideas face-to-face through a coordinated audio and video call (the video is displayed on the PC screen and the audio occurs through the soft phone).

Streamline communications:

- Find contact information quickly by using Cisco Unified Personal Communicator to search an existing corporate Lightweight Directory Access Protocol (LDAP) directory.
- Click-to-call from the contact list within Cisco Unified Personal Communicator instead of dialing telephone numbers.
- (Mac OS X only) Select the text of a phone number in almost any application and use the OS X **Services** menu (or key combination to that menu) to cause Cisco Unified Personal Communicator to dial the selected number.
- (Mac OS X only) From within the Apple Address Book application, dial phone numbers through Cisco Unified Personal Communicator. This capability is provided through integration with the address book.
- Make calls using the integrated soft phone registered through Cisco Unified CallManager.
- Control the Cisco Unified IP Phone through Cisco Unified Personal Communicator (phone-association mode) and click-to-dial capabilities. The computer telephony interface (CTI) is provided through integration with Cisco Unified CallManager.
- Make calls, place calls on hold, or merge calls (join any two-party call with another call).
- Create an audio session or an ad hoc audio plus video conferencing session easily (merge conversations without calling into a separate conference bridge). Audio and video support are provided through Cisco Unified Videoconferencing.
- View recent communication activities and respond faster. View a list of voice messages on screen through integration with Cisco Unity Connection, and click to play.
- Turn a call into a rich-media conference by adding video or a web-only meeting
- View a list of all participants on a call, eliminating the need to take roll calls.
- Receive pop-up notifications of incoming calls. View the caller ID and the call type (voice only or video call) before answering. Accept the call or divert the call to voice mail.

Related Topics

- How Cisco Unified Personal Communicator Fits into Your Network, page 1-2

How Cisco Unified Personal Communicator Fits into Your Network

Cisco Unified Personal Communicator interacts with these servers and applications as shown in Figure 1-1 on page 1-4:

- Cisco Unified CallManager call-processing system provides telephony features, video, and voice-over-IP capabilities to Cisco Unified Personal Communicator. Through the interaction with Cisco Unified CallManager, Cisco Unified Personal Communicator offers integrated soft-phone capabilities (audio and video) and computer telephony interface (CTI) control of the user's physical Cisco Unified IP Phone. You administer Cisco Unified Personal Communicator as a phone device by using the Cisco Unified CallManager Administration Phone Configuration window.

- Cisco Unified Presence Server delivers a Session Initiation Protocol (SIP) presence engine and a SIP proxy server functionality to Cisco Unified Personal Communicator. The presence engine provides Cisco Unified Personal Communicator with the infrastructure for user and device status information (for example, busy, idle, away) by using SIP Instant Messaging and Presence Leveraging Extensions (SIMPLE).

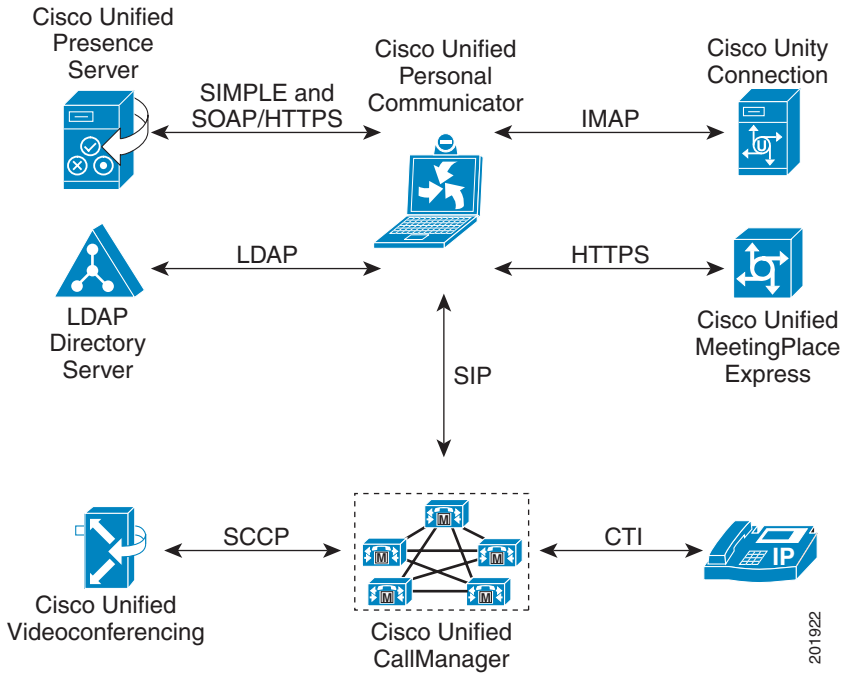
  It stores information about the user's preferred communication type (e-mail, voice, video) and the user's contact list. Cisco Unified Presence Server also maintains login authentication for and provides configuration information to Cisco Unified Personal Communicator by using Simple Object Access Protocol (SOAP) over HTTPS.

  The proxy server provides registration support for nonaudio and nonvideo clients and provides routing support for SIP clients and applications. The Cisco Unified Personal Communicator sends SIP messages to and receives SIP messages from this proxy server, which communicates with Cisco Unified CallManager or other servers. These SIP messages are for soft-phone support, presence information, and database change notifications.
- Cisco Unity Connection enables users to effectively manage communications messages (view, play back, sort, and delete) from within the Cisco Unified Personal Communicator application.
- Cisco Unified MeetingPlace Express provides access to a private, reservationless, web-only meeting for users who are in a Cisco Unified Personal Communicator conversation. Users can launch a web conferencing session at any time to share content, such as presentations, and to facilitate collaboration with others. Cisco Unified MeetingPlace Express does not reserve voice ports for web-only meetings initiated through Cisco Unified Personal Communicator.
- Corporate LDAP version 3 directories interact with Cisco Unified Personal Communicator to provide additional contact information (first name, last name, phone numbers, and so forth) through directory searches for each contact in a user's contact list.
- Cisco Unified Videoconferencing provides audio and video support for merged conference calls (three or more parties) placed through Cisco Unified Personal Communicator.

For information about supported releases for the applications and servers that interact with Cisco Unified Personal Communicator, see the release notes at this URL:

http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

Figure 1-1 How Cisco Unified Personal Communicator Fits into the Network



Related Topics

- Features and Benefits, page 1-1
- Understanding the Startup Process, page 1-4
- Chapter 2, "Preparing to Deploy Cisco Unified Personal Communicator"

Understanding the Startup Process

When Cisco Unified Personal Communicator launches, it performs these operations:

1. It makes a secure (encrypted) connection to the Cisco Unified Presence Server and downloads the user's contact list, network settings, user settings, and portable user preferences. For more information, see the "Network Settings" section on page 1-5, the "User Settings" section on page 1-5, and the "Portable User Preferences" section on page 1-6.
2. The application registers to receive presence information from the server. After it is registered, the application subscribes to receive live presence information for each user in the contact list.
3. If the user's configuration has soft-phone mode enabled, the application starts the soft-phone module and registers with Cisco Unified CallManager for call processing.

   Otherwise, if the user's phone is configured for phone-association mode, the application establishes a CTI connection to Cisco Unified CallManager and takes control of the desk phone, which is designated as the user's preferred CTI device in Cisco Unified Presence Server Administration (**Application > Unified Personal Communicator > User Settings**).
4. The application connects to the Cisco Unity Connection voice-mail server (if deployed), provides this user's credentials, and retrieves the headers of any currently stored voice-mail messages. Cisco Unified Personal Communicator stores the call history locally and records missed calls only if it is running.

5. The application attempts to look up directory information for call records and for the voice-mail messages that have been retrieved and presents the directory results to the user in the Recent pane.
6. When all directory searches are complete, the application stores the contact information for presence and voice mail in memory.
7. For each contact in the user's contact list, the application queries the LDAP directory to obtain information about contacts and phone numbers in the Recent pane.

Related Topics

- Network Settings, page 1-5
- User Settings, page 1-5
- Portable User Preferences, page 1-6

Network Settings

Network settings are needed by all users to access network resources. The application retrieves these network settings (configured in Cisco Unified Presence Server Administration, unless stated otherwise):

- List of servers (Cisco Unified CallManager, Cisco Unity Connection, Cisco Unified MeetingPlace Express, and LDAP) and their addresses, ports, and transport types
- LDAP schema mapping (data definition for the directory)
- LDAP user common name (cn) attribute (for limiting the LDAP search to names)
- LDAP search base (the location where all LDAP users exist) and recursive search flag (specifies whether to perform a recursive search of the directory starting at the search base)
- Bind anonymously to LDAP (specifies whether to use the user's credentials to log in to this LDAP server or to use an anonymous login for read-only access)
- Presence domain name (used for SIP registration in the form of *user@domainname*)
- Application dialing rules and directory lookup dialing rules (configured through the Cisco Unified CallManager Administration)
- Voice-mail pilot number (redirects an incoming call to voice mail)

These settings are read only; Cisco Unified Personal Communicator cannot modify them and write them to the server.

Related Topics

- Understanding the Startup Process, page 1-4
- User Settings, page 1-5
- Portable User Preferences, page 1-6

User Settings

You configure certain settings specific to each user in the Cisco Unified Presence Server and in Cisco Unified CallManager. Similar to the network settings, the application retrieves the user settings from the server, but it can neither modify the configuration nor write it to the server.

The application retrieves these user settings:

- Which phone line (number) the application should control when operating in CTI mode
- Licensing information including which capabilities are enabled

Related Topics

- Understanding the Startup Process, page 1-4
- Network Settings, page 1-5
- Portable User Preferences, page 1-6

Portable User Preferences

The application stores portable user-preference information on the Cisco Unified Presence Server so that the user can log in from any computer and retain various application settings. The application writes preference information to and retrieves preference information from the server. This preference information includes:

- The LDAP directory username and password (required only if nonanonymous bind is configured on the Cisco Unified Presence Server)
- Cisco Unified Presence Server digest password (not visible in the web administration but it is synchronized from Cisco Unified CallManager user configuration)
- Cisco Unity Connection username and password
- Cisco Unified MeetingPlace Express username and password
- User preference information configured through the Preferences window in Cisco Unified Personal Communicator

The contact list is stored on and downloaded from the Cisco Unified Presence Server. The recent communication records (missed, received, and sent, but *not* voice mail) are stored on the client PC's file system and are not stored on the Cisco Unified Presence Server.

Preference information for the Windows OS is stored at this location:

userdrive:\Documents and Settings*username*\Application Data\Cisco\Unified Personal Communicator

where *userdrive* is the local hard drive and *username* is the login name of the logged in user.

All data in the Documents and Settings*username*\Application Data directory is designed to follow the user around if you configure the Windows Roaming Profile option for the user. If the Windows user profile type is roaming, these settings will apply whenever the user logs in under the same Windows account on any other computer. For more information about roaming profiles, see the Microsoft website.

Preference information for the Mac OS X is stored at this location, where ~ is the user's home folder:

- ~/Library/Preferences/Cisco/UnifiedPersonalCommunicator/
- ~/Library/Preferences/com.cisco.CiscoUPC.plist

Related Topics

- Understanding the Startup Process, page 1-4
- Network Settings, page 1-5
- User Settings, page 1-5

CHAPTER 2

Preparing to Deploy Cisco Unified Personal Communicator

This chapter describes how to prepare your network before deploying Cisco Unified Personal Communicator.

Topics in this section include:

Predeployment Overview

This topic provides a high-level overview of the tasks that need to be completed before you deploy Cisco Unified Personal Communicator.

Note Use care when setting user names and passwords. Although passwords do not need to match across all servers, it will be easier for users to correctly configure the Cisco Unified Personal Communicator client if they do. Users cannot change passwords from Cisco Unified Personal Communicator; instead users must follow the password change instructions specific to each server.

