



Cisco CAD Installation Guide

CAD 6.2(1) for Cisco Unified Contact Center Express Release 4.5(1)
24-Feb-06

Corporate Headquarters

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



CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, 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. (0502R)

Cisco CAD Installation Guide

Copyright © 2002–2005 Cisco Systems, Inc. All rights reserved.

Revision History

Revision Date	Description
24-Feb-06	First Customer Ship (FCS)
3-Mar-06	Added link to CRS Compatibility Guide in System Requirements
31-May-06	Updated desktop monitoring requirements Added a note to System Configuration section
16-Aug-06	Removed list of supported IP phones and substituted a reference to the CRS Compatibility Matrix

Revision History

Contents

1	Before You Install CAD	
■	Overview	1
	Related Documentation	1
	Obtaining Documentation	1
	Documentation Feedback	2
	Cisco Product Security Overview	3
	Obtaining Technical Assistance	4
	Obtaining Additional Publications and Information	6
■	CAD Versions	8
■	CAD Elements	9
	Desktop Administrator	9
	Cisco Agent Desktop	9
	Cisco Supervisor Desktop	10
	Services	10
■	System Configuration	12
■	System Requirements	13
	System Environment	13
	Data Configuration Environment	13
	Operating Environment	13
	Software Environment	14
	Supported IP Phones	15
	Desktop Monitoring Requirements	15
	Server Monitoring Requirements	17
	Recording Requirements	18
	Setting Up Agents in CRS	19
■	System Capacity	20
■	Saving Recordings From an Earlier Version	21

2	Installation	
■	Overview	23
■	Installing Cisco Agent Desktop	24
	Before You Install	24

Contents

Upgrading From an Earlier Version	24
Installation Procedure	24
■ Installing Cisco Supervisor Desktop	26
Overview	26
Before You Install	26
Upgrading From an Earlier Version	26
Installation Procedure	26
■ Installing Cisco Desktop Administrator	28
Overview	28
Before You Install	28
Upgrading From an Earlier Version	28
Installation Procedure	28
■ CAD Configuration Setup	30
Window Navigation	31
Configuration Setup Windows	31
■ Changing CRS Cluster IP Addresses	36
■ Configuring IP Phones for Cisco IP Phone Agent	37
Passwords and User Names	37
Creating an IP Phone Service	37
Assigning the IP Phone Service to IP Agent Phones	38
Creating a CallManager User	39
URL Authentication Parameter	40

3 Removal

■ Removing CAD	43
■ Manually Removing CAD Applications	44

Before You Install CAD

1

Overview

The CAD Install Manager guides you through the process of installing Cisco Agent Desktop, Cisco Supervisor Desktop, and Cisco Desktop Administrator.

Starting with the Select Options window, Install Manager allows you to select one or more packages to install, making sure that each package is installed in the correct order.

After you have successfully installed CAD into a properly-configured Cisco Unified Contact Center Express environment and licensed the applications, the basic functionality of Cisco Agent Desktop, Cisco Supervisor Desktop, and Cisco Desktop Administrator are ready to use with no further configuration required.

Related Documentation

The following documents contain additional information about CAD:

- *Cisco Desktop Administrator User Guide*
- *Cisco Agent Desktop User Guide*
- *Cisco Supervisor Desktop User Guide*
- *Cisco IP Phone Agent User Guide*
- *Cisco CAD Service Information*

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 nonemergencies.
- For Nonemergencies – psirt@cisco.com

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

- 1 877 228-7302

- 1 408 525-6532

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

Never use a revoked 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/ciscoinq/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 Versions

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

	Standard	Enhanced	Premium
Cisco Agent Desktop			
Task buttons		•	•
Event-triggered work flows		•	•
Enterprise data thresholds		•	•
Integrated browser			•
Reason codes	•	•	•
Agent-initiated chat	•	•	•
Automated recording (part of a work flow)		•	•
Cisco IP Phone Agent			
Agent-initiated recording		•	•
Caller data	•	•	•
Reason codes	•	•	•
Contact service queue stats	•	•	•
Work agent state		•	•
Cisco Supervisor Desktop			
Silent monitoring		•	•
Barge-in		•	•
Intercept		•	•
Recording (up to 32 simultaneous recordings/playbacks)		•	•
Team Performance Messages	•	•	•
CSQ statistics	•	•	•
Reports	•	•	•
Cisco Desktop Administrator			
Configure CAD interface		•	•
Configure work flows		•	•
Configure integrated browser			•
Agent work flow HTTP Post/Get Action			•

CAD Elements

CAD includes the following elements:

Desktop Administrator

Desktop Administrator provides centralized administration tools to configure the Cisco Desktop components. It supports multiple administrators, each able to configure the same data.

Desktop Administrator includes the following components:

- Enterprise Data Configuration
- Desktop Configuration
- IPCC Express Configuration
- Personnel Configuration

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

Cisco Agent Desktop

Cisco Agent Desktop is a three-pane application that helps agents manage their customer contacts. These panes are:

- Dashboard Pane—provides overall control of Cisco Agent Desktop through a toolbar and a contact appearance window.
- Contact Management Pane—displays enterprise data and call activity information for the call selected in the Dashboard pane.
- Integrated Browser—enables the agent to view web-based pages and applications.

