Mobile Agent Guide for Cisco Unified CC Enterprise & Hosted

Release 7.1(1)

June 2007

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0833

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 UCBs 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.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, 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, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (0705R)

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.

Table of Contents

List of Figures

Preface

Purpose

This guide provides the information that agents and supervisors need to know in order to successfully configure and use the Cisco Unified Mobile Agent (Unified MA) feature for Cisco Unified CC Enterprise & Hosted.

Note:

- Refer to the *Cisco ICM/IPCC Hardware and System Software Specifications (Bill of Materials)* for this release (located on the **Cisco web page** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html)) for details about operating system and software requirements.

- Mobile Agent is a new feature in 7.1(1); its predecessor was the Remote Agent option. If you are upgrading to 7.1(1) and are planning to configure a mobile agent to use an *analog* phone or an IP Phone *without* Cisco Business Ready Teleworker setup, you should use the Mobile Agent Option. However, if you are planning to configure a mobile agent to use the deployment option of IP Phone *with* Cisco Business Ready Teleworker setup, use Remote Agent. (For more information, see the Configuration and Troubleshooting Appendix for Remote Agent (page 67).)

Audience

There are two major audiences for this guide:

- System Administrators – Configure Unified MA for contact center agents.

- Mobile agents – Use Unified MA on a regular basis to handle customer calls.

Important Information about Cisco Product Names

Effective with this release:

- Cisco ICM Enterprise Edition is renamed Cisco Unified Intelligent Contact Management Enterprise (abbreviated as Unified ICME).
- Cisco ICM Hosted Edition is renamed Cisco Unified Intelligent Contact Management Hosted (abbreviated as Unified ICMH).
- Cisco IPCC Enterprise Edition and Cisco IPCC Hosted Edition are renamed Cisco Unified Contact Center Enterprise (abbreviated as Unified CCE) and Cisco Unified Contact Center Hosted (abbreviated as Unified CCH), respectively.
- Cisco IPCC Express Edition is renamed Cisco Unified Contact Center Express (abbreviated as Unified CC Express.)

The new product names are being introduced in phases. In the 7.1(1) release, the new names refer to the product as a whole. They are not yet used for functions and utilities in the user interface.

This guide refers to the *product as a whole* by its new name. It refers to *components and utilities* by the names that appear in the user interface.

Organization

The following describes the information contained in the sections of this guide:

Section	Description
Part 1: Cisco Unified Mobile Agent	This section contains the following: • Chapter 1, "Introduction to Cisco Unified Mobile Agent for Cisco Unified CCE/CCH" - Describes Unified MA features. • Chapter 2, "System Configuration for Cisco Unified Mobile Agent" - Describes how to configure Unified MA. • Chapter 3, "Troubleshooting Cisco Unified Mobile Agent" - Provides troubleshooting tips for Unified MA.
Part 2: Using Unified Mobile Agent in Your Contact Center	This section contains the following: • Chapter 4, "Using Unified Mobile Agent (for Agents)" - Instructs agents how to use Unified MA to login and process calls. • Chapter 5, "Using Unified Mobile Agent (for Supervisors)" - Instructs supervisors how to use Unified MA to login and process calls and how to configure mobile agents.

Section	Description
Part 3: Configuration and Troubleshooting Appendix for Remote Agent	This section describes an earlier deployment model of Unified MA.

Related Documentation

For additional information about Cisco Unified Contact Center Enterprise software, see the **the Cisco web page** (http://www.cisco.com/en/US/products/sw/custcosw/ps1844/tsd_products_support_series_home.html) .

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example: • Choose **Edit** > **Find**. • Click **Finish**.
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • For emphasis. Example: *Do not* use the numerical naming convention. • A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*) • A book title. Example: See the *Cisco CRS Installation Guide*.
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: **`<html><title>Cisco Systems,Inc. </title></html>`**

Convention	Description
< >	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

Obtaining Documentation

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

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL::

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

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

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems Attn: Customer Document Ordering 170 West Tasman Drive San Jose, CA 95134-9883

We appreciate your comments.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can register to 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. Access the tool at this URL: **http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en**.

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:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- 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

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

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

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

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

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance 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 (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting**show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

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

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

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

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

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

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

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

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

  http://www.cisco.com/ipj

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

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

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

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

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

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

Part 1: Cisco Unified Mobile Agent

This section provides:

- An introduction to Cisco Unified MA.
- Instructions for system configuration of Unified MA.
- Information for troubleshooting Unified MA.

Chapter 1

Introduction to Cisco Unified Mobile Agent for Cisco Unified CCE/CCH

This section contains the following topics:

What is Unified MA for Unified CCE/CCH?

Unified MA makes it possible for Unified CCE/CCH to support agents using phones not directly controlled by Unified CCE/CCH. This could be an agent:

- Outside the contact center, using an analog phone at home or a cell phone.

- Inside the contact center, using an IP phone connection not controlled by Unified CCE/CCH or an associated CallManager.

Figure 1: An Agent at Home Using Unified MA

Mobile Agent phone
Agent Desktop (with broadband access) for call and agent state control

Note: Throughout this guide the term *local agent* refers to a Cisco Unified CCE/CCH agent who is configured as a *non-mobile* agent. (A local agent can be working within a contact center or at a remote location.) The term *mobile agent* refers to a Cisco Unified CCE/CCH agent who is using a phone that is not under control of Unified CCE/CCH; the agent can be physically located either *within* a contact center or at a *remote* location.

With Unified MA, contact center administrators can easily:

- Enable staff to work from home.
- Add contact center staff during busy periods.
- Hire skilled staff and knowledge workers in other regions.

Unified MA features make this possible without the overhead of additional off-site equipment or extensive on-site configuration and administration.

Note: Some caveats apply; for information, see Non-supported or Limited Unified CCE/CCH Features (page 21).

The sections that follow highlight some of the benefits of Unified MA and describe its features.

Unified MA Extends Cisco Unified CCE/CCH Capabilities

Prior to the development of the Unified MA, Unified CCE/CCH always used a JTAPI interface to CallManager to connect customer calls arriving on a voice gateway to an agent's IP phone. The Unified MA extends the Unified CCE/CCH architecture by enabling it to connect customer calls to an agent phone that *is not* controlled by Unified CCE/CCH.

Unified CCE/CCH does this by using a CallManager CTI Port as a proxy for the agent's phone. Once the proxy is configured, the JTAPI interface instructs the CallManager to place a call to the agent through an appropriate gateway and to connect the customer's call to the agent.

From the viewpoint of the customer calling a Cisco Unified CCE/CCH contact center, there is no difference between speaking to a local agent and a mobile agent, as the customer calls will be queued and routed identically.

Cisco Unified CC functionality remains intact whether an agent is mobile or local:

- Mobile agents have the same capabilities and functionality that local agents have.
- Mobile agents do not need any specialized equipment; they can receive calls on an analog or cellular phone.
- Unified MA supports Cisco CTI OS Agent Desktop, Cisco Agent Desktop (CAD), and Cisco Agent Desktop-Browser Edition (CAD-BE).
- Mobile agent activity is recorded in the same contact center reports as local agent activity.
- Mobile agent CTI and application data uses the same security mechanisms as local agent data.

Unified MA Provides Agent Login Flexibility

An agent, at various times, can be either a local agent or a mobile agent, depending on how they log in.

Regardless of whether an agent logs in as a local or mobile agent, the skill groups the agent belongs to will not change. In addition, since agents are chosen by existing selection rules, not how they are connected, the same routing applies regardless of how the agent logs in.

Note: If you want to use the scripting environment to control routing depending on whether an agent is local or mobile, you will need to assign the agent to different skill groups and design the script accordingly.

In addition, a mobile agent can be available through different phone numbers at different times; the agent enters the phone number at login time. (The phone number only needs to be dialable through the CallManager dial plan.)

Note: For more information about logging in to Unified MA, see Using Unified MA in Your Contact Center (page 49).

How does Unified MA deliver calls to agents?

Unified MA supports two call delivery modes:

- Call by call.
- Nailed connection.

Note: From a caller's perspective, the call by call delivery mode has a longer ring time compared to the nailed connection delivery mode. This is because, with call by call, only after the caller call is routed to the mobile agent that IPCC starts to dial the mobile agent's remote phone number, and connecting the caller call to the agent call after the agent answers. The caller hears ringing up to that point. From the IPCC reporting perspective, a call-by-call mobile agent has a longer Answer Wait Time on average for the same reason.

What is Call by Call Delivery Mode?

In a *call by call* delivery mode, the mobile agent's phone is dialed for each incoming call. When the call ends, the mobile agent's phone is disconnected before being made ready for the next call.

A call by call dialing flow works as follows:

1. At login, the agent specifies an assigned extension for a CTI port.
2. A customer call arrives in the system and, through normal ICM configuration and scripting, is queued for a skill group or an agent. (This is no different than existing processing for local agents.)
3. The system assigns an agent to the call. If the agent has a Desk Setting that is Unified MA-enabled and configured for either Call by call or Agent chooses mode, the router uses the extension of the agent's CTI port as a label.
4. The incoming call rings at the agent's CTI port. The JTAPI Gateway and PIM will notice this but not answer the call.
5. A call to the agent is initiated on another CTI port chosen from a preconfigured pool. If this fails, Redirect on No Answer processing will be initiated.

   Note: When using call by call mode, the answer wait time will be longer than in a local agent inbound call scenario (3-15 seconds). Specify a Redirect on No Answer setting large enough to accommodate the extra processing time. (For instructions, see How to Configure Unified MA on ICM Configuration Manager (page 38).)
6. When the agent takes the remote phone off-hook to answer the call, the system directs the customer call to the agent's call media address and the agent call to the customer's call media address.
7. When the call ends, both connections are terminated and the agent is ready for another call.

What is Nailed Connection Delivery Mode?

In *nailed connection* delivery mode, the agent is called once, at login, and the line stays connected through multiple customer calls.

A nailed connection call flow would work as follows:

1. At login, the agent specifies an assigned extension for a CTI port from a pool.
2. A call to the agent is initiated on another CTI port chosen from a preconfigured pool. The agent answers the call. (The agent must answer this setup call to complete the connection and finalize the login procedure.)
3. A customer call arrives in the system and, through normal ICM configuration and scripting, is queued for a skill group or an agent. (This is no different than existing processing for local agents.)
4. The system assigns an agent to the call. If the agent has a Desk Setting that is Unified MA-enabled and configured for either Nailed connection or Agent chooses mode, the router will use the extension of the agent's CTI port as a label.
5. The incoming call rings at the agent's CTI port. The JTAPI Gateway and PIM will notice this but not answer the call.
6. The Agent Desktop indicates a call is ringing and the agent clicks **Answer**.
7. Once the agent indicates that they will answer the phone, the system directs the customer call to the agent's call media address and the agent call to the customer's call media address.
8. When the call ends:
   - The customer connection is terminated.
   - The agent state is ready for the next call.

A nailed connection agent can logoff by using the desktop (preferable), or by just hanging up the phone.

If the agent is not configured for auto-answer, then the possibility exists for Redirect on No Answer processing. In that case, the Redirect on No Answer will be handled normally, and the agent will go Not Ready. This is visible in the desktop

How is Call Delivery Mode Configured?

The administrator specifies call delivery settings during system configuration for Agent Desktop.

Note: The administrator has the option of specifying an "Agent chooses" setting, which allows the agent to select the call delivery mode at login.

After an agent's Desktop settings have been configured to accommodate Unified MA, the remote agent can log in as a mobile agent and begin processing calls.

Feature Requirements

Hardware and Software Requirements

Hardware and software requirements for the Unified MA are identical to those of Cisco Unified CC Enterprise. For more information, refer to the *Cisco ICM/IPCC Hardware and System Software Specifications (Bill of Materials)* .

Phone Requirements

A mobile agent can handle calls using an analog, digital, or IP Phone.

Note: When Mobile Agent phones are located on a cluster and a SIP Trunk is used to connect the cluster to another cluster under Unified CCE control, you must use either SIP phones as the Mobile Agent phones or else you must check "MTP required" on the Unified CCE cluster in order for the Mobile Agent calls to work.

CTI Port Requirements

Unified MA uses CallManager CTI Port as a proxy for the agent's phone. Once this proxy is set up, whenever a mobile agent is selected to handle a customer call, the following happens:

- The call will be directed to the CTI port's extension.
- Unified CCE/CCH, using the JTAPI Gateway, intercepts the call arriving on the CTI Port and directs CallManager to connect the call to the mobile agent.

For Unified MA to work properly, you need to configure two pools of CTI Ports:

- One pool to serve as the agent's virtual extension.
- The other pool to initiate calls to the agent.

Each pool requires one port per mobile agent. These CTI Ports must be assigned to the Unified ICME application, and will be recognized by Unified ICME when receiving the CallManager configuration.

Note: For more information, see How to Configure CTI Port Pools (page 35).

Supported Unified CCE/CCH Features

Software Release Temporary Uninstallation Support

Unified CCE/Unified SCC Release 7.1(1) supports the ability to perform a temporary uninstallation while preserving mobile agent data.

Note: A temporary uninstallation simply removes the application software, while preserving data.

For more information on temporary uninstallation, see *Installation Guide for Cisco ICM/IPCC/System IPCC Enterprise & Hosted Editions*.

Redirect on No Answer Support

Unified MA supports Redirect on No Answer (RONA). If the mobile agent fails to answer, the agent is made Not Ready, and the call is redirected to a RONA DN route point.

Note: If using call by call mode, the answer wait time will be longer than in a local agent inbound call scenario, so increase the value of the Agent Desk Setting **Ring no answer time** field to accommodate the extra processing time.

Silent Monitoring Support

Unified MA supports silent monitoring in CTI OS deployments and in CAD 7.1(2) [but not in CAD 7.1(1)].

Note: For more information, see Silent Monitoring Limitations (page 23).

Reporting Support

No special reports exist for individual mobile agents. Unified CCE/CCH reports as they pertain to a Headquarter Contact Center are applicable.

For more information about reporting Unified MA data, see Unified MA Reporting (page 31).

Call Control Support

Unified MA supports the same call control capabilities as Unified CCE/CCH (answer, hold, transfer, etc.). All call control is done through the agent desktop.

Outbound Calls Support

Unified MA supports outbound calls in nailed connection delivery mode, *only*.

Codec Support

Unified MA supports either G.711 or G.729 codecs.

Multichannel Application Support

There is no direct interaction between Unified MA and multichannel applications. Email and Chat are IP applications that will continue to operate normally, assuming the mobile agent has a desktop with enough bandwidth on the broadband connection to support them.

Fault Tolerance Support

Fault tolerance for the Unified MA follows the behavior of Cisco Unified CCE/CCH:

- The JTAPI Gateway, IPCC PIM, and CTI components record key events related to Unified MA as part of their normal logging.
- As with standard Unified CC calls, if a PG component such as the JTAPI Gateway fails, the phone call will not be lost, but subsequent transfers of the call might not be possible.
- Where CTI data is delivered for screen pops, CTI data is preserved.