Procedure

Step 1 Comply with the network, server, and the client PC requirements that are described in the release notes at this URL:

http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

a. Make sure to use the correct software release for the supported servers.

b. Make sure that you read and understand the system requirements before you proceed with the installation.

Step 2 Install and configure Cisco Unified CallManager.

Cisco Unified CallManager manages the Cisco Unified IP Phones associated with Cisco Unified Personal Communicator and routes and processes calls. Cisco Unified CallManager provides licensing information to Cisco Unified Personal Communicator and provides controls for video conferencing when the Cisco Unified Videoconferencing Multipoint Control Unit (MCU) is installed.

Follow the system configuration overview instructions in the *Cisco Unified CallManager System Guide* and the instructions in the *Cisco Unified CallManager Administration Guide (*or in the Cisco Unified CallManager Administration online help).

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Step 3 Install and configure the Lightweight Directory Access Protocol (LDAP) server by following the instructions that shipped with the server.

The LDAP directory interacts with Cisco Unified Personal Communicator to provide additional contact information (first name, last name, phone numbers, and so forth) through directory searches for each contact in a user's contact list.

Step 4 Install and configure Cisco Unified Presence Server.

Cisco Unified Presence Server provides the client configuration and presence information to Cisco Unified Personal Communicator.

Follow the installation and configuration information at this URL:

http://www.cisco.com/en/US/products/ps6837/prod_installation_guides_list.html

Also follow the instructions in the administration guide (or in the online help in the Cisco Unified Presence Server Administration at this URL:

http://www.cisco.com/en/US/products/ps6837/prod_maintenance_guides_list.html

Step 5 For full functionality of Cisco Unified Personal Communicator, you need to have these products installed and operational:

- Cisco Unity Connection to provide voice-mail retrieval and playback

  See the install and upgrade guides, and the maintain and operate guides at this URL:

  http://www.cisco.com/en/US/products/ps6509/tsd_products_support_series_home.html

  You must configure the Cisco Unified Presence Server to interact with the Cisco Unity Connection server.

- Cisco Unified MeetingPlace Express to provide web conferencing

  See the install and upgrade guides, and the maintain and operate guides:

  http://www.cisco.com/en/US/products/ps6533/tsd_products_support_series_home.html

  You must configure the Cisco Unified Presence Server to interact with the Cisco Unified MeetingPlace Express server.

- Cisco Unified Videoconferencing MCU for video conferencing support when Cisco Unified Personal Communicator is used in soft-phone mode

  See the install and upgrade guides, and the maintain and operate guides at this URL:

  http://www.cisco.com/en/US/products/hw/video/ps1870/tsd_products_support_series_home.html

  You must configure Cisco Unified CallManager to interact with the MCU.

Step 6 Configure each of the servers for use with Cisco Unified Personal Communicator by following the instructions in this chapter.

Related Topics

- How Cisco Unified Personal Communicator Fits into Your Network, page 1-2
- Information to Gather Before Configuring Servers, page 2-3

Information to Gather Before Configuring Servers

Table 2-1 lists the information you need to gather to complete the server configuration tasks in this chapter.

Table 2-1 Information to Gather

Task	Where needed...
Information needed for Cisco Unified CallManager Configuration	
Cisco Unified IP Phone MAC address for each user	Adding Cisco Unified IP Phones to the Cisco Unified CallManager Database, page 2-4
Directory numbers for each user	Adding Cisco Unified IP Phones to the Cisco Unified CallManager Database, page 2-4
Cisco Unified CallManager user names	Adding Cisco Unified Personal Communicator as a Phone Type, page 2-8
Cisco Unified Videoconferencing MCU MAC address	Configuring Videoconferencing Resources, page 2-11
Cisco Unified CallManager MAC address	Licensing, page 2-13
Information needed for Cisco Unified Presence Server Configuration	
LDAP attribute mapping schema	Configuring the LDAP Attribute Map, page 2-23
LDAP server addresses	Specifying LDAP Server Names and Addresses, page 2-25
LDAP server password	Creating LDAP Server Profiles, page 2-26
Cisco Unity Connection server addresses	Specifying Cisco Unity Connection Server Names and Addresses, page 2-27
Cisco Unified MeetingPlace Express server addresses	Specifying Cisco Unified MeetingPlace Express Server Names and Addresses, page 2-29
Computer telephony interface (CTI) gateway server addresses	Specifying CTI Gateway Server Names and Addresses, page 2-31

Cisco Unified CallManager Configuration

This section describes the Cisco Unified CallManager configuration. Topics in this section include:

- Adding Cisco Unified IP Phones to the Cisco Unified CallManager Database, page 2-4 (required)
- Associating the Cisco Unified IP Phone to an End User and Adding the End User to a Group, page 2-5 (required)
- Creating a SIP Phone Security Profile for Cisco Unified Personal Communicator, page 2-7 (required)
- Adding Cisco Unified Personal Communicator as a Phone Type, page 2-8 (required for video soft-phone support)
- Configuring Extension Mobility, page 2-10 (optional)
- Configuring Videoconferencing Resources, page 2-11 (required for video conferencing support)
- Configuring Dialing Rules, page 2-12 (required)
- Licensing, page 2-13 (required)

For information about the supported Cisco Unified CallManager releases, see the release notes at this URL:

http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

Adding Cisco Unified IP Phones to the Cisco Unified CallManager Database

You must add and configure a Cisco Unified IP Phone supported for use with Cisco Unified Personal Communicator to the Cisco Unified CallManager database.

You complete these steps from Cisco Unified CallManager Administration through the **Device > Phone** menu:

Note You can automatically add phones to the Cisco Unified CallManager database by using auto-registration or by manually adding them through the Phone Configuration windows. For more information, see the online help topic “Configuring Cisco Unified IP Phones” in Cisco Unified CallManager Administration.

- Add a Cisco Unified IP Phone (if none exists) for the user. Configure the phone for your environment.
- Configure the phone to interoperate with Cisco Unified Personal Communicator by allowing control of the Cisco Unified IP Phone from the computer telephony interface (CTI). Verify that the **Allow Control of Device from CTI** check box is checked (the default setting).

  If this option is not provided in the Device Information section of the Phone Configuration window, the phone is not supported for use with Cisco Unified Personal Communicator.
- Assign a directory number, and associate this number with the phone.

For detailed instructions, use the Cisco Unified CallManager Administration online help or the *Cisco Unified CallManager Administration Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

For information about phones supported for use with Cisco Unified Personal Communicator, see the release notes at this URL:

http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

You can configure a Cisco Unified IP Phone with the optional features listed in Table 2-2, but these features are not used with Cisco Unified Personal Communicator. For a list of supported phone features, see the "Features and Benefits" section on page 1-1.

Table 2-2 Optional Cisco Unified IP Phones Features

Task	For details, see...[1]
Configure telephony features and settings, including extension mobility for environments where users are not permanently assigned to physical phones[2] (optional).	*Cisco Unified CallManager Administration Guide* *Cisco Unified CallManager Features and Services Guide* "Configuring Extension Mobility" section on page 2-10
Modify phone button templates (softkeys) (optional).	*Cisco Unified CallManager Administration Guide*
Configure Cisco Unified IP Phone services, such as access to stock quotes and weather reports (optional).	*Cisco Unified CallManager Administration Guide* *Cisco Unified CallManager Features and Services Guide*
Set up directories for Quick Search and Dialing Rules features (optional).	*Cisco Unified CallManager Administration Guide*
Add users to Cisco Unified CallManager, and associate users with device IDs for access to the User Options web pages (optional).	*Cisco Unified CallManager Administration Guide*

1. Cisco Unified CallManager documentation is available from the Help menu in the Cisco Unified CallManager Administration and at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
2. When you configure extension mobility, Cisco Unified Personal Communicator users can select the associated desk phone in Cisco Unified Personal Communicator. For more information, see the Cisco Unified Personal Communicator user guide at this URL: http://www.cisco.com/en/US/products/ps6844/products_user_guide_list.html

Related Topics

- Associating the Cisco Unified IP Phone to an End User and Adding the End User to a Group, page 2-5
- Creating a SIP Phone Security Profile for Cisco Unified Personal Communicator, page 2-7

Associating the Cisco Unified IP Phone to an End User and Adding the End User to a Group

After you add the Cisco Unified IP Phone to the Cisco Unified CallManager database and configure it to be controlled from CTI, you must perform these tasks (described in this section):

- Set up the user account, and associate the directory number (primary extension) to the user.
- Associate the phone to the end user.
- Add the end user to the CTI users group.
- Add the end user to a Cisco Unified CallManager user group.

Procedure

Complete these steps from Cisco Unified CallManager Administration:

Step 1 Choose **User Management > End User**.

Step 2 In the Find and List Users window, click **Add New** to add a new user.

Step 3 In the End User Configuration window, enter information for this user.

a. In the User Information section, enter values into the fields.

For details about these fields, see the online help topic "End User Configuration Settings" in Cisco Unified CallManager Administration.

Make sure to configure a digest credential for the user. Any value will work, but do not leave this field blank.

Note To avoid interoperability problems with Cisco Unified Personal Communicator, use care when specifying the username. You will convert it into a soft-phone device name in the "Adding Cisco Unified Personal Communicator as a Phone Type" section on page 2-8. For more information, see Table 2-3 on page 2-9.

b. In the Directory Number Associations section at the bottom of the window, select the primary extension (primary directory number) for this user from the drop-down list.

c. Click **Save**.

Step 4 In the Device Associations section, associate a Cisco Unified IP Phone with this end user by clicking the **Device Association** button.

a. In the User Device Association window, enter the MAC address of the phone for this user prefixed with SEP, and click **Find**.

b. Select the user's phone from the list (should be the only phone returned), and click **Save Selected/Changes** at the bottom of the page.

Step 5 Add the end user to the CTI users group:

a. Choose **User Management > User Group**.

b. In the search field of the Find and List User Groups window, enter **Standard CTI Enabled**, and click **Find**.

This is a standard group that is created when Cisco Unified CallManager installs.

c. Click the **Standard CTI Enabled** group to open the User Group Configuration window.

d. Click the **Add End Users to Group** button.

e. In the Find and List Users window, search for a user by using the search options, select the user's check box, and click **Add Selected**.

Step 6 Follow the instructions in Step 5, but search for the **Standard CCM End Users** group, and add the end user to this group.

Step 7 Click **Save**.

Related Topics

- Creating a SIP Phone Security Profile for Cisco Unified Personal Communicator, page 2-7
- Adding Cisco Unified Personal Communicator as a Phone Type, page 2-8

Creating a SIP Phone Security Profile for Cisco Unified Personal Communicator

Because the Cisco Unified Personal Communicator does not support Transport Layer Security (TLS) in Cisco Unified CallManager, you must configure a SIP security profile and then associate this profile when you add Cisco Unified Personal Communicator as a phone type.

Procedure

Complete these steps from Cisco Unified CallManager Administration:

Step 1 Choose **System > Security Profile > Phone Security Profile**.

Step 2 In the Find and List SIP Phone Security Profiles window, click **Add New**.

Step 3 In the Phone Security Profile Information section, enter settings for these fields:

a. In the Name field, enter a name for this security profile.

To ensure that you apply the correct profile to the device, include the device model in the security profile name.

b. In the Description field, enter a security profile description.

c. In the Nonce Validity Time field, enter the number of seconds that the nonce is valid.

The default value equals 600 (10 minutes). When the time expires, Cisco Unified CallManager generates a new value.

A nonce value is a random number that supports digest authentication and is used to calculate the MD5 hash of the digest authentication password.

d. For Device Security Mode, choose **Non Secure**.

No security features except image authentication exist for the phone. A TCP connection opens to Cisco Unified CallManager.

e. For Transport Type, choose **TCP + UDP**, **TCP**, or **UDP**.

Choose **TCP + UDP** if you want to use a combination of TCP and UDP.

Choose **TCP** to ensure that packets are received in the same order that they are sent. This protocol ensures that no packets get dropped.