The Chat window, accessed through a button on the toolbar, enables the agent to carry on instant messaging chat sessions with agents and supervisors on the same team. The agent can carry on multiple chat sessions at a time.

NOTE: Cisco Agent Desktop controls the telephony activities on the agent's IPCC Express phone line. It cannot coexist with other applications (for example, Cisco Attendant Console) that attempt to do the same.

See the *Cisco Agent Desktop 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. They can also silently monitor and record agent 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.

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

Services

The CAD base services include the following services: Directory Services, Enterprise, Chat, Recording & Statistics, IP Phone Agent, Sync, Licensing & Resource Manager, and LDAP Monitor services.

Chat Service

The Chat service acts as a message broker between the Chat clients and Cisco 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 marquee messages between agents (excluding IP Phone agents) and supervisors.

Directory Services

All other Cisco Desktop 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 CRS 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.

IP Phone Agent Service

The IP Phone Agent (IPPA) service enables IP phone agents to log in and out of CRS, change agent states, and enter reason codes without having the Cisco Agent Desktop software.

This service works in conjunction with the Services feature of CallManager and supported Cisco IP phones.

LDAP Monitor Service

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

Licensing & Resource Manager Service

The License & 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 & Statistics Service

The Recording & Statistics service maintains a 1-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 maintains a rolling 7-day history of recordings (unless they are saved, in which case they are saved for 30 days).

Sync Service

The Sync service connects to CRS via ACMI 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 CRS configuration.

Voice-Over IP Monitor Service

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

System Configuration

In CAD 6.2(1), the CAD services are always co-resident with the CRS engine.

NOTE: Hubs are not supported when located between switches and telephones or VoIP Monitor servers. While passive (dumb) hubs may function correctly, they have not been tested in any configuration. Intelligent (manageable) hubs and switching hubs can interfere with capturing voice packets during silent monitoring and recording. Also, hubs are not supported when used as a replacement for a SPAN port on a Catalyst switch.

NOTE: No other CTI application (such as Cisco Attendant Console) can share the same line as the agent ICD extension.

CAD can be used in a Citrix MetaFrame Presentation Server or Microsoft Terminal Services environment. For information on configuring CAD in this environment, see the document *Integrating CAD Into a Citrix MetaFrame Presentation Server or Microsoft Terminal Services Environment*.

System Requirements

The following are the minimum system requirements for running CAD.

Consult the *Cisco Customer Response Solutions (CRS) Software and Hardware Compatibility Guide* for the most recent information on compatible software and hardware. This document is located at:

www.cisco.com/univercd/cc/td/doc/product/voice/sw_ap_to/index.htm

System Environment

CAD is integrated into the following Cisco Unified Contact Center Express environment:

- Cisco Unified CallManager 5.0
- CRS 4.5(1)

Consult the *Cisco Unified CallManager Compatibility Matrix* for Cisco Unified Contact Center Express for the appropriate versions of other Cisco applications required in your contact center environment. The compatibility matrix is located at:

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

Data Configuration Environment

System configuration data is maintained using Directory Services. CAD supports OpenLDAP v2.1.29.

Operating Environment

CAD runs on the following minimum operating systems and hardware.

Table 1. CAD Minimum Operating System and Hardware Environment

Operating System	Desktop Applications	Servers
Windows 2000 Professional Service Pack 4	500 MHz processor 128 MB RAM 100 MB free space NIC supporting Ethernet 2	not supported
Windows XP Professional Edition * Service Packs 1 and 2	500 MHz processor 128 MB RAM 100 MB free space NIC supporting Ethernet 2	not supported

Table 1. CAD Minimum Operating System and Hardware Environment

Operating System	Desktop Applications	Servers
Windows 2000 Server Service Pack 4	not supported	1 GHz processor 1 GB RAM 100 MB free space [†] NIC supporting Ethernet 2
Windows 2000 Advanced Server	not supported	1 GHz processor 1 GB RAM 100 MB free space [†] NIC supporting Ethernet 2

* Windows XP Service Pack 1 includes support for Internet Protocol v6; this is not supported by CAD. In order for Cisco Agent Desktop and Cisco Supervisor Desktop to function correctly, Windows XP desktops must have the Internet Connection Firewall (ICF) disabled or configured so that the CAD services are allowed through the firewall.

† More free space is required for the Recording & Playback service database and recording files. See "[Recording Requirements](#)" for more information.

Operating Environment Language Requirements

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

Cisco Agent Desktop and Cisco Supervisor Desktop can be installed on machines running localized operating systems.

Cisco Desktop Administrator is always installed on the CRS server, which runs an English language operating system. However, in a non-English language environment, it is necessary to run a second instance of Cisco Desktop Administrator on a machine with a localized operating system so that chat messages, tooltips, enterprise data names, and other communications within the contact center are in the local language.

