



Cisco CAD Installation Guide

Cisco Unified Contact Center Enterprise Release 7.2
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: 408 527-0883

Customer Order Number:
Text Part Number: 7.2

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

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

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

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

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

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, RateMUX, ScriptShare, SlideCast, 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. (0704R)

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

Cisco CAD Installation Guide

© 2002-2007 Cisco Systems, Inc. All rights reserved.

Revision History

Revision Date	Description
June 2007	First Customer Ship (FCS) version 7.2(1)

Revision History

Contents

1	Before You Install CAD 7.2	
■	Overview	11
	Related CAD Documentation	11
	Obtaining Documentation	12
	Cisco.com	12
	Product Documentation DVD	12
	Ordering Documentation	12
	Documentation Feedback	13
	Cisco Product Security Overview	13
	Reporting Security Problems in Cisco Products	13
	Obtaining Technical Assistance	14
	Cisco Technical Support & Documentation Website	14
	Submitting a Service Request	15
	Definitions of Service Request Severity	16
	Obtaining Additional Publications and Information	16
■	CAD 7.2 Feature Levels	18
■	What's New in This Version	21
■	CAD 7.2 Components	22
	Desktop Applications	22
	Cisco Desktop Administrator	22
	Cisco Agent Desktop	22
	Cisco Agent Desktop—Browser Edition	22
	Cisco IP Phone Agent	23
	Cisco Supervisor Desktop	23
	Services	23
	Browser and IP Phone Agent Service	23
	Chat Service	23
	Directory Services	23
	Enterprise Service	24
	CAD Services LDAP Monitor Service	24
	Licensing and Resource Manager Service	24
	Recording & Playback Service	24
	Recording and Statistics Service	24

Contents

Sync Service	24
Voice over IP Monitor Service.....	24
■ Localization	25
Supported Languages	25
Installation in Localized Contact Centers	25
■ System Configurations	27
Citrix and Microsoft Terminal Services Environments.....	27
■ System Requirements	28
Operating Environment	28
Operating Environment Language Requirements	30
Third Party Software Requirements	30
■ Monitoring Requirements	32
Desktop Monitoring (CAD-based)	32
Required Device Settings for Desktop Monitoring	32
Qualifying NICs for Desktop Monitoring.....	33
Server Monitoring (CAD-based)	34
Unified CM-based Monitoring	34
Recording	34
Recording Functionality Overview	35
Mobile Agent Monitoring and Recording Requirements	36
Setting Up Agents in Unified ICM.	36
Setting Up Supervisors and Teams	36
Skills Statistics	36
Reason Codes	37
■ System Capacity.....	38
■ Supported IP Phones.....	39
Caveats on Using a Cisco 7920 Wireless Phone	39
■ Registry Key Modifications	40

2

Installation

■ Overview.....	41
Installation Locations.....	41

Contents

■ Installing CAD Services	42
■ Cisco Agent Desktop Configuration Setup	45
Entering Configuration Data in Initial Mode	46
Configuring a Single Server or Primary Server in a Replicated System.....	47
Configuring a Secondary Server in a Replicated System	48
CAD Configuration Setup Windows	49
CAD-BE Servers	49
CallManager	50
CallManager SOAP AXL Access	51
CTI OS	52
CTI OS Security Setup	53
CTI Server (CallManager).....	54
ICM Admin Workstation Database	55
ICM Admin Workstation Distributor.....	56
Recording and Statistics Service Database.....	57
Replication Setup.....	58
Restore Backup Data.....	59
Services Configuration.....	60
SNMP Configuration.....	61
Terminal Services.....	62
VoIP Monitor Service	63
■ Cisco Desktop Monitoring Console	64
■ Licensing CAD 7.2.....	66
Obtaining a License Account	66
Using IPCC License Administration	66
Recording Licenses	68
■ Installing Desktop Applications	69
Client Installation Failure	69
Error/Event and Debug Logs	70
Using Automated Package Distribution Tools	70
Cisco Desktop Administrator	70
Cisco Agent Desktop and Cisco Supervisor Desktop	71
Installation Notes	72

Contents

Cisco Agent Desktop—Browser Edition	72
Internet Explorer Settings for CAD-BE.....	73
Pop-up Blocker	73
Internet Options	73
Firefox Settings for CAD-BE	74
Popup Blocker.....	74
Content Settings	74
■ Upgrading From a Previous Version	75
Previous Version Hot Fixes and Service Releases	75
Changing Feature Levels in an Upgrade.....	76
Upgrading from CAD 6.0 to CAD 7.2.....	77
Upgrading from CAD 7.0 or 7.1 to CAD 7.2	78
Upgrading CAD 7.2 to a Newer Version	79
Rolling Back CAD 7.2 to an Earlier Version of CAD	80
Upgrade Notes	80
■ Backup and Restore (BARS).....	82
Backup File Location	82
Backing Up CAD Data.....	82
Restoring CAD Data	83
BackupDB Utility.....	84
InstallRestoreDB Utility	85
CDBRTool Utility	85
BARS Notes.....	87
■ Shutting Down and Restarting Replication	88
Shutting Down Replication (CAD 7.2)	88
Restarting Replication (CAD 7.2).....	89
Shutting Down Replication (CAD 7.1 and before)	90
■ Configuring IP Phones for Cisco IP Phone Agent.....	91
Creating an IP Phone Service	91
Assigning the IP Phone Service to IP Agent Phones.....	92
Creating a Unified CM User	93
Configuring a One-Button Login for IP Phone Agents	94
URL Authentication Parameter	94
Changing the Default URL Authentication Parameter	94

Contents

■ Configuring a Cisco IP Communicator Phone	95
■ Setting Up CTI OS Security	96
Steps to Perform on Each Element	96
CTI OS Server	96
Cisco Desktop Administrator PC	96
Cisco Agent Desktop Client PCs	97
Certificate PC	97
Signing Client CTI OS Security Certificates	98
Signing the Server CTI OS Security Certificate	98
Signing a Peer CTI OS Server Security Certificate	99
■ Repairing CAD	100

3

Removal

■ Removing CAD 7.2	101
--------------------------	-----

A

Using Multiple NICs with the VoIP Monitor Service

Overview	103
Limitations	103
Issues	103
Installing a Second NIC on a VoIP Monitor Service Computer	104

Contents

Before You Install CAD 7.2

1

Overview

CAD 7.2 is installed in 3 stages:

- Install the CAD services
- Install Cisco Desktop Administrator on the system administrator(s) desktop
- Install Cisco Agent Desktop and Cisco Supervisor Desktop on the agents' and supervisors' desktops, and install the Java Runtime Environment browser plug-in on CAD-BE agents' desktops

After you have successfully installed CAD into a properly-configured Cisco Unified Contact Center Enterprise or Hosted environment, run the CAD Configuration Setup tool, and licensed the applications, CAD's basic functionality is ready to use with no further configuration required.

Related CAD Documentation

The following documents contain additional information about CAD 7.2:

- *Cisco Desktop Administrator User Guide*
- *Cisco Agent Desktop User Guide*
- *Cisco Agent Desktop—Browser Edition User Guide*
- *Cisco Supervisor Desktop User Guide*
- *Cisco IP Phone Agent User Guide*
- *Mobile Agent Guide for Cisco Unified CC Enterprise*
- *Cisco CAD Service Information*
- *Integrating CAD Into a Citrix MetaFrame Presentation Server or Microsoft Terminal Services Environment*

Obtaining Documentation

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

Cisco.com

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

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

Ordering Documentation

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

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

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

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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, security notices, and security responses for Cisco products is available at this URL:

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

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

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

Reporting Security Problems in Cisco Products

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

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

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

- For Non emergencies—psirt@cisco.com

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

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

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

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

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

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

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

Obtaining Technical Assistance

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

Submitting a Service Request

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

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

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

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

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

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:
<http://www.cisco.com/go/guide>
- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and

Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

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

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

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

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

<http://www.cisco.com/ipj>

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

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

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

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

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

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

CAD 7.2 Feature Levels

There are three feature levels of CAD 7.2: Standard, Enhanced, and Premium. The following chart outlines the features available at each feature level. All features not listed here are present in all three versions.

Feature	Standard	Enhanced	Premium
Cisco Agent Desktop			
Task buttons		•	•
HTTP Post/Get action			•
Event-triggered workflows	•	•	•
IPC Receive action			•
Timer action		•	•
Enterprise data thresholds	•	•	•
Wrapup data	•	•	•
Reason codes	•	•	•
Integrated browser			•
Agent-initiated chat	•	•	•
Agent-initiated call recording		•	•
Cisco Unified Outbound Dialer		•	•
Cisco IP Communicator supported	•	•	•
Cisco Unified Mobile Agent supported	•	•	•
Cisco Agent Desktop—Browser Edition			
Task buttons		•	•
HTTP Get action		•	•
Event-triggered workflows	•	•	•
Enterprise data thresholds	•	•	•
Wrapup data	•	•	•
Reason codes	•	•	•
Integrated browser		•	•

Feature	Standard	Enhanced	Premium
Agent-initiated call recording		•	•
Cisco IP Communicator supported	•	•	•
Cisco Unified Mobile Agent supported	•	•	•
Cisco IP Phone Agent			
Enterprise data	•	•	•
Wrap-up data	•	•	•
Reason codes	•	•	•
Skill group data	•	•	•
Agent-initiated recording		•	•
Cisco Supervisor Desktop			
Silent monitoring	•	•	•
Barge-in	•	•	•
Intercept	•	•	•
Recording		•	•
Team messages (TMs)	•	•	•
Integrated browser	•	•	•
Supervisor work flows—tree control node actions only		•	•
Supervisor work flows—all actions			•
Skill statistics	•	•	•
Real-time displays (text)	•	•	•
Real-time displays (charts)			•
Web page push to agents			•
Cisco Desktop Administrator			
Configure CAD, CAD-BE interface		•	•
Configure work flows		•	•
Configure CAD, CAD-BE integrated browser			•

Feature	Standard	Enhanced	Premium
HTTP Post/Get action			•
IPC Receive action			•
Timer action		•	•

What's New in This Version

CAD 7.2 includes these new features.

- Localized in Russian and Traditional Chinese
- Support for Windows MUI language packs
- Improved legibility of Graphical User Interface (GUI)
- Support for Windows 2003 Server R2
- Support for Windows Vista

NOTE: Automated updates are not supported on Windows Vista.

- Login and password encryption in CAD-BE and IP Phone Agent
- Configurable support for Cisco Unified Communications Manager-based call silent monitoring via an IP phone instead of CAD-based (desktop or server) monitoring.
- Streamlined configuration setup during installation
- Integration of configuration of the CAD Services LDAP database and the Recording and Statistics Service database
- Support for Microsoft Simple Network Management Protocol (SNMP)
- Improved serviceability with enhanced logging message content
- Support for exporting and importing workflow actions

CAD 7.2 Components

CAD 7.2 is a suite of applications and services consisting of the following elements.

Desktop Applications

Cisco Desktop Administrator

Cisco Desktop Administrator provides centralized administration tools to configure the Cisco desktop applications. It supports multiple administrators, each able to configure the same data (although not at the same time; only one person can work in one node at any one time to ensure data integrity).

See the *Cisco Desktop Administrator User Guide* for more information.

Cisco Agent Desktop

Cisco Agent Desktop is an application that helps agents manage their customer contacts. It includes enterprise data, call activity information, reports, a chat client for chatting with other agents and supervisors, and an integrated browser window.

The agent can use a hard IP phone or the Cisco IP Communicator soft phone with Agent Desktop.

Cisco Agent Desktop controls the telephony activities on the agent's CCM phone line. CAD cannot coexist with other applications that attempt to share or control the agent's CCM phone line, such as Cisco Attendant Console and Cisco Unified Personal Communicator.

See the *Cisco Agent Desktop User Guide* for more information.

Cisco Agent Desktop—Browser Edition

Cisco Agent Desktop—Browser Edition (CAD-BE) is a Java applet version of Cisco Agent Desktop that runs in the Internet Explorer or Firefox web browser.

CAD-BE 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 the agent through an enterprise data window. CAD-BE also provides an integrated browser window so agents can view intranet, internet, and web application pages as needed.

See the *Cisco Agent Desktop—Browser Edition User Guide* for more information.

Cisco IP Phone Agent

Cisco IP Phone Agent is a service that runs on the agent's Cisco IP phone that enables agents to manage their customer contacts without the need of a computer. It includes enterprise data, agent states, wrap-up data, reason codes, and skill statistics.

See the *Cisco IP Phone Agent User Guide* for more information.

Cisco Supervisor Desktop

Cisco Supervisor Desktop allows contact center supervisors to manage agent teams in real time. They can observe, coach, and view agent status details, as well as view conference information. Without the caller's knowledge, supervisors can initiate chat sessions with agents to help them handle calls, and push web pages to the agent to assist the agent in serving the customer. They can also silently monitor and record customer calls and, if necessary, conference in or take over those calls using the barge-in and intercept features. Through the Supervisor Record Viewer, supervisors can play back and save recorded agent calls.

Services

Browser and IP Phone Agent Service

The Browser and IP Phone Agent (BIPPA) Service enables IP phone agents to log in and out of CTI server, change agent states, and enter wrap-up data and reason codes without using a computer. It also provides these functions to agents who use the browser-based CAD-BE.

This service works in conjunction with the Services feature of Cisco Unified Communications Manager (Unified CM) and Cisco IP phones.

Chat Service

The Chat Service acts as a message broker between the Chat clients and Supervisor Desktop. It is in constant communication with all agent and supervisor desktops.

Agents' desktops inform the Chat Service of all call activity. The service, in turn, sends this information to all appropriate supervisors. It also facilitates the sending of text chat and team messages between agents (excluding CAD-BE and IP Phone agents) and supervisors.

Directory Services

All other CAD services register with Directory Services at startup. Clients use Directory Services to determine how to connect to the other services.

The majority of the agent, supervisor, team, and skill information is kept in Directory Services. Most of this information is imported from the ICM logger and kept synchronized by the Sync (Synchronization) Service.

Enterprise Service

The Enterprise Service tracks calls in the system. It is used to attach IVR-collected data to a call in order to make it available at the agent desktop. It also provides real-time call history.

CAD Services LDAP Monitor Service

The CAD Services LDAP Monitor Service starts Directory Services and then monitors it to ensure that it keeps running.

Licensing and Resource Manager Service

The License and Resource Manager (LRM) Service distributes licenses to clients and oversees the health of the CAD services. In the event of a service failure, it initiates the failover process.

Recording & Playback Service

The Recording & Playback Service extends the capabilities of the VoIP Monitor Service by allowing supervisors and agents to record and play back calls.

Recording and Statistics Service

The Recording and Statistics Service maintains a 7-day history of agent and team statistics, such as average time an agent is in a particular agent state, last login time, number of calls an agent has received. It also stores real-time data, which is reset each day at midnight.

Sync Service

The Sync Service connects to the ICM Administration Workstation SQL database via an ODBC connection and retrieves agent, supervisor, team, and skill information. It then compares the information with the information in Directory Services and adds, updates, or deletes entries as needed to stay consistent with the Unified ICM configuration.

Voice over IP Monitor Service

NOTE: The VoIP Monitor Service is not used with Unified Communications Manager-based monitoring.

The Voice over IP (VoIP) Monitor Service enables supervisors to silently monitor agents. The service accomplishes this by “sniffing” network traffic for voice packets.

Multiple VoIP Monitor Services can be installed in one logical contact center to ensure there is enough capacity to handle the number of agents.

Localization

Supported Languages

In CAD 7.2, the CAD desktop applications (except for Cisco Desktop Administrator, which is available in English only) are localized in the languages displayed in [Table 1](#).

Table 1. supported languages and CAD desktop application availability.

Supported Language	CAD	CAD-BE	CSD	IPPA	CDA
Chinese--Simplified	x	x	x		
Chinese--Traditional	x	x	x		
Danish	x	x	x	x	
Dutch	x	x	x	x	
English	x	x	x	x	x
French	x	x	x	x	
German	x	x	x	x	
Italian	x	x	x	x	
Japanese	x	x	x	x [*]	
Korean	x	x	x		
Portuguese (Brazilian)	x	x	x	x	
Russian	x	x	x	x	
Spanish	x	x	x	x	
Swedish	x	x	x	x	

* IP Phone Agent does not support Japanese if it is running on a SIP phone. Reason codes and wrap-up data must be Katakana half-width in Shift-JIS format. Kanji will not display properly.

Installation in Localized Contact Centers

The CAD services must be installed on machines running an English language operating system.

The CAD desktop applications can be installed on machines running either an English language or a supported localized language operating system.