Unified MA can experience many of the same failure cases as Unified CC:

- Side A/B failure
- IVR failure
- CallManager failure
- CTI server failure

There are also some failure cases that are unique to Unified MA:

- A situation where a mobile agent is using a cellular phone and the connection is dropped due to non-availability of a signal, would be deemed as external failure. The agent would need to call back and login again.
- If a mobile agent's phone line disconnects while using Nailed Connection mode, the agent would need to login again in order to receive new calls.

Note: For information, see Failover (page 22) in the Non-Support/Limitations section.

Interactive Voice Response (IVR) and Queuing Capability Support

Unified MA supports Cisco Unified Customer Voice Portal and Cisco Unified IP IVR.

Non-supported or Limited Unified CCE/CCH Features

Agent Limitations

- A mobile agent uses more system resource/capacity than a local agent.

  Note: For more information, refer to the *Cisco ICM/IPCC Hardware and System Software Specifications (Bill of Materials)* for this release.

- Mobile agents cannot perform agent state and call control without a CTI Desktop.
- If a mobile agent on one PG calls a mobile agent on a different PG, and both PGs are connected to the same CallManager cluster, only blind transfer/conference are supported.
- A mobile agent in nailed connection mode will be logged out after 12 hours, due to a default Cisco CallManager Service Parameter setting.

  Note: For more information about this setting, see Configuring the CallManager Maximum Call Duration Timer (page 37).

- Answer wait time in Unified MA call by call delivery mode will be longer than in a standard Unified CCE/CCH inbound call scenario.

  Note: Increase the **Ring no answer time** field value in Agent Desk Settings to accommodate this extra processing time.

- For consult transfer or conference calls, the source mobile agent does not hear ring back after dialing another agent because the media stream cannot be bridged until the destination agent answers.
- If a mobile agent uses a phone with voice mail capability, whenever possible, the voice mail option should be disabled to prevent caller-access to the agent's voice mail box. (In a Unified MA deployment, if a call is being processed by the mobile agent's voice mail, the system "sees" the agent as talking and not ready for another call.) This situation can occur in both call by call and nailed connection modes.

  Note: In addition, in nailed connection mode, if the mobile agent rejects the setup call -- and voice mail has not been disabled -- the setup call will be sent to voicemail. The mobile agent can continue to be logged in to the CTI Desktop and be made Ready. However, since the setup call was not accepted, the system will logoff the mobile agent when the voice mail ends and the agent phone line disconnects..

- When CTI ports for a Unified MA are disassociated at the CallManager while the agent is on an active call, the call might be dropped.
- Unified MA supports Outbound Option calls in nailed connection delivery mode, *only*.
- By default, a mobile agent in nailed connection mode on CTI OS Agent Desktop *does not ring* when a call arrives.

  Note: For information about how to change the default setting, see How to enable a ring tone on the CTI OS Agent Desktop (page 54).

Failover Limitations

- During failover, if a call by call agent answers an alerting call, the call might be dropped. This happens because, when there is no active PG, media cannot be bridged.
- During a prolonged failover, if an agent takes call control action for a Unified MA-to-Unified MA call, the call might be dropped. This happens because the activating PG might not have information for all agents and calls at that point.

Performance Limitations

- Unified MA uses more system resources/capacity than a local agent because of the two CTI ports used per call to accommodate the customer call and the bridging of media.

  Note: For specific sizing guidelines to address this limitation, refer to the *Cisco ICM/IPCC Hardware and System Software Specifications (Bill of Materials)* and the *Cisco IP Contact Center Solution Reference Network Design*for this release.
- Since Unified MA adds processing steps to Unified CCE/CCH default functionality, mobile agents might experience some delay in screen pops.
- From a caller's perspective, the call by call delivery mode has a longer ring time compared to the nailed connection delivery mode. This is because Unified CCE/CCH does not start to dial the mobile agent's phone number until *after* the call information is routed to the Agent Desktop. In addition, the customer call media stream is not connected to the agent until after the agent answers the phone.

  While Unified CCE/CCH is making these connections, the caller hears a repeated ring tone.

Phone Feature Limitations

Unified MA is targeted at phones (analog, digital, or IP) over which Unified CC Enterprise has no direct control. Therefore, Mobile Agent does not support phone buttons such as hold, transfer, etc.

Note: This is also the case even if the mobile agent is using a Cisco IP phone on a CallManager separate from Unified CCE/CCH.

The mobile agent must use the Agent Desktop to perform the functions of the phone buttons.

Codec Limitations

Both in-coming customer call and out-going Unified MA calls must use the same codec because of the way the JTAPI connects them through the gateways.

Auto-answer Limitations

Unified MA supports auto-answer with the nailed connection mode, only; it does not support auto-answer with the call by call connection mode.

Silent Monitoring Limitations

- Unified MA does supports Silent Monitoring in a CAD 7.1(2) deployment but not in CAD 7.1(1).
- Unified MA requires that caller and agent voice gateways be on separate devices if Silent Monitoring is to be used.
- Unified MA does not support Desktop Monitoring.

Note: For more information about Silent Monitoring requirements in a Unified MA environment, see *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* .

Cisco Unified Contact Center Express Limitations

Unified MA is not supported on Cisco Unified Contact Center Express .

Unified MA Call Flows

This section provides sample Unified MA call flows for:

- Inbound calls
- Local consultation calls
- Remote consultation calls
- Remote conference calls

In all Unified MA call flows, the JTAPI Gateway maintains the signaling association between the inbound and outbound calls and, if necessary, performs further operations on the call. JTAPI Gateway, however, does not terminate media; it uses CTI to deliver the customer call from the inbound gateway port to the outbound gateway port.

This means that a mobile agent *must* use an agent desktop application to log in, change agent state, log out, and perform call control.

About The Figures in This Section

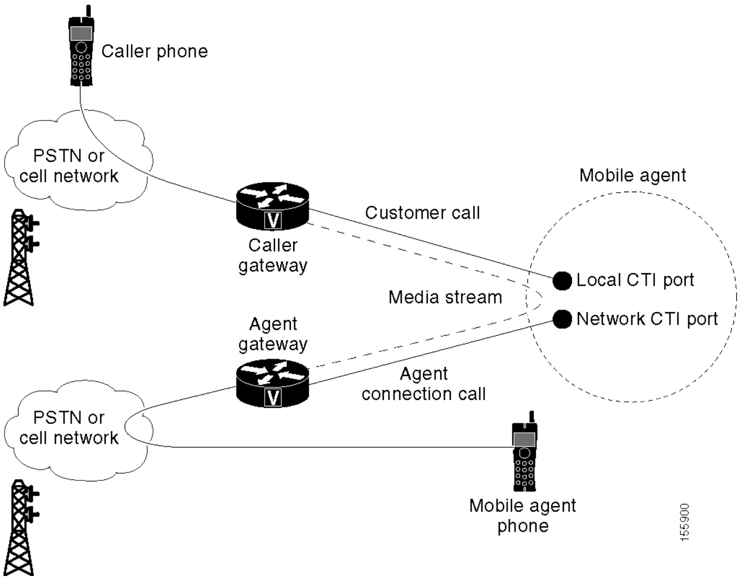
The figures in this section:

- Show a caller and a mobile agent in a cellular network. However, the same concepts apply whether the mobile agent is using an enterprise desk phone, an IP Phone spanning another CallManager cluster, standard analog phone, or a third-party ACD phone.
- Focus solely on call media flow; a mobile agent must use a CTI Desktop with broadband access to perform agent state and call control.
- Show only a sampling of the call flows possible with Unified MA.

Inbound Call Flow

The following figure shows an inbound call flow.

Figure 2: Mobile Agent Inbound Call Flow



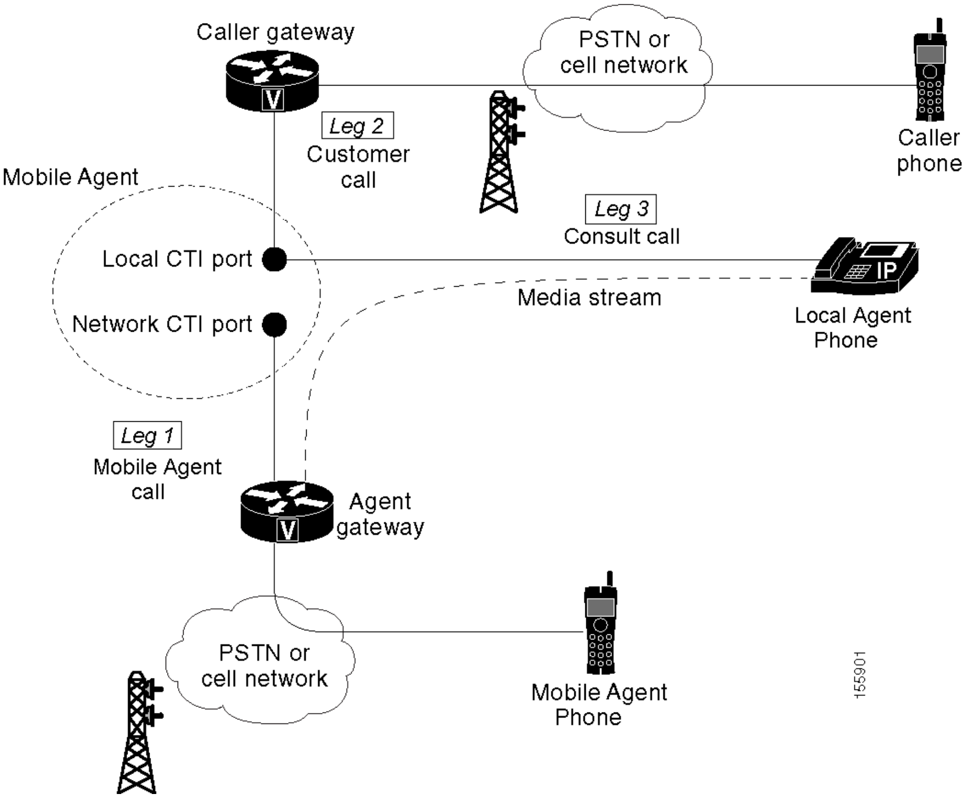
Note: Caller and Agent voice gateways can co-exist on one device, except in deployments where Silent Monitoring is required.

1. The mobile agent becomes available to answer calls by:
   - Logging on to the corporate domain using VPN over the ADSL/Cable connection.
   - Launching the agent desktop interface and logging in to the CTI server with their remote phone information.
   - Entering the Ready mode.
2. A customer call arrives at the Cisco Unified CC.
3. The JTAPI Gateway creates a mobile agent class to manage local and network CTI ports for a mobile agent.
4. The ICM Router passes the call to the *local* CTI Port of a mobile agent.
5. The JTAPI Gateway places a call on a *network* CTI port to the agent's cell phone.
6. The JTAPI Gateway uses local and network CTI ports of the mobile agent to stream the call's media from the inbound (caller) gateway port to the outbound (agent) gateway port.

Local Consult Calls

The following figure shows a consult call flow between a mobile agent and a local agent.

Figure 3: Mobile Agent Local Consult Call Flow



Note: Caller and Agent voice gateways can co-exist on one device, except in deployments where Silent Monitoring is required.

1. The mobile agent becomes available to answer calls by:
   - Logging on to the corporate domain using VPN over the ADSL/Cable connection.
   - Launching the agent desktop interface and logging in to the CTI server with their remote phone information.

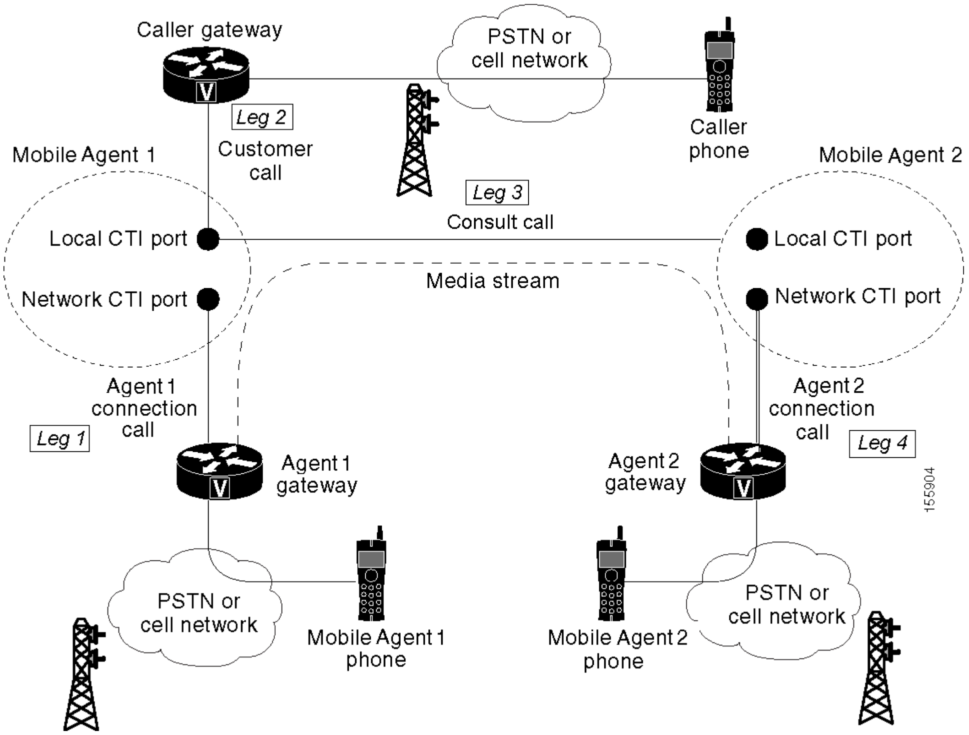
– Entering the Ready mode.

2. A customer call arrives at the Cisco Unified CC.
3. The JTAPI Gateway creates a mobile agent class to manage local and network CTI ports for a mobile agent.
4. The ICM Router passes the call to the *local* CTI Port of a mobile agent.
5. The JTAPI Gateway places Agent Connection Call 1 on a *network* CTI port to the agent's cell phone.
6. The mobile agent places the customer call on hold and consults a local Unified CCE/CCH agent.
7. The JTAPI Gateway uses local and network CTI ports of the mobile agent to stream the call's media from the IP hard phone to the outbound gateway port.

Remote Consult Calls

The following figure shows a remote consult call flow between two mobile agents.

Figure 4: Mobile Agent Remote Consult Call Flow



Note: Caller and Agent voice gateways can co-exist on one device, except in deployments where Silent Monitoring is required.