Software Environment

CAD requires the following software applications to run successfully:

Microsoft Internet Explorer

The CAD application installation web pages and the integrated browser in Cisco Agent Desktop require Microsoft Internet Explorer 6.0 or greater.

Apache Tomcat

Apache Tomcat is a Java-based webserver. If you are installing the IP Phone Agent application, it is needed to work with the XML pages displayed by IP phones. Tomcat is installed as part of the CRS engine installation.

More information about Tomcat can be found at <http://jakarta.apache.org>.

Microsoft SQL Server Licenses

The CAD services require two Microsoft SQL Server licenses.

Supported IP Phones

For a list of supported IP phones, see the *Cisco Customer Response Solutions (CRS) Software and Hardware Compatibility Guide*. This document is available on the web at

http://www.cisco.com/application/pdf/en/us/guest/products/ps1846/c1225/ccmigration_09186a00803d82f5.pdf

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.

Desktop Monitoring Requirements

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 CallManager Administration application.

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

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.

Desktop Monitoring and NIC Cards

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

A workaround solution is available from the Intel Technical Support website (Solution ID: CS-005897). Other solutions include:

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

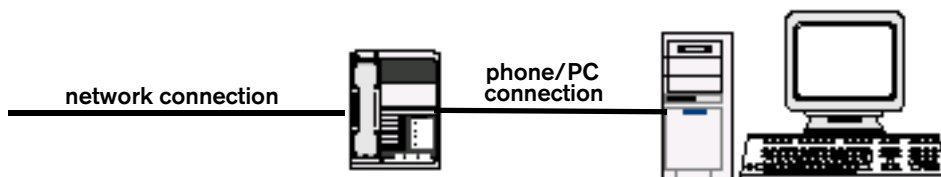
Desktop Monitoring Hardware Setup

For desktop monitoring to function, the phone is connected to the network, and the agent PC is daisy-chained to the phone (see Figure 1).

NOTE: Desktop monitoring of multiple phones daisy-chained to the agent PC is not supported.

NOTE: An agent should log into CAD using the extension of the phone daisy-chained to the agent PC for desktop monitoring to function.

Figure 1. Desktop monitoring hardware setup



Server Monitoring Requirements

The following device setting is required for server monitoring to function correctly with CAD. The setting is configured with the Cisco Unified CallManager 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.

Recording Requirements

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

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

Agent Data Store Database

The Agent Data Store database (the MSDE database associated with the Recording & Statistics service) requires 0.6 GB to store agent state and call activity records for a 7 days per week/10 hours per day contact center with 150 agents taking calls that last 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.

Table 2. Space required for recordings

Codec	Milliseconds of speech per packet	Disk space needed (KB/Call/Min)
G.711	10	1218.75
	20	1078.13
	30	1030.22
G.729	10	398.44
	20	257.81
	30	210.73
	40	187.50
	50	173.44
	60	162.43

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.

Setting Up Agents in CRS

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

System Capacity

CAD supports the following system capacities:

Maximum number of agents per site	300
Maximum number of agents per team	150
Maximum number of skills/CSQs per agent (for real-time reporting)	50
Maximum number of supervisors per site	32
Maximum number of supervisors per team	30
Average number of agents per supervisor	7.5:1
Maximum number of agents per monitor domain	300
Maximum number of simultaneous recordings/playbacks per Recording & Playback service	32

Saving Recordings From an Earlier Version

CAD archives recordings differently than it did in previous versions (as RAW files instead of WAV files). As a result, Supervisor Record Viewer is unable to display or play any recordings made by an earlier version of CAD.

The data from previous versions, including recordings, is automatically backed up and saved when the Cisco CRS Installer is run. The utility that saves the recordings creates a web page you can use to review the recording files you previously reviewed using the Supervisor Log Viewer. Like Supervisor Log Viewer, the web page gives you access to recordings made in the last seven days plus those that are marked to be saved for 30 days.

NOTE: The recordings must be located in the default location. If they are saved in another location, the utility will not be able to find them.

The utility copies files to your AudioFiles folder, including one named RecordLogView.html (see [Figure 2](#)). This web page displays the old recordings in a format similar to Supervisor Log Viewer.

Figure 2. Sample RecordLogView.html web page.

The screenshot shows a web page with a light purple background. At the top, it says "Select a Day:" followed by a row of seven buttons: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. The "Wednesday" button is highlighted. Below this, it says "Recordings for Wednesday:" followed by a table with the following data:

Agent	Team	Date	Start	Stop	File
John	Core	2004-10-08	16:10:04	16:11:30	2004100816100412101.wav
John	Core	2004-10-08	16:12:05	16:16:30	2004100816120512101.wav
John	Core	2004-10-08	17:30:21	17:35:00	2004100817302112101.wav

Installation

2

Overview

In a typical configuration, all services and Cisco Desktop Administrator are installed on the CRS server before the desktop applications are installed.

