



Cisco CAD Installation Guide

IP Contact Center Enterprise and Hosted Edition Release 7.0
31-Mar-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 © 2002–2006 Cisco Systems, Inc. All rights reserved.

Revision History

| Revision Date | Description |
|---------------|---|
| 31-Mar-06 | First Customer Ship (FCS) |
| 13-Dec-06 | Adding information on rolling back installations |
| 18-Jan-07 | Added support for Internet Explorer 7 |
| 04-Apr-07 | Updated version compatibility information and added a note to the CallManager SOAP AXL Configuration Setup section. |
| | |

Revision History

Contents

| | | |
|----------|---|----|
| 1 | Before You Install CAD 7.0 | |
| ■ | Overview | 1 |
| | Obtaining Documentation | 1 |
| | Cisco.com | 1 |
| | Documentation CD-ROM | 2 |
| | Ordering Documentation | 2 |
| | Documentation Feedback | 2 |
| | Obtaining Technical Assistance | 3 |
| | Cisco TAC Website | 3 |
| | Opening a TAC Case | 3 |
| | TAC Case Priority Definitions | 3 |
| | Obtaining Additional Publications and Information | 4 |
| ■ | CAD 7.0 Feature Levels | 6 |
| ■ | What's New in This Version | 8 |
| | General | 8 |
| | Cisco Agent Desktop | 8 |
| | Cisco Supervisor Desktop | 8 |
| | Cisco Desktop Administrator | 9 |
| ■ | CAD 7.0 Components | 10 |
| | Desktop Administrator | 10 |
| | Agent Desktop | 10 |
| | Supervisor Desktop | 11 |
| | Services | 11 |
| | Chat Service | 11 |
| | Directory Services | 11 |
| | Enterprise Service | 12 |
| | IP Phone Agent Service | 12 |
| | LDAP Monitor Service | 12 |
| | Licensing & Resource Manager Service | 12 |
| | Recording & Playback Service | 12 |
| | Recording & Statistics Service | 12 |
| | Sync Service | 12 |
| | Voice-Over IP Monitor Service | 13 |

Contents

- System Configurations 14
 - Citrix and Microsoft Terminal Services Environments. 14
- System Requirements 15
 - System Environment 15
 - Data Configuration Environment. 15
 - Operating Environment 15
 - Supported IP Phones 17
 - Caveats on Using a Cisco 7920 Wireless Phone. 17
 - Software Environment 18
 - Desktop Monitoring Requirements. 18
 - Desktop Monitoring and NIC Cards 19
 - Recording Requirements. 19
 - Setting Up Agents in ICM. 20
 - Setting Up Supervisors and Teams 20
 - Skills Statistics 20
- System Capacity 22
- Registry Key Modifications 23

2 Installation

- Overview 25
- Installing CAD Services 26
- CAD Configuration Setup 29
 - Entering Configuration Data in Initial Mode. 29
 - Configuration Setup Windows 33
 - CallManager Window. 33
 - CTI Server (CallManager) Window. 34
 - CTI Server (IP IVR) Window 35
 - IP IVR Window 36
 - CTI OS Window. 37
 - CallManager SOAP AXL Access Window. 38
 - Logger Database Window. 39
 - ICM Admin Workstation Distributor Window. 40

Contents

| | |
|---|----|
| ICM Admin Workstation Database | 41 |
| Recording and Statistics Service Database Window | 42 |
| VoIP Monitor Service Window | 43 |
| Services Configuration Window | 44 |
| Directory Services Replication Window | 45 |
| Restore Backup Data Window | 46 |
| ■ Cisco Desktop Monitoring Console | 47 |
| ■ Licensing CAD 7.0 | 48 |
| Recording Licenses | 50 |
| ■ Installing Desktop Applications | 51 |
| Using Automated Package Distribution Tools | 51 |
| Cisco Desktop Administrator | 51 |
| Cisco Agent Desktop and Cisco Supervisor Desktop | 52 |
| ■ Upgrading From a Previous Version | 54 |
| Hot Fixes and Service Releases for Previous Versions | 54 |
| Upgrading from CAD 4.6 | 54 |
| Upgrading from CAD 6.0 | 55 |
| Upgrading CAD 7.0 to a Newer Version | 55 |
| Rolling Back CAD 7.0 to an Earlier CAD Version | 56 |
| Backup and Restore Utilities | 56 |
| BackupDB Utility | 56 |
| CDBRTool Utility | 57 |
| DABackupTool Utility | 58 |
| RecordingBackup (Bulk Export) Utility | 60 |
| ■ Configuring Cisco CallManager IP Phones for Cisco IP Phone Agent | 61 |
| Configuration Procedure | 61 |
| Creating an IP Phone Service | 61 |
| Assigning the IP Phone Service to IP Agent Phones | 62 |
| Creating the CallManager IPPA Authentication User | 62 |
| Changing the Default URL Authentication Parameter | 63 |
| ■ Configuring a Cisco IP Communicator Phone | 65 |
| ■ Setting Up CTI OS Security | 66 |
| Steps to Perform on Each Element | 66 |