1. The mobile agent becomes available to answer calls by:

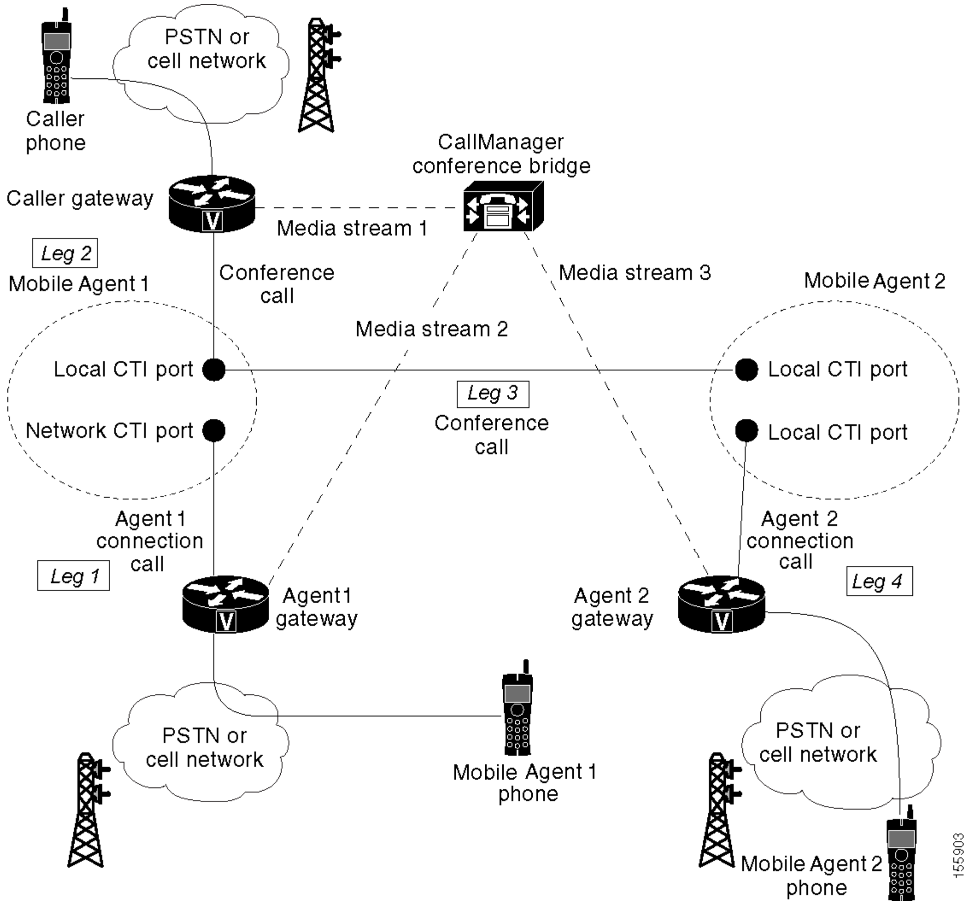
- Logging on to the corporate domain using VPN over the ADSL/Cable connection.
- Launching the agent desktop interface and logging in to the CTI server with their remote phone information.
- Entering the Ready mode.

2. A customer call arrives at the Cisco Unified CC.
3. The JTAPI Gateway creates a mobile agent class to manage local and network CTI ports for a mobile agent.
4. The ICM Router passes the call to the *local* CTI Port of a mobile agent.
5. The JTAPI Gateway places Agent Connection Call 1 on a *network* CTI port to the agent's cell phone.
6. Mobile Agent 1 puts the customer call on hold and consults Mobile Agent 2.
7. The JTAPI Gateway uses the network CTI port of Mobile Agent 1 and the network CTI port of Mobile Agent 2 to stream the call's media from the outbound gateway port on Agent Gateway 1 to the outbound gateway port on Agent Gateway 2.

Remote Conference Calls

The following figure shows a remote conference call flow between two mobile agents.

Figure 5: Mobile Agent Remote Conference Call Flow



Note: Caller and Agent voice gateways can co-exist on one device, except in deployments where Silent Monitoring is required.

1. The mobile agent becomes available to answer calls by:
   - Logging on to the corporate domain using VPN over the ADSL/Cable connection.
   - Launching the agent desktop interface and logging in to the CTI server with their remote phone information.

  - Entering the Ready mode.

2. A customer call arrives at the Cisco Unified CC.

3. The JTAPI Gateway creates a mobile agent class to manage local and network CTI ports for a mobile agent.

4. The ICM Router passes the call to the *local* CTI Port of a mobile agent.

5. CallManager redirects the media stream 1 from inbound gateway on the Caller Gateway to the conference bridge during call merging process.

6. The JTAPI Gateway uses local and network CTI ports of mobile agent 1 to loop the call's Media Stream 2 from the outbound gateway port on the Agent Gateway 1 to the conference bridge.

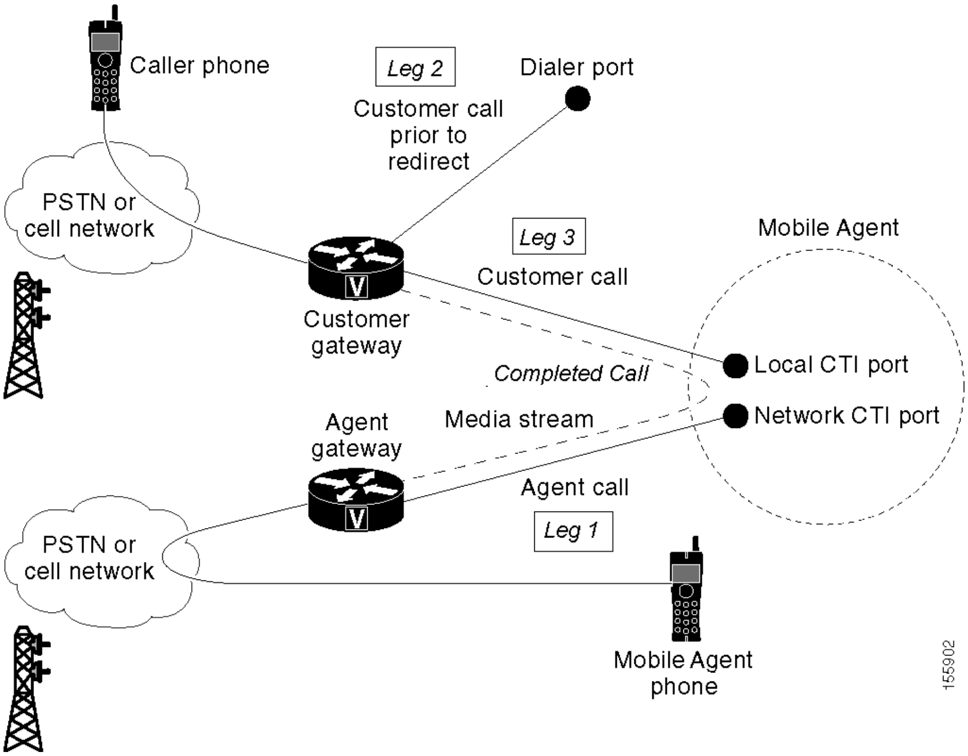
7. The JTAPI Gateway uses local and network CTI ports of mobile agent 2 to loop the call's Media Stream 3 from the outbound gateway port on the Agent Gateway 2 to the conference bridge.

Outbound Option Call Flow

The following figure shows a Outbound Option call flow between a customer and a mobile agent.

Note: Unified MA supports Outbound Option calls in nailed connection delivery mode, *only*.

Figure 6: Mobile Agent Outbound Call Flow



Note: Caller and Agent voice gateways can co-exist on one device, except in deployments where Silent Monitoring is required.

1. The mobile agent becomes available to answer calls by:
   - Logging on to the corporate domain using VPN over the ADSL/Cable connection.
   - Launching the agent desktop interface and logging in to the CTI server with their remote phone information.
   - Entering the Ready mode.
2. The JTAPI Gateway creates a mobile agent class to manage local and network CTI ports for a mobile agent.
3. Outbound Option dials the customer number and, after reaching a live customer, the Dialer redirects the customer call to the *local* CTI Port of an Outbound Option mobile agent.
4. The JTAPI Gateway places a call on a *network* CTI port to the agent's cell phone.
5. The JTAPI Gateway uses local and network CTI ports of the mobile agent to stream the call's media from the inbound gateway port to the outbound gateway port.

Unified Mobile Agent Reporting

Unified MA-specific call data is contained in the following Cisco Unified CC reports:

- **Agent Real time reports (Agent20, Agtper20, Agtskg30, Agteam20)**. These reports show what kind of call the agent is on (not mobile, call by call, nailed connection), and the mobile agent's phone number.
- **Agent Log Out Reports (Agent03, Agtper03, Agteam03)**. These reports show what kind of call the agent was on (not mobile, call by call, nailed connection) and the mobile agent's phone number.
- **Agent Real Time All Fields Reports (Agent28, Agtper28, Agtskg28, Agteam28)**. These reports show what kind of call the agent was on (not mobile, call by call, nailed connection etc.) and the mobile agents phone number.

Notes regarding mobile agents and reporting:

- The mobile agent must be *logged in* through the Agent Desktop for call data to be recorded in Cisco Unified CC reports.
- Service level for mobile agent calls might be different than local agent calls, since it takes longer to connect the call to the agent.

  For example, a call by call mobile agent might have a longer Answer Wait Time Average than a local agent. This is because Unified CCE/CCH does not start to dial the mobile agent's phone number until *after* the call information is routed to the Agent Desktop. In addition, the customer call media stream is not connected to the agent until after the agent answers the phone.

See Also

For more information about these reports, see *WebView Template Reference Guide for Cisco Unified CC Enterprise & Hosted*.

For information about Unified MA fields in the database schema, see *Database Schema Handbook for Cisco ICM/IPCC Enterprise & Hosted Editions*

Chapter 2

System Configuration for Unified Mobile Agent

This section contains the following topics:

Summary of Unified Mobile Agent System Configuration Tasks

This section describes the configuration tasks *specific* to Unified MA configuration. It *does not* describe Unified CCE/CCH.

Note: For complete details about installing and configuring Unified CCE/CCH, see *IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition*.

Table 1: Unified MA System Configuration Tasks

Task	See
Configure CallManager CTI Port pools and Call Duration Timer	Configuring CallManager for Unified MA (page 34) provides: • Information about naming conventions for CTI Port pools in a Unified MA deployment and instructions for configuring and mapping the port pools. • Instructions for configuring the CallManager Maximum Call Duration Timer.

Task	See
Configure Agent Desk Settings	Configuring Agent Desk Setting for Unified MA (page 38) for instructions for performing this task.
Configure Device Targets	Configuring Device Targets for Unified MA (page 40) for instructions for performing this task.
Configure CTI OS	Configuring Cisco CTI OS for Unified MA (page 41) for instructions for performing this task.

About Unified Mobile Agent Performance and Optimization

Unified MA is resource-intensive. Since it essentially uses two CTI ports for each mobile agent, you might find that your system's call capacity level will be lower.

For complete information about configuring Unified MA to maximize performance, refer to this release's version of the following documents:

- *Cisco ICM/IPCC Hardware and System Software Specifications (Bill of Materials)*
- *Cisco IP Contact Center Solution Reference Network Design*

Configuring CallManager for Unified MA

This section contains the following topics:

- Configuring and Mapping CallManager CTI Ports for Unified MA
- Configuring the CallManager Maximum Call Duration Timer

Configuring and Mapping CallManager CTI Ports for Unified MA

This section describes the CTI Port Pool configuration tasks *specific* to Mobile Agent Option configuration. It does not discuss installation or configuration of Cisco Unified CC Enterprise.

Note: For more information about installing and configuring CallManager with Cisco Unified CC Enterprise, see *IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition*.

Unified MA needs two CTI Port pools configured on CallManager:

- A *local* CTI port, which Unified MA uses as the agent's virtual extension.
- A *network* CTI port, which Unified MA uses to initiate a call to the mobile agent's phone.

Naming Conventions for Local and Network Ports

- The local port *must* begin with the string **LCP**.
- The network port *must* begin with the string **RCP**.
- Although not required, for best practices, use the following naming convention:
  - For a **local** CTI Port pool name, configure a name in the format LCPxxxxFyyyy, where **LCP** identifies a local CTI Port Pool, **xxxx** is the peripheral ID for the CallManager PIM, and **yyyy** is the number of local CTI Port.

    Example: **LCP5000F0000** would represent CTI Port: 0 in a local CTI Port pool for the CallManager PIM with the peripheral ID **5000**.)
  - For a **network** CTI Port pool name, use the same format, except substituting **RCP** as the first three characters.

Note: While a naming convention is not required, the substrings identifying the CallManager PIM peripheral ID and the CTI Port*must* match for each local/network pair.

CTI Port configuration consists of the following steps:

1. Adding the CTI port as you would for an IP Phone.
2. Using the naming convention described above to map the local and network CTI ports.

   Note: Each local CTI port needs to have a corresponding network CTI port.
3. Adding a directory number for the local CTI port (that is, the agent's virtual extension).
4. Mapping the local and network CTI ports with the PG user.

How to Configure CallManager CTI Port Pools for Unified MA

Follow the steps described below to configure CTI Ports.

Note: In Unified MA deployments, the CallManager Music on Hold (MoH) feature must be enabled for all *local* CTI ports so that callers can hear music when they are put on hold. However, the MoH feature should be disabled for all *network* CTI ports, as mobile agents do not need this feature. (For more information on MoH, see the CallManager Administration documentation or online Help.)

Step 1 In CallManager Administration, select **Device > Phone**.

Step 2 Click **Add a New Phone**.

Step 3 From Phone Type, select **CTI Port**.

Step 4 Click **Next**.

Step 5 In Device Name, enter a unique name for the **local** CTI Port pool name; click **OK** when finished.

Using the example naming convention format LCPxxxxFyyyy:

- **LCP** identifies the CTI Port as a local device.
- **xxxx** is the peripheral ID for the CallManager PIM.
- **yyyy** is the directory number (the agent extension) of the local CTI Port.

The name **LCP5000F0000** would represent CTI Port: 0 in a local CTI Port pool for the CallManager PIM with the peripheral ID **5000**.

Step 6 In Description, enter text identifying the local CTI Port pool.

Step 7 Use the Device Pool drop-down list to choose the device pool to which you want network CTI Port pool assigned. (The device pool defines sets of common characteristics for devices.)

Step 8 Click **Save**.

Step 9 Highlight a record and select Add a New DN.

Step 10 Add a unique directory number for the CTI port you just created.

Step 11 When finished, click **Save** and **Close**.

Step 12 Repeat the steps above to configure the **network** CTI Port pool.

In Device Name, using the example naming convention format RCPxxxxFyyyy, where:

- **RCP** identifies the CTI Port as a network device.
- **xxxx** is the peripheral ID for the CallManager PIM.
- **yyyy** is the directory number (the agent extension) of the network CTI Port.

The name **RCP5000F0000** would represent CTI Port: 0 in a network CTI Port pool for the CallManager PIM with the peripheral ID **5000**.

Step 13 In Description, enter text identifying the network CTI Port pool.

Step 14 Use the Device Pool drop-down list to choose the device pool to which you want network CTI Port pool assigned. (The device pool defines sets of common characteristics for devices.)

Step 15 Click **Save**.

Step 16 Highlight a record and select Add a New DN.

Step 17 Add a unique directory number for the CTI port you just created.

Step 18 When finished, click **Save** and **Close**.