NOTE: After you install the CAD services on the CRS server, do not change the name of that server. If you do change the computer's name, various required databases and licensing will no longer function correctly. To correct this problem, change the computer's name back to the original name and functionality will be restored.

This chapter describes the procedure for installing Cisco Supervisor Desktop and Cisco Agent Desktop, and the procedure for installing a second instance of Cisco Desktop Administrator.

Installing Cisco Agent Desktop

Before You Install

Before you install Cisco Agent Desktop, you need to know:

- The IP address of the CRS server
- The user ID and password to access the CRS User Options web page (the same user ID and password used to access Cisco Agent Desktop)

NOTE: See "[System Requirements](#)" on page 13 for information on what software is required for using the CRS User Options web page.

- The destination folder on the user's PC in which you will install the application

NOTE: You should not install Cisco Agent Desktop on the CRS server. However, if you do so, ensure that Cisco Agent Desktop's LDAP registry information does not point to your production CRS server.

Upgrading From an Earlier Version

If you are upgrading Cisco Agent Desktop from an earlier version, you must first uninstall that version before installing the new version.

NOTE: If the agent has a personal employee phone book set up in the previous version, that phone book will be lost in the upgrade.

Installation Procedure

To install Cisco Agent Desktop:

1. Open your web browser and access the Cisco CRS User web page at `http://servername/appuser`.
Replace *servername* with the host name or IP address of the Cisco CRS server.
The CRS User Options Authentication window appears.
2. At the prompt, enter your username and password, and then click **Log On**.
The Welcome window appears.
3. Click **IPCC Express Downloads**.

The Download Page window appears.

4. Click the **Cisco IPCC Express Agent Desktop** hyperlink.

Install Manager starts and displays the Welcome window.

5. Click **Next**.

The Installation Server: Location dialog box appears.

6. Enter the host name or IP address and port number of the CRS User webserver, and then click **Next**.

The host name or IP address is the same one you used to access the CRS User webpage in Step 1. The port number is **6293**. This is normally autofilled, but if the field is blank, enter the number.

The Select Options dialog box appears.

7. Check the version of CAD you wish to install, and then click **Next**.

The License Agreement dialog box appears.

8. Click **Yes** to accept the End User License Agreement.

The installation quits if you do not agree to the End User License Agreement.

The Choose Destination Location dialog box appears.

9. Accept the default destination folder, or click **Browse** to navigate to another destination folder, and then click **Next**.

The Start Copying Files dialog box appears.

10. Click **Next** to start the installation.

Install Manager installs the application you chose.

When the installation is complete, the Install Results dialog box appears.

11. Click **Finish** to complete the installation process.

If the PC Has Multiple NICs

If the agent PC has more than one NIC, you must run CAD Configuration Setup after installing Cisco Agent Desktop to select the NIC that will be used to sniff voice packets. See "[CAD Configuration Setup](#)" on page 30 for the procedure for running CAD Configuration Setup.

Installing Cisco Supervisor Desktop

Overview

When you install Cisco Supervisor Desktop, Cisco Agent Desktop is automatically installed with it.

NOTE: Do not install Cisco Supervisor Desktop on the CRS server. However, if you do so, ensure that Cisco Supervisor Desktop's LDAP registry information does not point to your production CRS server.

Before You Install

Before you install Cisco Supervisor Desktop, you need to know:

- The IP address of the CRS server
- The user ID and password to access the CRS Supervision web page (the same user ID and password used to access Cisco Agent Desktop)

NOTE: See "[System Requirements](#)" on page 13 for information on what software is required for using the CRS Supervision web page.

- The destination folder on the user's PC in which you will install the application

Upgrading From an Earlier Version

If you are upgrading Cisco Supervisor Desktop from an earlier version, you must first uninstall that version before installing the new version.

Installation Procedure

To install Cisco Supervisor Desktop:

1. Open your web browser and access the Cisco Customer Response Solutions Supervision web page at `http://servername/appsupervisor`.
Replace *servername* with the host name or IP address of the Cisco CRS server.
The Customer Response Solutions Supervision Authentication window appears.
2. At the prompt, enter your username and password, and then click **Log On**.

The Download window appears.

3. Click **Cisco IPCC Express Supervisor Desktop**.

Install Manager starts and displays the Welcome window.

4. Click **Next**.

The Installation Server: Location dialog box appears.

5. Enter the host name or IP address and port number of the CRS Supervision webserver, and then click **Next**.

The host name or IP address is the same one you used to access the CRS Supervision webpage in Step 1. The port number is **6293**. This should be autofilled.

The Options dialog box appears.

6. Check the version of Cisco Supervisor Desktop you wish to install, and then click **Next**.

The License Agreement dialog box appears.

7. Click **Yes** to accept the End User License Agreement.

The installation quits if you do not agree to the End User License Agreement.

The Choose Destination Location dialog box appears.

8. Accept the default destination folder, or click **Browse** to navigate to another destination folder, and then click **Next**.

The Start Copying Files dialog box appears.

9. Click **Next** to start the installation.

Install Manager installs the application you chose.