Contents

| | |
|---|----|
| CTI OS Server | 66 |
| Cisco Desktop Administrator PC | 66 |
| Cisco Agent Desktop Client PCs | 67 |
| Certificate PC | 67 |
| Signing Client CTI OS Security Certificates | 68 |
| Signing the Server CTI OS Security Certificate | 68 |
| Signing the Server CTI OS Security Certificate on a Peer CTI OS Server | 69 |
| ■ Repairing CAD | 70 |

3

Removal

| | |
|--------------------------|----|
| ■ Removing CAD 7.0 | 71 |
|--------------------------|----|

A

Using Multiple NICs with the VoIP Monitor Service

| | |
|--|----|
| Overview | 73 |
| Limitations | 73 |
| Issues | 74 |
| Installing a Second NIC on a VoIP Monitor Service Computer . . . | 74 |
| Required Registry Changes | 74 |
| Second NIC is Present Before IPCC Enterprise/Hosted Installation | 75 |
| Second NIC is Installed After IPCC Enterprise/Hosted Installation | 75 |

B

Testing Ethernet Cards for Silent Monitoring

| | |
|---|----|
| Overview | 77 |
| Test Procedure | 78 |
| Preparing the Test Target | 78 |
| Preparing the Packet Generator Host | 80 |

Contents

Executing the Test80

Contents

Before You Install CAD 7.0

1

Overview

CAD 7.0 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

After you have successfully installed CAD into a properly-configured IPCC Enterprise or IPCC Hosted environment, run the CAD Configuration Setup tool, and licensed the applications, the basic functionality of Agent Desktop and Supervisor Desktop are ready to use with no further configuration required.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain the most current technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

www.cisco.com

International Cisco websites can be accessed from this URL:

www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
www.cisco.com/en/US/partner/ordering/index.shtml
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click Feedback at the top of the page.

You can send your comments in e-mail to bug-doc@cisco.com.

You can submit comments 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (www.cisco.com/tac) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

The online TAC Case Open Tool (www.cisco.com/tac/caseopen) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

www.cisco.com/warp/public/687/Directory/DirTAC.shtml

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

- Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.
- Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.
- Priority 4 (P4)—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 Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
www.cisco.com/en/US/products/products_catalog_links_launch.html
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:
www.ciscopress.com
- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:
www.cisco.com/go/packet
- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

www.cisco.com/go/iqmagazine

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

www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

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

CAD 7.0 Feature Levels

There are three feature levels of CAD 7.0: 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.

Table 1.

| | Standard | Enhanced | Premium |
|---------------------------------|----------|----------|---------|
| Cisco Agent Desktop | | | |
| Task buttons | | • | • |
| Event-triggered work flows | | • | • |
| Enterprise data thresholds | • | • | • |
| Wrapup data | • | • | • |
| Reason codes | • | • | • |
| Integrated browser | | | • |
| Agent-initiated chat | • | • | • |
| Agent-initiated call recording | | • | • |
| Cisco Outbound Option | | • | • |
| Cisco IP Communicator 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) | • | • | • |

Table 1.

| | Standard | Enhanced | Premium |
|--|----------|----------|---------|
| Supervisor work flows—tree control node actions only | | • | • |
| Supervisor work flows—all actions | | | • |
| Skill statistics | • | • | • |
| Real-time displays (text) | • | • | • |
| Real-time displays (charts) | | | • |
| Cisco Desktop Administrator | | | |
| Configure CAD interface | | • | • |
| Configure work flows | | • | • |
| Configure embedded browser | | | • |
| Agent work flow HTTP Post/Get action | | | • |

What's New in This Version

CAD 7.0 includes these new features.