Cisco Desktop Administrator, although available only in English, must be installed on a machine with a supported localized language operating system in order to be able to create reason codes, wrap-up data, and other communication with agents in the localized language.

System Configurations

Supported system configurations are documented in the *Cisco IP Contact Center Solution Reference Network Design (SRND)*, available for download on www.cisco.com.

Citrix and Microsoft Terminal Services Environments

CAD is supported in Citrix and Microsoft Terminal Services environments. See the document, *Integrating CAD Into a Citrix MetaFrame Presentation Server or Microsoft Terminal Services Environment*, included in the CAD document set on your installation CD.

System Requirements

CAD 7.2 is integrated into the following Cisco Unified Contact Center Enterprise and Hosted environment:

CAD Version	Unified CM Version	Unified ICM Version	CTI Server
7.2(1)	4.1, 4.2, 5.0, 6.0	7.2(1)	CTI OS 7.2

Consult the following documents for the most current compatibility information:

Cisco Unified CallManager Compatibility Matrix

www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm

Cisco IP Contact Center Enterprise Edition Software Compatibility Guide

http://www.cisco.com/application/pdf/en/us/guest/products/ps1844/c1609/ccmigration_09186a008031a0a7.pdf

Operating Environment

CAD 7.2 runs on the following operating systems and hardware.

Table 2. Desktop minimum operating systems and hardware

Operating System	Desktop Applications
Windows 2000 Professional Service Pack 4	<p>All Desktops:</p> <ul style="list-style-type: none"> • 500 MHz processor • 128 MB RAM • 800 × 600 screen resolution • 100 Mbit NIC supporting Ethernet 2 <p>Agent, Supervisor, and Admin Desktops:</p> <ul style="list-style-type: none"> • 650 MB free space <p>CAD-BE Desktop only:</p> <ul style="list-style-type: none"> • IE 6 and 7 w/Sun JRE 5.0 Update 11 • Firefox 1.5 & 2 w/Sun JRE 5.0 Update 11
Windows XP Professional Edition Service Pack 2	<p>All Desktops:</p> <ul style="list-style-type: none"> • 500 MHz processor • 128 MB RAM • 800 × 600 screen resolution • 100 Mbit NIC supporting Ethernet 2 <p>Agent, Supervisor, and Admin Desktops:</p> <ul style="list-style-type: none"> • 650 MB free space <p>CAD-BE Desktop only:</p> <ul style="list-style-type: none"> • IE 6 and 7 w/Sun JRE 5.0 Update 11 • Firefox 1.5 & 2 w/Sun JRE 5.0 Update 11

Table 2. Desktop minimum operating systems and hardware — Continued

Operating System	Desktop Applications
Windows Vista Business or Enterprise	<p>All Desktops:</p> <ul style="list-style-type: none"> • 500 MHz processor • 512 MB RAM • 800 × 600 screen resolution • 100 Mbit NIC supporting Ethernet 2 <p>Agent, Supervisor, and Admin Desktops:</p> <ul style="list-style-type: none"> • 650 MB free space <p>CAD-BE Desktop only:</p> <ul style="list-style-type: none"> • IE 6 and 7 w/Sun JRE 5.0 Update 11 • Firefox 1.5 & 2 w/Sun JRE 5.0 Update 11
Red Hat Enterprise Linux v3, v4	<p>CAD-BE Desktop only:</p> <ul style="list-style-type: none"> • 1 GHz processor • 256 MB RAM • 1 GB free space • 100 Mbit NIC supporting Ethernet 2 • 800 by 600 screen resolution • Firefox 1.5 & 2 w/Sun JRE 5.0 Update 11
Citrix MetaFrame Presentation Server 4.0 Full window mode	<p>Agent Desktop only:</p> <p>Refer to Citrix documentation for minimum hardware requirements</p>
Microsoft Terminal Server for Windows 2003	<p>Agent Desktop only:</p> <p>Refer to Microsoft Terminal Server documentation for minimum hardware requirements</p>

Table 3. Server minimum operating systems and hardware

Operating System	VoIP and Recording & Playback services on a dedicated server	Base, VoIP, and Recording & Playback services coresident on a server
Windows 2000 Server Service Pack 4, Rollup Update 1 (30 day upgrade period only)	<p>1.4 GHz processor</p> <p>1 GB RAM</p> <p>1 GB free space</p> <p>100 Mbit NIC supporting Ethernet 2</p>	<p>2 × 1.4 GHz processor</p> <p>2 GB RAM</p> <p>1 GB free space</p> <p>100 Mbit NIC supporting Ethernet 2</p>
Windows 2000 Advanced Server, Service Pack 4, Rollup Update 1 (30 day upgrade period only)	<p>1.4 GHz processor</p> <p>1 GB RAM</p> <p>1 GB free space</p> <p>100 Mbit NIC supporting Ethernet 2</p>	<p>2 × 1.4 GHz processor</p> <p>2 GB RAM</p> <p>1 GB free space</p> <p>100 Mbit NIC supporting Ethernet 2</p>

Table 3. Server minimum operating systems and hardware

Operating System	VoIP and Recording & Playback services on a dedicated server	Base, VoIP, and Recording & Playback services coresident on a server
Windows 2003 Server, Standard and Enterprise Edition, Service Pack 1 or R2	1.4 GHz processor 1 GB RAM 1 GB free space 100 Mbit NIC supporting Ethernet 2	2 × 1.4 GHz processor 2 GB RAM 1 GB free space 100 Mbit NIC supporting Ethernet 2

Operating Environment Language Requirements

The CAD services must be installed on machines running an English language operating system.

The CAD desktop applications can be installed on machines running an English language or a localized operating system. The following desktop applications are localized:

- Cisco Agent Desktop
- Cisco Agent Desktop—Browser Edition
- Cisco Supervisor Desktop

Cisco Desktop Administrator is not localized. However, it must be run on a machine with a localized operating system in a non-English contact center so that chat messages, tooltips, enterprise data names, and other communications within the contact center are in the local language.

Third Party Software Requirements

CAD 7.2 requires the following software applications to run successfully:

Application	Where Installed/Description
Microsoft Internet Explorer 6 or 7	<p>Client desktops</p> <p>Internet Explorer is required for the Integrated Browser portion of Cisco Agent Desktop and Cisco Supervisor Desktop, and is a supported browser for CAD-BE.</p> <p>The Integrated Browser makes use of a Windows OS library distributed with the Microsoft IDEs that supports the rendering of HTML.</p>

Application	Where Installed/Description
Mozilla Firefox 1.5	CAD-BE client desktops Firefox is a supported browser for CAD-BE
Adobe Acrobat Reader 5.0 or newer	Client desktops The CAD documentation is distributed in Acrobat PDF format. The Adobe Acrobat Reader is available for free from www.adobe.com .
Apache Tomcat 5.5	Base Services server Tomcat is a Java-based webserver. If you are installing IP Phone Agent, it is needed to work with the XML pages displayed by IP phones. More information about Tomcat may be found at http://jakarta.apache.org . Tomcat is shipped with CAD 7.2 and is automatically installed.
Java Runtime Environment (JRE) 1.5.11, Windows or Linux version	Base Services server Client desktops accessing CAD-BE JRE is required to run the Java applets and JavaServer Pages (JSP) used by the IP Phone Agent and CAD-BE applications. JRE is shipped with CAD 7.2. JRE is installed automatically with the CAD services, but it must be installed manually on any desktop that accesses the CAD-BE web application. See " Installing Desktop Applications " on page 69 for more information.
"OpenLDAP V2.2.17	LDAP Server System configuration data is maintained using Directory Services.
Computer Telephony Integration Object Server (CTI OS)	CTI server CTI OS must be installed before installing the CAD services. You may want to edit several registry keys to enable Cisco Agent Desktop to receive all CTI events. See " Supported IP Phones " on page 39 for information on changing these registry keys.
Microsoft SQL Server 2000 Desktop Engine, Service Pack 4	Base Services server Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) is the free, redistributable version of SQL Server used as an embedded database. It is installed automatically with the CAD services.

Monitoring Requirements

If your system configuration uses Cisco CallManager 4.x or Cisco Unified Communications Manager 5.x (Unified CM), CAD supports one kind of monitoring: CAD-based (agent-based) monitoring. CAD-based monitoring can be implemented either through the desktop or the server.

If your system configuration uses Unified CM 6.0, CAD supports CAD-based monitoring and also Unified CM-based (call-based) monitoring.

The type of monitoring that is used is specified when the Cisco CTI OS is installed. CAD uses either Unified CM-based or CAD-based monitoring, not both. Supervisor Desktop automatically determines which kind of monitoring is used when it is launched.

NOTE: CAD-based monitoring requires codecs G.711 and G.729.

Desktop Monitoring (CAD-based)

The use of desktop monitoring in your contact center increases bandwidth requirements. Consult the best practices document, *Cisco Agent Desktop Bandwidth Requirements*, for more information.

Required Device Settings for Desktop Monitoring

The following device settings are required for desktop monitoring to function correctly with CAD. The settings are configured with the Cisco Unified Communications Manager (Unified CM) Administration application.

NOTE: Not all devices or Unified CM versions use all these settings. Configure those that do appear for your device and Unified CM version.

NOTE: CAD does not support Secure Realtime Transport Protocol (SRTP) in desktop monitoring.

In the Product Specific Configuration section of the Device Configuration screen, configure these settings as follows:

- **PC Port—Enabled.** If the PC Port is not enabled, the agent PC that is connected to the port will not have network access. No voice streams will be seen by the desktop monitor module.
- **PC Voice VLAN Access—Enabled.** If the PC Voice VLAN Access is not enabled, no voice streams will be seen by the desktop if the desktop is not a member of the same VLAN as the phone.

- **Span to PC Port—Enabled.** If the Span to PC Port is not enabled, the voice streams seen by the phone will not be seen by the desktop monitor module.

In the Device Information section of the Device Configuration screen, configure this setting as follows:

- **Device Security Mode—Non-Secure or Authenticated.** If the Device Security Mode is set to Encrypted, the voice streams can be seen but will not be converted correctly, causing the speech to be garbled.

Qualifying NICs for Desktop Monitoring

Desktop monitoring does not function with some NICs. The Intel PRO/100 and PRO/1000 NIC series are unable to detect both voice packets and data packets in a multiple VLAN environment, which prevents desktop monitoring from functioning properly. These NICs do not fully support NDIS Promiscuous Mode settings.

A list of NICs tested with Cisco Agent Desktop is located on the Cisco website at:

http://www.cisco.com/en/US/partner/products/sw/custcosw/ps14/prod_installation_guides_list.html

A workaround solution for the problems with the Intel PRO/100 and PRO/1000 NICs is available from the Intel Technical Support website (Solution ID: CS-005897). Other solutions include:

- Monitoring agents via a VoIP Monitor Service
- Using another type of NIC that is fully NDIS-compliant

The workaround described in CS-005897 may not work for some newer Intel PRO/100 and Intel PRO/1000 cards and drivers.

If the workaround does not solve the problem, the VLAN ID of the IP phone to which the agent computer is directly connected must be added to the VLANs tab of the Intel NIC's Network Connection Properties dialog box.

The IP phone's VLAN ID can be obtained from the phone's Network Configuration screen (press **Settings** and then choose **Network Configuration**). See the documentation specific to your version of Cisco Unified Communications Manager and IP phone model for more information.

You can test a NIC to verify that it is suitable for desktop monitoring by following the procedure, "Qualifying Ethernet Cards for Cisco Agent Desktop Monitoring" (Document ID 46301). This document is located on the Cisco website at:

http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1844/products_tech_note09186a00801f42f9.shtml

A sample packet capture file used in this procedure is located at:

<http://www.cisco.com/cgi-bin/tablebuild.pl/nic-qual>

Server Monitoring (CAD-based)

The following device setting is required for server monitoring to function correctly with CAD. The setting is configured with the Cisco Unified Communications Manager (Unified CM) Administration application.

In the Device Information section of the Device Configuration screen, set the Device Security Mode to Non-Secure or Authenticated. If it is set to Encrypted, the voice streams can be seen but will not be converted correctly, causing the speech to be garbled.

NOTE: CAD does not support Secure Realtime Transport Protocol (SRTP) in server monitoring.

Unified CM-based Monitoring

Unified CM-based monitoring requires the use of certain models of IP phones. The monitored call must be on a supported IP phone, which includes models 7906G, 7911G, 7931G, 7941G, 7941G-GE, 7961G, 7961G-GE, 7970G, and 7971G-GE.

Unified CM-based monitoring is configured with the Unified CM Administration application. The following settings are required to use Unified CM-based monitoring:

- On the Application User Configuration window, add PG user to the “Standard CTI Allow Call Monitor” user group. This window is available through the User Management menu.
- On the Phone Configuration (device) window of the agent who will be monitored, enable the “build-in-bridge” option. The monitored agent’s device must be one of the IP phone models listed above. This window is available through the Device menu.
- On the Directory Number Configuration (line appearance) window of the supervisor who will be monitoring the agent, add the DN partition of the monitored agent to the Monitoring Call Search Space. This window is available through the Device menu.

Recording

NOTE: The CAD recording functionality is intended for “on demand” use only, and not for recording all calls in a contact center.

The space requirements for the Recording & Playback Service and the Recording and Statistics Service depend on the size of the contact center. In general, requirements are as follows:

Recording and Statistics Service

The Recording and Statistics Service requires 4 GB to store agent state and call activity records for a 7 days per week/10 hours per day contact center with 1,000 agents taking calls that last an average of 1 minute each.

Recording & Playback Service

The Recording & Playback Service requires the following space. This space can be distributed between two servers in a redundant environment.

Protocol	Packet Size (msec)	Recording Size (KB/call/minute)
G.711	10	1220
	20	1080
	30	1030
G.729	10	400
	20	260
	30	210
	40	190
	50	180
	60	170

NOTE: If the audio files are stored on a partition using the FAT32 file system, a limit of 21,844 objects can be stored. If this recording limit is exceeded, supervisors will be unable to record any more audio files. There is no such limitation on an NTFS file system partition.

Recording Functionality Overview

For agent call recording, the Recording & Playback Service receives voice streams from either Desktop Monitoring or a VoIP Monitor Service, depending on how the system has been configured.

There can be up to two Recording & Playback Services installed for fault tolerance. All Recording & Playback Services are active (as opposed to active/standby).

For each recording, a Recording & Playback Service is chosen in round-robin fashion. The recordings are stored locally on the server that hosts the Recording & Playback Service that handled the recording request.

Mobile Agent Monitoring and Recording Requirements

The caller and agent voice gateways must be separate. In addition, the VoIP Monitor server must be located in the network where it can see the traffic flowing between the agents and customers. If the customer and agent are speaking to each other over the same voice gateway, then that voice stream will remain local to the gateway and not be exposed to the VoIP Monitor Service. SPAN will not send those packets to the VoIP Monitor Service, and the conversation will not be heard. For this reason, monitoring and recording of Agent-to-Agent calls is not supported.

Cisco Catalyst switches use SPAN (Switched Port ANalyzer) to monitor ports. VoIP Monitor Services must be connected to Cisco Catalyst switches that can sniff the agent voice gateways.

To set up mobile agent monitoring, you must configure mappings between the agent voice gateways and VoIP Monitor Services using Cisco Desktop Administrator. For instructions, see Mobile Agent Monitoring in *Cisco Desktop Administrator User Guide*.

The VoIP Monitor Service identifies voice packets using the IP Address of the Agent Voice Gateways. The layer-2 MAC address rewrite issues associated with SPAN-based monitoring/recording of non-mobile agents does not apply.

Setting Up Agents in Unified ICM

Setting Up Supervisors and Teams

For CAD 7.2 applications to work properly, your agents must be organized into teams and some must be designated as supervisors. This is accomplished in Unified ICM. See your Unified ICM documentation for information on how to do this.

Skills Statistics

The number displayed in the Skills statistic field “Waiting” in Agent Desktop and Supervisor Desktop (representing the number of calls currently queued to the skill group) is dependent on how you configure skill groups and set up queues in Unified ICM Configuration Manager. The following rules apply:

- If calls are queued to a base skill group, there must be no sub skill groups configured.
- If a skill group does have sub skill groups configured, calls cannot be queued to the base skill group.

If calls are queued to the base skill group, all the calls queued to that skill group are reported in the Waiting field.

If sub skill groups are configured, and calls are queued to those sub skill groups, only the calls queued to the primary sub skill group are reported in the Waiting field.

NOTE: Agents must be assigned to the base skill group in order for the supervisor to view a team's skill data in Supervisor Desktop. Only the base skill groups appear in the Supervisor Desktop skill statistics. If sub skill groups are enabled, agents must be assigned to those groups; they cannot be assigned to the base skill group. In that case, no skill data is displayed in Supervisor Desktop.