When the installation is complete, the Install Results dialog box appears.

10. Click **Finish** to complete the installation process.

If the PC Has Multiple NICs

If the supervisor PC has more than one NIC, you must run CAD Configuration Setup after installing Cisco Supervisor Desktop to select the NIC that will be used to sniff voice packets. See "[CAD Configuration Setup](#)" on page 30 for the procedure for running CAD Configuration Setup.

Installing Cisco Desktop Administrator

Overview

Cisco Desktop Administrator and the CAD documentation are installed with the Cisco Unified Contact Center Express applications on the CRS server.

This procedure tells you how to install a second instance of Cisco Desktop Administrator.

If you are operating in a non-English language environment, and you want chat messages, tooltips, and other communications within the CAD system to be in the local language, you must install a second instance of Cisco Desktop Administrator on a machine with a local language operating system.

Before You Install

Before you install a second instance of Cisco Desktop Administrator, you need to know:

- The IP Address of the CRS server
- The user ID and password to access the CRS Administration web application (the same user ID and password used to access Cisco Agent Desktop)

NOTE: See "[System Requirements](#)" on page 13 for information on what software is required for using the CRS Administration web application.

- The destination folder on the administrator's PC in which you will install the application

Upgrading From an Earlier Version

If you are upgrading Cisco Desktop Administrator from an earlier version, you must first uninstall that version before installing the new version.

Installation Procedure

To install Cisco Desktop Administrator, follow these steps:

1. Open your web browser and access the Cisco CRS User web page at `http://servername/appadmin`.

Replace *servername* with the host name or IP address of the Cisco CRS server.

The Customer Response Solutions Administration Authentication window appears.

2. At the prompt, enter your username and password, and then click **Log On**.

The CRS initial window appears.

3. From the menu bar, select **Tools > Plug-ins**.

The Plug-ins window appears.

4. Click **Cisco Desktop Product Suite**.

The Cisco Desktop Product Suite window appears.

5. Click **Cisco Desktop Administrator**.

Install Manager starts and displays the Welcome window.

6. Click **Next**.

The Installation Server: Location dialog box appears.

7. Enter the host name or IP address and port number of the CRS User webserver, and then click **Next**.

The host name or IP address is the same one you used to access the CRS User webpage in Step 1. The port number is **6293**. This should be autofilled.

The Options dialog box appears.

8. Check the Cisco Desktop Administrator check box, and then click **Next**.

The License Agreement dialog box appears.

9. Click **Yes** to accept the End User License Agreement.

The installation quits if you do not agree to the End User License Agreement.

The Choose Destination Location dialog box appears.

10. Accept the default destination folder, or click **Browse** to navigate to another destination folder, and then click **Next**.

The Start Copying Files dialog box appears.

11. Click **Next** to start the installation.

Installation Manager installs the application you chose.

When the installation is complete, the Install Results dialog box appears.

12. Click **Finish** to complete the installation process.

CAD Configuration Setup

The CAD Configuration Setup tool is used to enter the service setup information needed for a successful CAD installation.

You can launch CAD Configuration Setup either of two ways:

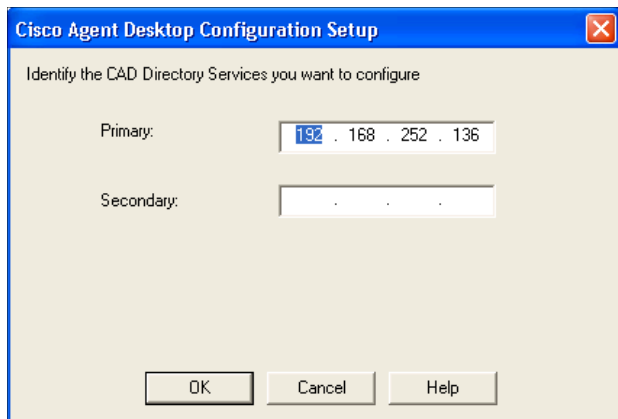
- From within Cisco Desktop Administrator
- By double-clicking PostInstall.exe, located in the ... \Program Files\Cisco\Desktop\bin folder on any machine where a CAD application has been installed

To run CAD Configuration Setup:

1. Start CAD Configuration Setup:
 - a. In Cisco Desktop Administrator, select the logical contact center from the navigation tree and then from the menu choose **Setup > Configure Systems**.
 - b. On the machine hosting the application you wish to configure, use Windows Explorer to navigate to ... \Program Files\Cisco\Desktop\bin and double-click **PostInstall.exe**.

Configuration Setup starts and displays the CAD Directory Services dialog box (see [Figure 3](#)).

Figure 3. Cisco Agent Desktop Directory Services dialog box.



2. Ensure that the correct Directory Services IP address(es) is entered, and then click **OK**.

The Cisco Agent Desktop Configuration Setup tool is displayed, with the CallManager window selected (see [Figure 4 on page 32](#)).