General

- Cisco IP Phone Agent is now offered as a standalone application in the standard, enhanced, and premium bundles.
- Desktop applications can be installed without the logged-in user having to have Administrator privileges on that computer (if enabled by the Administrator).
- Serviceability enhancements have been made to improve the performance of logging for diagnostic purposes.
- Installation enhancements have been made to support automatic upgrades of the desktop applications.
- CAD is now supported in a Citrix/Microsoft Terminal Services environment.

Cisco Agent Desktop

- Agents can now log in using their user name or their user ID, depending how the system administrator configures the system.
- An agent can chat with supervisors and agents on his or her team and receive team messages (TMs) even when logged out of the ACD as long as Cisco Agent Desktop is not closed.
- Cisco IP Communicator has replaced Media Termination as the supported soft phone.
- Enterprise data and call activity data is available on both inbound and outbound calls.
- Work flows can be applied to Cisco Outbound Option calling campaigns.
- Cisco Outbound Option functions are now controlled by a dedicated Outbound Option toolbar.
- A password is required whenever agents log in after logging out of (but not closing) Cisco Agent Desktop.
- Agents can dial a hyperlinked phone number from a web page displayed in the embedded browser just by clicking the hyperlink.

Cisco Supervisor Desktop

- Cisco Supervisor Desktop's interface can be configured using dockable panes and the supervisor's choice of real-time displays in graphical and tabular format.

- Supervisors can create Supervisor Work Flows for threshold alerts.
- Supervisors can re-skill their agents dynamically via a link to the web-based Cisco IPCC Agent Re-skilling Tool.
- IP phone agents are treated the same as desktop agents, with equal visibility and control by supervisors.
- Supervisors can push a web page to a monitored desktop agent.
- Enterprise data and call history are available for both inbound and outbound calls.
- A supervisor's last 10 team messages are saved for reuse.

Cisco Desktop Administrator

- Work flows are now divided into Voice Contact Work Flows and Agent Management Work Flows.
- The Time of Day event has been added to Agent Management Work Flows.
- The Agent Notification, Timer, and IPC actions have been added to work flows.
- Work flows now fully support Cisco Outbound Option calls.
- Reason codes can be defined and enabled separately for the Not Ready and Logout states.
- Large or small icons can be configured for the Cisco Agent Desktop toolbar.
- Cisco Outbound Option now has its own toolbar, the appearance of which depends on the dialing mode selected for the calling campaign.
- The administrator can monitor CAD services via the new Cisco Desktop Monitoring Console.

CAD 7.0 Components

CAD 7.0 is a suite of applications and services consisting of 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 (although not at the same time; only one person can work in one node at any one time).

Desktop Administrator includes:

Enterprise Data Configuration

Enterprise Data Configuration is used to:

- Define the fields for displaying the data collected by ICM or VRU (voice response unit) and stored in the Enterprise service.
- Assign MAC addresses to be monitored by specific Voice-Over IP Monitor servers within the contact center, by desktop monitoring, or by a default VoIP Monitor server.

Desktop Configuration

Desktop Configuration defines the look and feel of the agent's desktop and work flows. With it you control the configuration of:

- Dial Strings: format how dial strings are displayed
- Phone Book: create and enable global phone books
- Reason Codes: create and enable reason codes
- Work Flow Groups: configure work flows and wrap-up data

IPCC Configuration

IPCC Configuration enables you to use the IPCC component administrative applications, such as the Cisco CallManager Administration web-based application. You can also add a hyperlink to any web-based tool or application you wish.

Personnel Configuration

Personnel Configuration enables you to view the attributes for the contact center's resources as defined in ICM. You can view the attributes for agents, supervisors, and teams.

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

Agent Desktop

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

- **Dashboard.** The Dashboard provides overall control of Agent Desktop through a toolbar and a contact appearance window. The toolbar enables the agent to set the agent state, perform call control functions, make calls, initiate chat sessions with other agents, execute actions set up by the system administrator, view/hide the Contact Management and Integrated Browser panes, and access online help.
- **Contact Management.** The Contact Management pane displays enterprise data and call activity information for the call selected in the Dashboard.
- **Integrated Browser.** The Integrated Browser pane enables the agent to view web-based pages and applications. It hosts a version of Internet Explorer.

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.

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

Supervisor Desktop

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 log viewer, supervisors can play back and save recorded agent calls.

Services

The CAD 7.0 services are listed below.

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 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.

IP Phone Agent Service

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

This service works in conjunction with the Services feature of CallManager and model 7940, 7960, and 7970 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 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 logger 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 ICM configuration.