See your Unified ICM Configuration Manager documentation for more information on setting up skill groups and queues.

Reason Codes

In this version of CAD, reason codes are created and maintained in Unified ICM and pulled into CAD. In previous versions of CAD, reason codes could be created and maintained in both Unified ICM and in CAD.

If you are upgrading from a previous version of CAD, any reason codes you may have created in CAD will be lost in the upgrade. If you want those reason codes to be available in this version of CAD, make sure they are created in Unified ICM.

System Capacity

CAD 7.2 supports the following system capacities.

NOTE: Capacity numbers are goals. Actual numbers depend on your system configuration and are documented in the *Cisco IP Contact Center Solution Reference Network Design (SRND)*, available on www.cisco.com.

Table 4. CAD 7.2 system capacity

Description	Capacity
Maximum number of CAD agents per peripheral gateway (PG)	1500
Maximum number of IP phone agents per server	1000
Maximum number of CAD-BE agents per server	1000
Maximum number of agents per team*	100
Maximum number of skills per agent (for real-time reporting)*	52
Maximum number of supervisors per site	100
Maximum number of supervisors per team	20
Average number of agents per supervisor	10
Maximum number of agents per monitor domain†	1000
Maximum number of simultaneous recordings per Recording & Playback Service	80
Maximum number of simultaneous playbacks per Recording & Playback Service	8
Maximum number of CAD agents per outbound PG (a PG dedicated to outbound agents coresident with dialer and media routing)	200

* The CTI OS server supports 5 skills per agent at a 1000-agent load. A different set of skills is assumed for each 100 agents. When a 1000-agent system is installed, up to 50 skills can be configured in the system. Each agent can be assigned up to 5 skills. When a 500-agent system is installed, up to 30 skills can be configured.

† A system with more than 400 agents requires a VoIP Monitor Service server with a 1 GB NIC.

Supported IP Phones

For a list of supported IP phones, see the *Cisco IP Contact Center Enterprise Edition Software Compatibility Guide*. This document is available on the web at:

http://www.cisco.com/application/pdf/en/us/guest/products/ps1844/c1609/ccmigration_09186a008031a0a7.pdf

NOTE: Cisco IP Communicator is supported for Cisco Agent Desktop and Cisco Agent Desktop—Browser Edition. It is not supported for Cisco IP Phone Agent.

Caveats on Using a Cisco 7920 Wireless Phone

Only SPAN port monitoring can be used with the 7920 wireless IP phone. The port that is to be included in the SPAN is the one to which the access point is wired.

Due to the nature the 7920 phone's mobility, there are certain conditions under which monitoring and/or recording calls may result in gaps in the voice:

- Agent to agent conversations when both agents are using the same wireless access point
- When an agent roams from one monitoring domain to another

The 7920 phone is not supported as a second line appearance for an agent's wired phone.

Registry Key Modifications

A registry key on the peripheral gateway (PG) computer must be modified so that the Cisco Agent Desktop call activity pane displays the correct amount of time a caller spends at the IVR.

This modification must be done after the CAD services and desktops have been installed.

To modify the PG computer registry keys:

1. On the PG computer, open the Windows Registry Editor.
2. Navigate to the following key:
`HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<ICM customer> \PG <PG number>\PG\CurrentVersion\OPC\CallControl\pim <PIM number>\NewCallOffersUpdateDNIS`
3. Change the value of NewCallOffersUpdateDNIS to 1.
4. Close the Windows Registry Editor.

Overview

Install the CAD 7.2 applications in this order:

1. CAD Services
2. Cisco Desktop Administrator
3. Cisco Supervisor Desktop, Cisco Agent Desktop, and Cisco Agent Desktop—Browser Edition

NOTE: If you are using multiple monitors, make sure that the CAD installation wizard is displayed on your primary monitor. If it is displayed on your secondary monitor, you might experience undefined behavior. For example, you might not be able to check and uncheck selection boxes.

Installation Locations

The location of the first application or service you install on a computer determines the location where any subsequent applications or services will be installed.

For example, if you choose to install Cisco Desktop Administrator to D:\CAD, when you install Cisco Supervisor Desktop on that same computer it will automatically be installed to D:\CAD. You will not be able to specify any other location.

Installing CAD Services

The CAD Services installation is run from the product CD.

NOTE: The server on which you install the CAD services must be a member of a domain, not of a workgroup. If you change the domain after the services are installed, or switch from workgroup to domain, you must reinstall the services in order to avoid problems with partial or no service when running the desktop applications.

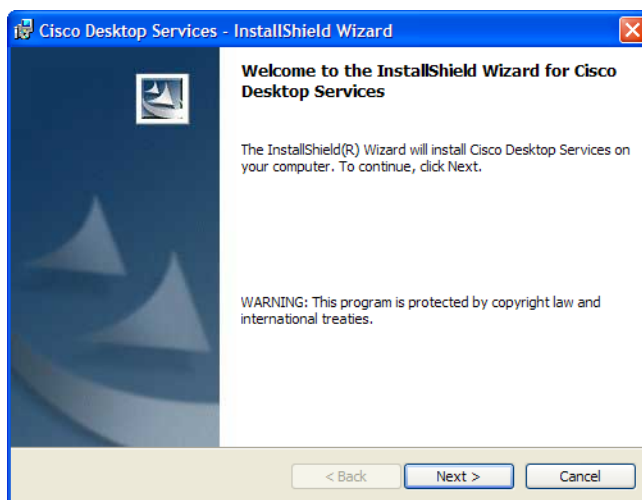
NOTE: If you are installing secondary (“Side B”) CAD services, the login account of each server on which CAD services are being installed must have a password. If any one of the servers does not have a password, replication setup will fail—the subscriber can not connect to the publisher to configure the replication. If you have already installed a CAD service on a Side B server without a password, set a password for the login account and then run CAD Configuration Setup again.

NOTE: You must install CAD Services as a local administrator. If you install CAD Services as a domain administrator, Recording and Statistics replication jobs will fail.

To install the CAD services:

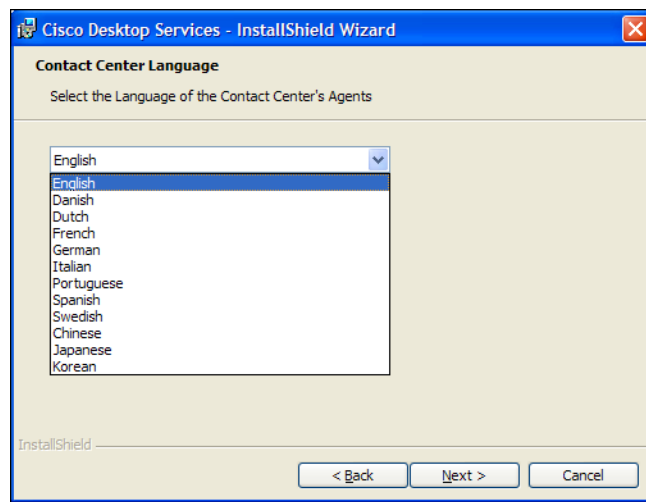
1. Launch the file **setup.exe** from the product CD to start the installation process (see [Figure 1](#)).

Figure 1. Cisco Desktop Services - InstallShield Wizard Welcome window.



2. Click **Next** to display the Contact Center Language window (see [Figure 2](#)).

Figure 2. Contact Center Language window.

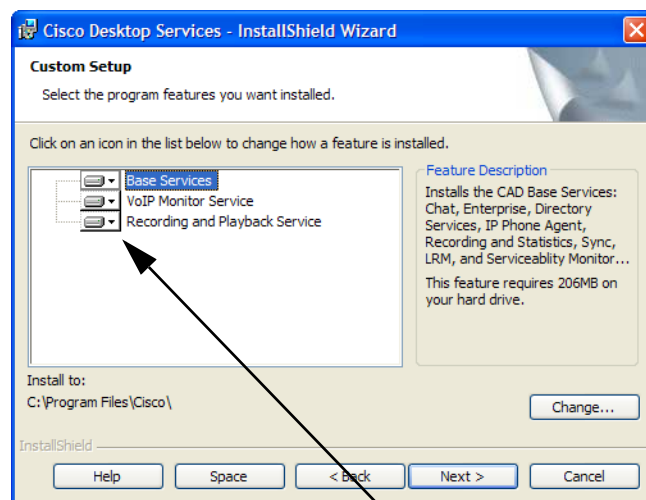


- From the drop-down list, select the language for contact center agents to use.




This selection determines which localized version of the desktop applications will be installed on agents' and supervisors' desktops. See ["Operating Environment Language Requirements" on page 30](#) for more information.

- Click **Next** to display the Custom Setup window (see [Figure 3](#)).

Figure 3. Custom Setup window.

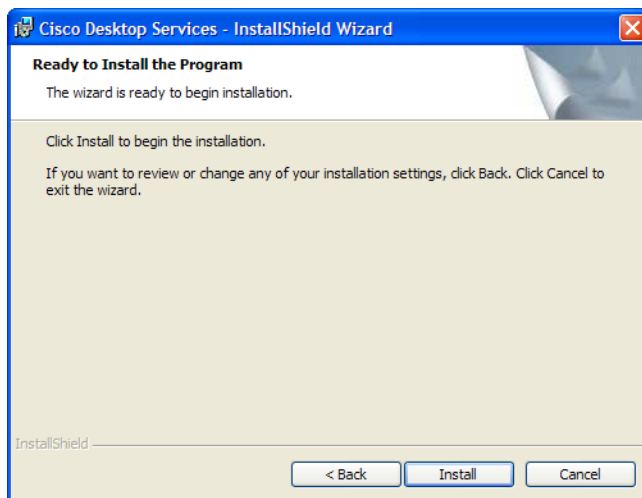


Click the down arrow next to the feature to add or remove it from the list of features to be installed.

-  This feature will be installed on local hard drive.
-  This feature, and all subfeatures, will be installed on local hard drive.
-  This feature will not be available.

- Click **Next** to display the Ready to Install the Program window (see [Figure 4](#)).

Figure 4. Ready to Install the Program window.



6. Click **Install** to start the installation.

NOTE: If Cisco Security Agent (CSA) is running on the server computer, the installation process stops it temporarily during the installation and restarts it after the installation finishes.

NOTE: If you are setting up replication for Directory Services and/or the Recording and Statistics Service, make sure that Cisco Security Agent is stopped on both computers.

NOTE: If you are installing the Base services on a Windows 2000 Server, the installation asks for a reboot in the middle of the install. If you click Yes to reboot, a reboot does not occur. This is expected behavior. The installation proceeds normally and will be completed successfully.

NOTE: The Sync Service must connect to the ICM Logger SQL database via a TCP/IP connection. To configure this, run the SQL Server Network Utility on the ICM Logger machine and, on the General tab, ensure that TCP/IP is enabled.

7. When the installation is completed, the CAD Configuration Setup tool starts. See ["Cisco Agent Desktop Configuration Setup" on page 45](#) for instructions on configuring your system using this tool.

Cisco Agent Desktop Configuration Setup

Use the Cisco Agent Desktop Configuration Setup utility to configure the CAD services. The Configuration Setup utility consists of a series of data entry windows. You must complete all of the windows in the utility to install and run CAD services successfully.

The Configuration Setup utility has two modes: Initial and Update. The utility is launched automatically in Initial Mode after the CAD service installation finishes. You can run the utility again later in Update Mode to change your configuration settings. To run the utility in Update Mode, choose one of the following methods:

- launch the utility from Desktop Administrator
- run PostInstall.exe, which is located on each CAD computer in C:\Program Files\Cisco\Desktop\bin

The windows that appear when you run this utility depend on the following factors:

- the host computer on which the Configuration Setup utility was launched
- the mode in which the Configuration Setup utility is running
- the services and applications that are running on the computer on which the Configuration Setup utility was launched

[Table 5](#) lists all of the windows that are part of the Configuration Setup utility in alphabetical order. For each window, the table indicates whether that window appears when the utility is run on the computer that hosts the named application or service. If you need to change a configuration setting, use the table to determine the computer on which you must run the Configuration Setup utility. The table has the following columns:

- Window title: The name of the window
- Mode: The mode in which the window appears (Update or Both initial/update)
- Base: The computer on which the CAD base services run
- VoIP: The computer on which the VoIP Monitor Service runs
- Rec: The computer on which the Recording and Statistics Service runs
- CAD/CSD: The computer on which Cisco Agent Desktop and Cisco Supervisor Desktop run
- CDA: The computer on which Cisco Desktop Administrator runs

Table 5. CAD Configuration Setup windows

Window Title	Mode	Base	VoIP	Rec	CAD CSD	CDA
CAD-BE Servers	Update	×				
CallManager	Both	×	×			×

Table 5. CAD Configuration Setup windows

Window Title	Mode	Base	VoIP	Rec	CAD CSD	CDA
CallManager SOAP AXL Access	Both	×	×			×
CTI OS	Both	×				×
CTI OS Security Setup	Both				×	
CTI Server (CallManager)	Both	×				×
ICM Admin Workstation Database	Both	×				
ICM Admin Workstation Distributor	Both	×				
Recording and Statistics Service Database	Both	×				
Replication Setup	Both	×				
Restore Backup Data	Both	×				
Services Configuration	Update	×	×	×		
SNMP Configuration	Update	×	×	×		
Terminal Services	Both				×	
VoIP Monitor Service	Update	×	×		×	

Entering Configuration Data in Initial Mode

After the Desktop services are installed, CAD Configuration Setup starts automatically and displays the CAD Directory Services dialog box.

You can set up Directory Services replication between two installations of the Base services, which includes Directory Services. To do this, you install the Base services on the primary server and complete the CAD Configuration Setup windows, then do the same on the secondary server, at that time identifying the computer that hosts the primary Directory Services.

If your system does not include Directory Services replication, follow the procedure for entering configuration data on the primary Base services computer only.

NOTE: Directory Services replication can be set up at a later time by running CAD Configuration Setup in Update Mode on the secondary Base Services computer and entering information in the Replication Setup window.

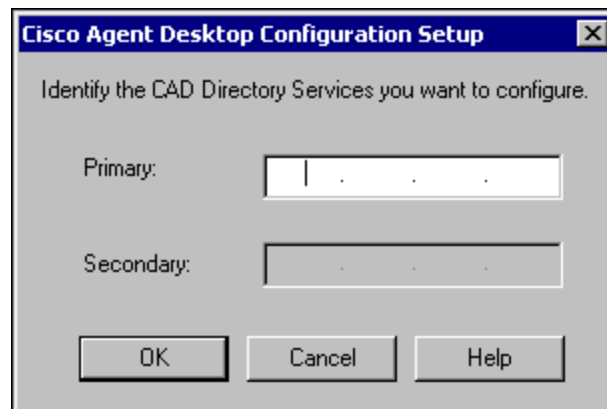
Configuring a Single Server or Primary Server in a Replicated System

Complete the following procedure if you are running CAD Configuration Setup in Initial Mode on a single server system or on the primary server in a replicated system.

To enter configuration data in Initial Mode on the primary Base services computer:

1. Configuration Setup starts automatically and displays the CAD Directory Services dialog box (see [Figure 5](#)).

Figure 5. CAD Directory Services dialog box.



2. Enter the IP address of the primary Directory Services and then click **OK**.
3. If Configuration Setup does not detect that it is installed in a System IPCC Environment, a dialog box appears, prompting you to indicate whether this is a System IPCC installation.
 - If you answer **Yes**, then default peripheral IDs are set to 1000, and agents and supervisor login by name becomes the only login option (login by login ID is disabled).
 - If you answer **No**, then peripheral IDs are set to 5000 and agents and supervisors can log in by login name or login ID. This option is configured later in Cisco Desktop Administrator.

The Configuration Setup tool appears, with the CallManager node selected.

4. Complete the fields in each window, using the right arrow on the toolbar to move forward to the next window.
 - You cannot move forward until all required information is entered.
 - You cannot skip a window.
 - You can go backwards at any time to revisit a previous window.
 - The Save button is not enabled until all windows are completed.

5. When you have completed all windows in the tool, click **Save** on the toolbar or choose **File > Save**.

When the data is successfully saved, the program ends automatically.

NOTE: The save process may take several minutes.

Configuring a Secondary Server in a Replicated System

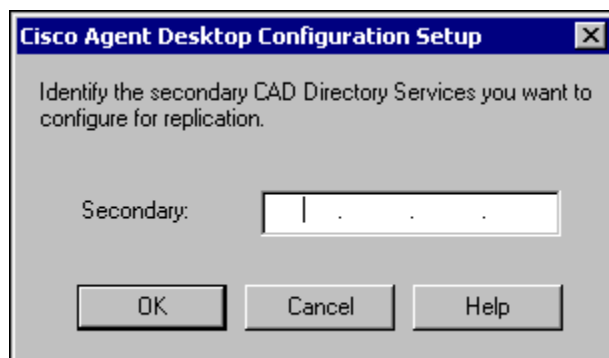
Complete the following procedure if you are running CAD Configuration Setup in Initial Mode on the secondary server in a replicated system.