How to map local and network CTI ports with PG user

Once you have defined the CTI Port pool, you must associate the CTI Ports with PG Users.

Step 1 In CallManager Administration, select **Application User**.

Step 2 Select a user name and associate ports with it.

Step 3 When finished, click **Save** and **Close**

Configuring the CallManager Maximum Call Duration Timer

By default, mobile agents in nailed connection mode will be logged out after 12 hours. This happens because a CallManager Service Parameter -- the Maximum Call Duration Timer -- determines the amount of time an agent phone can remain in the Connected state after login.

If you anticipate that nailed connection agents in your Unified MA deployment will be logged on *longer than* 12 hours, follow the instructions below to either:

- Increase the Maximum Call Duration Timer setting.
- Disable the timer entirely.

How to configure the CallManager Maximum Call Duration Timer

Note: This procedure applies *only* to Unified MA deployments where agents logged on in nailed connection mode are to remain connected *longer than* 12 hours.

Note: If your Mobile Agent deployment uses intercluster trunks, you must perform the following steps on both local and network CallManager clusters.

Step 1 In CallManager Administration, select **System > Service Parameters**.

Step 2 In the Server drop-down list, choose a server.

Step 3 In the Service drop-down list, choose **Cisco CallManager**.

The Service Parameters Configuration window appears.

Step 4 In the Clusterwide Parameters section, specify a **Maximum Call Duration Timer** setting.

The default is 720 minutes (12 hours); the maximum setting allowed is 35791 minutes.

Note: To disable the timer, enter **0**.

Step 5 Click **Save**.

Configuring Agent Desk Setting for Unified MA

This section describes Agent Desk Settings you should modify to accommodate Unified MA features.

You can configure Agent Desk settings through:

- ICM Configuration Manager
- System IPCC Web Administration

How to Configure Agent Desk Settings with ICM Configuration Manager

This section describes Agent Desk Settings configuration settings you should specify in ICM Configuration Manager to accommodate Unified MA features.

Note: The instructions below describe how to configure *one* Agent Desk Setting; repeat this process for each different Agent Desk Setting in your deployment.

Step 1 From the ICM Configuration Manager, choose **Configure ICM > Enterprise > Agent Desk Settings List**.

The ICM Agent Desk Settings List dialog box opens.

Step 2 Click **Retrieve**.

Step 3 Click **Add**.

Step 4 Fill in the following Attributes tab information, making sure to include settings for the following fields and checkboxes:

- **Ring no answer time**. Unified CCE/CCH will allow a call to ring at the agent's station before redirecting the call. This can be from 1 to 120 seconds.

  Note: If using call by call mode, the answer wait time will be longer than in a local agent inbound call scenario, so specify a value in this field to accommodate the extra processing time.

- **Logout non-activity time**. The number of seconds of agent inactivity while in the not ready state before IPCC will logout the agent. A blank entry will disable the timer.

  Note: In addition, the CTI OS ConnectionProfiles key **RejectIfAlreadyLoggedIn** should be set to 1 to prohibit an agent from logging in again as both a remote and a local agent. For more information, see Configuring Unified MA for Cisco CTI Object Server (CTI OS) (page 42).

- **Cisco Unified Mobile Agent** (checkbox). Enables the Unified MA feature so that the agent can login remotely and take calls from any phone.
- **Mobile agent mode**. Select how call connections are made to the mobile agent's phone:
  - **Agent chooses.** Agent selects call by call or nailed connection at login.
  - **Call by call**. Agent's phone is dialed for each incoming call. When a call ends, the connection is terminated before the agent is made ready for next call.
  - **Nailed connection**. Agent is called once, at login. The line stays connected through multiple customer calls.

Step 5 Click **Save**.

Note: For complete details configuring Agent Desk Settings in Unified CCE/CCH, see *IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition*.

How to Configure Agent Desk Settings with System IPCC Web Administration

This section describes Agent Desk Settings configuration settings you should specify through System IPCC Web Administration to accommodate Unified MA features.

Note: The instructions below describe how to configure *one* Agent Desk Setting; repeat this process for each different Agent Desk Setting in your deployment.

Step 1 Log in to the System IPCC Web Administration tool.

Step 2 Under Agent Management, click **Desk Settings**.

Step 3 Create a new Desk Setting or edit an existing Desk Setting, making sure to include settings for the following fields and checkboxes:

- **Ring no answer time**. Unified CCE/CCH will allow a call to ring at the agent's station before redirecting the call. This can be from 1 to 120 seconds.

Note: If using call by call mode, the answer wait time will be longer than in a local agent inbound call scenario, so specify a value in this field to accommodate the extra processing time.

- **Logout non-activity time**. The number of seconds of agent inactivity while in the not ready state before IPCC will logout the agent. A blank entry will disable the timer.
- **Enable Cisco Unified Mobile Agent** (checkbox). Enables the Unified MA feature so that the agent can login remotely and take calls from any phone.
- **Mobile agent mode**. Select how call connections are made to the mobile agent's phone:
  - **Agent chooses.** Agent selects call by call or nailed connection at login.
  - **Call by call**. Agent's phone is dialed for each incoming call. When a call ends, the connection is terminated before the agent is made ready for next call.
  - **Nailed connection**. Agent is called once, at login. The line stays connected through multiple customer calls.

Step 4 Click **Save**.

Step 5 Under Agent Management, click **Agents**.

Step 6 Click the hyperlinked name of an agent you want to be enabled for Unified MA and select a Unified MA Desk Setting from the pull-down on the Edit Agent page.

Step 7 Click **Save**.

Note: For complete details configuring Agent Desk Settings using the IPCC Web Administration Tool, see *System IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition* .

Configuring Device Targets for Unified MA

Unified CCE systems require that a device target be configured for each IP telephone that might be used by an agent. The only difference between configuring a device target for a local agent and a remote agent is that Unified MA uses the agent's *local CTI port* instead of the agent's *extension*.

How to Configure Device Targets

Note: This step is not required for deployments that use the System PG.

Step 1 From the ICM Configuration Manager, choose **Configure ICM > Targets > Device Target > Device Target Explorer**.

The Device Target Explorer window opens.

Step 2 Click **Retrieve** and then click **Add Device Target**.

The Device Target tab opens.

Step 3 Enter values for the following fields:

- **Name**. An enterprise name for the target. This name must be unique among all device targets in the enterprise.
- **Global Address.** The global address for the device. Must be set to a value that is unique from all other device targets in the enterprise. It is suggested that you use the same value that you entered in the Enterprise Name field.
- **Config Parameters**. Use this field to enter any specific configuration parameters that might be required:
  - /devtype (CiscoPhone)
  - /dn (full phone number)
  - /ext (extension)

    Note: For Unified MA, instead of entering the agent extension (ext) value, specify the local CTI Port assigned to the agent.

  The ICM software gives this string to the Cisco CallManager to initialize the device.
- **Description**. Enter a description of the device. This is an optional field used to provide additional information about the device.

Step 4 When finished, click the **Save**.

Note: For complete details configuring Device Targets in Unified CCE/CCH, see *IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition*.

Configuring Cisco CTI OS for Unified MA

This section describes information about CTI OS configuration settings that you need to know *after* initial installation of a Mobile Agent-enabled CTI OS Server.

Note: For complete instructions on installing and configuring CTI OS Server, see *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.

About CTI OS Installation and Unified MA

Note: Running the CTI OS 7.x server installer is not the same as running CTI OS 7.x installer from the CTI OS bin directory.

To configure Mobile Agent, first run the CTI OS 7.x server installer. Then run the CTI OS installer from the CTI OS bin directory. The first installer updates CTI OS server while the second installer allows you to configure mobile agent. Use this procedure for configuring any new feature made available in a maintenance release.

During the peripheral identification step of CTI OS Server installation:

- The Unified MA feature is enabled for the CTI Desktop (from the CTI OS bin directory).
- The call delivery mode (agent choose, call by call, nailed connection) is defined.

About Call Delivery Mode and Agent Profiles

- The call delivery mode selected during CTI OS Server installation enables CTI OS to send an agent profile to each desktop client for that mode.
- The call delivery mode the agent uses at login needs to match the mode configured for the agent in the Agent Desk Setting.
- Re-running the CTI OS installation and selecting a different Mobile Agent mode will overwrite the existing profile.
- Additional profiles can be added manually using the CTI OS registry.

How to prevent a CTI OS agent from logging in as both a remote and local agent

Step 1 To prevent an agent from logging in again as both a remote and a local agent, set the CTI OS ConnectionProfiles key **RejectIfAlreadyLoggedIn** to **1**.

Step 2 Optionally, configure the CTI OS CTI Driver key **IdleTimeout** to the same value as the ICM Agent Desk Settings **Logout non-activity time** value. (For information about this field, see How to Configure Unified MA on ICM Configuration Manager (page 38)).

Chapter 3

Troubleshooting Unified Mobile Agent

Troubleshooting Information

This section lists troubleshooting FAQs and recovery tips.

Table 2: Unified MA Failure Recovery Tips

Recovery Issue	Resolution
Power failure	Once the power is back up, verify that the Agent Desktop reboots properly and that the network is available. You can then login. **Note:** UPS can mitigate the risk of a power failure at home by keeping the cable modem and agent's PC powered up for a certain duration.
Internet failure	When the broadband connection is lost, the agent goes offline. Once the connection is reestablished, login again.
Agent Desktop reboot	See Power failure, above.
Agent Desktop application restart	Restart the application and log back into the server. If a call is still in progress, do not change the state to Ready.
VPN tunnel failure	If broadband access is available, but the connection to the corporate site is not, verify that the VPN tunnel is not misconfigured / broken. If it is broken, it will have to be reconfigured by the System Administrator.

Unified Mobile Agent checkbox unavailable in Agent Desktop Login dialog

Symptom:

The Unified Mobile Agent Mode checkbox does not appear in the dialog box.

Message:

None.

Cause:

Unified MA settings were not specified during CTI OS Server setup.

Action:

Rerun the CTI OS Server Setup program and specify the following on the Peripheral Identifier screen:

- Select the Enable Mobile Agent checkbox.
- Select an option from the Mobile Agent Mode drop-down list.

Call Mode unavailable in Agent Desktop Login dialog

Symptom:

You are unable to select a call mode in the Agent Desktop Login dialog; the call mode field is disabled and set to either Nailed connection or call by call without the option to change.

Message:

None.

Cause:

"Agent chooses" was not specified as the Mobile Agent Mode during CTI OS Server setup.

Action:

If the "Agent chooses" option is required, rerun the CTI OS Server Setup program and specify the following on the Peripheral Identifier screen:

- Select the Enable Mobile Agent checkbox.
- Select "Agent chooses" from the Mobile Agent Mode drop-down list.

Agent login fails

Symptom:

When you attempt to log in, the login fails and an error message appears.

Message:

See the table below.

Cause:

Agent login failures can result from a number of causes, as described in the table below.

Message	Cause	Action
IPCC Error [10151] - PERERR_ TELDRIVE_ MOBILEAGENT_ INCORRECT_LCP	You are unable to login to a device due to an incorrect LCP configuration in CallManager.	Check the Phone Configuration page in CallManager and make sure that the device name of the LCP Port starts with the string `LCP`.
IPCC Error [10152] - PERERR_TELDRIVE_ MOBILEAGENT_ INCORRECT_RCP	You are unable to login to a device due an incorrect RCP configuration in CallManager.	Check the Phone Configuration page in CallManager and make sure that the device name of the RCP Port starts with the string `RCP`. Also check the device name of the corresponding LCP Port.
IPCC Error [10153] - PERERR_TELDRIVE_ MOBILEAGENT_MODE_ NOT_ALLOWED	You are unable to login because the ICM Agent Desk Settings are not configured properly. (Either the "Cisco Unified Mobile Agent" checkbox is not selected or the "Mobile agent mode" setting does not correspond to the agent call mode selected in the Login dialog.)	Enable the Mobile Agent checkbox in the ICM Agent Desk Settings and verify that the agent mode configured in ICM is the same as the agent call mode selected in the Login dialog.
IPCC Error [10154] - PERERR_TELDRIVE_ AGENT_INVALID_ LOGIN_CTIPORT	This error can be generated when: • A non-mobile agent tries to login to a CTI port. • A mobile agent tries to login to an invalid CTI port.	Do one of the following: • If you are not configured as a mobile agent, enter your IP Phone extension in the Instrument field of the CTI Login dialog box. • If you are configured as a mobile agent, check the CTI Port configuration.
RESOURCE_NOT_AVAILABLE appears in JTAPI Gateway Log	The codec settings on the PG and Voice Gateway do not match. **Note:** This issue occurs for attempted Nailed connection login, only.	Change the codec configuration on either the PG or Voice Gateway.

Action:

See the table above.

Call by call or nailed connection delivery mode fails and mobile agent is logged out

Symptom:

Call by call delivery mode fails and mobile agent is logged out.

Message:

None.

Cause:

Agent call cannot connect due to invalid phone number.

Action:

Check to make sure mobile agent phone number is entered correctly before logging back in.

Call by call delivery mode fails and mobile agent is set to Not Ready

Symptom:

Call by call delivery mode fails and mobile agent is set to Not Ready.

Message:

None.

Cause:

The call cannot connect because:

- The mobile agent phone line is busy.
- The mobile agent did not answer the call.

Action:

Check mobile agent phone line and make sure the line is available.

Call by call delivery mode fails with RESOURCE_NOT_AVAILABLE message

Symptom:

Call by call delivery mode fails.

Message:

RESOURCE_NOT_AVAILABLE appears in JTAPI Gateway Log

Cause:

The codec settings on the PG and Voice Gateway do not match.

Action:

Use the CtiPortMediaCapability registry key (...\PG\CurrentVersion\JGWS\Jgw#\JGWData\Config\CtiPortMediaCapability) to change the codec configuration on either the PG or Voice Gateway.

Valid values are: **`0`** (the default for G.711 support and **`1`** for G.729 codec support.

Note: Voice Gateways participating in Unified MA calls need to have dial-peer to support the correct codec.

Part 2: Using Unified Mobile Agent in Your Contact Center

This section provides the following:

- Instructions for call processing for agents using the Cisco CTI OS Agent Desktop or the Cisco Agent Desktop.
- Instructions for call processing and agent management for supervisors using the Cisco CTI OS Supervisor Desktop or CAD Supervisor Desktop.

Note:

- This section describes tasks that are *specific* to interacting with Unified MA. For complete information about using these desktops, refer to the Cisco CTI OS documentation (located on the **Cisco web page** (http://www.cisco.com/en/US/products/sw/custcosw/ps14/products_user_guide_list.html)) and the CAD documentation (located on the **Cisco web page** (http://www.cisco.com/en/US/products/sw/custcosw/ps427/products_user_guide_list.html)).
- Refer to the *Cisco ICM/IPCC Hardware and System Software Specifications (Bill of Materials)* for this release (located on the **Cisco web page** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html)) for details about desktop operating system and software requirements.