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.

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.

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

System Configurations

Supported system configurations are documented in the *Cisco IP Contact Center Enterprise Edition 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 Environment* for details.

System Requirements

The following are the minimum system requirements for running CAD 7.0.

System Environment

CAD 7.0 is integrated into the following IPCC Enterprise and IPCC Hosted environments:

| CAD Version | CallManager Version | ICM Version |
|-------------|---------------------|-------------|
| 7.0(0) | 4.0, 4.1 | 7.0(0) |
| 7.0(1) | 4.0, 4.1, 4.2, 5.0 | 7.0(1) |
| 7.0(2) | 4.0, 4.1, 4.2, 5.0 | 7.0(2) |

Consult the following documents for the most current compatibility information:

Cisco 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

Data Configuration Environment

System configuration data is maintained using Directory Services. CAD 7.0 supports OpenLDAP v2.2.

Operating Environment

CAD 7.0 runs on the following operating systems and hardware.

NOTE: The CAD services must be installed on machines running an English language operating system. The CAD desktop applications may be installed on machines running localized operating systems.

Table 2. Supported operating systems and hardware

| Operating System | Desktop Applications | Services |
|---|---|---|
| Windows 2000 Professional Service Pack 4 | <p>Minimum 500 MHz processor 128 MB RAM 100 MB free space NIC supporting Ethernet 2 800 × 600 screen resolution</p> <p>Recommended 1 GHz processor 256 MB RAM 200 MB free space NIC supporting Ethernet 2 800 × 600 screen resolution</p> | not supported |
| Windows XP Professional Edition Service Packs 1 and 2 | <p>Minimum 500 MHz processor 128 MB RAM 100 MB free space NIC supporting Ethernet 2 800 × 600 screen resolution</p> <p>Recommended 1 GHz processor 256 MB RAM 200 MB free space NIC supporting Ethernet 2 800 × 600 screen resolution</p> | not supported |
| Windows 2000 Server Service Pack 4 | not supported | <p>Up to 100 agents 1.4 GHz processor 1 GB RAM 500 MB free space* NIC supporting Ethernet 2</p> <p>Over 100 agents 1.4 GHz dual processor 2 GB RAM 500 MB free space* NIC supporting Ethernet 2</p> |

Table 2. Supported operating systems and hardware – *Continued*

| Operating System | Desktop Applications | Services |
|--|----------------------|---|
| Windows 2000 Advanced Server, Service Pack 4 | not supported | <p>Up to 100 agents 1.4 GHz processor 1 GB RAM 500 MB free space* NIC supporting Ethernet 2</p> <p>Over 100 agents 1.4 GHz dual processor 2 GB RAM 500 MB free space* NIC supporting Ethernet 2</p> |
| Windows 2003 Server, Standard and Enterprise Edition, Service Pack 1 | not supported | <p>Up to 100 agents 1.4 GHz processor 1 GB RAM 500 MB free space* NIC supporting Ethernet 2</p> <p>Over 100 agents 1.4 GHz dual processor 2 GB RAM 500 MB free space* NIC supporting Ethernet 2</p> |

* More free space is required for the Recording & Playback service recording files. See "[Recording Requirements](#)" on page 19 for more information.

Supported IP Phones

Cisco Agent Desktop supports the following IP phones:

- Cisco IP Phone 7902 series, 7905 series, 7910 series, 7912 series, 7920 series, 7940 series, 7960 series, and 7970 series
- Cisco IP Communicator Soft Phone

Cisco IP Phone Agent supports the Cisco IP Phone 7920, 7940, 7960, and 7970 series.

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.

Software Environment

CAD 7.0 requires the following software applications to run successfully:

Microsoft Internet Explorer 6 and 7

Internet Explorer is required for the Integrated Browser portion of Cisco Agent Desktop and for the web page produced when the Bulk Export Utility is run (see "[RecordingBackup \(Bulk Export\) Utility](#)" on page 60).

Adobe Acrobat Reader

The CAD documentation is distributed in Acrobat PDF format. The Adobe Acrobat Reader is available for free from www.adobe.com.

Tomcat v4

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. More information about Tomcat may be found at <http://jakarta.apache.org>. Tomcat is shipped with CAD 7.0 and is automatically installed if the installation program does not detect an existing, current version on the PC.

Java Runtime Environment (JRE)

JRE is required to run the Java applets and JavaServer Pages (JSP) used by the IP Phone Agent application. JRE is shipped with CAD 7.0 and is automatically installed if the installation program does not detect an existing, current version on the PC.