3. Select the window you want to modify from the left pane, enter the new data in the right pane, and then click **Apply**.
 - You can select and modify the windows in any order you wish.
 - If you modify something in a window, you must click Apply to save your changes before you move on to another window.
4. When you are done making your changes, choose **File > Exit** from the menu or click **Close**.

Configuration Setup closes.
5. Stop and restart the modified service and all desktops for the change to go into effect.

Window Navigation

You can use the following shortcut keys to navigate the CAD Configuration Setup window:

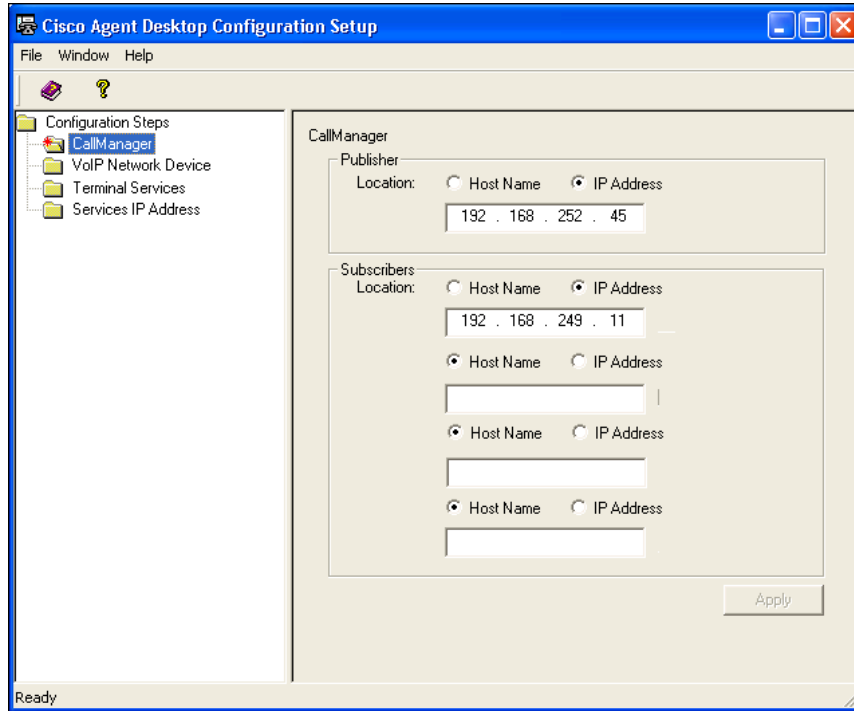
- Press F6 to switch between the left and right panes.
- In the left pane, move up and down the navigation tree with the Up and Down arrow keys.

Configuration Setup Windows

The following are the windows you might see in CAD Configuration Setup. Which windows you see depends on how your system is set up and on which computer you run CAD Configuration Setup.

CallManager Window

Figure 4. CallManager window.



NOTE: You must be running the CAD Configuration Setup tool on the PC where the CAD services are hosted in order to view this window.

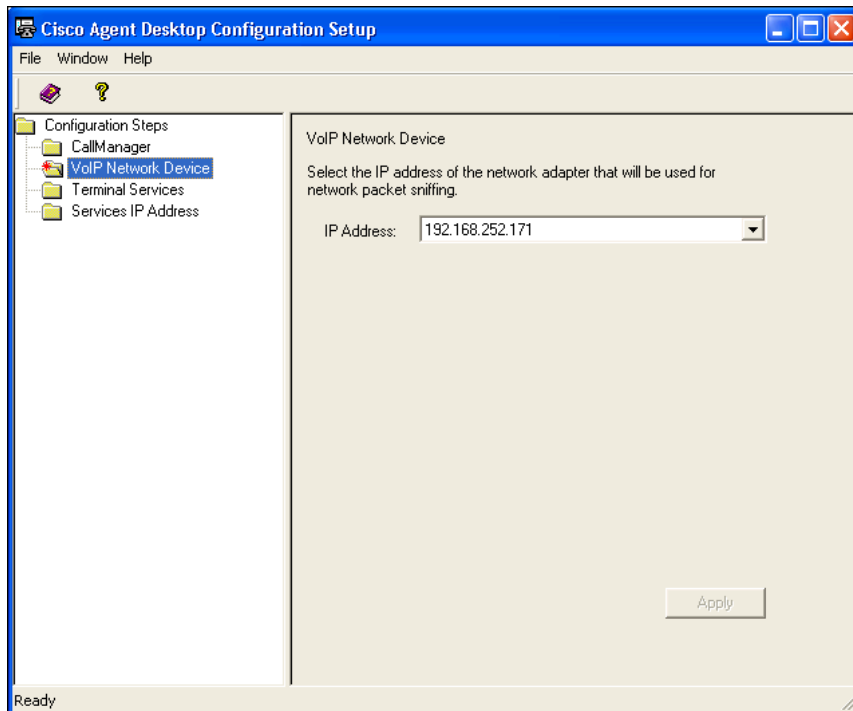
Enter the host name or IP address of your CallManager.