To enter configuration data in Initial Mode on the secondary Base services computer:

1. Configuration Setup starts automatically and displays the CAD Directory Services dialog box (see [Figure 5](#)).
2. Enter the IP address of the primary Directory Services and then click **OK**.
A dialog box appears, asking you if you want to set up Directory Services replication.
3. Click **Yes**.

The Secondary Directory Services dialog box appears (see [Figure 6](#)).

Figure 6. Secondary Directory Services dialog box.



4. Enter the IP address of the secondary Directory Services, and then click **OK**.
A confirmation dialog box appears, prompting you to indicate whether the primary and secondary IP addresses are correct.
5. Click **Yes** to set up replication.
When replication is done, the Configuration Setup tool appears, with the CallManager node selected.
6. Complete the fields in each window, using the right arrow on the toolbar to move forward to the next window.

- You cannot move forward until all required information is entered.
 - You cannot skip a window.
 - You can go backwards at any time to revisit a previous window.
 - The Save button is not enabled until all windows are completed.
7. When you have completed all windows in the tool, click **Save** on the toolbar or choose **File > Save**.

When the data is successfully saved, the program ends automatically.

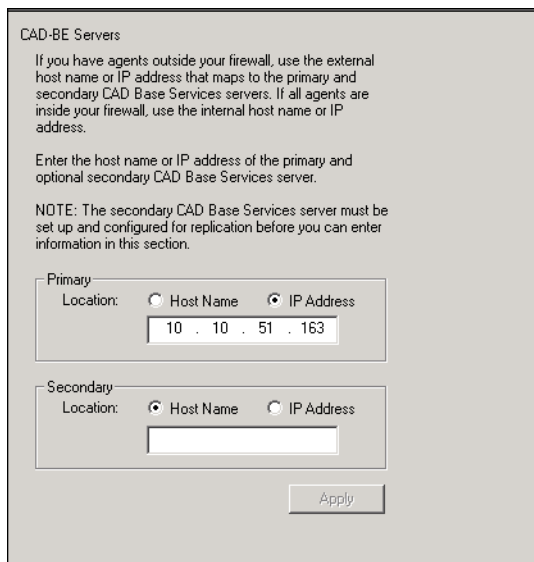
NOTE: The save process may take several minutes.

CAD Configuration Setup Windows

The following pages describe all of the windows in the CAD Configuration Setup utility. The windows are described in alphabetical order.

CAD-BE Servers

Figure 7. CAD-BE Servers window.



The screenshot shows the 'CAD-BE Servers' window. It contains the following text and controls:

CAD-BE Servers

If you have agents outside your firewall, use the external host name or IP address that maps to the primary and secondary CAD Base Services servers. If all agents are inside your firewall, use the internal host name or IP address.

Enter the host name or IP address of the primary and optional secondary CAD Base Services server.

NOTE: The secondary CAD Base Services server must be set up and configured for replication before you can enter information in this section.

Primary

Location: ☐ Host Name ☒ IP Address

10 . 10 . 51 . 163

Secondary

Location: ☒ Host Name ☐ IP Address

[Empty text box]

Apply

The CAD-BE Servers window only appears during Update mode.

Enter the hostname or IP address of the CAD Base Services servers. This is where the Tomcat webserver required to run CAD-BE is installed.

If you have agents outside your firewall, use the external hostname or IP address that maps to the primary and secondary CAD Base Services servers. If all agents are inside your firewall, use the internal hostname or IP address.

- If you have only one instance of the CAD Base Services, enter the information in the Primary section.
- If you are also using a secondary instance of the CAD Base Services and have configured replication, enter its location in the Secondary section.

NOTE: The Secondary section is not enabled until the secondary CAD Base Services are set up and replication is configured.

NOTE: If you set up replication during initial mode, the Secondary Location will be filled automatically.

CallManager

Figure 8. CallManager window.

CallManager
Enter the host name or IP address of your CallManager(s).

Publisher
Location: ☐ Host Name ☒ IP Address
192 . 168 . 252 . 38

Subscribers
Location:
Subscriber
192.168.252.31

Add... Edit... Remove

Apply

The CallManager window has two sections: the Publisher section and the Subscriber section. If you have only one CallManager, complete the Publisher section and leave the Subscriber section blank. If you have a CallManager cluster, which consists of one publisher CallManager and one or more subscriber CallManagers, complete both sections.

For the Publisher section, select Hostname or IP Address. Then type the location of the CallManager (the publisher CallManager if you have a CallManager cluster).

If you have a single CallManager, leave the Subscriber section blank and click **Apply**.

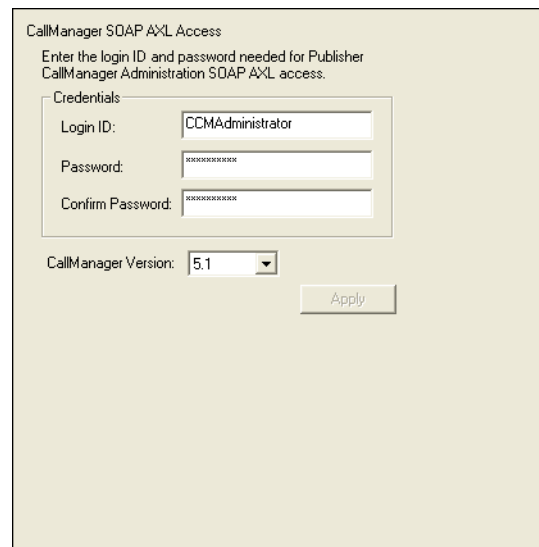
If you have a CallManager cluster, add the locations of all of the subscriber CallManagers in the Subscribers section. To add a subscriber location, click **Add**. The Add/Edit Host dialog box appears. Enter the location of the subscriber CallManager in one of the following ways, then click **Apply**.

- Select Hostname, then type the hostname of the subscriber CallManager.
- Select Hostname, then choose the hostname of the subscriber CallManager from the drop-down list.
- Select IP Address, then type the IP address of the subscriber CallManager.

NOTE: If you change these settings after initial setup, you must restart the Sync Service and the VoIP Monitor Service to ensure that the change is registered with them properly.

CallManager SOAP AXL Access

Figure 9. CallManager SOAP AXL Access window.

The image shows a window titled "CallManager SOAP AXL Access". Inside the window, there is a text prompt: "Enter the login ID and password needed for Publisher CallManager Administration SOAP AXL access." Below this prompt is a section labeled "Credentials" which contains three input fields: "Login ID:" with the text "CCMAdministrator", "Password:" with masked characters "XXXXXXXX", and "Confirm Password:" with masked characters "XXXXXXXX". Below the credentials section is a "CallManager Version:" label followed by a dropdown menu showing "5.1". At the bottom right of the window is an "Apply" button.

Enter the login ID and password required for the Publisher CallManager Administration to access SOAP AXL (Simple Object Access Protocol Administrative XML Layer), and select the CallManager version.

The login ID and password are the same used to access the Publisher CallManager.

NOTE: If you change these settings after initial setup, you must restart the Sync Service and the VoIP Monitor Service to ensure that the change is registered with them properly.

CTI OS

Figure 10. CTI OS window.

CTI OS
Enter information about the CTI OS server(s).

CTI OS A
Location: ☐ Host Name ☒ IP Address
192 . 168 . 252 . 141
Port: 42028

CTI OS B
Location: ☐ Host Name ☒ IP Address
192 . 168 . 252 . 22
Port: 42028

Is the CTI OS security setting enabled? ☐ Yes ☒ No

Apply

Enter the hostname or IP address, port number, and peripheral ID of the CTI OS (Computer Telephony Integration Object Server).

- If you have only one CTI OS, enter the information in the CTI OS A section.
- If you are also using a redundant CTI OS in a duplexed environment, enter the location of the redundant CTI OS in the CTI OS B section.

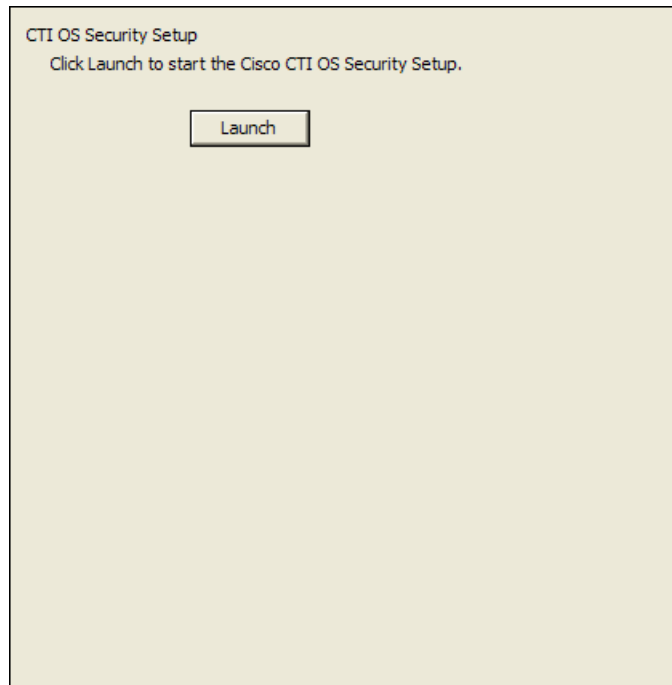
If you are running CAD Configuration Setup in Upgrade mode, the question Is the CTI OS Security Setting Enabled appears. Select **Yes** or **No**.

NOTE: If you are running CAD Configuration Setup in Initial mode (immediately after installation), the question Is the CTI OS Security Setting Enabled does not appear.

If you choose Yes, ensure that CTI OS security is enabled on the CTI OS server. Then, follow the procedures in ["Setting Up CTI OS Security" on page 96](#).

CTI OS Security Setup

Figure 11. CTI OS Security Setup window.



Click **Launch** to start the Cisco CTI OS Security Setup installation program and install the CTI OS Security client on the PC.

This window appears only if CTI OS Security is enabled for your system.

For more information, see ["Setting Up CTI OS Security" on page 96](#).

CTI Server (CallManager)

Figure 12. CTI Server (CallManager) window.

CTI Server (CallManager)

Enter information about the ICM CTI Server(s) associated with the CallManager or CallManager cluster.

Side A

Location: ☐ Host Name ☒ IP Address

192 . 168 . 252 . 141

Port: 42027

Side B

Location: ☐ Host Name ☒ IP Address

192 . 168 . 252 . 22

Port: 43027

Peripheral ID: 5000

Apply

Enter the hostname or IP address, port number, and peripheral ID of the ICM CTI Server associated with the CallManager or CallManager cluster.

- If the CTI Server is entered with a hostname in ICM, enter a hostname. If it is entered as an IP address, enter an IP address. Mixing hostname and IP address between the ICM and Configuration Setup can result in failing to display enterprise data in desktop applications.
- If you have only one ICM CTI server, enter the information in the Side A section.
- If you are also using a redundant ICM CTI server in a duplexed environment, enter the location of the redundant ICM CTI server in the Side B section.
- The peripheral ID is used by services to filter information such as agents and skills. You can find the peripheral ID by using PG Explorer in the ICM Configuration Manager.

NOTE: If you change the peripheral ID, you must restart the Sync Service, the Enterprise Service, and the Browser and IP Phone Agent Service to ensure that the change is registered with them properly.

NOTE: If you are running System IPCC and change the Peripheral ID, your system will not work.

ICM Admin Workstation Database

Figure 13. ICM Admin Workstation Database window.

AW Database

Enter information about the ICM Admin Workstation database.

Locations:

Primary: 10.192.252.51

Secondary:

Authentication:

☒ SQL ☐ NT

ICM Instance Name: ipcc

Login ID: sa

Password: **

Confirm: **

Connection:

☒ TCP/IP ☐ Named Pipe

Port: 1433

Apply

The ICM Admin Workstation database locations are autofilled based on what you entered in the ICM Admin Workstation Distributor window.

Select the database type, SQL or NT, then type the instance name and a user login ID/password. The user must have read privileges for the ICM Admin Workstation database.

- If you select NT, the user must also have an account on the ICM Admin Workstation computer. Use the format <domain>\<username> or .\<username> for the login ID.

Select the connection type, TCP/IP or Named Pipes.

- If TCP/IP, type the port number used to connect to the database.
- If Named Pipes, type the share path in the format \\<path> in the Port field.

NOTE: If you change these settings after initial setup, you must restart each Recording and Statistics Service and the Sync Service to ensure that the change is registered with them properly.

ICM Admin Workstation Distributor

Figure 14. ICM Admin Workstation Distributor window.

ICM Admin Workstation Distributor

Enter the hostname or IP address of the ICM Admin Workstation Distributor.

Primary

Location: ☐ Host Name ☒ IP Address

10 . 192 . 252 . 51

Secondary

Location: ☒ Host Name ☐ IP Address

Dynamic Reskilling

☐ Enabled

☐ Secured client connection

System IPCC Environment

Is this a System IPCC installation?

☒ Yes ☐ No

Apply

Type the hostname or IP address of the ICM Admin Workstation (AW) Distributor.

- If you have only one ICM AW Distributor, complete the Primary section only.
- If you are using a secondary ICM AW Distributor, type its location in the Secondary section.

NOTE: If you change either location after initial setup, you must restart each Recording and Statistics Service and the Sync Service to ensure that the change is registered with them properly.

If you are running CAD Configuration Setup in Update mode, the Dynamic Reskilling and System IPCC Environment sections appear.

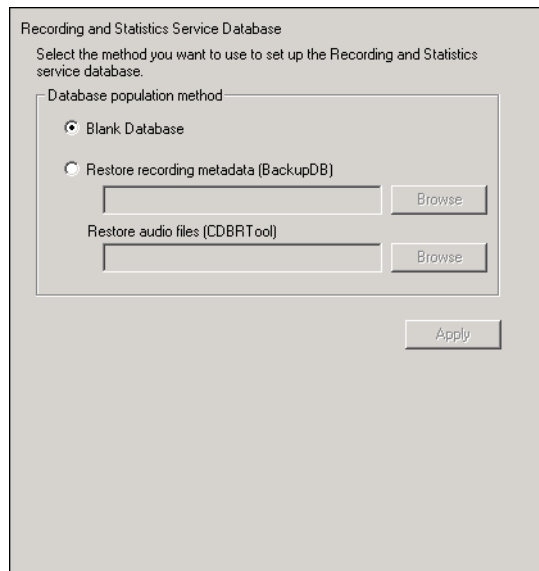
- **Dynamic Reskilling:** To enable supervisors to dynamically re-skill agents on their teams using the Cisco Unified Contact Center Enterprise Web Administration Agent Re-skilling tool, check **Enabled**. This tool is a web-based application. If it is located on a secured server and requires a secure socket URL (https), select the **Secured client connection** check box. If you leave this box unchecked, the URL will use the http prefix.
- **System IPCC Environment:** Select **Yes** or **No** to indicate whether or not your configuration is running in a System IPCC environment.

If you are running CAD Configuration Setup in Initial mode (immediately after installation), the Dynamic Reskilling and System IPCC Environment sections do not appear in the ICM Admin Workstation Distributor window.

NOTE: If Configuration Setup does not detect that it is installed in a System IPCC Environment, a dialog box will appear during Initial mode, prompting you to indicate whether it is a System IPCC Environment.

Recording and Statistics Service Database

Figure 15. Recording and Statistics Service Database window.



This window is displayed if you are running CAD Configuration Setup in both Initial and Update modes. If you are running CAD Configuration Setup on the secondary server in a replicated system, this window does not appear, because the database information was already entered on the primary system.

NOTE: If you change these settings after initial setup, you must restart each Recording and Statistics Service to ensure that the change is registered with them properly.

In the Database Population Method section, select the method you want to use to set up the Recording and Statistics Service database.

- Select **Blank Database** (the default) when installing a single service or a primary service in a replicated environment. This option creates the Recording and Statistics Service schema.

- Select **Restore From** if you are restoring a previously backed-up database. If you are running CAD in a replicated environment, a dialog box appears, reminding you to shut down replication before restoring data. After dismissing the dialog box, use the Browse button to navigate to the location of the backup database created using the BackupDB and CDBRTool utilities.