Choose **UDP** to ensure that packets are received quickly. This protocol, which can drop packets, does not ensure that packets are received in the order that they are sent.

None of these settings provides security.

f. Check **Enable Digest Authentication** to enable SIP authentication.

Check this box if you want Cisco Unified CallManager to challenge the identity of the phone when it sends a request to Cisco Unified CallManager. After Cisco Unified CallManager challenges the identity, the phone responds with a MD5 checksum, and Cisco Unified CallManager verifies the information based on the credentials that you configured in Cisco Unified CallManager Administration. If the credentials match, digest authentication of the phone is successful.

You specified the digest authentication credentials in the End User window in Cisco CallManager Administration in the "Associating the Cisco Unified IP Phone to an End User and Adding the End User to a Group" section on page 2-5. To associate the credentials with the phone after you configure the user, you choose a Digest User and an end user in the Phone Configuration window.

g. None of the settings in the Phone Security Profile CAPF Information section apply to Cisco Unified Personal Communicator. You can use any value.

h. For Phone Port, enter the port number that you want Cisco SIP IP Phones to use to listen for SIP messages from Cisco Unified CallManager. The default is 5060.

Step 4 Click **Save**.

Step 5 If you want this user to have only a presence-enabled directory with desk phone control through Cisco Unified Personal Communicator, skip these configuration sections:

- "Adding Cisco Unified Personal Communicator as a Phone Type" section on page 2-8
- "Configuring Videoconferencing Resources" section on page 2-11
- "Video Telephony Camera Configuration" section on page 2-35

Proceed to the "Configuring Dialing Rules" section on page 2-12.

Adding Cisco Unified Personal Communicator as a Phone Type

To enable Cisco Unified Personal Communicator soft-phone features, you must manually create a new soft-phone device per user. The auto-registration features in Cisco Unified CallManager are not supported for use with Cisco Unified Personal Communicator. Completing this procedure causes three device licenses to be consumed.

Procedure

Complete these steps from Cisco Unified CallManager Administration:

Step 1 Choose **Device > Phone**.

Step 2 In the Find and List Phones window, click **Add New**.

Step 3 In the Add a New Phone window, in the Phone Type drop-down list, select **Cisco Unified Personal Communicator**, and click **Next**.

Step 4 In the Phone Configuration window, in the Device Information section, perform these steps:

a. In the Device Name field, specify the soft-phone device name according to these guidelines:

- It must match the user name.
- It must start with *UPC*.
- It must contain the letters A through Z and numerals 0 through 9, ignoring all other characters.
- It can contain 12 additional characters after *UPC*.

See Table 2-3 for examples.

Table 2-3 Username Conversion for Cisco Unified Personal Communicator Soft-Phone Device

Cisco Unified CallManager Username	Associated Soft-Phone Device Name
jjackson	UPCJJACKSON
johnnie_jackson	UPCJOHNNIEJACKS
johnniejackson	UPCJOHNNIEJACKS
john.jackson	UPCJOHNJACKSON

Note As shown in Table 2-3, the usernames *johnnie_jackson* and *johnniejackson* translate to the same soft-phone device name and are said to collide. You must take care to create usernames that will not result in a collision when the soft-phone device name is configured. If Cisco Unified Personal Communicator is unable to derive its soft-phone device name, it will not be able to properly register and will not function as expected. You might have to reconfigure a user to use a name other than their normal username to avoid this problem.

b. In the Description field, enter the purpose of the phone; for example, Richard's soft phone.

c. Configure all required fields for your environment.

d. For Owner User ID, select the user ID from the drop-down list.

e. Make sure to uncheck **Allow Control of Device from CTI** to disable CTI to control and monitor this device.

Step 5 In the Protocol Specific Information section, perform these steps:

a. For Presence Group, select **Standard Presence Group**.

b. For SIP Phone Security Profile, select the security profile from the drop-down list that you created in the "Creating a SIP Phone Security Profile for Cisco Unified Personal Communicator" section on page 2-7.

c. For SIP Profile, select **Standard SIP Profile** to specify the default SIP profile. SIP profiles provide specific SIP information for the phone such as registration and keepalive timers, media ports, and do-not-disturb control.

d. For Digest User, select the user ID. It should be the same as that selected for the Owner User ID.

Step 6 Click **Save**.

The Phone Configuration window redisplays with the new information. Verify that the status shown at the top of the page indicates a successful save. If an error is displayed, the most common problems result from incorrectly formatted device names or the failure to specify a mandatory parameter.

Step 7 In the Association Information pane that displays on the left side of the window, click the **Add a New DN** link.

Step 8 In the Directory Number Information section, enter the directory number and route partition for the Cisco Unified Personal Communicator that are the same as the ones used by the Cisco Unified IP Phone for this user.

This configuration causes the Cisco Unified Personal Communicator to share the line with the Cisco Unified IP Phone for this user.

Step 9 For the Line 1 on Device *Device-Name* section, for the Display (Internal Caller ID), enter a string (20 characters maximum) as the callerID; for example, *Richard Jonnes*. This string is displayed as the callerID on phones that are called.

Step 10 In the Multiple Call/Call Waiting Settings on Device section, perform these steps:

a. In the Maximum Number of Calls field, type **2** to specify the maximum number of calls that can be presented to Cisco Unified Personal Communicator.

b. In the Busy Trigger field, type **2** to specify the number after which an incoming call receives a busy signal.

   For example, if you answer a call and then receive another call, you can put the first call on hold and answer the second. If a third person tries to call you, Cisco Unified CallManager enforces the busy limit; it sees that there are already two calls in process and responds to the third caller with a busy signal.

Step 11 Click **Save**.

Ensure that the status shown at the top of the page indicates a successful save and that the resulting status is *Ready*.

Cisco Unified CallManager reminds you that changes to line or directory number settings require a restart. However, a restart is required only when you edit lines on Cisco Unified IP Phones that are up and running at the time of the modifications.

Related Topics

- Configuring Videoconferencing Resources, page 2-11
- Configuring Videoconferencing Resources, page 2-11
- Video Telephony Camera Configuration, page 2-35

Configuring Extension Mobility

Use the extension mobility feature to allow users to configure a Cisco Unified IP Phone as their own, on a temporary basis, by logging in to that phone. After a user logs in, the phone adopts the user individual user default device profile information, including line numbers, speed dials, services links, and other user-specific phone properties.

For example, when user A occupies a desk and logs in to the phone, that user's directory numbers, services, speed dials, and other properties appear on that phone. But when user B uses the same desk at a different time, user B's information appears. The extension mobility feature dynamically configures a phone according to the current user.

By using extension mobility, Cisco Unified Personal Communicator users can associate this application with one of several desk phones.

Procedure

Step 1 Make sure to remove all devices from the user's phone association list (if any) in Cisco Unified CallManager Administration (choose **Device > Phone** and access the Directory Number Configuration window).

This action also removes the Preferred CTI Device selection in Cisco Unified Presence Server Administration (**Application > Unified Personal Communicator > User Settings** window).

Step 2 Follow the Cisco Unified CallManager extension mobility configuration information in the *Cisco Unified CallManager Features and Services Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

When you create the device user profile (**Device > Device Settings > Device Profile**), make sure that it is controllable by CTI (along with the line).

When you add the Cisco Unified IP Phone to Cisco Unified CallManager (**Device > Phone**), make sure that is controllable by CTI as described in "Adding Cisco Unified IP Phones to the Cisco Unified CallManager Database" section on page 2-4.

Configuring Videoconferencing Resources

You can enable Cisco Unified Personal Communicator soft-phone users to have merged conference calls (three or more parties) with audio and video support.

Procedure

Complete these tasks:

Step 1 Install a supported videoconferencing server.

For information about the servers supported for use with Cisco Unified Personal Communicator, see the release notes at this URL:

http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

For installation information, see this URL:

http://www.cisco.com/en/US/products/hw/video/ps1870/tsd_products_support_series_home.html

Step 2 In Cisco Unified CallManager Administration, configure the media resources:

- Add the video conference bridge to Cisco Unified CallManager by choosing the **Media Resources > Conference Bridge** menu.

  You need the MAC address of the videoconference bridge to complete this task.
- Create a media resource group list, and add the video conference bridge to it by choosing the **Media Resources > Media Resource Group List** menu.
- Create a media resource group, and add a media resource to it by choosing the **Media Resources > Media Resource Group** menu.

For detailed configuration instructions, use the Cisco Unified CallManager Administration online help or the *Cisco Unified CallManager Administration Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Related Topics

- Adding Cisco Unified Personal Communicator as a Phone Type, page 2-8
- Video Telephony Camera Configuration, page 2-35

Configuring Dialing Rules

Based on your company's dial plan and the information stored in the LDAP directory (telephone number for the end user), you might need to define application dialing rules and directory dialing rules through the Cisco Unified CallManager routing information administration pages. The Cisco Unified Presence Server queries Cisco Unified CallManager to obtain these dialing rules for the Cisco Unified Personal Communicator.

These rules define how Cisco Unified Personal Communicator can reformat the inbound call ID to be used as a directory lookup key and how to transform a phone number retrieved from the LDAP directory for outbound dialing.

Application dial rules automatically strip numbers from or add numbers to telephone numbers that the user dials. For example, you can configure a dial rule that automatically adds the digit 9 in front of a 7-digit telephone number to provide access to an outside line. Application dial rules are used to manipulate numbers that are dialed from Cisco Unified Personal Communicator. You configure these dial rules through Cisco Unified CallManager Administration from the **Call Routing > Dial Rules > Application Dial Rules** menu.

Directory lookup rules transform caller identification numbers into numbers that can be looked up in the directory from Cisco Unified Personal Communicator. Each rule specifies which numbers to transform based on the beginning digits and length of the number. For example, you can create a directory lookup rule that automatically removes the area code and two prefix digits from a 10-digit telephone, which would transform 4089023139 into 23139. You configure these dial rules through Cisco Unified CallManager Administration from the **Call Routing > Dial Rules > Directory Lookup Dial Rules** menu.

Before Cisco Unified Personal Communicator places a call through contact information, it removes everything from the phone number to be dialed except for letters and digits. It transforms the letters to digits and applies the dialing rules it obtains from Cisco Unified Presence Server. The letter-to-digit mapping is locale specific and corresponds to the letters found on a standard telephone keypad for that locale (for example, for an US English locale, 1800-GOTMILK transforms to 18004686455).

Users cannot view or modify transformed numbers before Cisco Unified Personal Communicator places them. If there is a problem with the dialed number because of mistransformations, you must correct the dialing rules so that the attempted dialed number will work.

For detailed conceptual and task-based information on dial rules, see the Cisco Unified CallManager Administration online help or the *Cisco Unified CallManager Administration Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

For dial-plan details, deployment, and installation of these dial plans for certain countries other than North America, see this URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/idp/dpdep502.htm

You can download Cisco Unified CallManager Dial Plan applications at this URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/IDP50

Licensing

Cisco Unified CallManager Administration tracks the number of Cisco Unified Personal Communicator devices that are connected to it and compares it with the number of device licenses that have been purchased.

You can configure Cisco Unified Personal Communicator in these ways:

- Base functionality—This configuration provides a user with a presence-enabled directory with desk phone control.

  Two devices licenses are required: one for Cisco Unified Personal Communicator user enablement and one for Cisco Unified Presence Server enablement.

- Base plus soft-phone functionality—In addition to the base capabilities, you can configure Cisco Unified Personal Communicator as a video soft phone.

  Five device licenses units are required: one for Cisco Unified Personal Communicator user enablement, one for Cisco Unified Presence Server enablement, and three for the soft-phone enablement.

Topics in this section include:

Obtaining a License File

When you place an order for Cisco devices, Cisco provides a Product Authorization Key (PAK). The PAK provides the software activation key and the license file.