- If you have only one CallManager, enter the information in the Publisher section.
- If you have a CallManager cluster (a primary CallManager and one or more secondary CallManagers), enter the primary CallManager's location in the Publisher section and the location of up to four secondary CallManagers in the Subscribers section.

NOTE: If you are adding a secondary CallManager after the initial system setup, enter it in the Subscribers section and then restart the Cisco Desktop Sync service and the Cisco Desktop VoIP Monitor service using the Customer Response Solution (CRS) Administration application's Control Center (from the home page, select **System > Control Center > [host name of CRS server]**).

VoIP Network Device Window

Figure 5. VoIP Network Device window.

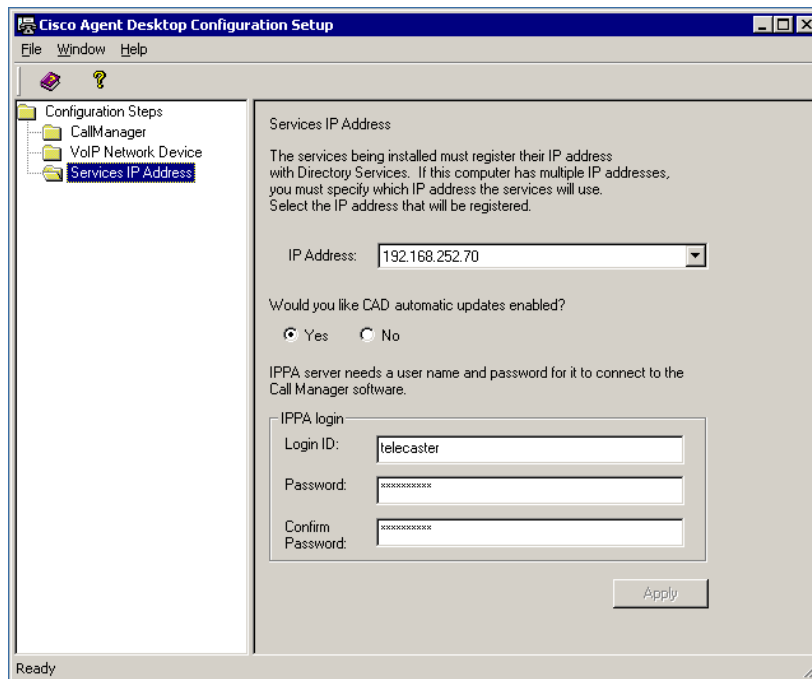


Select the IP address of the network adaptor (NIC) to which voice packets are sent to be sniffed by the VoIP Monitor service.

NOTE: You must be running the CAD Configuration Setup tool on the PC where the CAD application is hosted in order to view this window.

Services IP Address Window

Figure 6. Services IP Address window.



Enter the IP address of the machine on which the services are installed.

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 enabled network adapter card (NIC), it will have more than one IP address. To register the services correctly, select the IP address associated with the NIC being used to connect to the LAN.

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 of CAD available (for example, if the CAD services have been upgraded). If there is, it automatically runs the update process on the user's desktop.

To enable automated updates, select **Yes** (Yes is the default setting).

NOTE: Running different versions of the CAD clients and services is not supported. If you have disabled automated updates (for instance, to speed up logging in to client applications), it is recommended that you enable this feature again before upgrading the CAD services. This will ensure that service and client versions remain in sync.

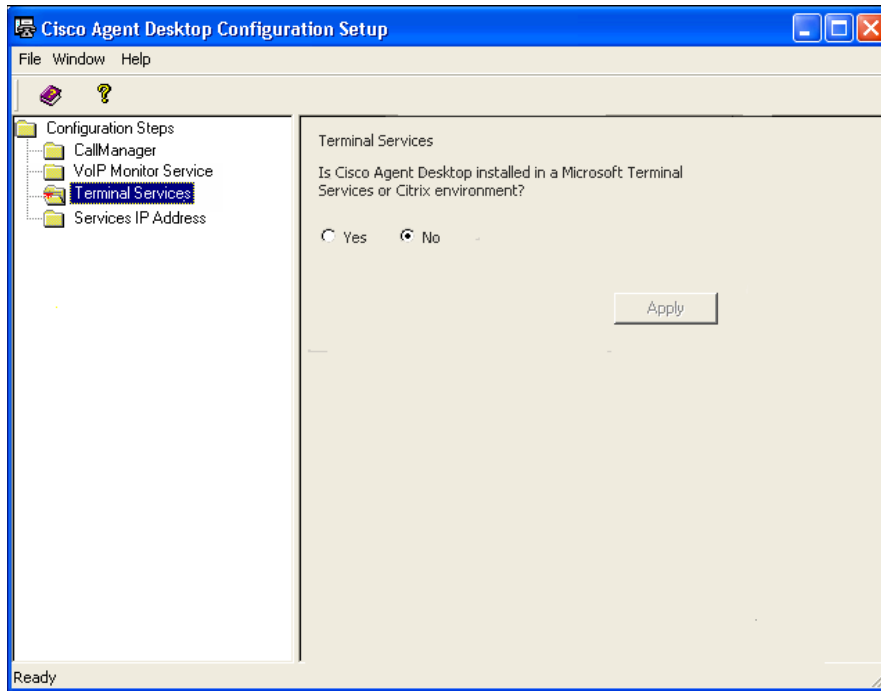
In the IPPA Login section, enter a login ID, password, and confirm the password to enter into Directory Services the CallManager user that is used by the IP Phone Agent service to push pages to agent IP phones. The password you choose can be complex if required for security by your system. The Login ID and password are case sensitive. (See "[Creating a CallManager User](#)" on page 39 for more information.)