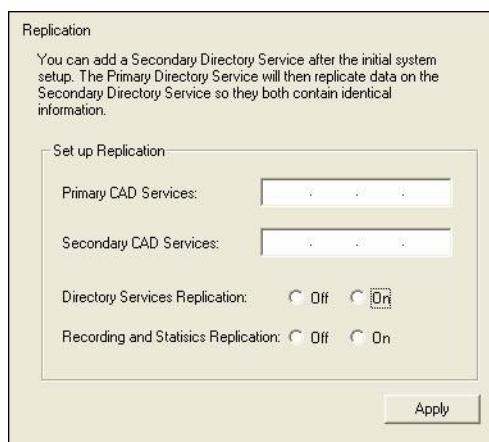
When you continue to the next window, a dialog box appears, reminding you to re-establish replication after the restore is done.

NOTE: You can restore recording metadata without restoring audio files, but you cannot restore audio files without recording metadata.

For information about backing up and restoring CAD data, see "[Backup and Restore \(BARS\)](#)" on page 82.

Replication Setup

Figure 16. Replication Setup window.



This window is displayed only when you run CAD Configuration Setup in Update mode on the secondary CAD Services server.

Use the Replication Setup window to add a secondary Directory Services, a secondary Recording and Statistics Service, or both, after the initial system setup. The primary service will then replicate data on the secondary service so that they both contain identical information.

NOTE: If you are setting up replication for the Directory Services and/or the Recording and Statistics Service, make sure that Cisco Security Agent is stopped on both computers.

If you want to set up Directory Services replication, select **On** for Directory Services Replication. If you want to set up Recording and Statistics replication, select **On** for Recording and Statistics Replication. If you select **On** for one or both services, type the IP addresses of the primary and secondary servers in the corresponding fields.

To save your settings, click **Apply**. A dialog box appears and prompts you to type the hostname of the computer you have identified as the primary server for Recording and Statistics replication. Type the primary server hostname and click **OK**. A dialog box appears and prompts you to type the hostname of the computer you have identified as the secondary server for Recording and Statistics replication. Type the second server hostname and click **OK**.

Restore Backup Data

Figure 17. Restore Backup Data window.



This window appears only when CAD Configuration Setup is run for the first time during CAD services installation.

If you want to restore data that was saved from a previous version of CAD, click **Yes**. A dialog box appears, reminding you to shut down replication before you start restoring backup data.

NOTE: If you do not shut down replication before restoring your data, your database may become corrupted.

Click **OK** and then enter the path to the backup folder. When you move to the next window or click **Apply**, a dialog box appears, reminding you to re-establish replication after you exit CAD Configuration Setup.

The tool used to save data is CDBRTool utility, used to back up data from CAD 6.0 and CAD 7.0.

For information about using these tools, see ["Upgrading From a Previous Version" on page 75](#).

Services Configuration

Figure 18. Services Configuration window.

Services Configuration

Services must register their IP address with Directory Services in order to function correctly. If the PC on which the services are installed has more than one network adapter card (NIC), it will have more than one IP address.

Select the IP address to register

IP Address: 10.10.51.87

Would you like CAD automatic updates enabled?

☒ Yes ☐ No

The BIPPA service needs a user name and password to connect to the CallManager.

BIPPA user login

Login ID: telecaster

Password: xxxxxxxx

Confirm Password: xxxxxxxx

Apply

The Services Configuration window only appears during Update mode.

If the computer has more than one IP address, select the IP address of the NIC used to connect to the LAN—it must be accessible by the client desktops.

If you enable automated CAD updates, every time a user starts Agent Desktop, Supervisor Desktop, or Desktop Administrator the system checks if there is a newer version available. If there is, it automatically runs the update process.

To enable automated updates, select **Yes**.

NOTE: Automated updates are disabled for Windows Vista.

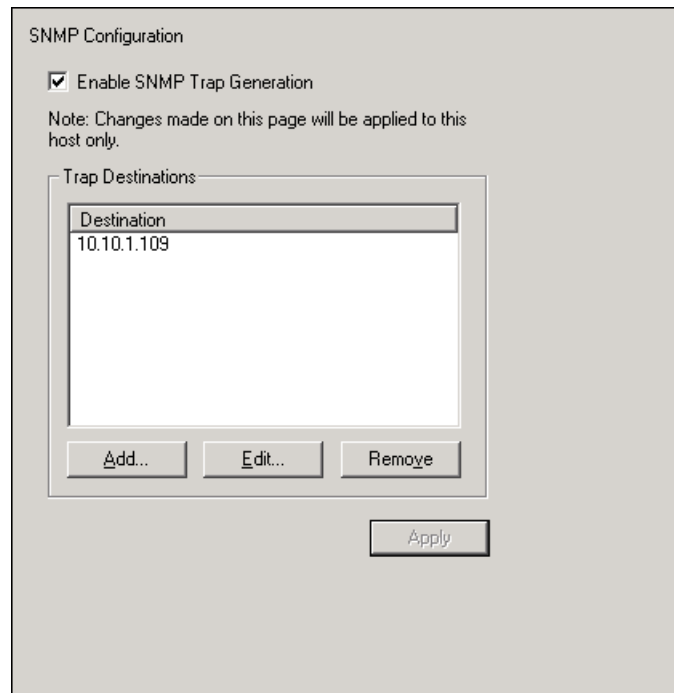
In order to connect to the CallManager, the BIPPA Service must have a user ID and password. This user ID and password are also set up in CallManager. You can complete these fields before actually setting up the user in CallManager, but the user ID and password must be identical in both places. If they are changed in this window or in CallManager, they must be changed in both.

NOTE: If you change these settings after initial setup, you must restart the all CAD services to ensure that the change is registered with them properly.

To set up the user ID and password, see ["Creating a Unified CM User" on page 93](#).

SNMP Configuration

Figure 19. SNMP Configuration window.



The SNMP Configuration window appears only during the Update mode if the Microsoft Simple Network Management Protocol (SNMP) Service is installed on the CAD services server.

If you select the **Enable SNMP Trap Generation** check box, INFO and higher error messages are sent from the CAD services server to the IP addresses configured in the Destination pane. Use the **Add**, **Edit**, and **Remove** buttons to manage the list of destination IP addresses.

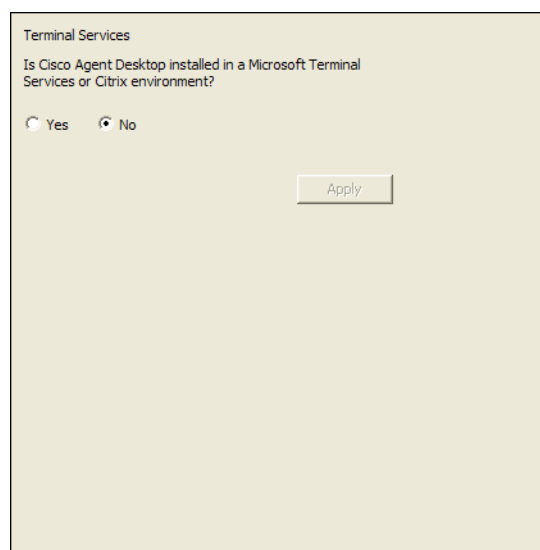
The SNMP Service can be installed using the Add/Remove Windows Components button in the Add or Remove Programs utility in Control Panel (select Management and Monitoring Tools from the list of available components, and then choose Simple Network Management Protocol).

SNMP allows you to monitor and manage a network from a single workstation or several workstations, called SNMP managers. SNMP is actually a family of specifications that provide a means for collecting network management data from the devices residing in a network. It also provides a method for those devices to report any problems they are experiencing to the management station.

Consult Microsoft SNMP documentation for more information on using this tool.

Terminal Services

Figure 20. Terminal Services window.

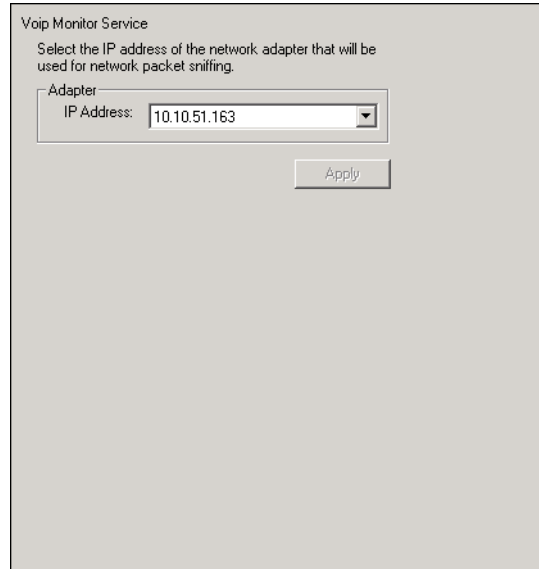


If this installation of Cisco Agent Desktop is installed in a Microsoft Terminal Services or Citrix environment, click **Yes**. If not, click **No**.

NOTE: You must be running CAD Configuration Setup on the PC where the Citrix/Microsoft Terminal Services Service is hosted in order to view this window.

VoIP Monitor Service

Figure 21. VoIP Monitor Service window.



The VoIP Monitor Service window only appears during Update mode.

Select the IP address of the network adaptor to which voice packets are sent to be sniffed by the VoIP Monitor Service (if this is a server box) or the desktop monitor (if this is a client desktop).

- On a VoIP Monitor Service server, it is the IP address of the NIC that is connected to the port configured for SPAN.
- On a client desktop computer, it is the IP address of the NIC on which the computer is daisy-chained to the phone.

NOTE: If you change these settings after initial setup, you must restart the VoIP Monitor Service or the client application (depending on where you run Configuration Setup) to ensure that the change is registered with them properly.

Cisco Desktop Monitoring Console

The Cisco Desktop Monitoring Console is a Java application that monitors the status of the CAD services and Directory Services (LDAP). It is installed automatically when the CAD base services are installed. The console is accessed from the web page:

`http://<CAD base services IP address>:8088/smc/monitor.jsp`

The system administrator can hyperlink this URL to the IPCC Configuration node in Cisco Desktop Administrator for easy access to the Monitoring Console tool.

Any computer running a CAD service must have the Windows Management and Monitoring Tool component installed in order for the Desktop Monitoring Console to be able to monitor that service's status.

To install the Windows Management and Monitoring Tool component:

1. On the server where the CAD service(s) is installed, access the Windows Control Panel and start the **Add/Remove Programs** utility.
2. From the button bar on the left of the Add/Remove Programs window, click **Add/Remove Windows Components**.
3. In the Windows Components Wizard, select the Management and Monitoring Tool from the selection pane and click **Next** to start the installation.
4. Follow the instructions in the wizard to install the component.
5. When the installation is complete, close the Add/Remove Programs window.
6. In the Control Panel, start the **Administrative Tools** utility and click **Services** to display a list of available services.
7. Right-click **SNMP Service** and select **Properties**.
8. In the SNMP Service Properties window, select the Security tab.
 - a. In the Accepted Community Names section, ensure that **public** has READ-ONLY rights.

NOTE: "public" is case sensitive, and must be all lowercase.

- b. Select one of the following SNMP options.
 - Accept SNMP Packets From Any Host
 - Accept SNMP Packets From These Hosts

If security is a concern, select this option. Using this option enables you to identify one or more specific machines that can send SNMP packets to this server.

- c. If you selected Accept SNMP Packets From These Hosts, add the IP addresses for all of the servers on which CAD Base Services are installed.

NOTE: Do not use LocalHost or any other DNS name. Using DNS names may lead to problems if DNS does not properly resolve the hostnames to IP addresses.

9. Click **Apply** to save your changes, and then **OK** to close the window.
10. After making any changes to the SNMP Service, restart the service for the changes to take effect.

Licensing CAD 7.2

After you have installed the CAD services and configured them using CAD Configuration Setup, IPCC License Administration automatically starts. You can license your software at this point, or close the application and license it at a later time. Do this whenever you want to update the number of seats purchased after the initial licensing.

Until you have licensed it, none of your CAD software will run.

NOTE: Licensing your software can only be completed by a Cisco channel partner or Cisco Professional Services.

Obtaining a License Account

If you do not already have one, you must first obtain a license account user ID and password before you can license your software.

To obtain a license account:

1. Open Internet Explorer.
2. Navigate to this address:
<http://209.46.83.138/sws/WebLicensingInitial/InitialLicensePage.html>
3. Click the hyperlink **Create a License Account**.
4. Complete the Partner License Request Form and then click **Email Request**.

After your request has been processed, your license account user ID and password will be emailed to you.

Using IPCC License Administration

If you are installing the CAD services on a computer running Windows Server 2003, you may be unable to access the licensing web site. Internet Explorer will display the following popup message:

“Content from the web site listed below is being blocked by the Internet Explorer Enhanced Security Configuration”.

You must change some Internet Explorer settings to enable access to the licensing web site.

To enable access to the licensing web site:

1. In Internet Explorer, choose **Tools > Internet Options** and select the **Security** tab.

2. Select **Trusted Sites**, and then click **Sites**.
3. Enter the URL of the licensing web site in the appropriate field and then click **Add**.
4. Uncheck **Require server verification (https:) for all sites in this zone**.
5. Click **OK**.

To start IPCC License Administration:

1. Start Windows Explorer.
2. Navigate to the ... \Program Files\Cisco\Desktop\bin folder.
3. In the folder, double-click **LicenseAdmin.exe**.

IPCC License Administration starts. (See [Figure 22](#).)

NOTE: Licensing your software can only be completed by a Cisco channel partner or Cisco Professional Services.

Figure 22. IPCC License Administration window.

Site Keys	
Customer ID	0
Computer ID	1341567

License				
	Current	Request #	License Code	Verification #
Agents/Seats	0	279125053		
Package		287513607		

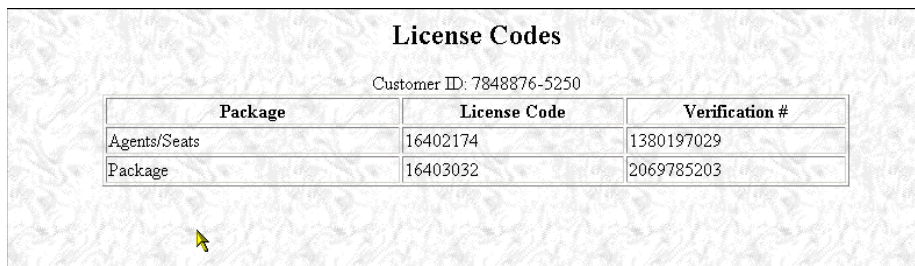
License URL Finish Cancel

To license CAD 7.2:

1. In the IPCC License Administration window, click **License URL**.
Your web browser is started and the secured licensing website at <http://209.46.83.138/sws/ciscoLicense/LicenseRegister.html> is accessed.
2. Follow the instructions on the website, entering installer and contact center information, customer ID, and license request numbers.

3. After you submit the information, the website returns with a page listing the license codes and verification numbers you need to license the products. (See [Figure 23.](#))

Figure 23. Web page showing returned license codes and verification numbers.



Customer ID: 7848876-5250		
Package	License Code	Verification #
Agents/Seats	16402174	1380197029
Package	16403032	2069785203

4. Enter the license codes and verification numbers in the appropriate fields in the IPCC License Administration window, and then click **Finish**.

IPCC License Administration creates a licensing file and places it in the folder where the global configuration files are located. It then activates all the licensed applications.

Recording Licenses

Recording and playback are licensed features. The number of licenses available is determined by the type of bundle you purchase:

- Standard:no license
- Enhanced:32 licenses
- Premium:80 licenses

A license is used whenever a supervisor or agent triggers the recording function, and is released when the recording is stopped. A license is also used when a supervisor opens the Supervisor Record Viewer, and is released when the Supervisor Record Viewer is closed.

If all licenses are in use:

- Agents and supervisors cannot record calls
- Supervisors cannot open Supervisor Record Viewer and an error message saying that a licensing error has occurred is displayed

Installing Desktop Applications

Cisco Desktop Administrator, Cisco Supervisor Desktop, and Cisco Agent Desktop are installed from web pages that are created during the CAD services installation. The web pages are located on servers that host the CAD Base services.

Cisco Agent Desktop—Browser Edition (CAD-BE) is a Java applet that runs on the server that hosts the CAD base services and is accessed by agents through their Windows Internet Explorer or Mozilla Firefox browser. The Java Runtime Environment (JRE) browser plug-in must be installed on each user's computer.

NOTE: You cannot install any of the desktop applications on a server unless you are running CAD in a Citrix/MTS environment. See ["Citrix and Microsoft Terminal Services Environments" on page 27](#) for more information.

If you want users with limited privileges to their computer to be able to install a desktop application (for example, Agent Desktop) you must enable the Windows policy "Always Install with Elevated Privileges" for both the User Configuration and the Computer Configuration. When this policy is enabled, Windows Installer installations run in a context with elevated privileges, allowing the install to successfully complete complex tasks which require a privilege level beyond that of the logged-on user.