To obtain the license files for Cisco Unified Personal Communicator, follow the instructions in the Cisco Unified CallManager Administration online help or the *Cisco Unified CallManager Administration Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

- After you enter the MAC address of the Cisco Unified CallManager server for which you are requesting the licenses and a valid e-mail ID, enter the number of nodes and devices for which you want licenses.

  To determine the number of device licenses that you need, use the license unit calculator in Cisco Unified CallManager Administration (**System > Licensing > License Unit Calculator**).

- After the license is uploaded, assign capabilities to users. See the "Assigning Capabilities to Users" section on page 2-14.

Related Topics

Uploading a License File

After you obtain the license file, you must copy it to your local machine and then upload it to the server.

To upload the Cisco Unified Personal Communicator license file to Cisco Unified CallManager, use the **System > Licensing > License File Upload** menu, and follow the instructions in the Cisco Unified CallManager Administration online help or the *Cisco Unified CallManager Administration Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

License files must have a *.lic* suffix.

Related Topics

- Obtaining a License File, page 2-13
- Assigning Capabilities to Users, page 2-14

Assigning Capabilities to Users

After the Cisco Unified Personal Communicator license files are uploaded, you must assign the capabilities to existing users in the Cisco Unified CallManager database.

Note You must upload the license file before you can assign capabilities to users. For more information, see the "Uploading a License File" section on page 2-14.

Procedure

Complete these steps from Cisco Unified CallManager Administration:

Step 1 Choose **System > Licensing > Capabilities Assignment**.

Step 2 In the Find and List Capabilities Assignments window, click **Find** to display a list of all users.

Step 3 In the search results section, click the user's link to display the Capabilities Assignment Configuration window.

Tip To assign capabilities to more than one user, select multiple user check boxes, and click **Bulk Assignment**.

Step 4 Check **Enable UPS** to enable the user to log in to Cisco Unified Presence Server. (One device license is consumed.)

Step 5 Check **Enable UPC** to enable Cisco Unified Personal Communicator to obtain presence information for the contact list from Cisco Unified Presence Server. (One device license is consumed.)

If you completed the "Adding Cisco Unified Personal Communicator as a Phone Type" section on page 2-8, three device licenses are consumed per user for video soft-phone capabilities.

Step 6 Click **Save**.

Related Topics

- Viewing the License Report, page 2-15

Viewing the License Report

You can display the license report from Cisco Unified CallManager Administration by choosing **System > Licensing > License Unit Report**. The report lists the number of authorized, used, and remaining licenses.

To determine the number of license unit that are required for Cisco Unified Personal Communicator, choose **System > Licensing > License Unit Calculator**.

Related Topics

- Obtaining a License File, page 2-13
- Uploading a License File, page 2-14

LDAP Server Configuration

The LDAP directory interacts with Cisco Unified Personal Communicator to provide contact information through directory searches.

Note Make sure the LDAP server is installed *before* attempting LDAP-specific configuration on the Cisco Unified Presence Server.

Procedure

Step 1 Purchase a supported LDAP directory server.

For information about the supported LDAP directory servers, see the release notes at this URL:

http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

Step 2 Install the server and software according to the manufacturer's instructions.

For Microsoft Active Directory, see the "Configuring Microsoft Active Directory for Anonymous Queries" section on page 2-15. See the Microsoft Active Directory documentation for complete information.

Step 3 Perform the LDAP-specific configuration on the Cisco Unified Presence Server:

- Configuring the LDAP Attribute Map, page 2-23 (required)
- Specifying LDAP Server Names and Addresses, page 2-25 (required)
- Creating LDAP Server Profiles, page 2-26 (required)

Configuring Microsoft Active Directory for Anonymous Queries

This section describes how to configure Microsoft Active Directory 2000 and 2003 for anonymous queries.

By default, anonymous LDAP operations are not permitted in Active Directory. This means that an attempt to perform anonymous search in Active Directory results in the server requesting authenticated connection to LDAP and refusing the query. Therefore, some additional configuration on the Active Directory server and the Cisco Unified Presence Server are required to make anonymous queries work.

Topics in this section include:

- Assigning Permissions, page 2-16 (required)
- Inheriting Permissions from the Parent Object, page 2-17 (required)
- Configuring Additional Information for Microsoft Active Directory 2003, page 2-18 (required)
- Verifying Permissions for Microsoft Active Directory, page 2-19 (required)
- Configuring Cisco Unified Presence Server LDAP Settings for Microsoft Active Directory, page 2-19 (required)

Assigning Permissions

To enable anonymous queries, you must grant Anonymous Logon access to user objects that need to be located by anonymous search. Table 2-4 lists the rights that must be given to all user objects to enable anonymous search.

Table 2-4 Anonymous Permissions

User Object	Permissions	Inheritance	Permission Type
ANONYMOUS LOGON	List Contents	This object and all child objects	Object
ANONYMOUS LOGON	Read name	This object and all child objects	Property
ANONYMOUS LOGON	Read Name	This object and all child objects	Property
ANONYMOUS LOGON	Read objectClass	This object and all child objects	Property

Note The strings and images are specific to the Windows 2000 server. There might be minor GUI changes for other Windows servers.

Procedure

To assign permissions for Active Directory 2000 and 2003, complete these steps:

Step 1 Launch ADSIEDIT (from **Start > Run**, enter **ADSIEDIT.msc**).

If ADSIEDIT is not installed on your server, manually install it from the Windows server CD.

Step 2 In the left panel, navigate to the user container, right-click it, and view properties.

Normally, in the CN=Users Properties window, the user container is CN=Users, DC=*domain name*, DC=com. If the user objects are present in different containers, repeat the procedure on each of the containers.

Step 3 Click the **Security** tab, and then click the **Advanced** button.

Step 4 In the Access Control Settings for Users window, click **Add**.

Step 5 If this is a Windows 2000 server, a User List window displays. Select **Anonymous Logon**, and click **OK**.

or

If this is a Windows 2003 server, a Select User window displays, prompting you to enter the object name. Enter **Anonymous Logon**, and click **OK**.

Step 6 In the Permission Entry for Users window, click the **Object** tab, and set these values:

- For Apply Onto, select **This Object and All Child Objects**.
- In the Permissions list, check **Allow** for List Contents.

Step 7 Click the **Properties** tab, and set these values:

- For Apply Onto, select **This Object and All Child Objects**.
- Click **Clear All** to clear permissions (if any are already set).
- In the Permissions list, check **Allow** for Read name, Read Name, and Read objectClass.
- Check **Apply These Permissions to Objects and/or Containers Within this Container Only**.

Step 8 Click **OK** to close the Permission Entry for Users window.

The Access Control Settings for Users window now has four Anonymous Logon permissions.

Step 9 Click **Apply**, then **OK** twice to close the Properties window.

Related Topics

- Inheriting Permissions from the Parent Object, page 2-17

Inheriting Permissions from the Parent Object

The permissions applied for the user container affect all the user objects within that container. But some users, especially administrator users, might not inherit these permissions. In this situation, you must explicitly configure those users to inherit permissions from the parent object.

Procedure

To make the user inherit permissions from parent object in Active Directory 2000 and 2003, complete these steps:

Step 1 Launch the ADSIEDIT (from **Start > Run**, enter **ADSIEDIT.msc**), and navigate to the user container.

Step 2 Select the user, right-click, and view properties.

The Properties window displays.

Step 3 In the Properties window, click the **Security** tab, and then click the **Advanced** button.

Step 4 Check **Allow Inheritable Permissions from Parent to Propagate to this Object**.

Step 5 Click **Apply** and then **OK** to close the windows.

Related Topics

- Configuring Additional Information for Microsoft Active Directory 2003, page 2-18
- Verifying Permissions for Microsoft Active Directory, page 2-19

Configuring Additional Information for Microsoft Active Directory 2003

Windows 2003 servers require certain additional configuration to enable anonymous queries.

Procedure

To enable anonymous queries on Windows 2003 servers, complete these additional steps:

Step 1 Launch ADSIEdit (from **Start > Run**, enter **ADSIEDIT.msc**).

Step 2 Navigate to CN=Directory Service, CN= Windows NT, CN = Services, CN= Configuration, DC=*domain name*, DC=com.

Step 3 Right-click the CN=Directory Service container, click **Properties**, and scroll to the dsHeuristics attribute.

Note The Properties window varies for various Windows 2003 servers. On certain servers, you might see a list box for properties instead of a selection box.

Step 4 In Edit Attribute field, enter **0000002** if the dsHeuristics attribute is not already set.

The seventh character (2) controls the way you can bind to the LDAP service.

If, instead of 2, the character is 0 or absent, it means that anonymous LDAP operations are disabled. Setting the seventh character to 2 permits anonymous operations.

Note If the attribute already contains a value, make sure you are changing only the seventh character from the left. This is the only character that needs to be changed to enable anonymous binds.

For example, if the current value is 0010000, change it to 0010002.

If the current value is less than 7 characters, add zeros followed by 2; for example, 001 becomes 0010002.

Step 5 Click **Apply** and then **OK** to close the window.

Related Topics

- Verifying Permissions for Microsoft Active Directory, page 2-19
- Configuring Cisco Unified Presence Server LDAP Settings for Microsoft Active Directory, page 2-19

Verifying Permissions for Microsoft Active Directory

After you complete the permission configuration, you should verify it.

Procedure

To verify permissions for Microsoft Active Directory 2000 and 2003, complete these steps.

Step 1 Launch ADSIEDIT (from **Start > Run**, enter **ADSIEDIT.msc**).

Step 2 In the left panel, navigate to the user container, find the user name. Right click to view the Properties window.

Step 3 On the Properties window, select the **Security** tab, and then click the **Advanced** button.

The Access Control Settings for the user appear.

Step 4 On the **Permissions** tab, sort by name.

You should see four Anonymous Logon entries. The first entry should have the List Contents permission, and the other three entries should have the Read Property permissions.

If this is not the case, check **Allow Inheritable Permissions to Propagate to this Object**.

Step 5 Click **Apply** and then **OK** to close the windows.

Related Topics

- Configuring Cisco Unified Presence Server LDAP Settings for Microsoft Active Directory, page 2-19

Configuring Cisco Unified Presence Server LDAP Settings for Microsoft Active Directory

After you configure Microsoft Active Directory for anonymous queries, you must complete other LDAP-specific configuration on the Cisco Unified Presence Server.

Procedure

Complete these tasks from Cisco Unified Presence Server Administration:

Step 1 Set up the LDAP attribute map with this mapping:

- LastName = SN
- UserID = sAMAccountName

For more information, see the "Configuring the LDAP Attribute Map" section on page 2-23.

Step 2 Follow the instructions in the "Specifying LDAP Server Names and Addresses" section on page 2-25 and include these steps:

a. Match the port number setting in Cisco Unified Presence Server with that used on the Active Directory LDAP server. The default is 389.

If the server is Global Catalogue, enter **3268** as the port number.

b. For protocol, select **TCP** if the Global Catalogue server is used.

Step 3 In Cisco Unified Presence Server Administration, configure the LDAP server profile.

Follow the instructions in the "Creating LDAP Server Profiles" section on page 2-26 and include these steps:

a. In the LDAP Directory Information section, make sure to:
   - Leave the Bind Distinguished Name field blank.
   - Leave the Password field blank.
   - Check **Anonymous Bind**.

b. In the LDAP Search Context Information section, specify the search context. Set O and OU (OU must contain users; for example, ou=users,dc=cisco,dc=com).

   For Microsoft Active Directory, cn=users,DC=EFT-LA,DC=cisco,DC=com.

   The search base should include all users of Cisco Unified Personal Communicator.

c. In the LDAP Server Information section, select the primary and backup servers that you configured in the "Specifying LDAP Server Names and Addresses" section on page 2-25.

Cisco Unity Connection Configuration

Cisco Unity Connection provides the voice-mail features described in the "Features and Benefits" section on page 1-1 to Cisco Unified Personal Communicator.

Procedure

Step 1 Install a supported release of Cisco Unity Connection.