Computer Telephony Integration Object Server (CTI OS)

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 "[Registry Key Modifications](#)" on page 23 for information on changing these registry keys.

Microsoft SQL Server 2000 Desktop Engine

Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) is the free, redistributable version of SQL Server used as an embedded database.

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.

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. For a procedure for testing if a NIC card is fully NDIS-compliant, see www.cisco.com/en/US/customer/products/sw/custcosw/ps427/prod_tech_notes_list.html).
- Monitoring agents via a VoIP Monitor service.

Recording Requirements

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 & Statistics service depend on the size of the contact center. In general, requirements are as follows:

Recording & Statistics Service

The Recording & 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 |

| Protocol | Packet Size (msec) | Recording Size (KB/call/minute) |
|----------|--------------------|---------------------------------|
| 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.

Setting Up Agents in ICM

Setting Up Supervisors and Teams

For CAD 7.0 applications to work properly, your agents must be organized into teams and some must be designated as supervisors. This is accomplished in ICM. See your 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 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 ICM Configuration Manager documentation for more information on setting up skill groups and queues.

System Capacity

CAD 7.0 supports the following system capacities:

Table 3.

| | |
|--|------|
| Maximum number of agents per site | 1000 |
| Maximum number of IP phone agents per server | 500 |
| Maximum number of agents per team* | 100 |
| Maximum number of skills per agent (for real-time reporting)* | 52 |
| Maximum number of supervisors per site | 80 |
| Maximum number of supervisors per team | 20 |
| Average number of agents per supervisor | 10 |
| Maximum number of agents per monitor domain | 400 |
| Maximum number of simultaneous recordings per Recording & Playback service | 80 |
| Maximum number of simultaneous playbacks per Recording & Playback service | 8 |

* May be limited based on CTI OS server capacity.

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.

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.

A registry key on the CTI OS computer may be modified so that more call data is displayed for incoming calls. If you make this modification, the Calling# and Called# data will be displayed for incoming calls when they are ringing. If you do not make this modification, this data is available to the agent only after the call is answered.

To modify the CTI OS registry key:

1. On the CTI OS computer, open the Windows Registry Editor.
2. Navigate to the following key:
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Ctios\<CTI OS Instance Name>\<CTI OS Server Name>\Server\CallObject
3. Under the CallObject key, select the key **MinimizeEventArgs** and change the value from **1** to **0**.
4. Close the Windows Registry Editor.
5. Recycle CTI OS so the changes go into effect.

Installation

2

Overview

Install the CAD 7.0 applications in this order:

1. CAD Services
2. Cisco Desktop Administrator
3. Cisco Supervisor Desktop and Cisco Agent Desktop

NOTE: When you install Cisco Supervisor Desktop, Cisco Agent Desktop is automatically installed with it. Do not install Cisco Agent Desktop and then attempt to install Cisco Supervisor Desktop on the same machine.

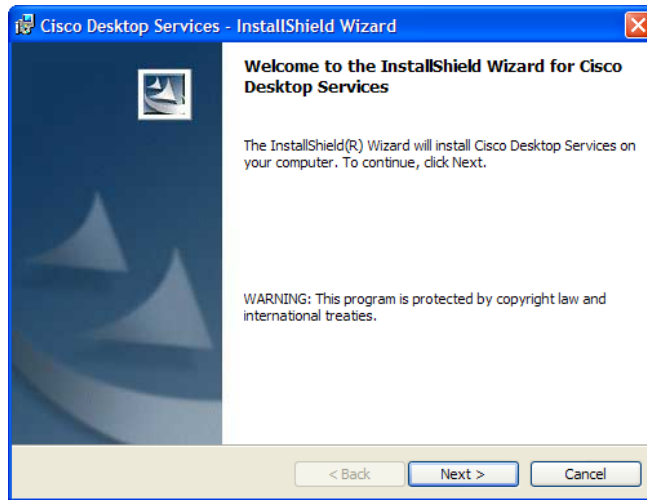
Installing CAD Services

The CAD Services installation is run from the product CD.