Client Installation Failure

If the installation program for any CAD client application will not run, and you receive the error message, "This installation is not fully configured. See product documentation for properly configuring your system", it means that the installation programs are not correctly configured through CAD Configuration Setup. You must reconfigure the client installation programs.

To correct this problem, follow this procedure.

NOTE: In a redundant configuration, you must complete this procedure on both the primary and secondary CAD Base Services servers.

To reconfigure CAD client installation programs:

1. Run CAD Configuration Setup on the CAD Base Services server (see ["Cisco Agent Desktop Configuration Setup" on page 45](#) for more information).
2. From the menu, choose **File > Reset Client Installs**.

This process reconfigures the client installation programs.

3. When the process is complete, the message, “Client installs reset” is displayed. Click **OK** to close the message.

You can now install the client applications from the installation web pages.

Error/Event and Debug Logs

The CAD event/error and debugging logs can help you discover where problems exist if you experience difficulties in installing the CAD desktop applications. You must enable logging from the command line prompt for all new installs and most upgrade scenarios. The exception to this requirement is the client-side automated update feature.

For detailed information on logs and debugging, see Chapter 4, “Logs and Debugging”, in the *Cisco CAD Service Information Manual*.

Using Automated Package Distribution Tools

CAD desktop applications can be pushed (installed or upgraded on multiple desktops on a per-machine basis) through the use of automated package distribution tools that make use of the Microsoft Windows Installer service.

Consult the distribution tool’s documentation for information on how to do this.

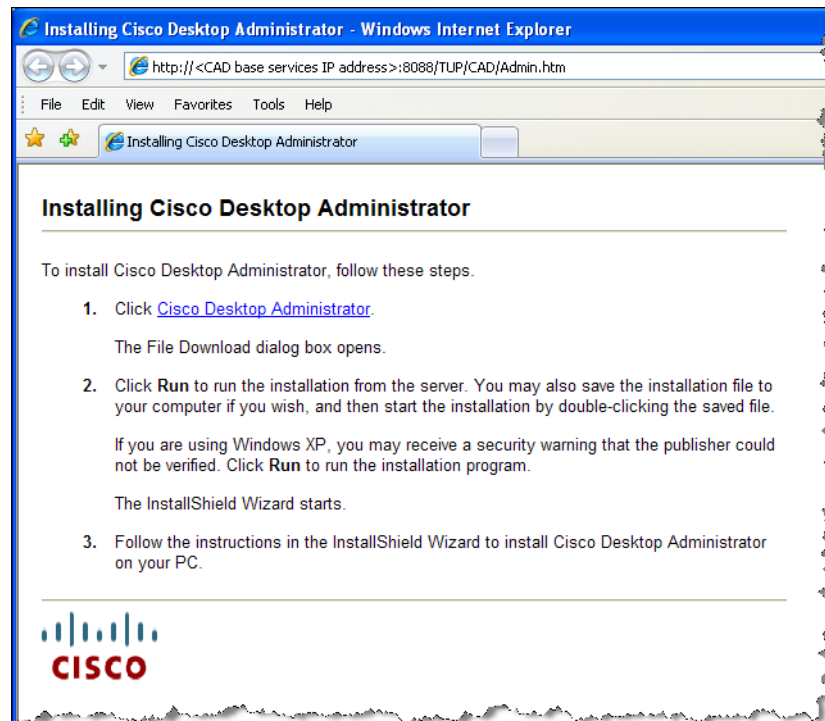
Cisco Desktop Administrator

To install Desktop Administrator:

1. From the desktop where you wish to install Desktop Administrator, access the web page located at:

<http://<CAD base services IP address>:8088/TUP/CAD/Admin.htm>

The Desktop Administrator Installation web page appears.

Figure 24. Cisco Desktop Administrator Installation web page

Follow the instructions on the web page to install the application.

Cisco Agent Desktop and Cisco Supervisor Desktop

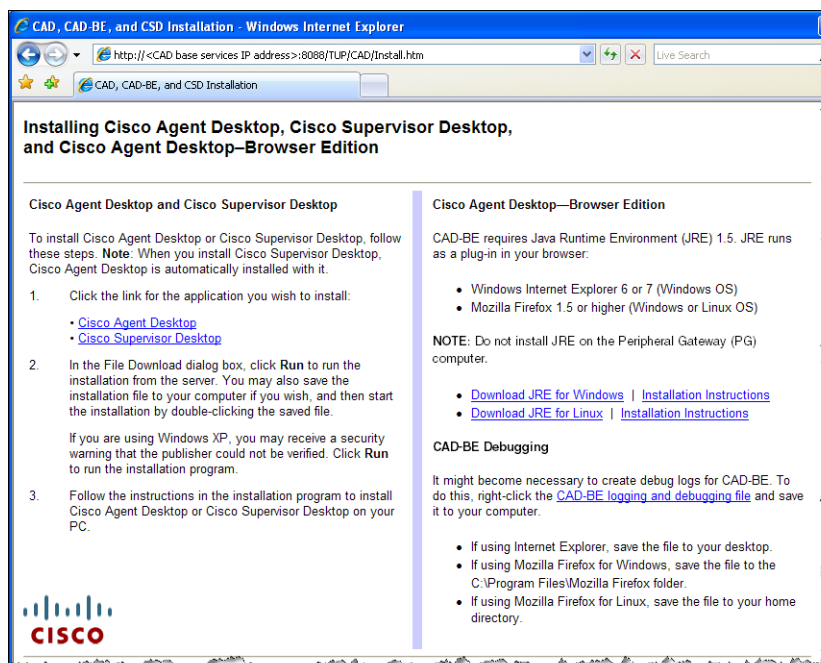
To install Agent Desktop and Supervisor Desktop:

1. From the desktop where you wish to install Agent Desktop or Supervisor Desktop, access the web page located at:

http://<CAD base services IP address>:8088/TUP/CAD/Install.htm

The Agent Desktop/Supervisor Desktop/CAD-BE Installation web page appears (see [Figure 25](#)).

Figure 25. CAD desktop applications installation web page



- Follow the instructions on the web page to install the selected application.

Installation Notes

- When you install Supervisor Desktop, Agent Desktop is automatically installed. Both applications are needed for a supervisor to use all the functionality of Supervisor Desktop.
- If you attempt to install Supervisor Desktop on a computer that already hosts Agent Desktop, you will receive error messages that a conflicting application has been detected. You must first uninstall Agent Desktop to avoid this.

Cisco Agent Desktop—Browser Edition

The CAD-BE Java applet is installed when the Browser and IP Phone Agent Service is installed, and on the same computer as the BIPPA Service.

In order to run CAD-BE in an agent's browser, the Java Runtime Environment (JRE) plug-in for Internet Explorer or Firefox (Windows) or for Firefox (Linux) must be installed.

See "[Internet Explorer Settings for CAD-BE](#)" and "[Firefox Settings for CAD-BE](#)" for information on how to configure your web browser to run CAD-BE.

To install the JRE plug-in:

1. From the desktop where you wish to install the JRE plug-in, access the web page located at:

http://<CAD base services IP address>:8088/TUP/CAD/Install.htm

The Agent Desktop/Supervisor Desktop/CAD-BE Installation web page appears (see [Figure 25](#)).
2. From the CAD-BE section, download JRE for your operating system (Windows or Linux).
3. Click the appropriate **Installation Instructions** link and follow the procedure for your operating system.

If the correct version of JRE already exists on the agent desktop, you will see a message telling you this and the installation will not proceed. If an older or newer version of JRE than the version required exists on the agent desktop, the installation goes forward with no messages displayed.

Internet Explorer Settings for CAD-BE

The following settings must be configured in Internet Explorer in order for CAD-BE to run successfully.

Pop-up Blocker

Disable the pop-up blocker, or create an exception to enable pop-ups from the CAD-BE IP address:

- Choose **Tools > Pop-up Blocker > Turn Off Pop-up Blocker**.

OR

- Choose **Tools > Pop-up Blocker > Pop-up Blocker Settings** and add the CAD-BE IP address(es) to the list of allowed sites.

Internet Options

Set the following internet options:

1. Choose **Tools > Internet Options** and select the Security tab.
2. Click **Custom Level**.
3. In the Settings pane, set the following options:
 - Under the ActiveX controls and plug-ins section, set **Run ActiveX controls and plug-ins** to **Enable**.
 - Under the Miscellaneous section, set **Launching programs and files in an IFRAME** to **Prompt** or **Enable**.
 - Under the Scripting section, set **Active Scripting** to **Enable**.

Firefox Settings for CAD-BE

The following settings must be configured in Firefox in order for CAD-BE to run successfully.

Popup Blocker

Disable the pop-up blocker, or create an exception to enable pop-ups from the CAD-BE IP address:

- Choose **Tools > Options > Content**. Deselect **Block Popup Windows**.

OR

- Choose **Tools > Options > Content**. Click **Allowed Sites** and add the CAD-BE IP address(es) to the list of allowed sites.

Content Settings

Configure the following settings:

1. Choose **Tools > Options > Content**, and select these check boxes:
 - Enable Java
 - Enable JavaScript
2. Next to the Enable JavaScript check box, click **Advanced** and select these check boxes in the Advanced JavaScript Settings dialog box:
 - Raise or lower windows
 - Disable or replace context menus
3. In the browser address field, type:
about:config
4. Locate the preference **dom.allow_scripts_to_close_windows**.
5. Right-click the preference and select **Toggle** from the resulting menu to set the value to **True**.

Upgrading From a Previous Version

NOTE: If you are upgrading a replicated system, you must shut down replication before doing the upgrade. After you finish the upgrade, re-establish replication.

If you are upgrading to CAD 7.2 from CAD 6.0 or a previous version, you must complete the following steps in the order shown.

1. Back up your configuration data using the CAD backup and restore utilities for the version you are upgrading.
2. Uninstall the previous version of CAD.
3. Install CAD 7.2 and restore the data you backed up during the installation process.

If you are upgrading to CAD 7.2 from CAD 7.0 or 7.1, you can install CAD 7.2 directly over the previous version. You can also upgrade a previous version of CAD 7.2 to the current version of CAD 7.2 by installing the current version over the previous version.

NOTE: It is recommended that you upgrade the CAD services only when no CAD users (agents, supervisors, and administrators) are logged into the system. If users are logged in, they may receive error messages when the services go offline during the upgrade.

NOTE: In CAD 7.2, reason codes are created and maintained in Cisco Unified Intelligent Contact Management (Unified ICM). Any reason codes that you created using Desktop Administrator in previous versions of CAD will be lost in an upgrade. To continue using previously-created reason codes, re-create them in Unified ICM.

The backup and restore utilities used in the following upgrade procedures are described in detail in the section ["Backup and Restore \(BARS\)" on page 82](#).

NOTE: You must use the utilities from the Installation disks of the version you are backing up. For example, if you are upgrading from CAD 6.0 to CAD 7.2, use the utilities on your CAD 6.0 installation disk, not those on the CAD 7.2 installation disk.

Previous Version Hot Fixes and Service Releases

If you have any CAD hot fixes or service releases for previous versions installed, uninstall them before upgrading to CAD 7.2.

Hot fixes can be identified by their listing in the Add/Remove Programs utility in Windows Control Panel. The listing follows the format:

- Hot Fix [number] for: [installed CAD bundle(s)]
- Desktop SR [number]

For instance,

- Hot Fix 01 for: Servers, Admin
- Desktop SR 02

Service releases can be identified by their listing in the Add/Remove Programs utility in Windows Control Panel. The listing follows the format:

- CAD Service Release
- CAD Clients Service Release

Changing Feature Levels in an Upgrade

If you are changing feature levels (for instance, changing from CAD Standard to CAD Premium), you must run License Administration (LicenseAdmin.exe) after the upgrade is completed and then restart the BIPPA Service.

NOTE: Licensing your software can only be completed by a Cisco channel partner or Cisco Professional Services.

Best practices recommends that any backups made before changing the feature level should be deleted, and new backups at the new feature level be created.

For information on the features provided at each feature level, see ["CAD 7.2 Feature Levels" on page 18](#).

To change feature levels in an upgrade:

1. On the computer that hosts the CAD services, using Windows Explorer, navigate to C:\Program Files\Cisco\Desktop\bin.
2. Run **LicenseAdmin.exe** to start IPCC License Administration.
3. In the IPCC License Administration window, click **License URL**.

Your web browser starts and opens the secured licensing website at <http://209.46.83.138/sws/ciscoLicense/LicenseRegister.html>.

4. In the Customer ID field, enter **0** (zero), and then click **Continue**.

You must enter the website as a new customer (triggered by entering 0 in the customer ID field) even though you might already have a customer ID number.

5. Enter the product information. This includes the new package (feature level) you have purchased.
6. Continue through the licensing process (see ["Licensing CAD 7.2" on page 66](#)).
7. When licensing is completed, restart the Browser and IP Phone Agent Service.

Upgrading from CAD 6.0 to CAD 7.2

If you are upgrading a single server:

- Complete steps 1-5 only in the following procedure.

If you are upgrading a replicated system:

- Shut down replication on both servers before beginning the following procedure. For instructions, see ["Shutting Down Replication \(CAD 7.1 and before\)" on page 90](#).
- Complete steps 1-5 on the primary server and the remaining steps on the secondary server.

NOTE: If you do not shut down replication before beginning the procedure, your CAD Services LDAP database may become corrupted.

To upgrade from CAD 6.0 to CAD 7.2:

1. Back up your CAD 6.0 LDAP configuration data, recordings, and Recording and Statistics Service database.
 - a. Back up your LDAP configuration data and recordings by running CDBRTool twice. For instructions, see ["CDBRTool Utility" on page 85](#).
 - b. Back up your Recording and Statistics database using BackupDB. For instructions, see ["BackupDB Utility" on page 84](#).

NOTE: Save the three types of backup files to different folders. Keeping the backup files separated prevents the backup and restore tools from reading from or writing to the wrong type of file.

NOTE: Keep your backups in case you need to roll back to your previous version of CAD.

2. Uninstall CAD 6.0.
3. Install CAD 7.2.

After the installation finishes, CAD Configuration Setup starts automatically.

4. In CAD Configuration Setup, complete the data entry windows as described in ["Configuring a Single Server or Primary Server in a Replicated System" on page 47](#).
 - a. In the Recording and Statistics Service Database window, select **Restore From** and enter the location to which you backed up the database in step 1b. Then, click **Apply** to restore the database.
 - b. In the Restore Backup Data window, enter the location to which you backed up the CAD Services LDAP configuration data (see ["CAD Configuration Setup Windows" on page 49](#)). Then, click **Apply** to restore the CAD Services LDAP configuration data.
 - c. Exit CAD Configuration Setup.
5. Restore your recording backups using CDBRTool. For instructions, see ["CDBRTool Utility" on page 85](#).

If you are upgrading a single server, you have completed the upgrade.

If you are upgrading a replicated system, complete the remaining steps on the secondary server.
6. Log on to the secondary server.
7. Uninstall CAD 6.0.
8. Install CAD 7.2.

After the installation finishes, CAD Configuration Setup starts automatically.

9. In CAD Configuration Setup, complete the data entry windows as described in ["Configuring a Secondary Server in a Replicated System" on page 48](#). When you have finished, exit CAD Configuration Setup.
10. The upgrade on both servers is now done and replication has been re-established.

Upgrading from CAD 7.0 or 7.1 to CAD 7.2

NOTE: When you upgrade from CAD 7.0 or 7.1 to CAD 7.2, the install process automatically backs up your CAD Services LDAP configuration data. It is a good idea, however, to manually back up your data as well. For instructions, see ["CDBRTool Utility" on page 85](#) and ["BackupDB Utility" on page 84](#).

NOTE: Keep your backups in case you need to roll back to your previous version of CAD.

If you are upgrading a single server:

- Complete steps 1 and 2 only in the following procedure.

If you are upgrading a replicated system:

- Shut down replication on both servers before beginning the following procedure. For instructions, see ["Shutting Down Replication \(CAD 7.1 and before\)" on page 90](#).

NOTE: If you do not shut down replication before beginning the procedure, your CAD Services LDAP database may become corrupted.

- Complete steps 1 and 2 on the primary server and the remaining steps on the secondary server.

To upgrade from CAD 7.0 or 7.1 to CAD 7.2:

1. Install CAD 7.2.

After the installation finishes, CAD Configuration Setup starts automatically.

2. In CAD Configuration Setup, verify that the data is correct in the data entry windows as described in ["Configuring a Single Server or Primary Server in a Replicated System" on page 47](#).
 - a. In the Recording and Statistics Service Database window, leave Blank Database selected. Your recording and statistics data will be restored automatically. A new database will not be configured.
 - b. In the Restore Backup Data window, leave No selected. Your CAD LDAP configuration data will be restored automatically.
 - c. Exit CAD Configuration Setup.