For information about the supported releases, see the release notes at this URL:

http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

Step 2 In Cisco Unity Connection Administration, enable Internet Mail Access Protocol (IMAP) client access to voice messages for users associated with a class of service.

a. Expand **Class of Service** in the left pane, and then click **Class of Service**.

b. On the Search Class of Service window, in the Search Results table, click the display name of the applicable class of service.

c. On the Edit Class of Service window, under Licensed Features, check **Allow Users to Access Voice Mail Using an IMAP Client**.

d. Select **Allow Users to Access Message Bodies** so that users have access to the entire voice mail.

e. Click **Save**.

For more information, see the *Cisco Unity Connection User Moves, Adds, and Changes Guide* at this URL:

http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html

Step 3 Set up an account on the Cisco Unity Connection server for each Cisco Unified Personal Communicator user with a voice mailbox.

Make sure that the user ID and the password used for logging in to Cisco Unity Connection are the same as the ones you created in the Cisco Unified CallManager for each Cisco Unified Personal Communicator user.

For information about setting up the account, see the *Cisco Unity Connection User Moves, Adds, and Changes Guide* at this URL:

http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html

Step 4 Configure a new e-mail account to enable Cisco Unified Personal Communicator users to access Cisco Unity Connection voice messages from their IMAP client application. For more information, see the *Cisco Unity Connection User Setup Guide* at this URL:

http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html

Step 5 Perform the Cisco Unity Connection server-specific configuration on the Cisco Unified Presence Server:

- Specifying Cisco Unity Connection Server Names and Addresses, page 2-27
- Creating Cisco Unity Connection Server Profiles, page 2-28

Cisco Unified MeetingPlace Express Configuration

Cisco Unified MeetingPlace Express provides Cisco Unified Personal Communicator users with the ability to escalate to a web-only meeting from within an existing audio or video communication session. Cisco Unified MeetingPlace Express does not reserve voice ports for web-only meetings initiated through Cisco Unified Personal Communicator.

For detailed Cisco Unified MeetingPlace Express-specific information for the integration with Cisco Unified Personal Communicator, managing certificates, creating user profiles, and for call-control integration, see the configuration and maintenance guide at this URL:

http://www.cisco.com/en/US/products/ps6533/prod_maintenance_guides_list.html

Procedure

Complete these tasks to enable web-only meetings to be initiated from Cisco Unified Personal Communicator:

Step 1 Install a supported release of Cisco Unified MeetingPlace Express.

For information about the supported releases, see the release notes at this URL:

http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

Step 2 Through Cisco Unified MeetingPlace Express Administration Center, install enough web-conferencing licenses on Cisco Unified MeetingPlace Express to accommodate both the full web meetings that are initiated from Cisco Unified MeetingPlace Express and the web-only meetings that are initiated from Cisco Unified Personal Communicator.

Step 3 If not already enabled, enable the Secure Sockets Layer (SSL) encryption technology on the Cisco Unified MeetingPlace Express server by obtaining and uploading the required certificates from a trusted certificate authority (CA).

The certificate is required for secure communications between Cisco Unified Personal Communicator and Cisco Unified MeetingPlace Express.

Step 4 Set up a user profile on the Cisco Unified MeetingPlace Express server for each Cisco Unified Personal Communicator user who might initiate web-only meetings from a Cisco Unified Personal Communicator conversation.

Make sure to set the **Method of Attending** to **I'll Call In** for users who might initiate web-only meetings; otherwise, the Cisco Unified MeetingPlace Express system will try to contact the user who clicked the **Escalate to Web Conference** button in Cisco Unified Personal Communicator. Make sure to tell users not to change this Cisco Unified MeetingPlace Express setting.

You do not need to create a Cisco Unified MeetingPlace Express profile for Cisco Unified Personal Communicator users who attend web meetings. They join the web meeting as guests, and a password is not needed.

Tip As an alternative, you can configure the Administrative XML Layer Simple Object Access Protocol (AXL SOAP) authentication on Cisco Unified CallManager to simplify Cisco Unified MeetingPlace Express user profile administration. With this configuration, the Cisco Unified Personal Communicator meeting initiator needs a Cisco Unified CallManager profile instead of a Cisco Unified MeetingPlace Express user profile. With AXL authentication, when the initiator requests a meeting for the first time through Cisco Unified Personal Communicator, a Cisco Unified MeetingPlace Express profile is automatically created for the initiator.

Step 5 Change the network configuration so that inbound calls from the public switched telephone network (PSTN) to Cisco Unified Personal Communicator support RFC2833.

- For inbound calls, Cisco Unified Personal Communicator requires RFC2833 support if these calls require dual tone multifrequency (DTMF) digit collection. Inbound calls to the client will not be answered with key press markup language (KPML) support.

  A typical inbound call scenario is when Cisco Unified MeetingPlace calls the user as a conference is being set up. In this situation, if the inbound call from the PSTN supports RFC2833, the Cisco Unified Personal Communicator user can join the meeting by using the session dial pad.
- For outbound calls, Cisco Unified Personal Communicator supports both KPML and RFC2833 digit collection.

Step 6 Perform the Cisco Unified MeetingPlace Express server-specific configuration on the Cisco Unified Presence Server:

- Specifying Cisco Unified MeetingPlace Express Server Names and Addresses, page 2-29
- Creating Cisco Unified MeetingPlace Express Server Profiles, page 2-30

Cisco Unified Presence Server Configuration

This section describes the Cisco Unified Presence Server configuration needed for Cisco Unified Personal Communicator. Cisco Unified Presence Server provides client configuration and presence information to Cisco Unified Personal Communicator. For information about the supported Cisco Unified Presence Server releases, see the release notes at this URL:

http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

Topics in this section include:

Configuring the LDAP Attribute Map

You must configure the LDAP attribute map through the Cisco Unified Presence Server. You enter LDAP attributes for your environment, which map to the given Cisco Unified Personal Communicator attribute names.

Procedure

Complete these steps from Cisco Unified Presence Server Administration:

Step 1 Choose **Application > Unified Personal Communicator > Settings** to display the Cisco Unified Personal Communicator Settings window.

Step 2 In the LDAP Attribute Map section, for each Cisco Unified Personal Communicator attribute name (contact schema), enter the corresponding LDAP user object attribute into the LDAP field. Table 2-5 lists the Cisco Unified Personal Communicator attribute names, the default LDAP attribute names, and provides a place for you to enter the corresponding attributes for your directory.

Change any default LDAP attribute name if it does not match with your LDAP directory. Ensure that an LDAP attribute is paired to only one Cisco Unified Personal Communicator attribute.

For information on LDAP settings for Microsoft Active Directory, see the "Configuring Microsoft Active Directory for Anonymous Queries" section on page 2-15.

Table 2-5 LDAP Attribute Map

UPC Attribute Name	LDAP Attribute Name (default)	Your LDAP Attribute Name
UID	employeenumber	
LastName[1]	sn	
Nickname[1]	nickname	
Photo	jpegPhoto	
DisplayName	displayName	
NameSuffix		

Table 2-5 LDAP Attribute Map (continued)

UPC Attribute Name	LDAP Attribute Name (default)	Your LDAP Attribute Name
BusinessEMail	mail	
BusinessPhoneNumber[1]	telephoneNumber	
BusinessMobilePhone	mobile	
BusinessFax	facsimileTelephoneNumber	
HomeEMail		
HomeFax		
FirstName[1]	givenName	
MiddleName	initials	
UserID[1]	uid	
Title	title	
NamePrefix		
Gender		
IM		
BusinessVoiceMail	voicemail	
BusinessPager	pager	
BusinessOtherPhone		
HomeMobilePhone		
URL	labeledURI	

1. For maximum performance (faster LDAP searches in Cisco Unified Personal Communicator), make sure to index these attributes. For information on how to enable indexing, see your LDAP server documentation.

For information about mapping the UserID attribute, see the "Rules for Mapping the UserID Attribute" section on page 2-24.

The values are global to all LDAP server hosts.

Step 3 Click **Save**.

Related Topics

- Rules for Mapping the UserID Attribute, page 2-24
- Rules for a Displayed Contact Name, page 2-25
- Photo Attributes and Format, page 2-25
- Specifying LDAP Server Names and Addresses, page 2-25

Rules for Mapping the UserID Attribute

The UPC UserID attribute in the LDAP attribute map in Table 2-5 must match the Cisco Unified CallManager user ID.

This mapping is required for a contact in LDAP to be added to the Contact list in Cisco Unified Personal Communicator. This field associates the LDAP user with the associated user on Cisco Unified CallManager and Cisco Unified Presence Server.

Rules for a Displayed Contact Name

These rules determine how a name is displayed as a contact in Cisco Unified Personal Communicator:

- If the end user edits a contact name in Cisco Unified Personal Communicator (**Actions > Edit Contact Nickname**), display this name.
- If you configured an LDAP attribute for DisplayName, display this name.
- If you configured an LDAP attribute for Nickname, display this name with the last name.
- Otherwise, display the configured LDAP attributes for the first and last names in the Contact pane.
- If you did not configure LDAP attributes for the FirstName and LastName, display the LDAP UserID or the Cisco Unified Presence Server user ID in the Contact pane.

Photo Attributes and Format

By default, Cisco Unified Personal Communicator uses the *jpegPhoto* LDAP attribute, which is present in the Windows 2003 Active Directory schema. By contrast, the Windows 2000 Active Directory uses the *thumbnailPhoto* attribute. You can change the field in which Cisco Unified Personal Communicator looks for the photo through the LDAP attribute map in Cisco Unified Presence Server administration described in the "Configuring the LDAP Attribute Map" section on page 2-23.

You cannot configure the Cisco Unified Presence Server, Cisco Unified Personal Communicator, or the Windows Active Directory with image URLs because the image data must be stored in Active Directory as a base-64 encoded JPEG binary object.

You can use any application that supports storing photos to LDAP servers; for example, http://phpldapadmin.sourceforge.net/.

For the photo to be displayed in the contact details in Cisco Unified Personal Communicator, the user must have permission to read it; that is, the Read/List All attributes on the subtree must be correct. You set this through the AD Directory Administrator tool or through ADSI EDIT.

Specifying LDAP Server Names and Addresses

You must specify the LDAP server names, addresses ports, and protocol types on Cisco Unified Presence Server so that Cisco Unified Personal Communicator can interact with them.

Procedure

Complete these steps from Cisco Unified Presence Server Administration:

Step 1 Choose **Application > Unified Personal Communicator > LDAP Server**.

Step 2 In the Find and List LDAP Hosts window, click **Add New** to add a new server.

Step 3 In the LDAP Host Configuration window, enter information into the fields:

a. For the Name field, enter the name of the server. It is limited to 128 characters.

b. (Optional) For the Description field, enter a description of the server. It is limited to 128 characters. You can enter alphanumeric characters, spaces, and these characters: !#$'()*+,./:;=?@^_`{|}~-

c. For the Hostname/IP Address field, enter an IP address or a fully qualified domain name for the server.

d. For the Port field, enter **389** as the port number used by the LDAP server.

   Check the LDAP server documentation or the LDAP server configuration for this information.

e. For the Protocol Type drop-down list, select **TCP** as the protocol to use when contacting this server.

Step 4 Click **Save**.

You can add more servers, select all servers, delete selected servers, clear all selections, and adjust the number of rows displayed on the page.

Related Topics

- Creating LDAP Server Profiles, page 2-26

Creating LDAP Server Profiles

You must create an LDAP server profile on the Cisco Unified Presence Server to configure primary and backup servers for redundancy and to add users to the profile. The LDAP server profile also has LDAP directory configuration settings and search context information.

Procedure

Complete these steps from Cisco Unified Presence Server Administration:

Step 1 Choose **Application > Unified Personal Communicator > LDAP Profile**.

Step 2 In the Find and List LDAP Profiles window, click **Add New** to add a new profile and to display the LDAP Profile Configuration window.