Chapter 4

Using Unified Mobile Agent (for Agents)

Unified MA is available on the following Cisco agent desktops:

- Cisco CTI OS Agent Desktop
- Cisco Agent Desktop (CAD) and Cisco Agent Desktop-Browser Edition (CAD-BE)

This section contains the following topics:

Before You Begin

Before you login as a mobile agent, first disable home or cell phone calling features that could impact a customer call experience. Examples of such features are:

- Call waiting
- Call forwarding
- Voice mail

In addition, there are Unified MA limitations you need to be aware of before you begin processing calls:

- Mobile agents cannot perform agent state and call control without a CTI Desktop.
- If you login using nailed connection mode, you *must* answer the setup call before login is complete.
- Unified MA supports Outbound Option calls in nailed connection delivery mode, *only*.
- If a mobile agent on one PG calls a mobile agent on a different PG, and both PGs are connected to the same CallManager cluster, only blind transfer/conference are supported.
- During consult transfer or conference calls, a source Unified MA agent will not hear a ring back after dialing another agent; instead, the source agent will hear Music on Hold, if it is configured.
- You cannot transfer or conference a call using the buttons on your mobile agent phone; you need to use the Agent Desktop to perform these functions.
- If a mobile agent logged on in call by call mode places an outbound call -- that is, uses the CTI OS Agent Desktop **Dial** button or the Cisco Agent Desktop **Make Call** button -- the agent's phone will ring before the destination phone rings. This happens because Unified CEE establishes the agent call leg before it establishes the destination call leg.
- By default, a mobile agent in nailed connection mode on CTI OS Agent Desktop *does not ring* when a call arrives.

  Note: For information about how to change the default setting, see How to enable a ring tone on the CTI OS Agent Desktop (page 54).

Using the CTI OS Agent Desktop

Unified MA is available with the Cisco CTI OS Agent Desktop.

CTI OS Agent Desktop provides an interface that:

- Enables you to perform telephony call control -- such as call answer, hold, conference, and transfer -- and agent state control -- such as ready/not ready, wrap up, etc.
- Presents customer call data in the form of a screen pop.
- Provides you with agent statistics and chat capability.

  Note: CTI OS only supports chat between agents on the same peripheral.

Note: For more information about using CTI OS Agent Desktop to handle calls, see the *CTI OS Agent Desktop User Guide for Cisco Unified ICM/CC Enterprise & Hosted*.

How to login

Step 1 Click the **Login** button.

Step 2 Enter the following information in the dialog box:

- **Connect to**. Use the drop-down menu to select the connection mode that you want to use.
- **Agent ID** or **Agent Login Name**. The agent ID as assigned by the agent's manager.

  Note: Depending on the option chosen for logging in during the installation of the CTI OS Server, the Login dialog on the Agent desktop will prompt for either the Agent ID or the Agent Login Name.
- **Password**. The password as assigned by the agent's manager.
- **Instrument**. The directory number for the local CTI port (the agent's virtual extension).
- **Mobile Agent**. Check this box to log in as a mobile agent.
- **Phone Number**. The dial number for the phone the mobile agent is using.

  Note: The format for the phone number should follow the CallManager dial plan, for example, 91978-936-xxxx.
- **Call Mode**. Choose Nailed Connection or Call by call. (For more information, see How does Unified MA deliver calls to mobile agents? (page 15)) One of the following happens:
  - Login succeeds and the agent is available for incoming calls.
  - Login fails and an error message appears. (For information about how to resolve the problem, see Agent Login Fails (page 44) entry in the Troubleshooting section.)

Note:

- Auto answer is supported with the Unified MA Nailed Connection mode. It is not supported with the Unified MA call by call connection mode.
- If you login using nailed connection mode, you *must* answer a setup call before login is complete.

Step 3 Click **OK**.

The desktop automatically enters the state configured on the switch (either Ready or Not Ready) and the buttons for actions that are allowed from that agent state are enabled.

Note: However, for a Nailed connection, a setup call must be received and *answered* before agent login is complete.

How to verify that login was successful

Step 1 Check that your desktop is in the Ready or Not Ready state.

Note: Switch configuration determines the state the desktop enters upon login.

Step 2 Check that the status bar of your Unified MA Desktop displays the following:

- Agent ID for the logged in agent
- Agent Extension
- Agent Instrument
- Current Agent Status
- The server that the desktop is connected to

Step 3 Check that buttons for actions that are allowed from your current agent state are enabled.

How to enable a ring tone on the CTI OS Agent Desktop

Note: This procedure applies to agents using CTI OS Agent Desktop in nailed connection delivery mode, only.

By default, a CTI OS Agent Desktop in nailed connection delivery mode *does not ring* when a call arrives. The only indication that a call is arriving is an alert message that appears on the desktop. This means that, if you are not looking at the desktop when the alert appears, you will not know that a call has arrived.

Note: For more information, see What is Nailed Connection Delivery Mode? (page 16)

To set up your desktop to generate a ring tone follow the steps below:

Step 1 Click **Dial**.

The CTI Dialing Pad dialog appears.

Step 2 Click **More**.

The Options dialog appears.

Step 3 Select the Mute Tones tab and uncheck the **Ring Back** check box.

This disables the muting of the ring back tone.

Step 4 Click **Close**.

This setting will remain in effect until you change it or logout. You will need to repeat these steps each time you login.

How to enter the Ready state

You must become Ready to accept calls. Depending on your system switch, you will be placed in either the Ready or Not Ready state upon completion of a successful login.

Step 1 If you are in the Not Ready state and the **Ready** button is enabled, click the **Ready** button.

How to login with another phone number

Step 1 Click **Log off**.

Step 2 Follow the Agent Desktop login procedure, specifying another phone number.

How to make calls

Step 1 Enter a state from which you can make a call. (You are in the correct state to make a call if the **Dial** button is enabled.)

Note: Depending on the switch, you might also be able to make calls if the **Ready** or **Not Ready** buttons are enabled.

Step 2 Use the CTI Dial Pad to enter a phone number.

How to make a transfer

Step 1 Click the **Transfer** button. The CTI Dialing Pad dialog box appears.

Step 2 Enter the phone number to be dialed in the Dialed Number field or select a destination from the pull-down menu. The pull-down menu contains the last six numbers dialed from this desktop.

Step 3 Optionally, click the **More** button to display the Call Data tab, where you can optionally enter data associated with the call.

Step 4 Do one of the following:

a. If you *do want to speak* with the consulted agent, click the **Transfer Init** button. Once the **Transfer Init** button is pressed, the call will be put on hold. The agent has an opportunity to speak to the consulted agent before completing the transfer. When the consult call is answered, the button changes to **Transfer Complete**. To complete the transfer, click the **Transfer Complete** button.

b. If you *do not want to speak* with the consulted agent, click the **Single Step** button. The call is transferred automatically.

How to make a conference call

Step 1 Click the **Conference** button. The CTI Dialing Pad dialog box appears.

Step 2 Enter the phone number to be dialed in the Dialed Number field or select a destination from the pull-down menu. The pull-down menu contains the last six numbers dialed from this desktop.

Step 3 Optionally, click the **More** button to display the CTI Dialing Pad.

Step 4 Click the **Conference Init** button. The call is now put on hold. The agent will have an opportunity to speak to the consulted agent before completing the conference. When the consult call is answered, the button changes to **Conference Complete**. To complete the conference, click the **Conference Complete** button.

When the conference operation completes, the two calls appear on the Call Information Grid as one call.

Using the Cisco Agent Desktop (CAD)

Unified MA is available with the Cisco Agent Desktop.

CAD:

- Provides call control capabilities—such as call answer, hold, conference, and transfer, and ACD state control—ready/not ready, wrap up, etc.
- Presents customer information through an enterprise data window and an optional screen pop.
- Requires minimum screen real estate and enables agents to customize its functionality to meet their individual needs.

Note: For complete information about using CAD to handle calls, see the *Cisco Agent Desktop User Guide for Cisco Unified ICM/CC Enterprise & Hosted*.

How to log in

To start Cisco Agent Desktop and login as a Unified MA:

Step 1 Choose **Start** > **Programs** > **Cisco** > **Desktop** > **Agent**.

The Agent Login dialog box appears.

Note:

- You will be prompted for either your Login ID or Login Name in the Login dialog box; which appears depends on how your administrator has configured the system.
- If the login method (Login Name or Login ID) is changed while you are in the process of logging in, you will see an error message stating that the login method has changed. You must restart Agent Desktop in order to log in using the new method.

Step 2 Enter your **Login ID/Login Name**.

Step 3 Enter your **Password**.

Step 4 Enter your **Extension**.

Step 5 Click the **Mobile Agent Mode** checkbox.

The Mobile Agent Login dialog box appears.

Step 6 Choose a call delivery mode:

- **Nailed Connection Mode**. You receive one call when you log in and that line stays connected through multiple customer calls. Agent Desktop plays a phone ring sound file when a customer call arrives, and you handle all call control through Agent Desktop, including disconnecting the customer call. If you hang up your phone, you are logged out.

  Note: If you login using nailed connection mode, you *must* answer a setup call before login is complete.

- **Call by Call Mode.** You receive one call for each customer call. Once you answer your phone, all call control is handled through Agent Desktop. When you hang up your phone, you are placed in Ready state and are available to receive another customer call.

  Note: For information, see How does Unified MA deliver calls to mobile agents? (page 15))

Step 7 Specify a **Mobile Agent Phone Number**. The dial number for the phone you are using.

Note: The phone number must consist only of numbers. It cannot include any spaces, dashes, parentheses, or other non-numeric characters.

Step 8 Click **OK**.

The Agent Desktop starts and is immediately minimized on the taskbar at the bottom of the mobile agent's Windows desktop.

Login notes:

- The Login Name field can be a maximum of 32 characters. The Login ID, Extension, and Password fields can be a maximum of 12 characters.
- Agent Desktop can control only those calls on the extension entered in the Login dialog box, even if the mobile agent is configured with multiple extensions.
- When logging in, the mobile agent might see the error message, “A licensing error has occurred. Please see your administrator.” This generally appears when all Agent Desktop software licenses are in use. For this reason, it is important that the mobile agent close Agent Desktop completely when finished using it, rather than simply logging off. As long as Agent Desktop is running, one license is being used.

How to verify that login was successful

Step 1 Check that your CAD displays the following:

- Your agent name, as configured in ICM.
- Your agent extension, as entered in the Login dialog box.
- Your agent ID or name, as entered in the Login dialog box.
- Your current agent state and the time spent in that state.
- Current status of agent desktop features.
- Current system time.

Note: Remember, you must enter the Ready state before you can begin processing calls.

How to login with another phone number

Step 1 Click **Log off**.

Step 2 Follow the Agent Desktop login procedure, specifying a new phone number.

How to enter the Ready state

You must be in the Ready state to answer an ACD call.

Step 1 Click **Ready** on the toolbar.

How to make calls

Step 1 Click **Not Ready**.

Note: You must be in the **Not Ready** state to make a call.

Step 2 Click **Make Call**.

The Make a Call window appears.

Step 3 Enter a number in the Name: Number field.

Step 4 Click **Dial**

How to transfer a call

There are two types of transfer calls:

- **Supervised transfers**. In a supervised transfer, the mobile agent speaks to the third party to whom the call is being transferred before connecting the active call, in order to confirm that the third party is ready to accept the call.
- **Blind transfers**. In a blind transfer, the mobile agent transfers the active call to the third party without speaking. The remote agent hangs up before the third party answers the phone and therefore, can't confirm if the third party is ready to accept the call.

Follow the instructions below to transfer a call.

Step 1 With a call active, click **Transfer**.

The Transferring Call window appears.

Step 2 Enter the phone number to which the remote agent is transferring the call in the Name: Number field.

Step 3 Click **Dial**.

Step 4 When the phone rings, the **Dial** button changes to the Transfer button.

Step 5

If:	Then:
You want to do a supervised transfer.	Wait for the third person to answer the phone, announce the transfer, then click Transfer.
You want to do a blind transfer.	Click Transfer without waiting for the third person to pick up the phone.

How to make a conference call

There are two types of conference calls:

- **Supervised conference**. In a supervised conference, the mobile agent speaks to the third party he or she wants to add to the call before completing the conference, in order to confirm that the third party is ready to accept the call.
- **Blind conference**. In a blind conference, the mobile agent adds the third party to the conference without speaking to him or her.

  Note: When using a blind conference to add someone to the call, the remote agent might or might not see the call tagged as a conference call in the dashboard pane.

Follow the instructions below to make a conference call.

Step 1 With a call active, click **Conference**.

The Conferencing window appears.

Step 2 Enter the phone number of the person the mobile agent wants to add to the call in the Name: Number field.

Step 3 Click **Dial**.

When the phone rings, the **Dial** button changes to the **Add to Conf.** button.

Step 4

If:	Then:
If you want a supervised conference.	Wait for the third person to answer the phone, announce the conference, then click Add to Conf.
If you want a blind conference.	Click Add to Conf. without waiting for the third person to pick up the phone.

The Conferencing window closes.

Step 5 To add one or more people to the conference call, repeat Steps 1 to 4 for each person.

Note: The total number of conference call participants on a call is determined by settings on the Cisco CallManager. Ask you supervisor for the total number configured for your contact center.

Chapter 5

Using Unified Mobile Agent (for Supervisors)

Unified MA is available on the following Cisco supervisor desktops:

- Cisco CTI OS Supervisor Desktop
- CAD Supervisor Desktop

This section contains the following topics:

Before You Begin

Before you login as a mobile agent, first disable home or cell phone calling features that could impact a customer call experience. Examples of such features are:

- Call waiting
- Call forwarding
- Voice mail

In addition, there are Unified MA limitations you need to be aware of before you begin processing calls:

- Mobile agents cannot perform agent state and call control without a CTI Desktop.
- If you login in nailed connection mode, you *must* answer a setup call before login is complete.
- Unified MA supports Outbound Option calls in nailed connection delivery mode, *only*.
- If a mobile agent on one PG calls a mobile agent on a different PG, and both PGs are connected to the same CallManager cluster, only blind transfer/conference are supported.
- During consult transfer or conference calls, a source Unified MA agent will not hear a ring back after dialing another agent; instead, the source agent will hear Music on Hold, if configured.
- You cannot transfer or conference a call using the buttons on your mobile agent phone; you need to use the Agent Desktop to perform these functions.

Using the CTI OS Supervisor Desktop

Unified MA is available with CTI OS Supervisor Desktop. The CTI OS Supervisor Desktop has all of the functionality of the Agent Desktop, with additional functions for monitoring and managing Agent Team members.

Note: CTI OS Supervisor Desktop is supported for use on Unified CCE/CCH, *only*. It is not supported for use on TDM peripherals.

The instructions that follow describe CTI OS Supervisor Desktop tasks that are *specific* to configuring and interacting with mobile agents. For complete information about using this desktop, see *CTI OS Supervisor Desktop User Guide for Cisco Unified ICM/CC Enterprise & Hosted* .

How to login to the CTI OS Supervisor Desktop

Step 1 Select **Start > Programs > Cisco Systems CTI Toolkit > IPCC Supervisor Desktop**.