If you are upgrading a single server, you have completed the upgrade.

If you are upgrading a replicated system, complete the remaining steps on the secondary server.

3. Log on to the secondary server.

4. Install CAD 7.2.

After the installation finishes, CAD Configuration Setup starts automatically.

5. In CAD Configuration Setup, complete the data entry windows as described in ["Configuring a Secondary Server in a Replicated System" on page 48](#).
6. After you complete all of the data entry windows and exit CAD Configuration Setup, the upgrade is done and replication is re-established.

Upgrading CAD 7.2 to a Newer Version

CAD 7.2 can be upgraded to a newer version of 7.2 by installing the new version over the old version. Configuration data and recordings are preserved during the upgrade and do not need to be backed up.

NOTE: Custom application configuration settings, such as logging levels, debug levels, and file locations, will be lost if you repair or upgrade the application when you do not have Administrator privileges on the client machine. If you do have Administrator privileges, those configuration settings will be preserved.

Rolling Back CAD 7.2 to an Earlier Version of CAD

To use the following procedure, you must have backed up your original version of CAD before installing CAD 7.2.

To uninstall CAD 7.2 and revert to an earlier version of CAD:

1. If you are rolling back CAD 7.2 on a replicated system, shut down replication now. For instructions, see ["Shutting Down and Restarting Replication" on page 88](#).

NOTE: If you do not shut down replication before completing this procedure, your CAD Services LDAP database may become corrupted.

2. Uninstall CAD 7.2.
3. Install your previous CAD version according to the product documentation.
4. Restore your backed-up data using the CAD Configuration Setup tool:
 - The configuration data backed up with CDBRTool or DABackupTool is restored by entering the location of the backup file in the Restore Backup Data window.
 - The Recording and Statistics database backed up with BackupDB is restored by selecting "Restore From" and entering the location of the backup file in the Recording and Statistics Service Database window.
5. If you are rolling back a replicated system, re-establish replication. For instructions, see the instructions for setting up replication in the appropriate version of *Cisco CAD Installation Guide*.

Upgrade Notes

- Any work sites configured for the Agent Desktop integrated browser in CAD 6.0 or 7.0 will become work flow browser tabs in CAD 7.2. The first tab, which is reserved for a supervisor push page, is automatically set to www.cisco.com.
- Any reason codes created using Desktop Administrator in previous versions of CAD will be lost after upgrading to CAD 7.2. All reason codes are created and maintained in Unified ICM in CAD 7.2. To continue using the reason codes created in previous versions, ensure they are set up in Unified ICM.

- All reserved reason codes are automatically enabled in CAD 7.2.
- Phone books from previous CAD versions will be saved as global phone books in CAD 7.2.
- Wrap-up data from previous CAD versions will be enabled at the work flow group level and disabled at the global level. It can be enabled later at the global level as needed.
- If you changed the IP address of any server in your configuration after you backed up data, you must run CAD Configuration Setup and enter the current IP addresses after you have restored your data, because the old IP addresses will be restored.

Backup and Restore (BARS)

This section describes how to back up and restore CAD configuration settings and recordings using the CAD backup and restore (BARS) utilities.

NOTE: For the most recent information on BARS procedures and utilities, consult the Release Notes.

NOTE: Save each type of backup file to a different folder. Keeping the backup files separated prevents the backup and restore tools from reading from or writing to the wrong type of file.

NOTE: You must use the utilities that were provided with the version of CAD you are backing up and with the version of CAD to which you are restoring the data. For example, if you are upgrading from CAD 6.0 to CAD 7.2, you must use the utilities installed with CAD 6.0 to back up data, and the utilities installed with CAD 7.2 to restore data.

Backup File Location

The BARS tools enable you to save backup files to either network or local drives. However, due to file permission issues, CAD Configuration Setup cannot restore files if the backups are located on a network drive.

For this reason it is recommended that you save backup files to a local drive, and copy those backups to a secure location elsewhere if desired.

Backing Up CAD Data

The process for backing up your CAD configuration settings and recordings is outlined here. You can back up the settings and recordings from a previous version of CAD and restore them to CAD 7.2, or make a backup of CAD 7.2 data for safety purposes.

It is recommended that you perform backups during down times when all agents are logged out.

In a redundant system, run the CDBRTool utility on both Side A and Side B to back up audio recordings that are saved on both sides. However, run the BackupDB tool only on one side, not on both sides.

To back up CAD data:

1. On the server hosting the CAD base services, run the CDBRTool utility to back up the CAD Services LDAP configuration data and/or recordings (see ["CDBRTool Utility" on page 85](#)).

2. On the server hosting the Recording and Statistics Service, run the BackupDB utility to back up recording metadata (see ["BackupDB Utility" on page 84](#)).

NOTE: To prevent possible file permission issues upon restore, save backup files for the Recording and Statistics Service database to a local drive. Copy the backup files to a secure location elsewhere if desired.

Restoring CAD Data

The process for restoring your CAD configuration data and recordings is outlined here.

To restore CAD data if you are upgrading to CAD 7.2 or reinstalling CAD 7.2:

After you have upgraded or reinstalled the CAD services, CAD Configuration Setup runs. Part of CAD Configuration Setup is restoring backed-up data.

1. In the Recording and Statistics Service Database window, select **Restore recording metadata (BackupDB)** and enter:
 - The path where the recording metadata backup file created by the BackupDB utility is saved
 - The path where the backup audio files created by the CDBRTool utility are saved

This restores the recording metadata and recordings. See ["Recording and Statistics Service Database" on page 57](#) for more information.

2. In the Restore Backup Data window, answer **Yes** and enter the path where the backup files created by the CDBRTool utility are saved.

This restores the CAD Services LDAP (Directory Services) database. (See ["Replication Setup" on page 58](#) for more information.)

NOTE: In a redundant system, restore data only on Side A. The restored data will be replicated on Side B the next time the two sides are synchronized.

To restore CAD data if you are restoring a backup of an existing CAD 7.2 installation:

1. On the server hosting the CAD base services, run the CDBRTool utility (see ["CDBRTool Utility" on page 85](#)).

This restores the CAD Services LDAP configuration data and the recordings.

2. On the server hosting the Recording and Statistics Service, run the InstallRestoreDB utility (see ["InstallRestoreDB Utility" on page 85](#)).

This restores the recording metadata.

BackupDB Utility

To preserve the Recording and Statistics Service database, use the BackupDB utility (BackupDB.bat). This utility backs up the recording metadata in the database. Recording metadata is the information saved about a recording—time and date of recording, the agent recorded, and so on.

NOTE: The recordings themselves are preserved using the CDBRTool utility. See ["CDBRTool Utility" on page 85](#) for more information.

NOTE: If you are running Cisco Security Agent (CSA) on your CAD base services server, shut it down before running BackupDB on the server. If CSA is running when you launch BackupDB, the backup will fail.

To run BackupDB:

1. Log in to the server hosting the CAD Recording and Statistics Service.

NOTE: On a redundant system, do this on the Side A server. You can obtain the IP address of the Side A server by running CAD Configuration Setup and noting the IP addresses in the Replication Setup window.

2. In a command window, navigate to C:\Program Files\Cisco\Desktop\db.
This is the default location for the BackupDB utility.
3. At the prompt, run the following command.

```
BackupDB "<dbUser>" "<dbPassword>" "<server>" "<dir>"  
where:
```

<dbUser> is the user ID for the old database. The default is **sa**.

<dbPassword> is the password for the old database. The default is **sa**.

NOTE: If the user ID and password are not the default values and you have forgotten what they are, contact technical support for assistance.

<server> is the hostname of the server on which the database is located, or the local loopback IP address of 127.0.0.1.

<dir> is the directory in which the backup file is to be saved. <dir> must be a local drive.

4. Press **Enter**.

The utility backs up the database to a file named **Cadbkp.dat** in the folder you specified.

InstallRestoreDB Utility

The InstallRestoreDB utility restores the recording metadata that was backed up using the BackupDB utility.

To run InstallRestoreDB:

1. On the server hosting the CAD Recording and Statistics Service, open a command window.

NOTE: On a redundant system, do this on the Side A server. You can obtain the IP address of the Side A server by running CAD Configuration Setup.

2. Navigate to the folder where InstallRestoreDB.bat is located. The default location is:

C:\Program Files\cisco\Desktop\DB

3. On the command line, type:

```
InstallRestoreDB.bat "<userID>" "<password>"  
"<dbserver>" "<backup file path>"  
"<InstallRestoreDB.bat path>"
```

where:

<userID>User ID needed to access the destination database. The default userID is **sa**.

<password>Password needed to access the destination database. The default password is **sa**.

NOTE: if the user ID and password are not the default values and you have forgotten what they are, contact technical support for assistance.

<dbserver>Hostname or IP address of the server where the database is located, or the local loopback IP address of 127.0.0.1.

<backup file path>Folder where the backup file is located. The location must be a local drive.

<InstallRestoreDB.bat path>Folder where the InstallRestoreDB utility is located.

4. Press **Enter**.

The utility restores the recording metadata to the database you specified.

CDBRTool Utility

The CDBRTool utility backs up the following data:

- Desktop Administrator configuration settings (excluding reason codes and personnel configuration, which are managed in Unified ICM)
- Supervisor Desktop metadata
- Agent Desktop preferences and personal phone books
- audio recordings

Use CDBRTool to back up configuration data when upgrading CAD to a newer version, or to create a safety backup file of your CAD configuration.

NOTE: Both Directory Services sides must be running in order for the CDBRTool utility to run correctly.

NOTE: The CDBRTool utility does not preserve recordings tagged with the 30-day extended lifetime. In order to preserve these recordings, it is recommended that you use the Play and Save function in Supervisor Record Viewer to save them as *.wav files. Refer to the *Cisco Supervisor Desktop User Guide* for more information.

If you are running CDBRTool on a replicated system:

- Shut down replication on both servers before beginning the following procedure. When you have completed the procedure, restart replication. For instructions, see ["Shutting Down and Restarting Replication" on page 88](#).

NOTE: If you do not shut down replication before beginning the procedure, your CAD Services LDAP database may become corrupted.

To run CDBRTool:

1. On the computer that hosts the CAD Base services, stop all CAD services except the CAD Services LDAP Monitor Service, and ensure that all users are logged out of the CAD desktop applications.
2. In a command window, navigate to C:\Program Files\Cisco\Desktop\bin.
This is the default location for CAD utilities.
3. At the prompt, run the following command.

```
CDBRTool <switches> "<pathname>"
```

where:

<switches> is one of the switch combinations listed in [Table 6](#)

<pathname> is the folder in which backup files are located

NOTE: You cannot back up or restore CAD Services LDAP configuration data and audio files at the same time. You must run CDBRTool twice, once to back up or restore CAD Services LDAP data and once to back up or restore audio files.

Permissible switch combinations and their meaning are listed in the following table.

For disaster recovery, back up using /B /L and restore using /R /L.
For upgrades, back up using /B /L and restore using /R /P.

Table 6. CDBRTool switches

Switches	Description
/B /L	Back up CAD Services LDAP configuration data.
/R /P	Restore CAD Services LDAP configuration data (merge).
/R /L	Clear the Logical Call Center (LCC) in the CAD Services LDAP database, then restore CAD Services LDAP configuration data (overlay).
/B /A	Back up audio files.
/R /A	Restore audio files.
/B /C	Back up server types, DSNs, and LCC from the company level.
/R /C	Restore server types, DSNs, and LCC from the company level (overlay).
/B /D	Deprecated. Do not use.
/R /D	Deprecated. Do not use.

BARS Notes

- Voice contact work flows that were enabled before a backup might be disabled after a restore. The work flows can be re-enabled in Cisco Desktop Administrator.
- CDBRTool creates files with the same name in every backup you run. If you want to keep multiple backups, they must be written to different folders. If the backup is written to the same folder, the existing files will be overwritten by the most recent backup.
- Files created by the backup and restore tools on a localized system must not be modified or saved using Microsoft WordPad or Notepad. These editors will corrupt the file when saved.

Shutting Down and Restarting Replication

If you have configured your system with Directory Services replication or Recording and Statistics Service replication, you may occasionally need to temporarily shut down replication. Temporarily shutting down replication may be required for the following situations.

- You move one of the Directory Services or Recording and Statistics Service instances to another server.
- You need to upgrade CAD.
- One of the Directory Services servers is shut down for two days or more.

When one of the servers in a replicated system is down for an extended time such as this, the remaining Directory Services server experiences high resource usage. The longer that server is down, the higher the resource usage becomes on the remaining server.

If you are shutting down replication because you are upgrading from a version of CAD before 7.2, complete the shutdown procedure in ["Shutting Down Replication \(CAD 7.1 and before\)" on page 90](#).

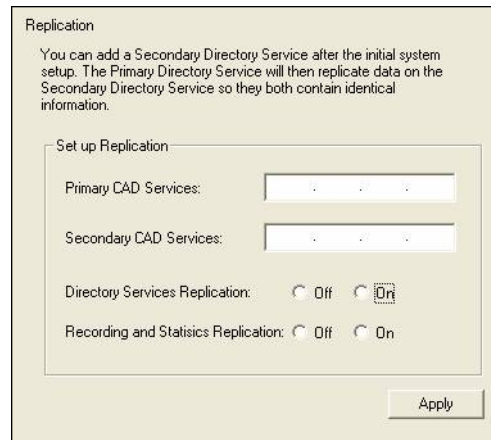
NOTE: If you are setting up replication for Directory Services and/or the Recording and Statistics Service, make sure that Cisco Security Agent is stopped on both computers.

Shutting Down Replication (CAD 7.2)

To shut down replication in CAD 7.2:

1. Log in to either the primary or secondary server.
2. In Windows Explorer, navigate to C:\Program Files\Cisco\Desktop\bin.
This is the default location for CAD utilities.
3. Run **PostInstall.exe** to start the CAD Configuration Setup utility.
4. Select the Replication Setup window (see [Figure 26](#)).

Figure 26. Replication Setup window.



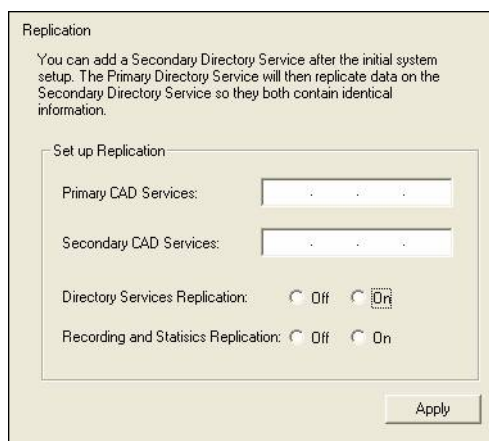
5. In the Replication Setup window, select **Off** for both services.
6. Click **Apply** and exit CAD Configuration Setup.
Replication is now shut down.

Restarting Replication (CAD 7.2)

To restart replication:

1. Log in to either the primary or the secondary server.
2. In Windows Explorer, navigate to C:\Program Files\Cisco\Desktop\bin.
This is the default location for CAD utilities.
3. Run **PostInstall.exe** to start the CAD Configuration Setup utility.
4. Select the Replication Setup window (see [Figure 27](#)).

Figure 27. Replication Setup window.



5. In the window, select **On** for the service(s) you want to replicate. Then enter the IP addresses of the primary and secondary servers.
6. Click **Apply**.

Replication is now re-established between the primary and secondary servers.

If you are shutting down replication because you are upgrading from a previous version of CAD, complete the following procedure.

Shutting Down Replication (CAD 7.1 and before)

To shut down replication in versions of CAD before 7.2:

1. Log in to the secondary server.
2. In a command window, navigate to C:\Program Files\Cisco\Desktop\bin.
This is the default location for CAD utilities.
3. Run the following command, where <IP address> is the IP address of the secondary server.

```
ldaputil /C <IP address>
```

4. Log in to the primary server. If the server is down, restart it.
5. In a command window, navigate to C:\Program Files\Cisco\Desktop\bin.
6. Run the following command, where <IP address> is the IP address of the primary server.

```
ldaputil /C <IP address>
```

Replication is now shut down.

Configuring IP Phones for Cisco IP Phone Agent

After all IP agent phones are added to the Cisco Unified Contact Manager (Unified CM), you must perform the following tasks in Cisco Unified CM Administration:

1. Create an IP phone service.
2. Assign the IP phone service to each IP agent phone.
3. Create an application user named “telecaster” and assign to it all the IP agent phones.
4. Change the default URL Authentication parameter.

These procedures can be done before or after CAD has been installed on your system.