Step 3 In the LDAP Profile Information section, enter information into the fields:

a. In the Name field, enter the profile name limited to 128 characters.

b. (Optional) In the Description field, enter a description limited to 128 characters. You can enter alphanumeric characters, spaces, and these characters: !#$'()*+,./:;=?@^_`{|}~-

Step 4 In the LDAP Directory Information section, enter information into the fields:

a. In the Bind Distinguished Name field, enter the administrator-level account information limited to 128 character s in the form *useraccount*@*domain*.**com**.

   This is the distinguished name with which you bind for authenticated bind.

b. In the Password field, enter the LDAP bind password (the password for the administrator-level account that you provided in the Bind Distinguished Name string) so users can access this LDAP server.

   Enter the same password in the Confirm Password field. The password is limited to 128 characters.

c. After configuring Cisco Unified Presence Server for authenticated bind with the LDAP server, you must configure the LDAP server for anonymous permissions and anonymous login so that all directory information (name, number, mail, fax, home number, and so forth) is passed to the Cisco Unified Personal Communicator client. For more information, see the "Configuring Microsoft Active Directory for Anonymous Queries" section on page 2-15.

d. (Optional) Select **Anonymous Bind** so that users can log in anonymously to this LDAP server for read-only access.

   Deselect this check box to use the user credentials to log in to this LDAP server.

Step 5 In the LDAP Search Context Information section, enter information into the fields:

a. (Optional) In the Search Context field, enter the location where all LDAP users exist. This location is a container or directory. The name is limited to 256 characters.

b. (Optional) Select **Recursive Search** to perform a recursive search of the directory starting at the search base.

Step 6 In the LDAP Server Information section, select the primary LDAP server and optional backup servers from the drop-down lists.

Only servers you specified in the "Specifying LDAP Server Names and Addresses" section on page 2-25 appear in the primary and backup server drop-down lists.

Step 7 Click **Add Users to Profile**.

Step 8 In the Find and List Users window, click **Find** to populate the search results fields, or search for a specific user, and then click **Find**.

Step 9 Select users by clicking their check boxes, and add them to this profile by clicking **Add Selected**.

You can add more users, select all users, delete selected users, clear all selections, and adjust the number of rows displayed on the page.

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

If you want to create another profile, click **Add New**. If you want to delete the profile, click **Delete**.

Related Topics

- Changing Application Profiles on a Per-User Basis, page 2-34

Specifying Cisco Unity Connection Server Names and Addresses

You must specify Cisco Unity Connection server names, addresses, ports, and protocol types on the Cisco Unified Presence Server so that Cisco Unified Personal Communicator can interact with them.

Procedure

Complete these steps from Cisco Unified Presence Server Administration:

Step 1 Choose **Application > Unified Personal Communicator > Unity Connection Server**.

Step 2 In the Find and List Unity Connection Hosts window, click **Add New** to add a new server.

Step 3 In the Unity Connection Host Configuration window, enter information into the fields:

a. For the Name field, enter the name of the server. It is limited to 128 characters.

b. (Optional) For the Description field, enter a description of the server. It is limited to 128 characters. You can enter alphanumeric characters, spaces, and these characters: !#$'()*+,./:;=?@^_`{|}~-

c. For the Hostname/IP Address field, enter an IP address or a fully qualified domain name for the server.

d. For the Port field, specify the port number configured for the server. Enter **143**.

e. For the Protocol Type drop-down list, select **TCP** as the protocol to use when contacting this server.

Step 4 Click **Save**.

You can add more servers, select all servers, delete selected servers, clear all selections, and adjust the number of rows displayed on the page.

Related Topics

- Creating Cisco Unity Connection Server Profiles, page 2-28

Creating Cisco Unity Connection Server Profiles

You must create a Cisco Unity Connection server profile on the Cisco Unified Presence Server to configure primary and backup servers for redundancy and to add users to the profile.

Procedure

Complete these steps from Cisco Unified Presence Server Administration:

Step 1 Choose **Application > Unified Personal Communicator > Unity Connection Profile**.

Step 2 In the Find and List Unity Connection Profiles window, click **Add New** to add a new profile.

Step 3 In the Unity Connection Profile Configuration window, enter information into the fields.

a. For the Name field, enter the profile name limited to 128 characters.

b. (Optional) For the Description field, enter a description of the profile limited to 128 characters. You can enter alphanumeric characters, spaces, and these characters: !#$'()*+,./:;=?@^_`{|}~-

c. (Optional) Select an option from the Voice Messaging Pilot drop-down list.

With this setting, the software obtains the directory number (pilot number) for the voice-mail system (if any) to which unanswered calls are redirected.

- *Number*—Use the default voice-mail pilot for the system per the configuration in Cisco Unified CallManager Administration from the **Voice Mail > Voice Mail Pilot** menu.

  The voice-mail pilot number is the directory number that a user dials to access their voice messages. Cisco Unified CallManager automatically dials the voice-messaging number when a user presses the Messages button on their phone. Each pilot number can belong to a different voice-messaging system.

- **No Voice Mail**—Disable sending an unanswered incoming call to voice mail.

d. From the Primary Unity Connection Server and the Backup Unity Connection Server drop-down lists, select a primary server and backup servers.

Only servers you specified in the "Specifying Cisco Unity Connection Server Names and Addresses" section on page 2-27 appear in the primary and backup server drop-down lists.

Step 4 Click **Add Users to Profile**.

Step 5 In the Find and List Users window, click **Find** to populate the search results fields, or search for a specific user, and then click **Find**.

Step 6 Select users by clicking their check boxes, and add them to this profile by clicking **Add Selected**.

You can add more users, select all users, delete selected users, clear all selections, and adjust the number of rows displayed on the page.

Step 7 Click **Save** to save the profile.

If you want to create another profile, click **Add New**. If you want to delete the profile, click **Delete**.

Related Topics

- Changing Application Profiles on a Per-User Basis, page 2-34

Specifying Cisco Unified MeetingPlace Express Server Names and Addresses

You must specify the Cisco Unified MeetingPlace Express server names, addresses, ports, and protocol types on the Cisco Unified Presence Server so that Cisco Unified Personal Communicator can interact with them.

Procedure

Complete these steps from Cisco Unified Presence Server Administration:

Step 1 Choose **Application > Unified Personal Communicator > MeetingPlace Express Server**.

Step 2 In the Find and List MeetingPlace Express Hosts window, click **Add New** to add a new server.

Step 3 In the MeetingPlace Express Host Configuration window, enter information into the fields:

a. For the Name field, enter the name of the server. The limit is 128 characters.

b. (Optional) For the Description field, enter a description of the server. The limit is 128 characters. You can enter alphanumeric characters, spaces, and these characters: !#$'()*+,./:;=?@^_`{|}~-

c. For the Hostname/IP Address field, enter an IP address or a fully qualified domain name for the server.

d. For the Port field, specify the port number configured for the server. Enter **80** for HTTP, and enter port **443** for HTTPS.

e. For the Protocol drop-down list, specify the protocol to use when contacting this server.

- **HTTP**: selects Hypertext Transfer Protocol as the standard method for transferring data between the server and the browser. Choose this option if the Cisco Unified MeetingPlace Express server *does not have* SSL enabled.
- **HTTPS**: selects Hypertext Transfer Protocol over SSL as the method for securely transferring data between the server and the browser. Choose this option if the Cisco Unified MeetingPlace Express server has SSL enabled.

Step 4 Click **Save**.

You can add more servers, select all servers, delete selected servers, clear all selections, and adjust the number of rows displayed on the page.

Related Topics

- Creating Cisco Unified MeetingPlace Express Server Profiles, page 2-30

Creating Cisco Unified MeetingPlace Express Server Profiles

You must create a Cisco Unified MeetingPlace Express server profile on the Cisco Unified Presence Server to configure primary and backup servers for redundancy and to add users to the profile.

Note By contrast, a profile in Cisco Unified MeetingPlace Express defines the privileges and preferences configured for a specific user in this application.

Procedure

Complete these steps from Cisco Unified Presence Server Administration:

Step 1 Choose **Application > Unified Personal Communicator > MeetingPlace Express Profile**.

Step 2 In the Find and List MeetingPlace Express Profiles window, click **Add New** to add a new profile.

The MeetingPlace Express Profile Configuration window redisplays.

Step 3 In the MeetingPlace Express Profile Configuration window, enter information into the fields.

a. For the Name field, enter the profile name limited to 128 characters.

b. (Optional) For the Description field, enter a description of the profile limited to 128 characters. You can enter alphanumeric characters, spaces, and these characters: !#$'()*+,./:;=?@^_`{|}~-

c. From the Primary MeetingPlace Express Server and the Backup MeetingPlace Express Server drop-down lists, select a primary server and backup servers.

Only servers you specified in the "Specifying Cisco Unified MeetingPlace Express Server Names and Addresses" section on page 2-29 appear in the primary and backup server drop-down lists.

Step 4 Click **Add Users to Profile**.

Step 5 In the Find and List Users window, click **Find** to populate the search results fields, or search for a specific user, and then click **Find**.

Step 6 Select users by clicking their check boxes, and add them to this profile by clicking **Add Selected**.

You can add more users, select all users, delete selected users, clear all selections, and adjust the number of rows displayed on the page.

Step 7 Click **Save** to save the profile.

If you want to create another profile, click **Add New**. If you want to delete the profile, click **Delete**.

Related Topics

- Changing Application Profiles on a Per-User Basis, page 2-34

How Participants Join the Web-Only Meeting

For information about how participants add web conferencing to their conversation sessions (join the web-only meeting), see the *User Guide for Cisco Unified Personal Communicator* at this URL:

http://www.cisco.com/en/US/products/ps6844/products_user_guide_list.html

Related Topics

- Participant Privileges and Meeting Controls, page 2-31

Participant Privileges and Meeting Controls

Cisco Unified Personal Communicator meeting participants join the web meeting as guests. Guests do *not* require a Cisco Unified MeetingPlace Express profile or a password to attend web meetings that are initiated from Cisco Unified Personal Communicator.

All participants have presenter privileges and can share data if the Cisco Unified MeetingPlace Express Presenter Add-In is installed.

For information about installing the Presenter Add-In, see the user guide for Cisco Unified MeetingPlace Express at this URL:

http://www.cisco.com/en/US/products/ps6533/products_user_guide_list.html

For information about supported and unsupported Cisco Unified MeetingPlace Express meeting controls, see the release notes at this URL:

http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

For a description of the characteristics of a web conference that you add to a Cisco Unified Personal Communicator conversation, see the user guide for Cisco Unified Personal Communicator at this URL:

http://www.cisco.com/en/US/products/ps6844/products_user_guide_list.html

For an overview of the meeting room (and what users can expect to see in a web-only meeting) and for information about presenting and working with shared content, see the user guide for Cisco Unified MeetingPlace Express at this URL:

http://www.cisco.com/en/US/products/ps6533/products_user_guide_list.html

Related Topics

- How Participants Join the Web-Only Meeting, page 2-30

Specifying CTI Gateway Server Names and Addresses

The CTI gateway, which is the CTIManager component of Cisco Unified CallManager, provides desk phone control (phone-association mode) to Cisco Unified Personal Communicator users. The CTIManager program is installed when Cisco Unified CallManager is installed.

You must specify CTI gateway server names, addresses, ports, and protocol types on the Cisco Unified Presence Server so that the information for reaching the CTI gateway server can be downloaded when the end user logs in to Cisco Unified Personal Communicator.

Cisco Unified Presence Server dynamically creates a TCP-based CTI gateway host profile based on the *hostname* of Cisco Unified CallManager. Before using this profile, verify that the Cisco Unified Presence Server and Cisco Unified Personal Communicator clients can ping Cisco Unified CallManager by its DNS name. If they cannot reach the server, you need to add a new server based on the *IP address* of Cisco Unified CallManager as described in the next procedure. You do not need to delete the automatically created host profiles.