The Supervisor Softphone and Team Real-Time Status windows appear.

Step 2 On the Softphone, click **Login**.

The Login dialog box appears.

Step 3 Enter the following information in the dialog box:

- **Connect to**. Use the drop-down menu to select the connection mode that you want to use.
- **Agent ID** or **Agent Login Name**. The agent ID as assigned by the agent's manager.

Note: Depending on the option chosen for logging in during the installation of the CTI OS Server, the Login dialog on the Agent desktop will prompt for either the Agent ID or the Agent Login Name.

- **Password**. The password as assigned by the agent's manager.
- **Instrument**. The directory number for the local CTI port (the agent's virtual extension).
- **Mobile Agent**. Check this box to log in as a mobile agent.
- **Phone Number**. The dial number for the phone the mobile agent is using. This should include all dial-plan information Unified CCE/CCH needs to reach the agent phone.
- **Call Mode**. Choose Nailed Connection or Call by Call. A new call is placed to the agent for each incoming call. (For more information, see How does Unified MA deliver calls to mobile agents? (page 15))

  Note:

  - If you login using nailed connection mode, you *must* answer a setup call before login is complete.
  - Auto answer is supported with the Unified MA Nailed Connection mode. It is not supported with the Unified MA call by call connection mode.

Step 4 Click **OK**.

The supervisor automatically enters the Not Ready state and the **Ready**, **Dial**, and **Logout** agent state control buttons are enabled.

How to verify that login was successful

Step 1 Check that your desktop is in the Not Ready state.

Step 2 Check that the status bar of your Unified MA Supervisor Desktop displays the following:

- Agent ID for the logged in supervisor
- Supervisor Extension
- Supervisor Instrument
- Current Supervisor Status
- The server that the Supervisor is connected to

Step 3 Check that the **Ready**, **Dial**, and **Logout** agent state control buttons are enabled.

How to configure an agent as a mobile agent

CTI Desktop agent configuration is handled through ICM Configuration Manager or, in System IPCC, through the Web Administration tool. For more information, see How to Configure Unified Mobile Agent on ICM Configuration Manager (page 38).

How to monitor mobile agent calls

A supervisor can choose to silent monitor an agent on his/her team. Silent Monitoring means that voice packets sent to and received by the agent's IP device are captured from the network and sent to the supervisor desktop. At the supervisor desktop, these voice packets are decoded and played on the supervisor's system sound card.

Note: For more information about silent monitoring, see *CTI OS Supervisor Desktop User Guide for Cisco Unified ICM/CC Enterprise & Hosted* and *Cisco Supervisor Desktop User Guide, Release 7.1(2)*.

Step 1 Select a logged in agent from the Team State Information grid.

Step 2 In the Team State window, click **Start Silent Monitor**.

When the targeted agent desktop accepts the session, the voice conversation between the monitored agent and the caller will be forwarded to the supervisor desktop and played back on the soundcard of the system.

Step 3 Click **Stop Monitoring Agent** to end the monitoring session.

Using the CAD Supervisor Desktop

Unified MA is available with CAD Supervisor Desktop. The CTI OS Supervisor Desktop has all of the functionality of the Agent Desktop, with additional functions for monitoring and managing Agent Team members.

The instructions that describe CAD Supervisor Desktop tasks that are *specific* to configuring and interacting with mobile agents. For complete information about using this desktop, see *CAD Supervisor Desktop User Guide for Cisco Unified ICM/CC Enterprise & Hosted* .

How to log into Supervisor Desktop

Step 1 First, log into Cisco Agent Desktop.

Note: You must be logged in to be able to use all of Supervisor Desktop's functionality.

Step 2 Choose **Start** > **Programs** > **Cisco** > **Desktop** > **Supervisor**. The Supervisor Login dialog box appears.

Step 3 Enter your Supervisor Desktop login ID and password, and then click **OK** or press **Enter**.

Supervisor Desktop starts. The application will show no data and the status bar will display “No Service” until you select a team from the Team drop-down list.

Note:

- Supervisor Desktop can be configured by the Administrator so that you log in using your login name, not your login ID. The field name (Login ID or Login Name) will reflect which login method you should use.
- The first time you log into Supervisor Desktop, the password is empty by default—all you need to enter is your Login ID. Create your own password by using the Change Password function.
- It might take some time for Supervisor Desktop to start because default report data must be generated.

How to view mobile agents

Step 1 In Supervisor Desktop, choose **View > Preferences**, and then select the Agents node.

Step 2 In the Format node text grid, check the elements you want to use to identify an agent.

The elements are:

- Name
- Extension
- Application used by the agent (CAD, CAD-BE, or IPPA)
- Type of agent (mobile)

A sample of what the name will look like appears on the Sample line.

Step 3 Click **OK**.

For example, if you enter John Doe x1000 CAD 6125551234 (Mobile):

- *John Doe* is the agent name.
- *x1000* is the CTI port the agent is connected to when logging in.
- *CAD* is the application the agent uses.
- *6125551234 (Mobile)* is the number of the phone device the mobile agent is using to handle calls.

How to monitor agents using Unified Mobile Agent

You cannot perform silent monitor or record agents using the Mobile Agent Option using CAD.

Part 3: Configuration and Troubleshooting Appendix for Remote Agent

Remote Agent, the predecessor of Mobile Agent, offers two deployment options:

- Remote Agent with IP Phone (over a Cisco Business Ready Teleworker setup).
- Remote Agent with analog phone.

Mobile Agent provides flexibility and ease of use benefits compared to the Remote Agent with analog phone. Remote Agent will continue to be supported for customers who already have it installed.

However, if you are upgrading to 7.1(1) and are planning to configure a mobile agent to use an *analog* phone or an IP Phone *without* Cisco Business Ready Teleworker setup, you should use the Mobile Agent Option.

Note: Remote Agent continues to be the product of choice for remote IP Phone with the Cisco Business Ready Teleworker setup.

Chapter 6

Introduction to IPCC Remote Agent Option

IPCC Remote Agent Option provides the capability to use remote agents when staffing contact centers.

Note: A *remote agent* is classified as limited to a single agent working at a remote site, such as the agent's home or in an office outside the contact center's headquarters. They are not classified as agents working at one of the contact center's sites. Multiple agents sitting in remote sites are considered *branch agents*.

Support is provided for remote agents using one of the following options:

- Remote Agent with IP Phone (over a Cisco Business Ready Teleworker setup)

  Note: Refer to the Teleworker documentation set at the following web sites: **http://www.cisco.com/go/teleworker**, **http://www.cisco.com/go/v3pn**, and **http://www.cisco.com/go/srnd**.

- Remote Agent with analog phone

By means of this support, Cisco IPCC remote agents *with IP Phone* can benefit from standard Cisco 8xx series Router support, persistent VPN, Cisco IOS based security, and QoS for voice.

Agents are connected to the corporate network using a residential broadband (cable or DSL) network connection that can support voice, data, and video traffic. The connection is secure, and provides "always-on" access to call-center applications using a VPN. Built-in, end-to-end security helps ensure that confidential customer information, such as medical records and financial information, is protected, and the corporate network is secure from "back door" attacks.

This section contains the following topics:

- Remote Agent with Analog Phone Call Flow, page 73

About IPCC Remote Agent Option Primary Components

The primary components of the IPCC Remote Agent Option are:

- **Cisco IP Contact Center solution**: Cisco IP Contact Center combines Cisco IP telephony and ready-to-use computer telephony integration (CTI) capabilities in a call-center product suite. The software includes intelligent call routing, multichannel automatic call distribution (ACD) capability, IVR, call queuing, and consolidated reporting features.

  Cisco IP Contact Center components include the following:

  – Cisco CallManager: Provides traditional private branch exchange (PBX) telephony features and functions to packet-telephony devices. Installed on a server-class PC, Cisco CallManager software provides basic call processing, signaling, and connection services to Cisco IP Phones, VoIP gateways, and software applications.

  – Cisco Computer Telephony Integration Object Server (CTI OS) Desktop and Cisco Agent Desktop (CAD): Allow an agent to control the remote agent state (for example, Login, Available/Unavailable, and Work or Wrap Up) and perform call control (answer, release, hold, and transfer).

  – Cisco Customer Voice Portal (formerly Internet Service Node) or Cisco IP IVR: Provides announcements, prompting, gathering of caller-entered digits, and a queue point to park calls when all remote agents are busy.

  – VoIP gateways.

  – Centralized monitoring and recording: Provides call-center managers with real-time and historic data for all remote agents.

- **Cisco Business Ready Teleworker architecture** (for IP Phone only): The Cisco Business Ready Teleworker architecture, combined with Cisco IP Contact Center, gives remote agents the same accessibility to call-center applications as staff based at central sites. Cisco Business Ready Teleworker provides the most comprehensive security and network management available in a teleworking environment over a standard cable or broadband connection. This includes QoS to help ensure prioritization of mission-critical or delay-sensitive traffic. Cisco Business Ready Teleworker can be quickly and cost-effectively deployed to deliver high-quality, consistent application access for remote agents through an always-on, secure, and centrally managed connection to the enterprise network.

  Note: A remote agent using an analog phone does not require a Cisco 8xx Series Router and does not use the Cisco Business Ready Teleworker setup.

  Cisco Business Ready Teleworker components include the following:

  – VPN: Provides secure, consistent access to information, call-center applications, and customer data. The VPN tunnel is transparent to applications and the end user, and promotes stable and consistent application behavior over the WAN, protecting and extending existing infrastructure investments.

Note: Agents will receive persistent VPN communication from the Cisco 800 Series Router.

– Advanced application access: With IP telephony a separate PBX, voice switch, or ACD call-control platform at the remote-agent location is not needed. Network-based ACD extends call-center services to thousands of remote-agent locations simultaneously.

– QoS: Helps ensure high-quality voice communication between the caller and remote agent. Voice, data, and video can be delivered over the same line by prioritizing applications based on bandwidth requirements or business priorities.

Note: QoS delivers marked tagged packets, but the service is not guaranteed since it is over a service provider network.

– Network security and authentication: Security is integrated completely with all other functions. End-to-end security options for remote agents include trust and identity options (802.1x authentication), integrated firewall, intrusion detection system (IDS), and host-based intrusion detection with Cisco Security Agent.

– Centralized management and support: Helps ensure control over the performance of remote agents as though they were based on the main call center. Administrators can push policies and configurations transparently to remote-agent locations, perform quality surveys, and do real-time remote monitoring.

See Also

Refer to the Cisco IPCC, CTI OS, and CAD documentation set at **the Cisco web page** (http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm) for detailed information about these applications.

Refer to the Teleworker documentation set at the following web sites: **http://www.cisco.com/go/teleworker**, **http://www.cisco.com/go/v3pn**, and **http://www.cisco.com/go/srnd**.

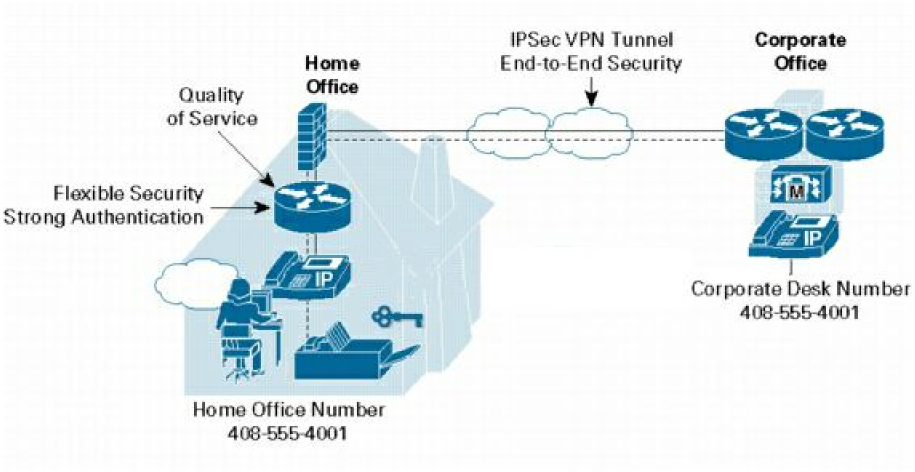
How Cisco IPCC Remote Agent Option Works with an IP Phone

Note: IPCC Remote Agent Option with IP Phone is supported on the Cisco IPCC Enterprise Edition, the Cisco IPCC Hosted Edition, and the Cisco IPCC Express Edition solutions.

At the remote agent site, a Cisco IP Phone, with an ACD extension number, connects to a Cisco 8xx Series secure, persistent Broadband Router that provides a secure VPN connection back to the call center over a broadband facility. The router, based on Cisco IOS Software, provides all the features necessary for an always-on, business-ready connection in a single cost-effective platform. A Cisco CallManager on the corporate network provides the call management on the IP Phone.

Note: This is one option available when using IPCC Remote Agent Option. This product is also available using the Remote Agent with analog phone.

Figure 7: IPCC Remote Agent Option with IP Phone



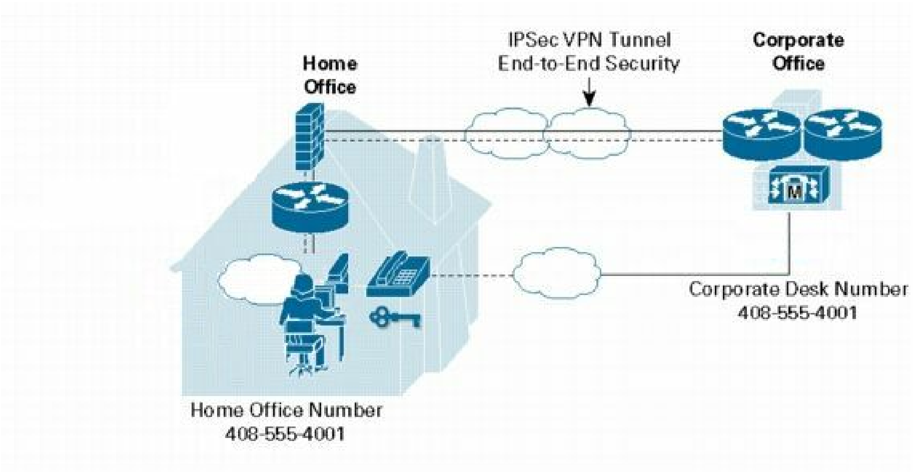
When a call comes in to the call center, the Cisco CallManager alerts the Cisco IP Contact Center, which then finds the best available remote agent based on customer-defined business rules. If no remote agents are available, the call is held in an IVR queue (so customers can listen to a recorded message or music) until an agent becomes available.

How Cisco IPCC Remote Agent Option Works with an Analog Phone

Note: IPCC Remote Agent Option with analog phone is supported on the Cisco IPCC Enterprise Edition and the Cisco IPCC Hosted Edition solutions, *only*.

At the remote agent site, an analog phone connects to the PSTN and using an active broadband connection, the agent uses VPN to access the corporate site (using SoftVPN client) from his/her PC.