NOTE: If you change the login ID and password of the CallManager user on this window, you must also change it in CallManager.

NOTE: When you change either the login ID or password, you must also restart the IP Phone Agent service. At that time, any logged-in IP phone agents will be logged out of the system and will have to log back in.

Terminal Services Window

Figure 7. 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 the CAD Configuration Setup tool on the PC where the Citrix/Microsoft Terminal Services service is hosted in order to view this window.

Changing CRS Cluster IP Addresses

It might become necessary to change the IP address of a server in the Cisco CRS cluster. When this happens, you must update the configuration so that the new IP address is properly registered.

To change a CRS server IP address:

1. Stop the CRS Node Managers of all nodes in the cluster.
2. Change the IP address and DNS of the CRS server.
3. On the CRS server, start the CAD Configuration Setup utility.
For instructions on running this utility, see "[CAD Configuration Setup](#)" on [page 30](#).
4. In the Service IP Address window (see [Figure 6 on page 34](#)), select the new IP address from the drop-down window and then click **Apply**.
The IOR Host Name is updated in the server's Windows registry.
5. Close the CAD Configuration Setup utility.
6. Run the Cisco CRS Serviceability Tool utility.
For information on running this utility, see the *Cisco Customer Response Solutions Administration Guide*.
7. Repeat steps 2 through 6 for any other machines that need an IP address change.
8. Reboot all the machines in the cluster.

Configuring IP Phones for Cisco IP Phone Agent

After all IP agent phones are added to the Cisco Unified CallManager, you must perform the following tasks in Cisco Unified CallManager 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.

Passwords and User Names

If you are using Active Directory 2003 on the machine hosting the CallManager, you must disable password complexity. If password complexity is enabled, “telecaster” is not a valid password because it does not contain any capital letters or numbers.

To disable password complexity:

1. On the machine using Active Directory 2003, click **Start > Administration Tools > Local Security Policy**.

The Local Security Settings window appears.

2. Choose **Account Policies > Password Policy > Password Must Meet Complexity Requirements**.

The Local Security Policy Setting dialog box appears.

3. Under Local Policy Setting, select **Disabled** and then click **OK**.

Password complexity is now disabled, and you can use the “telecaster” password.

Creating an IP Phone Service

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

If you have a redundant system, you should create two IP Phone services, one for each CRS engine server IP address.

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://192.168.252.44:6293/ipphone/jsp/sciphonexml/IPAgentInitial.jsp`

where:

- 192.168.252.44 is the IP address of the machine where the IP Phone Agent service is loaded
- 6293 is the Tomcat webserver port (if 6293 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 IPPA 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 CallManager 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 CallManager User

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

The CallManager user is used by the IP Phone Agent service to push pages to agent IP phones.

NOTE: The CallManager user ID and password are also entered in CAD Configuration Setup and must match what is configured in CallManager. If you change them in CallManager, you must also change them in CAD Configuration Setup. See "[Services IP Address Window](#)" on page 34 for more information.

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

To create the CallManager 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 CallManager 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 telecaster from the search results and then click **Add Selected**.
The window closes and the CallManager user is added to the Standard CTI Enabled group.

URL Authentication Parameter

If you are upgrading from Cisco Unified Contact Center Express 3.x, and you changed the default URL Authentication parameter in Cisco CallManager Administration, you should now change it back to the original parameter.

This parameter is located on the System > Enterprise Parameters page, in the Phone URL Parameters section. It should be:

`http://<CallManager IP address>:8080/ccmcip/authenticate.jsp`

NOTE: You must use the CallManager's IP address, not the host name, in this URL.

Removal

3

Removing CAD

Remove CAD applications in this order:

1. Cisco Supervisor Desktop
2. Cisco Agent Desktop
3. Cisco Desktop Administrator
4. Base

IMPORTANT: Always remove Base last.

To remove a CAD application:

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

The application is removed. You might be prompted to reboot your computer in order to completely remove all CAD files.

NOTE: You must reboot your computer before reinstalling any CAD applications, or remnants of the previous installation might interfere with the new installation.

Manually Removing CAD Applications

It might become necessary to manually remove CAD applications. Some reasons for this are:

- The Windows Add/Remove Programs utility does not completely remove a CAD application.
- You are unable to upgrade CAD applications due to files and settings created in a previous version.

See [“Manually Removing CAD Applications” on page 150](#) of the *Cisco CAD Service Information* manual for step-by-step instructions.