As an alternative, if you configure Cisco Unified CallManager with an IP address through the Cisco Unified CallManager Administration **System > Server** menu, Cisco Unified Presence Server will dynamically create a TCP-based CTI gateway host profile for that address. The fields in Cisco Unified Presence Server Administration (**Application > Unified Personal Communicator > CTI Gateway Server**) are automatically populated, and you do not need to perform this procedure. Proceed to the "Creating CTI Gateway Server Profiles" section on page 2-32 to add users to this profile.

Procedure

Complete these steps from Cisco Unified Presence Server Administration:

Step 1 Choose **Application > Unified Personal Communicator > CTI Gateway Server**.

Step 2 In the Find and List CTI Gateway Hosts window, click **Add New** to add a new server.

Step 3 In the CTI Gateway Host Configuration window, enter information into the fields:

a. For the Name field, enter the name of the server. The limit is 128 characters.

b. (Optional) For the Description field, enter a description of the server. The limit is 128 characters. You can enter alphanumeric characters, spaces, and these characters: !#$'()*+,./:;=?@^_`{|}~-

c. For the Hostname/IP Address field, enter an IP address or a fully qualified domain name of the Cisco Unified CallManager server that is running the CTI service.

d. For the Port field, enter **2748** as the port number configured for the server.

e. For the Protocol Type drop-down list, select **TCP** as the protocol to use when contacting this server.

Step 4 Click **Save**.

You can add more servers, select all servers, delete selected servers, clear all selections, and adjust the number of rows displayed on the page.

Related Topics

- Creating CTI Gateway Server Profiles, page 2-32

Creating CTI Gateway Server Profiles

You must create a CTI gateway server profile on the Cisco Unified Presence Server to configure primary and backup servers for redundancy and to add users to the profile.

Cisco Unified Presence Server dynamically creates a TCP-based CTI gateway server profile based on the *hostname* of Cisco Unified CallManager. Before using this profile, verify that Cisco Unified Presence Server and Cisco Unified Personal Communicator clients can ping Cisco Unified CallManager by its DNS name. If they cannot reach the server, you need to add a new server based on the *IP address* of Cisco Unified CallManager as described in the next procedure. You do not need to delete the automatically created host profiles.

As an alternative, if you configure Cisco Unified CallManager with an IP address through the Cisco Unified CallManager Administration **System > Server** menu, Cisco Unified Presence Server dynamically creates a TCP-based CTI gateway server profile based on that address. The fields in Cisco Unified Presence Server Administration (**Application > Unified Personal Communicator > CTI Gateway Profile**) are automatically populated, and you need only to add users to the default CTI TCP profile that is created (see Step 4).

Procedure

Complete these steps from Cisco Unified Presence Server Administration:

Step 1 Choose **Application > Unified Personal Communicator > CTI Gateway Profile**.

Step 2 In the Find and List CTI Gateway Profiles window, click **Add New** to add a new profile.

Step 3 In the CTI Gateway Profile Configuration window, enter information into the fields.

a. For the Name field, enter the profile name limited to 128 characters.

b. (Optional) For the Description field, enter a description of the profile limited to 128 characters. You can enter alphanumeric characters, spaces, and these characters: !#$'()*+,./:;=?@^_`{|}~-

c. From the Primary CTI Gateway Server and the Backup CTI Gateway Server drop-down lists, select a primary server and backup servers.

Only servers you specified in the "Specifying CTI Gateway Server Names and Addresses" section on page 2-31 appear in the primary and backup server drop-down lists.

Step 4 Click **Add Users to Profile**.

Step 5 In the Find and List Users window, click **Find** to populate the search results fields, or search for a specific user, and then click **Find**.

Step 6 Select users by clicking their check boxes, and add them to this profile by clicking **Add Selected**.

You can add more users, select all users, delete selected users, clear all selections, and adjust the number of rows displayed on the page.

Step 7 Click **Save** to save the profile.

If you want to create another profile, click **Add New**. If you want to delete the profile, click **Delete**.

Related Topics

- Changing Application Profiles on a Per-User Basis, page 2-34

Creating SIP Proxy Server Profiles

You must create a SIP proxy server profile on the Cisco Unified Presence Server to configure primary and backup servers for redundancy and to add users to the profile. The Cisco Unified Personal Communicator sends SIP messages to and receives SIP messages from this proxy server, which communicates with Cisco Unified CallManager or other servers.

Procedure

Complete these steps from Cisco Unified Presence Server Administration:

Step 1 Choose **Application > Unified Personal Communicator > Proxy Profile**.

Step 2 In the Find and List Proxy Profiles window, click **Add New** to add a new profile.

Step 3 In the Proxy Profile Configuration window, enter information into the fields.

a. For the Name field, enter the profile name limited to 128 characters.

b. (Optional) For the Description field, enter a description of the profile limited to 128 characters. You can enter alphanumeric characters, spaces, and these characters: !#$'()*+,./:;=?@^_`{|}~-

c. For Proxy Listener, select **Default Cisco SIP Proxy TCP Listener** from the drop-down list.

With this setting, Cisco Unified Personal Communicator uses TCP to communicate with the proxy server.

Do not select **Default Cisco SIP Proxy UDP Listener**. For more information, see the "Important Notes" section in the release notes at this URL:

http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

d. For the Primary Proxy Server and the Backup Proxy server (optional), select a primary and a backup server from the drop-down lists.

These servers were configured during the Cisco Unified Presence Server installation from the **System > Server** menu.

Step 4 Click **Add Users to Profile**.

Step 5 In the Find and List Users window, click **Find** to populate the search results fields, or search for a specific user, and then click **Find**.

Step 6 Select users by clicking their check boxes, and to add them to this profile by clicking **Add Selected**.

You can add more users, select all users, delete selected users, clear all selections, and adjust the number of rows displayed on the page.

Step 7 Click **Save** to save the profile.

If you want to create another profile, click **Add New**. If you want to delete the profile, click **Delete**.

Related Topics

- Changing Application Profiles on a Per-User Basis, page 2-34

Changing Application Profiles on a Per-User Basis

You can change individual application profiles on a per-user basis. Application profiles are not required; it is possible that some Cisco Unified Personal Communicator users might not have a Cisco Unity Connection or a Cisco Unified MeetingPlace Express profile. In this situation, the drop-down selection displays **None**.

Prerequisites

You must first create the server profile before you can modify the user settings as described in these sections:

- Creating LDAP Server Profiles, page 2-26
- Creating Cisco Unity Connection Server Profiles, page 2-28
- Creating Cisco Unified MeetingPlace Express Server Profiles, page 2-30
- Creating CTI Gateway Server Profiles, page 2-32
- Creating SIP Proxy Server Profiles, page 2-33

Procedure

Complete these steps from Cisco Unified Presence Server Administration:

Step 1 Choose **Application > Unified Personal Communicator > User Settings**.

Step 2 In the Unified Personal Communicator User Settings Find and List window, click **Find** to populate the search results fields, or search for a specific user, and then click **Find**.

Step 3 Select the user by clicking their link.

Step 4 In the CTI Control Information section, assign the preferred CTI device from the drop-down list to this user.

The preferred CTI device is the MAC address of the user's primary desk phone in the form of *SEPxxxxxxxxxxx*. You must select this address whether or not the user intends to use the application only in soft-phone mode. The preferred CTI device is the device that the end user wants to control when in phone-association (desk phone) mode.

If the user does not specify a preferred device in Cisco Unified Personal Communicator, the one you specify as the preferred CTI device in Cisco Unified Presence Server is used.

Step 5 In the Application Profile Information section, decide which application profile to change for this user.

If you change a user application profile in this window (for example, change from Unity Profile 1 to Unity Profile 2), the change is reflected in **Application > Unified Personal Communicator > Unity Connection Profile** window.

If a user does not have an application profile for a specific server, select **None**.

Step 6 Click **Save**.

Firewall Configuration

Frequently used by corporations and educational institutions for increased security, firewalls work by blocking certain Internet traffic from entering or leaving a network.

Internet traffic moves through a firewall based on service identification numbers that are known as *ports*. Certain ports must be open for Cisco Unified Personal Communicator to work. Network administrators typically open a minimal number of network ports, allowing the traffic for approved applications to enter and leave the network while blocking other network traffic.

If users have a software firewall installed on their PCs or if there is a hardware firewall in the network between the Cisco Unified Presence Server and Cisco Unified Personal Communicator, you must configure the firewall to pass Cisco Unified Personal Communicator traffic. Failure to do so will result in missing, incorrect, or intermittent reachability status displayed in Cisco Unified Personal Communicator. For information about the network ports used by Cisco Unified Personal Communicator, see the release notes at this URL:

http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

Video Telephony Camera Configuration

You can configure users for point-to-point and for multipoint videoconferencing support.

Procedure

Step 1 Distribute video telephony (VT) cameras supported for use with Cisco Unified Personal Communicator to users. For more information, see the release notes at this URL:

http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

Step 2 Configure users for soft-phone use. For more information, see the "Adding Cisco Unified Personal Communicator as a Phone Type" section on page 2-8.

Step 3 Set up videoconferencing resources in Cisco Unified CallManager. For more information, see the "Configuring Videoconferencing Resources" section on page 2-11.

Step 4 Provide end users with the appropriate documentation to complete the installation:

- *Cisco VT Camera Quick Start Guide* (for use with Windows-based PC clients)

  http://www.cisco.com/en/US/products/sw/voicesw/ps5662/prod_installation_guides_list.html
- *iSight User Guide* (for use with Macintosh-based PC clients)

  http://www.apple.com/support/manuals/
- See the "Providing Information to End Users" section on page 3-4.

Headsets and Other Audio Devices Configuration

You or the end user should install and configure any audio devices that require drivers, such as sound cards or USB headsets. Follow the headset instructions that are supplied with the headset.

For information on establishing the audio device and the control panel settings, see the user guide for Cisco Unified Personal Communicator at this URL:

http://www.cisco.com/en/US/products/ps6844/products_user_guide_list.html

For information about supported headsets and other audio devices, see the release notes at this URL:

http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

Related Topics

- Use of Third-Party Headsets with Cisco Unified Personal Communicator, page 2-36

Use of Third-Party Headsets with Cisco Unified Personal Communicator

While Cisco does perform basic testing of third-party headsets for use with the Cisco Unified Personal Communicator application, it is ultimately the customer's responsibility to test this equipment in their own environment to determine suitable performance. Because of the many inherent environmental and hardware inconsistencies in the locations where this application is deployed, there is not a single *best* solution that is optimal for all environments.

Before customers begin deploying any headsets (especially deployment in quantity) in their production network, Cisco recommends thorough testing at the customer site to check for voice quality issues, especially hum and echo.

The primary reason that support of a headset would be inappropriate for an installation is the potential for an audible hum. This hum can either be heard by the remote party or by both the remote party and this application user. Causes for this humming sound range from electrical lights near the PC to the PC power source itself. In some cases, a hum heard on a headset plugged directly into the PC Universal Serial Bus (USB) port might be reduced or eliminated by using a powered USB hub.

In some instances, the mechanics or electronics of various headsets can cause remote parties to hear an echo of their own voice when they speak to Cisco Unified Personal Communicator users. The application user will not be aware of this echo.

Finally, some analog headsets do not match the electrical characteristics for which some soundcards are designed. The microphones on such headsets are frequently too sensitive, even when the input levels in Cisco Unified Personal Communicator are reduced to their lowest values. The users of such headsets will sound distorted to remote parties.

It is important to ask Cisco Unified Personal Communicator users whether a particular headset sounds good to them. In addition, remote parties should be queried as to the reception from this application when using a particular headset.

Related Topics

- Headsets and Other Audio Devices Configuration, page 2-36

CHAPTER 3

Deploying Cisco Unified Personal Communicator

This chapter describes how to deploy Cisco Unified Personal Communicator. Topics in this section include:

Before beginning the deployment tasks, be sure to read Chapter 2, "Preparing to Deploy Cisco Unified Personal Communicator." It describes the tasks that you need to perform before deployment.