Figure 8: IPCC Remote Agent Option with Analog Phone

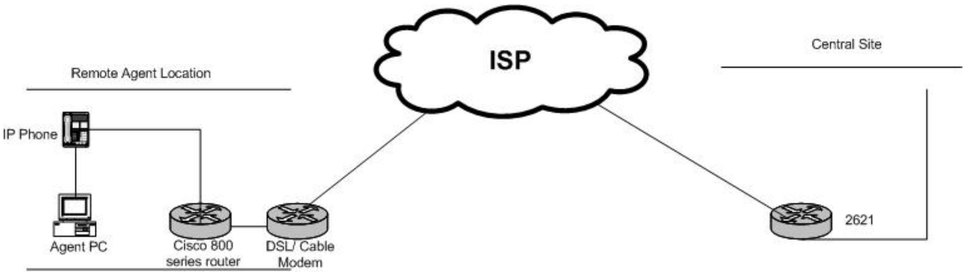


When a call comes in to the contact center, the Cisco CallManager alerts the Cisco IP Contact Center, which then finds the best available remote agent based on customer-defined business rules. If the remote agent is on an analog phone, CallManager sends the call to the Voice Gateway (VG248) which in turn sends it to the PSTN through the VoIP gateway's PRI lines. If no remote agents are available, the call is held in an IVR queue (so customers can listen to a recorded message or music) until an agent becomes available.

Remote Agent with IP Phone Call Flow

The following figure displays a typical call flow.

Figure 9: Remote Agent with IP Phone Call Flow



1. The remote agent becomes available by logging on to the corporate domain using VPN over the ADSL/Cable connection, and by launching the agent desktop interface to log on the CTI server. The remote agent then goes into a ready mode.

2. Customer calls in from PSTN.

3. Call flows in on PRI VoIP gateway.

4. Call is processed by CallManager and routed to Cisco IP IVR.

5. Call is sent to the remote agent.

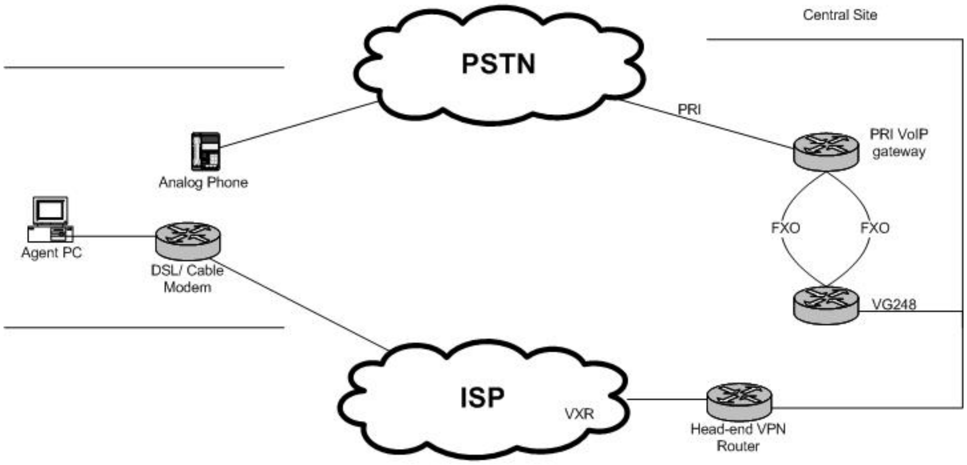
6. The remote agent's IP Phone rings and the agent desktop receives a screen pop with the incoming call.

7. The supervisor, whether remote or in contact center, can fully control an agent, including barge, intercept, chat, and state controls.

Remote Agent with Analog Phone Call Flow

The following figure displays a typical call flow.

Figure 10: Remote Agent with Analog Phone Call Flow



1. The remote agent becomes available by logging on to the corporate domain using VPN over the ADSL/Cable connection, and by launching the agent desktop interface to log on the CTI server. The remote agent then goes into a ready mode.

2. Customer calls in from PSTN.

3. Call flows in on PRI VoIP gateway.

4. Call is processed by CallManager and routed to Cisco IP IVR.

5. A VG248 port is designated as the remote agent phone. An incoming call to IPCC sends a ring command to the VG248 port.

6. The VG248 FXS port is connected to the FXO port on the voice gateway.

7. The voice gateway using Private line automatic ring down (PLAR) forwards the ring command over PSTN to the remote agent's analog phone.

8. The analog phone receives the ring command from its local PSTN provider. (This happens because the PLAR was sent from the IPCC voice gateway.)

9. The remote agent's analog phone rings and the agent desktop receives a screen pop with the incoming call.

Chapter 7

System Configuration for Remote Agent with IP Phone

This section contains the following topics:

Configuration Guidelines

The following tables provide configuration checklists and guidelines to follow when using the Remote Agent with IP Phone.

Note: Refer to the *Cisco ICM/IPCC Enterprise & Hosted Editions Release Hardware and System Software Specifications (Bill of Materials)* for this release (located on the **Cisco web page** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html)) and the *Cisco Response Solutions (CRS) Software and Hardware Compatibility Guide* (located on the **Cisco web page** (http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_documentation_roadmaps_list.html)) for details about operating system and software requirements.

Configuring Remote Agent with IP Phone

Note: IPCC Remote Agent Option with IP Phone is supported on the Cisco IPCC Enterprise Edition, the Cisco IPCC Hosted Edition, and the Cisco IPCC Express Edition solutions.

Step	Description
1.	Provision the remote agent PC and IP Phone on the IPCC central site to ensure operability *before* distributing it to a remote agent site.
2.	At a remote agent site, connect the agent desktop to the RJ45 port on the back of the IP Phone.

Step	Description
	Note: The IP Phone and agent desktop PC get their network settings from DHCP.
3.	Create a DNS entry for the remote agent desktop; otherwise, an agent will not be able to connect to a CTI server. DNS entries can be dynamically updated or entered as static updates.
4.	Configure the agent desktop PC at the remote site with an IP address, network mask, DNS, and default gateway configured for DHCP.
5.	Make sure the 7960 IP Phone has a power supply. (The Cisco 8xx Series Router will not supply power to the IP Phone.)
6.	Critical remote agents must have a backup power supply. The backup power supply must be able to power a PC, an 831 Router, a broadband modem, and an IP Phone.

Remote Agent with IP Phone Network Requirements Checklist

Network Requirements
Ensure the ADSL and Cable bandwidth values are set to at least 256kb uplink and 1 Mbps downlink.
Do not exceed 60ms to 90ms of jitter delay each way on the maximum ADSL network delay. If the ADSL delay is greater than the maximum, the IPCC application will encounter longer response times.
Make sure the IPCC bandwidth value does not exceed 128k uplink; otherwise, the remote agent solution might not work properly.
The default codec for 256kb uplink is the G.729. To achieve higher voice quality, use the G.711.
Only unicast Music on Hold (MOH) streams are supported.
Set up a transcoder to enable outside callers to receive MOH, if the MOH server is not set up to stream G.729 codec.
As a backup to the remote agent desktop, you can configure the remote agent to use the IP Phone as a login device when possible.

Remote Agent with IP Phone Considerations

IP Phones supported with IPCC Remote Agent Option are those currently compatible with IPCC as listed in the *Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) Hardware and System Software Specifications (Bill of Materials).*

Chapter 8

System Configuration for Remote Agent with Analog Phone

This section contains the following topics:

Configuration Guidelines

The following tables provide configuration checklists and guidelines to follow when using the Remote Agent with analog phone.

Note: Refer to the *Cisco ICM/IPCC Enterprise & Hosted Editions Release Hardware and System Software Specifications (Bill of Materials)* for this release (located on the **Cisco web page** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html)) and the *Cisco Response Solutions (CRS) Software and Hardware Compatibility Guide* (located on the **Cisco web page** (http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_documentation_roadmaps_list.html)) for details about operating system and software requirements.

Configuring Remote Agent with Analog Phone at the Central Office Site

Note: IPCC Remote Agent Option with analog phone is supported on the Cisco IPCC Enterprise Edition and the Cisco IPCC Hosted Edition solutions, *only*.

Provision the remote agent PC and analog Phone on the IPCC central site to ensure operability *before* distributing it to a remote agent site.

Configuration Summary: Add the VG248 voice gateway to the Cisco Unified Communications Manager configuration at the central office site. Each of the ports on the VG248 are what the agents use as their login devices when they are remote. These are the extensions they use when they log in. The configuration on the VG248 is a connection through PLAR routing direct to the agents home (or remote) phone. For an example configuration, See also Sample Cisco IOS Configuration for Analog FXO to PRI Gateway (page 93)

Step	Description
1.	On the Cisco Unified Communications Manager, assign a Directory Number (DN) to a port on the VG248; for example: 6777.
2.	On the DC (Domain Controller)/ DNS Server, create a DNS entry for the remote agent's desktop; otherwise the agent will not be able to connect to a CTI server. DNS entries can be dynamically updated or entered as static updates. If DNS entries are not desired, ensure that theclient connects to the CTI server through IP.
3.	Create labels for the new extension connected to the Unified Communications Manager and the Unified IP IVR peripheral.
4.	Add the device target to the IPCC configuration. See the IPCC Administration & Configuration Guide.
5.	Add the device to pguser. This is described in the Cisco Unified Communications Manager Administration Guide. Go to the 'Users' - Application and select the user associated with the PG. From the list of unregistered devices, add the appropriate device to the list of associated devices.
6.	Directly connect the VG248 FXS port to a FXO port on the gateway router. Each FXS port you are using on the VG248 is connected to an FXO port on the voice gateway router.
7.	Configure the gateway FXO port as a connection plar to your (the agent's) home (or remote) phone number; for example: 6035551212. **Note:** The phone number must match the dial plan setup in the Unified Cisco Communications Manager. The connection plar command goes on the FXO port of the gateway router(s).

Agent's Home (Remote) Configuration and Setup

Step	Description
1.	Configure the agent desktop PC at the remote site with an IP address, a network mask, DNS, and default gateway configured for DHCP.
2.	Set up the VPN client to connect to the contact center's hedquarters.

Example Remote Connection Process

Step	Description
1.	Ensure that the VPN connection is up.
2.	Log into the CTIOS server.
3.	Agent logs in on extension 6777 and goes Available on extension 6777. Unified IPCC Enterprise knows to send the call to 6777. The phone number 6777 is the agent's remote number that is configured at the gateway. This needs to be done ahead of time. Every port on the VG248 that will be used for agents should have an associated remote phone number to call using the connection plar command.

Step	Description
4.	The agent gets notification that a call is coming and the home (or remote) phone rings.

Remote Agent with Analog Phone Network Requirements Checklist

Network Requirements
Do not exceed 150ms Round Trip Time (RTT) of ADSL/Cable network delay.
Do not exceed not exceed 60ms of jitter delay.
The minimum broadband bandwidth for the agent desktop is 256kb uplink and 1 Mbps downlink.
Configure the voice gateway/access server with at least one active PRI, T1, E1, or DS3 connection to the PSTN.
The remote agent's phone number is the number assigned via PLAR routing in the VoIP gateway. **Note:** The remote agent PSTN phone number might vary in an actual deployment.
The phones at the remote sites will be analog phones only connected to the PSTN.
The current configuration only supports unicast Music on Hold (MoH) streams. A Cisco CallManager is the MoH server.
The maximum PSTN delay supported is 250ms.
Configure the VG248 to use G.711.

Remote Agent with Analog Phone Considerations

An analog phone is classified as any PSTN phone; for example, a regular touchtone phone or a mobile/cell phone both qualify as analog phones.

Chapter 9

Remote Agent User Information

IPCC Remote Agent Option is available on the following Cisco desktops:

- **Cisco CTI Toolkit Agent Desktop**: Provides an interface that enables agents to perform telephony call control and agent state control. The CTI Toolkit Agent Desktop provides an interface to allow call data to be presented to an agent in the form of a screen pop. The CTI Toolkit Agent Desktop also provides agents with statistics and chat capability.

  Note: CTI OS only supports chat between agents on the same peripheral.

- **Cisco CTI Toolkit IPCC Supervisor Desktop**: The Supervisor Desktop has all of the functionality of the Agent Desktop, with additional functions for monitoring and managing Agent Team members.

  Note: The CTI Toolkit IPCC Supervisor Desktop is supported for use on Cisco IPCC Enterprise only. It is not supported for use on TDM peripherals.

- **Cisco Agent Desktop**: Provides call control capabilities—such as call answer, hold, conference, and transfer, and ACD state control—ready/not ready, wrap up, etc. Customer information is presented to an agent through an enterprise data window and an optional screen pop. Cisco Agent Desktop requires minimum screen real estate and enables agents to customize its functionality to meet their individual needs.

  Note: CAD is *not* available with IP Phone Agent using an analog phone.

Note:

- Refer to the Cisco CTI OS documentation (located on the **Cisco web page** (http://www.cisco.com/en/US/products/sw/custcosw/ps14/products_user_guide_list.html)) and the CAD documentation (located on the **Cisco web page** (http://www.cisco.com/en/US/products/sw/custcosw/ps427/products_user_guide_list.html)).

- Refer to the *Cisco ICM/IPCC Enterprise & Hosted Editions Release Hardware and System Software Specifications (Bill of Materials)* for this release (located on the **Cisco web page** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html)) and the *Cisco Response Solutions (CRS) Software and Hardware Compatibility Guide* (located on the **Cisco web page** (http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_documentation_roadmaps_list.html)) for details about operating system and software requirements.

This section contains the following topics:

Using CTI Toolkit and CAD Desktops

Using the CTI Toolkit Agent Desktop

Action	Resolution
How does an agent log in to the desktop?	To log into CTI Toolkit Agent Desktop, click the **Login** button. The **Login** button connects agents to the CTI Server and logs agents into a selected ACD switch. When an agent clicks the **Login** button, the CTI Login dialog box appears. Enter the following information in the dialog box: • **Connect to**. Use the drop-down menu to select the connection profile that you want to use. • **Agent ID**. The agent ID as assigned by the agent's manager. **Note:** Depending on the option chosen for logging in during the installation of the CTI OS Server, the Login dialog on the Agent desktop will prompt for either the Agent ID or the Login Name. • **Password**. The password as assigned by the agent's manager. • **Instrument**. The device ID assigned to the teleset where the agent will receive calls. After entering this information, click the **OK** button. On a successful login, the following occurs: • The agent automatically enters the state configured on the switch, either Ready or Not Ready state. • The status bar on the bottom of the CTI Toolkit Agent Desktop Screen displays the following information – Agent ID for the logged in agent – Agent Extension

Action	Resolution
	– Agent Instrument – Current Agent Status – The server that the agent is connected to • Buttons for actions that are allowed from your current agent state are enabled. **Note:** If the **Login** button is not enabled when the CTI Toolkit Agent Desktop displays, the remote agent did not successfully log in.
How can an agent verify a successful login?	On a successful login, the following occurs: • The remote agent automatically enters the state configured on the switch, either Ready or Not Ready state. • The status bar on the bottom of the CTI Toolkit Agent Desktop window displays the following information: – Agent ID for the logged in agent – Agent Extension – Agent Instrument – Current Agent Status – The server that the agent is connected to • Buttons for actions that are allowed from your current agent state are enabled.
How does an agent enter the Ready state to start accepting calls?	An agent enters either Ready or Not Ready state on completion of a successful login, depending on the configuration of the agent's switch. If the agent is in the Not Ready state and the **Ready** button is enabled, enter the Ready state by clicking the **Ready** button.
How does an agent perform a transfer?	To transfer a call, perform the following steps: 1. Click the **Transfer** button. The CTI Dialing Pad dialog box appears. 2. Enter the phone number to be dialed in the Dialed Number field or select a destination from the pull-down menu. The pull-down menu contains the last six numbers dialed from this desktop. 3. Optionally, click the **More** button to display the Call Data tab, where you can enter data associated with the call.