Creating an IP Phone Service

From the Cisco Unified CM Administration web-based application, follow these steps to create a new IP phone service.

To create a new IP phone service:

1. From the menu at the top of the page, click **Device > Device Settings > Phone Services**.
2. On the Find and List IP Phone Services page, click **Add New**.
3. On the Cisco IP Phone Services Configuration page, enter the following information:

Service Name. Enter the name of the service as it will display on the menu of available services in the Cisco IP Phone User Options application. Enter up to 32 characters for the service name.

Service Name (ASCII Format). Enter the name of the service to display if the phone cannot display Unicode.

Service Description. Optional. Enter a description of the content that the service provides.

Service URL. Enter the URL of the server where the Cisco IP Phone Services application is located. For example:

`http://192.168.252.44:8088/ipphone/jsp/sciphonexml/IPAgentInitial.jsp`
where:

- 192.168.252.44 is the IP address of the machine where the BIPPA Service is installed

- 8088 is the Tomcat webserver port (if 8088 is not the port number, check the port parameter in the file C:\Program Files\Cisco\Desktop\Tomcat\conf\server.xml for the correct value.)
- ipphone/jsp/... is the path to the jsp page under Tomcat on the machine where the BIPPA Service is loaded

NOTE: You will not find a file called IPAgentInitial.jsp at this location; there will be a file called IPAgentInitial.class, which contains the implementation of the *.jsp file.

NOTE: The Tomcat webserver is included with the installation.

4. Click **Save** to create the new IP phone service. The new service is now listed on the Find and List IP Phone Services page.

Assigning the IP Phone Service to IP Agent Phones

Once the IP phone service is created, each agent's phone must be configured to use it.

From the Cisco Unified CM Administration web-based application, follow these steps to configure each IP phone.

To assign the IP phone service to IP agent phones:

1. On the Device menu, choose **Phone**.
The Find and List Phones window appears.
2. Use the search function to find the phone. Search results are listed at the bottom of the page.
3. Locate the phone in the list of results and click the hyperlink.
The Phone Configuration page appears.
4. In the upper right corner of the page, select **Subscribe/Unsubscribe Services** from the Related Links drop-down list, and then click **Go**.
A popup window for subscribing to services for that device appears.
5. From the **Select a Service** drop-down list, choose the new service, and then click **Next**.
A popup window showing the new service appears.
6. Click **Subscribe**.
The service is added to the Subscribed Services section of the popup window.
7. Click **Save**, and then close the popup window.

Creating a Unified CM User

The next task to accomplish is to create a Unified CM user, and then add the Unified CM user to the Standard CTI Enabled group.

The Unified CM user is used by the BIPPA Service to push pages to agent IP phones.

NOTE: The Unified CM user ID and password are also entered in CAD Configuration Setup and must match what is configured in Unified CM. If you change them in Unified CM, you must also change them in CAD Configuration Setup. See ["Services Configuration" on page 60](#) for more information.

From the Cisco Unified CM Administration web-based application, follow these steps to set up the new user.

To create the Unified CM user:

1. From the User Management menu, choose **Application User**.
The Find and Add Users page appears.
2. Click **Add New**.
3. In the User Information section, enter a user ID and password for the new user. Entries are case sensitive. If your system is set up to require password complexity, be sure to choose a password that satisfies those requirements.
4. In the Associated Devices pane, use the arrows to move phones from the Available Devices pane to the Controlled Devices pane.
5. When you are done, click **Save** at the bottom of the page.

To add the Unified CM user as part of the Standard CTI Enabled group:

1. From the User Management menu, choose **User Group**.
The Find and List User Groups page appears.
2. Click **Find** to display a list of all user groups.
3. From the list of search results, click **Standard CTI Enabled**.
The User Group Configuration page appears.
4. Click **Add Application Users to Group**.
The Find and List Application Users window appears.
5. Select the BIPPA user name from the search results and then click **Add Selected**.
The window closes and the Unified CM user is added to the Standard CTI Enabled group.

Configuring a One-Button Login for IP Phone Agents

When IP phone agents log in to their phones, they must manually enter their username, password, and extension. Unified CM can be configured so that these parameters are mapped to a particular phone so that the agent does not have to enter them, but can instead log in using one button. One-button login can be used in conjunction with extension mobility.

For more information, see the Cisco document #60134, *Configure a “One Button” Login for IP Phone Agents*, available on the Cisco website at:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_tech_note09186a008029e6d5.shtml#proc

URL Authentication Parameter

Changing the Default URL Authentication Parameter

It is recommended that you bypass the default URL Authentication parameter to maximize system performance. This prevents the Unified CM from polling all devices in the system to authenticate a specific device every time that device pushes information to the Unified CM.

1. From the System menu, choose **Enterprise Parameters**.

The Enterprise Parameters Configuration window appears.

2. Locate the URL Authentication parameter.
3. Change the default value to the following:

`http://Tomcat webserver IP address:8088/ipphone/
jsp/sciphonexml/IPAgentAuthenticate.jsp`

Note: This URL is case sensitive.

4. Click **Update**.
5. Enter * * # * * on all IP Phone Agent phone number pads to reset them.

Configuring a Cisco IP Communicator Phone

From the Cisco Unified CM Administration web-based application, follow these steps to configure a Cisco IP Communicator soft phone.

1. On the Device menu, choose **Add a New Device**.

The Add a New Device window appears.

2. In the Device Type field, choose **Phone**, and then click **Next**.

The Add a New Phone window appears.

3. From the Phone Type drop-down list, choose **Cisco IP Communicator**, and then click **Next**.

The Phone Configuration window appears.

4. Complete the fields in the Phone Configuration window, and then click **Insert**.

In the MAC Address field, enter the MAC address of the computer on which the Cisco IP Communicator phone is installed.

The Cisco IP Communicator phone is inserted into the Unified CM database.

NOTE: A Cisco IP Communicator phone registers with the Unified CM only when Agent Desktop is running on the agent PC.

Setting Up CTI OS Security

There are four elements involved in setting up CTI OS security. They are:

Element	Functions performed on this element
CTI OS Server	<ul style="list-style-type: none"> • Enable security via CTI OS setup • Automatically creates an unsigned certificate
Cisco Desktop Administrator PC	<ul style="list-style-type: none"> • Run CAD Configuration Setup tool and enable CTI OS security, thus setting a flag in CAD Services LDAP that enables the CTI OS node to display in the client CAD Configuration Setup tool
Cisco Agent Desktop Client PC	<ul style="list-style-type: none"> • Run CAD Configuration Setup tool to enable CTI OS security • Automatically create an unsigned certificate
Certificate PC (can be located anywhere, ideally this is located on the CTI OS server)	<ul style="list-style-type: none"> • Runs program to create the certificate of authority (CA) • Runs program to sign a client unsigned certificate using the CA

Steps to Perform on Each Element

CTI OS Server

The first task is to enable security on each CTI OS server via the CTI OS Setup program. To do this, refer to the Cisco document, *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise and Hosted Edition*.

When security is enabled, SecuritySetupPackage.exe runs automatically to create two files, CtiosServerKey.pem and CtiosServerReq.pem, located at:

C:\ICM\<instance name>\CTIOS1\security

The SecuritySetupPackage.exe will ask you for a password. Enter a unique password for each CTI service to ensure strong encryption.

Cisco Desktop Administrator PC

After security is enabled on the CTI OS servers, configure the CAD system to enable security.

1. Start Cisco Desktop Administrator.

2. Select the logical contact center node, and then choose **Setup > Configure Systems** to start the CAD Configuration Setup tool.
3. In the left pane, select the CTI OS node to display the CTI OS settings in the right pane.
4. Answer **Yes** to the question, “Is the CTI OS security setting enabled?” and then click **Apply**.

This sets a flag in CAD Services LDAP to display the CTI OS window whenever the CAD Configuration Setup tool is run on a Cisco Agent Desktop PC, thereby making it possible for the SecuritySetupPackage.exe program to run automatically on that agent's PC.

It also automatically starts the SecuritySetupPackage.exe program, which is installed with every CAD desktop. However, this just creates an unnecessary certificate which can be ignored.

Cisco Agent Desktop Client PCs

After Cisco Desktop Administrator has run CAD Configuration Setup and enabled security, run the CAD Configuration Setup tool on each CAD client PC.

1. Using Windows Explorer, navigate to the C:\Program Files\Cisco\Desktop\bin folder.
2. Locate and then double-click **PostInstall.exe** to start the CAD Configuration Setup tool.
3. In the left pane, select the CTI OS node to display the CTI OS settings in the right pane.
4. Answer **Yes** to the question, “Is the CTI OS security setting enabled?” and then click **Apply**.

The SecuritySetupPackage.exe program runs and creates two files, CtiosClientkey.pem and Ctiosclientreq.pem, located at:

C:\Program Files\Cisco Systems\CTIOS Client\Security

These files are used when signing the client certificate.

The SecuritySetupPackage.exe will ask you for a password. Enter a unique password for each computer to ensure strong encryption.

Certificate PC

Two programs run on the Certificate PC (on the CAD Base Services server, at C:\Program Files\Cisco\bin\):

- CreateSelfSignedCASetupPackage.exe, which creates a certificate of authority for each client box's certificate.

- **SignCertificateSetupPackage.exe**, which signs the client box's certificate with the certificate of authority

Signing Client CTI OS Security Certificates

Follow these steps to sign a CTI OS security certificate for a client box.

1. On the Certificate PC, run **CreateSelfSignedCASetupPackage.exe**, create a CTIOS Certificate Authority password of between 8 and 30 characters when prompted, and store the resulting files in a secure location.
2. Copy the **CtiosClientKey.pem** and **CtiosClientReq.pem** files from the CAD client PC to C:\Program Files\Cisco Systems\CTIOS Client\Security on the Certificate PC, where the **CtiosRoot.pem** and **CtiosRootCert.pem** files are stored.
3. On the Certificate PC, run **SignCertificateSetupPackage.exe** in the same folder where the copied *.pem files are located, select **CTI OS Client Certificate Request** when prompted, and enter the CTI OS Certificate Authority password you created in Step 1. The program generates a file called **CtiosClient.pem** if successful, or displays an error message if not successful.
4. Copy the **CtiosClient.pem** and **CtiosRootCert.pem** files from the Certificate PC to the C:\Program Files\Cisco Systems\CTIOS Client\Security folder on the CAD client PC.
5. On the CAD client PC, delete the **CtiosClientKey.pem** file.
6. On the Certificate PC, delete the **CtiosClientReq.pem**, **CtiosClientKey.pem**, and **CtiosClient.pem** files.
7. Repeat Steps 2 through 6 for every CAD client PC in the system.

Signing the Server CTI OS Security Certificate

Follow these steps to sign a CTI OS security certificate for a server box.

1. If you haven't already done so, on the Certificate box, run **CreateSelfSignedCASetupPackage.exe**, create a CTIOS Certificate Authority password of between 8 and 30 characters when prompted, and store the resulting files in a secure location.

NOTE: Run **CreatSelfSignedCASetupPackage.exe** only once. Running it more than once can result in file corruption.

2. Copy the **CtiosServerKey.pem** and **CtiosServerReq.pem** files from the CTI OS server (C:\ICM\<instance name>\CTIOS1\security) to the folder on the Certificate PC where the **CtiosRoot.pem** and **CtiosRootCert.pem** files are stored.

3. On the Certificate PC, run **SignCertificateSetupPackage.exe** in the same folder where the copied *.pem files are located, select **CTI OS Server Certificate Request** when prompted, and enter the CTI OS Certificate Authority password you created in Step 1. The program generates a file called **CtiosServer.pem** if successful, or displays an error message if not successful.
4. Copy the **CtiosServer.pem** and **CtiosRootCert.pem** files from the Certificate PC to the **C:\ICM\<instance name>\CTIOS1\security** folder on the CTI OS server.
5. On the CTI OS server, delete the **CtiosServerKey.pem** file.
6. On the Certificate PC, delete the **CtiosServerReq.pem**, **CtiosServerKey.pem**, and **CtiosServer.pem** files.

Signing a Peer CTI OS Server Security Certificate

If there is more than one CTI OS server in the system, only one CTI OS server uses the server security certificate. Any peer CTI OS servers use client security certificates.

To sign a peer CTI OS server security certificate, follow the procedure for signing a CAD client security certificate.

Repairing CAD

If one of the CAD client or server applications is not functioning properly, you can use the Repair function to reinstall it. If you do repair a CAD application, you must also repair any service release that has been installed.

NOTE: If you repair any of the desktop applications and you do not have Administrator privileges on the client machine, any custom configuration settings (logging and debug levels and file locations) for that application will be lost. If you do have Administrator privileges, those configuration settings will be preserved.

To repair a CAD client or server application:

1. In Windows Control Panel, start the Add or Remove Programs tool.
2. In the list of currently installed programs, locate the CAD application you want to repair.
3. Click the **Click here for support information** link to display the Support Info dialog box.
4. Click Repair. The program will be reinstalled.
5. Repeat Steps 2 through 4 on the CAD service release, if one has been installed.

Removal

3

Removing CAD 7.2

It is recommended that you remove CAD applications in this order:

1. Supervisor Desktop or Agent Desktop
2. Desktop Administrator
3. CAD Services

NOTE: If you intend to reinstall CAD after uninstalling it, after you remove the CAD services, you must also remove Microsoft SQL Server Desktop Engine (CADSQL). If you do not do this, the reinstallation will be corrupted.

To remove a CAD application:

1. Open the Windows Control Panel.
2. Double-click **Add/Remove Programs**.
3. From the list, select the application you wish to remove and click **Remove**.

The application is removed.

NOTE: During the uninstallation process, the Microsoft installer may display a message telling you that you should shut down an application that is running. You can shut down the specified application, or ignore the message and continue with the uninstallation.

Using Multiple NICs with the VoIP Monitor Service



Overview

The VoIP Monitor Service sniffs RTP traffic from the network and sends it to registered clients. This requires support from the switch to which the service is connected.

The VoIP Monitor Service must be connected to the destination port of a configured SPAN/RSPAN. Any traffic that crosses the SPAN/RSPAN source ports is copied to the SPAN/RSPAN destination port and consequently is seen by the VoIP Monitor Service.

Not all Catalyst switches allow the VoIP Monitor Service to use the SPAN port for both receiving and sending traffic. There are switches that do not allow normal network traffic on a SPAN destination port. A solution to this problem is to use two NICs in the machine running the VoIP Monitor Service:

- One NIC for sniffing the RTP streams, connected to the SPAN port
- One NIC for sending/receiving normal traffic, such as requests from clients and sniffed RTP streams, connected to a normal switch port not monitored by the above-mentioned SPAN port.

Limitations

Since Cisco Unified Communications Manager (Unified CM) does not support two NICs, using multiple NICs works only in configurations where Unified CM is not co-resident with the VoIP Monitor Service.

SplkPCap 3.0, the packet sniffing library, works only with NICs that are bound to TCP/IP. Make sure the sniffing card is bound to TCP/IP.

Issues

The VoIP Monitor Service does not specify which NIC should be used when sending out packets. This is not a problem when using a single NIC for both sniffing and normal traffic. With two NICs, however, normal traffic should be restricted so that it

does not go through the NIC used for sniffing. Otherwise, the sniffed RTP streams of a currently-monitored call might not reach the supervisor because the SPAN destination port does not allow outgoing traffic.

To resolve this, use the route command to customize the static routing table so that normal traffic does not go through the sniffing NIC. Contact your network administrator for details.

An alternative solution is to give the sniffing NIC an IP address that no other host on the network uses, and a subnet mask of "255.255.255.0". Leave the default gateway field blank for this NIC's TCP/IP binding.

Installing a Second NIC on a VoIP Monitor Service Computer

This procedure applies only to computers running Windows 2000.

1. Install the second NIC in the computer.
2. Start the computer.
3. Make sure that neither adapter is using dynamic host configuration protocol (DHCP) to get its IP address.
4. Give the adapters valid IP addresses.
5. Determine which of the two adapters is to be used for sniffing.
6. Connect the sniffing adapter with the switch SPAN port.
7. Connect the second adapter with a normal switch port that is not monitored by the SPAN port.
8. Use the route command to customize the local routing table so that normal traffic does not go through the sniffing adapter.
9. Verify that the sniffing adapter is not registered with DNS and WINS by using the PING <local hostname> command. This ensures that the local name always resolves to the normal traffic card IP address.
10. Using Windows Explorer, navigate to the C:\Program Files\Cisco\Desktop\bin folder and double-click **PostInstall.exe** to start CAD Configuration Setup.
11. Select the VoIP Monitor Service window, and then choose the IP address of the NIC you just installed from the drop-down list.
12. Click **Apply** to save your changes and then exit CAD Configuration Setup.