Deciding Which Installer Package to Use

You can deploy Cisco Unified Personal Communicator by using the installer packages listed in Table 3-1:

Table 3-1 Installer Packages

Filename	Description
CiscoUnifiedPersonalCommunicatorSetupK9.exe	This executable contains the required Windows Installer engine, Cisco VT Camera and Cisco VT Camera II drivers, the user interface, and a set of related DLLs[1] for deployment. This package is typically used for individual users installing the application.
CiscoUnifiedPersonalCommunicatorSetupK9.msi	This Microsoft Windows Installer (MSI) package contains Cisco VT Camera and Cisco VT Camera II drivers, the user interface, and a set of related DLLs for deployment. This package is typically used by IT administrators with the corporate deployment tool (for example, Altiris, System Management Server (SMS), and Active Directory) to push the install to end users.
CiscoUnifiedPersonalCommunicator-K9.dmg	This package is the disk image (.dmg) of the application for Mac OS X.

1. DLL = dynamic link libraries

Related Topics

- Deploying the Application in an Apple Macintosh Environment, page 3-2
- Deploying the Application in a Microsoft Windows Environment, page 3-2

Deploying the Application in an Apple Macintosh Environment

In a Macintosh environment, download the disk image (.dmg) from Cisco.com and put it on an internal server so that users can download it from that location. Alternately, you can burn the disk image on a CD for internal distribution.

The end user must complete the installation of Cisco Unified Personal Communicator, and they should follow the instructions in the Cisco Unified Personal Communicator user guide at this URL:

http://www.cisco.com/en/US/products/ps6844/products_user_guide_list.html

Related Topics

Updating the Application, page 3-4

Deploying the Application in a Microsoft Windows Environment

This section describes how to deploy the application in a Windows environment. Topics in this section include:

- Deploying to a Shared Location, page 3-2
- Using the Installer on the Client PC, page 3-2
- Using a Software Deployment Tool, page 3-3
- Setting Up the Problem Report Support Alias for the Windows Installer, page 3-3
- Updating the Application, page 3-4

Deploying to a Shared Location

You can deploy the executable or MSI package to a shared location, such as a web server, where users can access it. You must push the installer at an elevated privilege so that users can complete the installation (run the installer and follow the installation wizard).

Related Topics

- Deciding Which Installer Package to Use, page 3-1
- Setting Up the Problem Report Support Alias for the Windows Installer, page 3-3
- Providing Information to End Users, page 3-4

Using the Installer on the Client PC

You can deploy either the executable or the MSI package directly to the client PC. You must push the installer at an elevated privilege so that users can complete the installation (run the installer and follow the installation wizard).

You can also perform the installation operation directly on an individual's computer while logged in as the administrator.

Related Topics

- Deciding Which Installer Package to Use, page 3-1
- Setting Up the Problem Report Support Alias for the Windows Installer, page 3-3
- Providing Information to End Users, page 3-4

Using a Software Deployment Tool

You can use a software deployment tool to distribute Cisco Unified Personal Communicator to client PCs. Software deployment tools include group policy-based tools, such as Active Directory, or more advanced tools, such as the System Management Server (SMS) software from Microsoft.

To use this method, you must push the installer at an elevated privilege so that users can complete the installation (run the installer and follow the installation wizard).

Note Cisco Unified Personal Communicator does not support the *advertising* or *publishing* deployment in which a user installs the application by opening an icon that the administrator has placed on the user's desktop.

Related Topics

- Deciding Which Installer Package to Use, page 3-1
- Setting Up the Problem Report Support Alias for the Windows Installer, page 3-3
- Providing Information to End Users, page 3-4

Setting Up the Problem Report Support Alias for the Windows Installer

Cisco Unified Personal Communicator for the Window OS is equipped with the Cisco Unified Problem Reporting Tool. You (and end users) can use it to automate the collection of information necessary to troubleshoot problems on the Cisco Unified Personal Communicator PC client. The tool generates a report that can be saved to client PC desktop or automatically e-mailed to the support alias of your choice.

By default, the application is deployed *without* the support alias configured.

You set the support alias at the time the application is deployed or installed:

- For the MSI package that is deployed through a software deployment tool, use this command:

  userdrive:\CiscoUnifiedPersonalCommunicatorSetupK9.msi /qb PROBLEMREPORTMAILER=email@*your-support-alias*

- For the executable (.exe), enter this command on each user's PC:

  userdrive:\CiscoUnifiedPersonalCommunicatorSetupK9.exe /s /v" /qb PROBLEMREPORTMAILER=email@*your-support-alias*"

If you do not set the support alias, the error report is saved to the client PC desktop.

For more information, see the Cisco Unified Personal Communicator troubleshooting guide at this URL:

http://cisco.com/en/US/products/ps6844/prod_troubleshooting_guides_list.html

Updating the Application

You can download the latest available Cisco Unified Personal Communicator software from the Software Center:

http://www.cisco.com/public/sw-center/sw-voice.shtml

You must have an account on Cisco.com to access this site.

After you obtain updated software, you need to make the updated software available for deployment as described in these sections:

- Deploying the Application in an Apple Macintosh Environment, page 3-2
- Deploying the Application in a Microsoft Windows Environment, page 3-2

Note In a Windows OS environment, command-line options are not supported on upgrades. They are supported only on new installations.

In a Windows environment, users can uninstall the previous version of Cisco Unified Personal Communicator through the **Control Panel,** but it is not required. The camera drivers are removed only if Cisco Unified Personal Communicator is the last Cisco application on the client PC; that is, if Cisco Unified Video Advantage is not installed.

In a Macintosh environment, users should uninstall the previous version of Cisco Unified Personal Communicator by dragging the application icon to the Trash. Users should also drag the address book plug-in to the Trash. For more information, see the Cisco Unified Personal Communicator user guide at this URL:

http://www.cisco.com/en/US/products/ps6844/products_user_guide_list.html

Providing Information to End Users

After Cisco Unified Personal Communicator is deployed, provide the information listed in Table 3-2 to end users.

Table 3-2 Information Needed by End Users

Provide This	Explanation	Give to Users Who Install	Give to Users If You Install
Information about client hardware and software requirements.	Leverage information from the release notes at this URL: http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html	Yes	Yes
Location of Cisco Unified Personal Communicator installer.	Provide the shared folder location or the CD with the software executable.	Yes	No

Table 3-2 Information Needed by End Users (continued)

Provide This	Explanation	Give to Users Who Install	Give to Users If You Install
Instructions for installing and setting up the application.	Provide the user guide for Cisco Unified Personal Communicator. http://www.cisco.com/en/US/products/ps6844/products_user_guide_list.html Direct users to read the introduction chapter for the installation and set-up information.	Yes	No
Login information.	Provide this information: • User name. • Password. You configured the username and password in Cisco Unified CallManager Administration. See the "Associating the Cisco Unified IP Phone to an End User and Adding the End User to a Group" section on page 2-5. • Cisco Unified Presence Server host name or IP address.	Yes	Yes
User capabilities (presence, video soft phone) available through Cisco Unified CallManager licenses.	Provide each user with information about the capabilities (license) they have. You assigned capabilities in Cisco Unified CallManager Administration in the "Assigning Capabilities to Users" section on page 2-14.	Yes	Yes
Supported features: directory services, voice-mail retrieval and playback, access to web-only meetings, and Cisco Unified CallManager extension mobility.	Provide users with information about which Cisco Unified Personal Communicator features are supported based on the integration with the LDAP directory, Cisco Unity Connection, and Cisco Unified MeetingPlace Express. Inform users that have the ability to initiate web-only meetings from a Cisco Unified Personal Communicator conversation. For more information, see "How Cisco Unified Personal Communicator Fits into Your Network" section on page 1-2. Inform users that you configured for Cisco Unified CallManager extension mobility. For a description of the type of information to provide to them, see the *Cisco Unified CallManager Features and Services Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html	Yes	Yes

Table 3-2 Information Needed by End Users (continued)

Provide This	Explanation	Give to Users Who Install	Give to Users If You Install
Account information	Provide account information to be entered into the Preferences window: • Cisco Unity Connection: username and web password (to use voice-mail features supported by Cisco Unified Personal Communicator) You created an e-mail account in Cisco Unity Connection. For more information, see the "Cisco Unity Connection Configuration" section on page 2-20. • Cisco Unified MeetingPlace Express: username and password (to add web conferencing to a Cisco Unified Personal Communicator conversation) You created user profiles in Cisco Unified MeetingPlace Express. For more information, see the "Cisco Unified MeetingPlace Express Configuration" section on page 2-21.	Yes	Yes
Instructions for using the application.	Provide the user guide and quick start guide for Cisco Unified Personal Communicator. Remind users to use the online help that is embedded in the application. http://www.cisco.com/en/US/products/ps6844/products_user_guide_list.html	Yes	Yes
Information about the Cisco Unified MeetingPlace Express meeting room (and what users can expect to see in a web-only meeting) and information about presenting and working with shared content.	Provide the user guide for Cisco Unified MeetingPlace Express.	Yes	Yes
Internal company support for the application.	Provide users with the names of people to contact for assistance and with instructions for contacting those people.	Yes	Yes

CHAPTER 4

Adding a New User After the Initial Deployment

Table 4-1 lists the required configuration steps to add a new user with full functionality in Cisco Unified Personal Communicator after the initial deployment of the application.

Table 4-1 Configuring a New User for Full Functionality in Cisco Unified Personal Communicator

Configuration	Where to Find Information
Cisco Unified CallManager Configuration	
Add the phone to the Cisco Unified CallManager database. Allow control of the Cisco Unified IP Phone from the computer telephony interface (CTI). Associate a directory number with the phone.	"Adding Cisco Unified IP Phones to the Cisco Unified CallManager Database" section on page 2-4
Set up the user account, and associate the directory number to the user. Associate the phone to the end user. Add the end user to the Standard CTI Enabled group. Add the end user to the CCM End User group.	"Associating the Cisco Unified IP Phone to an End User and Adding the End User to a Group" section on page 2-5
Enable Cisco Unified Personal Communicator soft-phone features by manually creating a new device per user.	"Adding Cisco Unified Personal Communicator as a Phone Type" section on page 2-8
Obtain a license file, if necessary. Upload the license file, if necessary. Assign capabilities.	"Obtaining a License File" section on page 2-13 "Uploading a License File" section on page 2-14 "Assigning Capabilities to Users" section on page 2-14
Cisco Unity Connection Server Configuration	
Set up an account for the new user.	"Cisco Unity Connection Configuration" section on page 2-20
Cisco Unified MeetingPlace Express Server Configuration	
Set up a user profile for the new user.	"Cisco Unified MeetingPlace Express Configuration" section on page 2-21
Cisco Unified Presence Server Configuration	
Configure the LDAP attribute map for the new user.	"Configuring the LDAP Attribute Map" section on page 2-23

Table 4-1 Configuring a New User for Full Functionality in Cisco Unified Personal Communicator (continued)

Configuration	Where to Find Information
Add the new user to the server profiles.	"Creating LDAP Server Profiles" section on page 2-26 "Creating Cisco Unity Connection Server Profiles" section on page 2-28 "Creating Cisco Unified MeetingPlace Express Server Profiles" section on page 2-30 "Creating CTI Gateway Server Profiles" section on page 2-32 "Creating SIP Proxy Server Profiles" section on page 2-33
Configure the preferred CTI device to the MAC address of the user's primary desk phone.	"Changing Application Profiles on a Per-User Basis" section on page 2-34
Video Telephony Camera Configuration	"Video Telephony Camera Configuration" section on page 2-35
Headset and Audio Device Configuration	"Headsets and Other Audio Devices Configuration" section on page 2-36
Provide information to users	"Providing Information to End Users" section on page 3-4

INDEX

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W