Action	Resolution
	The remaining steps depend on whether or not the agent wants to speak with the consulted agent upon call transfer. • If the agent does not want to speak with the consulted agent, click the **Single Step** button. The call is transferred automatically. • If the agent wants to speak with the consulted agent, click the **Transfer Init** button. Once the **Transfer Init** button is pressed, the call will be put on hold. The agent has an opportunity to speak to the consulted agent before completing the transfer. When the consult call is answered, the button changes to **Transfer Complete**. To complete the transfer, click the **Transfer Complete** button.
How does an agent initiate a conference call?	To initiate a conference call, perform the following steps: 1. Click the **Conference** button. The CTI Dialing Pad dialog box appears. 2. Enter the phone number to be dialed in the Dialed Number field or select a destination from the pull-down menu. The pull-down menu contains the last six numbers dialed from this desktop. 3. Optionally, click the **More** button to display the CTI Dialing Pad. 4. Click the **Conference Init** button. The call is now put on hold. The agent will have an opportunity to speak to the consulted agent before completing the conference. When the consult call is answered, the button changes to **Conference Complete**. To complete the conference, click the **Conference Complete** button. When the conference operation completes, the two calls then appear on the Call Information Grid as one call.
When is an agent available to make calls?	An agent is able to make calls if the **Dial** button is enabled. Depending on the agent's switch, the agent might also be able to make calls if the **Ready** or **Not Ready** buttons are enabled.

Using the CAD Desktop

Action	Resolution
How does an agent log in to the desktop?	To start Agent Desktop: 1. Choose **Start > Programs > Cisco > Desktop > Agent**. The Agent Login dialog box appears. **Note:** • For IPCC Enterprise only, Agent Desktop prompts for either the remote agent's Login ID or the Login Name in the Login dialog box. Which prompt appears depends on how the administrator has configured the system. • If the login method (Login Name or Login ID) is changed while the remote agent is in the process of logging in, an error message appears stating that the login method

Action	Resolution
	has changed. The remote agent must restart Agent Desktop in order to log in using the new method. (The information in this note is not applicable to IPCC Express.) 2. Enter the remote agent login ID or login name, password, and extension in the appropriate fields, and then click OK or press Enter. – If the remote agent attempts to log in and the login ID/login name (with or without the same extension used in association with it) is already in use by another agent, the remote agent will be asked to forcibly log in. If the remote agent opts to do so, that agent is logged in and the other agent using that ID will be logged out. – If the remote agent attempts to log in and the extension is already in use by another agent, that agent will not be able to log in unless a different extension is entered. Agent Desktop starts and is immediately minimized on the taskbar at the bottom of the remote agent's Windows desktop. Login notes: • The Login Name field can be a maximum of 32 characters. The Login ID, Extension, and Password fields can be a maximum of 12 characters. • Agent Desktop can control only those calls on the extension entered in the Login dialog box, even if the remote agent is configured with multiple extensions. • When logging in, the remote agent might see the error message, “A licensing error has occurred. Please see your administrator.” This generally appears when all Agent Desktop software licenses are in use. For this reason, it is important that the remote agent close Agent Desktop completely when finished using it, rather than simply logging off. As long as Agent Desktop is running, one license is being used.
How does an agent get into the Ready state to start accepting calls?	Clicking the **Ready** button changes the state to Ready, indicating that the remote agent is available to receive ACD calls.
How does an agent transfer a call?	There are two types of transfer calls: • **Supervised transfers**. In a supervised transfer, the remote agent speaks to the third party to whom the call is being transferred before connecting the active call, in order to confirm that the third party is ready to accept the call. • **Blind transfers**. In a blind transfer, the remote agent transfers the active call to the third party without speaking. The remote agent hangs up before the third party answers the phone and, therefore, cannot confirm if the third party is ready to accept the call.

Action	Resolution
	To transfer a call: 1. With a call active, click **Transfer**. The Transferring Call window appears. 2. Enter the phone number to which the remote agent is transferring the call in the Name: Number field. 3. Click **Dial**. When the phone rings, the **Dial** button changes to the Transfer button. 4. Take one of the following actions: – For a supervised transfer, wait for the third person to answer the phone, announce the transfer, then click **Transfer**. – For a blind transfer, click **Transfer** without waiting for the third person to pick up the phone.
How does an agent initiate a conference call?	There are two types of conference calls: • **Supervised conference**. In a supervised conference, the remote agent speaks to the third party he or she wants to add to the call before completing the conference, in order to confirm that the third party is ready to accept the call. • **Blind conference**. In a blind conference, the remote agent adds the third party to the conference without speaking to him or her. **Note:** When using a blind conference to add someone to the call, the remote agent might or might not see the call tagged as a conference call in the dashboard pane. To make a conference call: 1. With a call active, click **Conference**. The Conferencing window appears. 2. Enter the phone number of the person the remote agent wants to add to the call in the Name: Number field. 3. Click **Dial**. When the phone rings, the **Dial** button changes to the **Add to Conf.** button. 4. Take one of the following actions: – For a supervised conference, wait for the third person to answer the phone, announce the conference, then click **Add to Conf**.

Action	Resolution
	– For a blind conference, click **Add to Conf.** without waiting for the third person to pick up the phone. The Conferencing window closes. 5. To add one or more people to the conference call, repeat Steps 1 to 4 for each person. **Note:** The total number of conference call participants on a call is determined by settings on the Cisco CallManager. Ask you supervisor for the total number configured for your contact center.
When is an agent available to make calls?	When the remote agent is in the Not Ready state and the system is functioning to enable call control, the agent is available to make and receive calls.

Installation and Configuration Checklists

Validating Installation and Configuration of Remote Agent with IP Phone Components Checklist

Issue	Resolution
Does the IP Phone boot?	Make sure the separate power supply is used for the phone. The 831 router does not supply power to the IP Phone.
Does the IP Phone register with CallManager?	The phone must be configured for DHCP; also, domain information must be entered in to the phone configuration.
Is the IPsec tunnel running?	Reboot the 831.
Do you have internet access?	Make sure you have network access to the internet.
Can the agent desktop log in to CTI OS Server?	Make sure the PC is registered in DNS. Make sure the agent login ID/password is valid.
When you pick up the IP Phone, does the desktop reflect that the line is off hook?	Cycle the PG for the remote agent.
Are callers routed to the remote agent?	Make sure callers are routing to the remote agent and the PG is online.
When the remote agent receives a call, does the desktop client's main window display the incoming call?	Check to see if the desktop client's main window displays the incoming call.
Is the desktop window displaying the incoming call correctly?	Check to see if the desktop window displays the incoming call correctly.
Does the MTP application log in?	If you are using the Platronics headset, make sure the USB connection is secure and that it is able to play sound from the desktop.

Issue	Resolution
What's the agent's readiness state when taking a call using an IP Phone?	Once the agent takes a call (either via the IP Phone or the agent desktop), the agent state changes to either the Talking state or the Not Ready state and the agent is unavailable for calls. (The agent *will not* receive any calls while already on a call.)

Validating Installation and Configuration of Remote Agent with Analog Phone Components Checklist

Issue	Resolution
Can the agent desktop log in to CTI OS Server?	Make sure the PC is registered in DNS. Make sure the agent login ID/password is valid.
Is there a dial tone?	Pick up the analog phone and listen for a dial tone to ensure the phone is connected.
Do you have internet access?	Make sure you have network access to the internet.
Are callers routed to the remote agent?	Make sure callers are routing to the remote agent and the PG is online.
What's the agent's readiness state when taking a call using an analog phone?	Remote agents using an analog phone must manually place themselves in the Not Ready state after taking a call.

Hardware Installation and Configuration

Refer to the *Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) Hardware and System Software Specifications (Bill of Materials)* and the *Cisco Response Solutions (CRS) Software and Hardware Compatibility Guide* (located on the **Cisco web site** (http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm)) for details about desktop hardware requirements.

Chapter 10

Troubleshooting Cisco IPCC Remote Agent Option

This section contains the following topics:

Caveats and Limitations

Remote Agent has limitations regarding the following:

- Agents
- Supervisors
- Network
- Security
- Reporting

Agent Limitations

- Only one IPCC Remote Agent Option per household is supported.
- Media Termination for CTI OS and CAD is *not* supported.
- CTI OS Agent Login might take up to 30 seconds. CAD Agent Login might take up to two minutes. Other operations such as Ready/Not ready are not impacted.
- There might be times when the ADSL/Cable link goes down. When the link is back up, the remote agent might have to reset their ADSL/Cable modem, 8xx Series Router, and IP Phone.

The remote agent must become familiar with restarting the 8xx Series Router. Total time for the router to cycle is about two minutes, after which the remote agent will have to re-login again for CTI application.

- Cisco CAD-based IP Phone only agent and Cisco IP Phone control for CTI OS is *not* supported for remote agents.
- Remote agents might experience a delay in screen pop.
- The analog phone itself cannot initiate transfers, conferences, and holds. These functions can only be executed via the CTI OS/CAD desktop agent interface, and only to another agent.
- Remote agents can use the agent desktop interface to initiate calls, but only to other agents.

Supervisor Limitations

- Desktop-based Silent Monitoring/Recording will not work and is not supported. (Silent Monitor—for both CTI OS and CAD—is not supported with Network Address Translation.)
- Remote supervisors are *only* supported for the Remote Agent with IP Phone.

Network Limitations

- Network Address Translation (NAT) is supported when IPCC Remote Agent Option is used with the Cisco Business Ready Teleworker Model. Design guides for Business Ready Teleworker can be found at:
  - **http://www.cisco.com/go/teleworker**
  - **http://www.cisco.com/go/v3pn**
  - **http://www.cisco.com/go/srnd**
- Routing through a Cisco 800 Series Router with Firewall enabled is supported.
- The G.729 codec is not supported for software conference bridges. Voice quality might degrade when the remote agent IP Phone is configured using a G.729 codec and an agent enters a call manager software conference bridge. The conference bridge must be configured on a DSP hardware device. There is no loss of conference voice quality using a DSP conference bridge.

  Note: Use this solution even for pure IP telephony deployments.
- The IPCC server recognizes failures when the remote agent desktop or connection breaks. It will stop routing calls to that agent until an agent logs back in and goes to a ready call state. Callers will be routed to other available agents.
- The only traffic that is marked for priority AF31 from the agent desktop is voice. CTI traffic and Desktop Application traffic is not marked. Voice gets the priority. CRM Desktops like

Siebel and Oracle are supported; however, Silent Monitoring and Recording is not supported for CRM Desktops such as Siebel, Oracle, and so forth. Silent Monitoring, both Desktop based and SPAN Port based, is not supported with CRM Desktops and will not work.

- Do not use soft VPN clients to establish VPN connectivity for remote agents with IP Phones. VPN connection has to be set up using hardware-based VPN through a 8xx Series Router.
- If the remote agent PC modem is down or the connection goes down, Unified ICME software via CTI/CAD/CTI OS server will recognize the failure and will stop routing calls to that agent, until an agent logs back in again, and goes to a ready call state.
- If the ADSL/Cable delay is greater than the maximum, the IPCC application encounters longer application response times.

Security Limitations

- Wireless access points are supported; however, determine their use by the enterprise security policies of the customer. Wireless use does not affect remote agent performance since the bandwidth that wireless supports is greater than the broadband link.

  Note: 7920 Wireless IP Phones are not supported.
- This solution has only been tested with centralized IPCC and CallManager Clusters. Testing was *not* performed with CTI OS using security and Cisco Support Tools.

Reporting Limitations

- No special reports exist for individual remote agents. IPCC Enterprise reports as they pertain to a Headquarter Contact Center are applicable.
- Real Time reporting, Historical reporting, and the monitoring of desktop queue statistics are not supported.

Troubleshooting Information

This section lists troubleshooting FAQs and recovery tips.

Problem	Resolution
How do I find out what Codec is being used?	On Cisco 7960 IP Phones, press the information button twice (this is the "?" or the "I" button, depending on the model you are using).

Table 3: IPCC Remote Agent Option Failure Recovery Tips

Recovery Issue	Resolution
Power failure	Once the power is back up, verify that the machine comes back up properly and that the network is available. For CTI OS, start the CTI desktop and login to the CTI OS server. For Remote Option with IP Phone configuration, the IP Phone needs to contact the tftp server and register with Cisco CallManager. **Note:** UPS can mitigate the risk of a power failure at home by keeping the cable modem and agent's PC powered up for a certain duration.
Internet failure	Once the internet goes down, the connection is lost and the agent goes offline. For CTI OS, once the internet is back up, the agent must re-connect to the CTI OS server and log back in. For Remote Option with IP Phone configuration, the IP Phone will also be disconnected and needs to be reconnected with Cisco CallManager.
Reconnection of the phone to the desktop	Connect the desktop to the IP Phone's second switch port, then connect the IP Phone to the 800 Series Router.
Agent Desktop reboot	See Power failure, above.
Agent Desktop Application restart	Restart the application and log back into the server. If a call is still in progress, do not change the state to Ready.
IP Phone registration failure	Verify that the Internet is available, followed by the network. If yes, check if the tftp server and Cisco CallManager are online.
VPN tunnel failure	If Internet access is available, but the connection to the corporate site is not, verify that the VPN tunnel is not misconfigured / broken. If it is broken, it will have to be reconfigured by the System Administrator.

Chapter 11

Sample Cisco IOS Configuration for Analog FXO to PRI Gateway

The following section provides a sample Cisco IOS configuration for an analog FXO to PRI gateway.

Analog FXO to PRI Gateway

```
hostname pri-fxo-gateway
!
isdn switch-type primary-ni
!
controller T1 3/0
framing esf
linecode b8zs
cablelength short 133
pri-group timeslots 1-24
!
interface Serial3/0:23
bandwidth 230400
no ip address
encapsulation hdlc
no logging event link-status
isdn switch-type primary-ni
isdn incoming-voice voice
no cdp enable
!
voice-port 1/0/0
connection plar opx 4085551234
!
voice-port 1/0/1
```

```
connection plar opx 4085551235
!
dial-peer cor custom
!
dial-peer voice 1 pots
destination-pattern 4085551234
no digit-strip
port 3/0:23
!
dial-peer voice 100 pots
destination-pattern 4085551235
no digit-strip
port 3/0:23
!
end
```

Index