To install the CAD services:

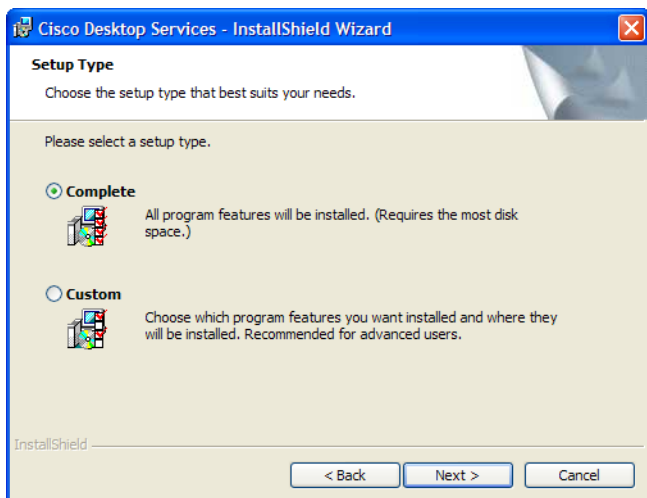
1. Navigate to the CD in My Computer or Windows Explorer and double-click the file **setup.exe** to start the InstallShield Wizard Welcome window (see [Figure 1](#)).

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



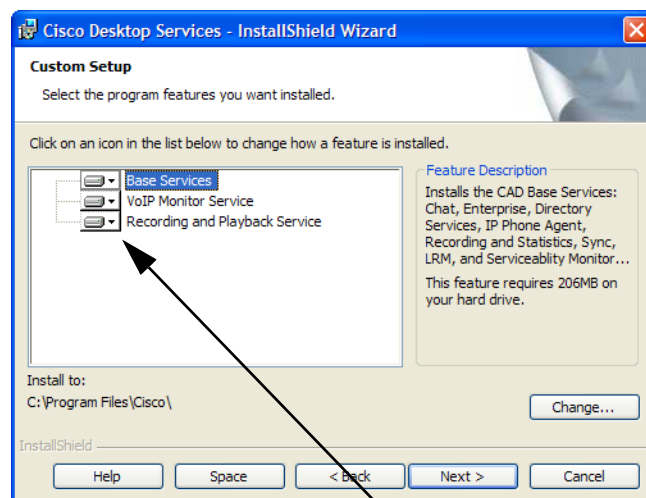
2. Click **Next** to display the Setup window (see [Figure 2](#)).

Figure 2. Setup window.






3. Select the setup type you want:
 - Complete—the Base services, VoIP Monitor service, and Recording & Playback service will be installed on this computer.
 - Custom—choose which services you want installed on this computer. For example, you use this to install an off-board VoIP Monitor service or Recording & Playback service. By default, all services are selected. Click the down arrow next to any service you don't want installed and select "This feature will not be available" to remove it from the installation list (see [Figure 3](#)).

Figure 3. Custom Setup window.

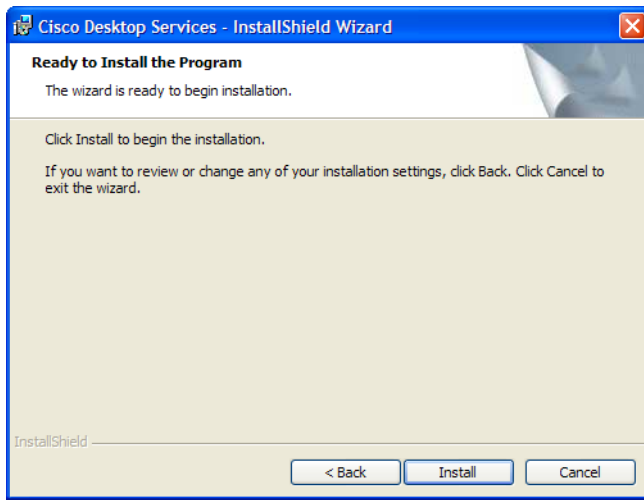


Click the down arrow next to the feature to add or remove it from the list of features to be installed.

-  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.

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

Figure 4. Ready to Install the Program window.



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

NOTE: If Cisco Security Agent is running on the server computer, you will see messages that the installation program stops it temporarily and then starts it again after the installation is complete.

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

6. When the installation is completed, the CAD Configuration Setup tool starts. See "[CAD Configuration Setup](#)" on page 29 for instructions on configuring your system using this tool.

CAD Configuration Setup

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

CAD Configuration Setup is launched automatically after you install the CAD services in Initial Mode. Any time you launch the Configuration Setup tool after this, it is launched in Update Mode.

In Initial Mode, you must complete all windows in sequence. If you do not complete a window, you cannot go forward to the next window. You can go backwards and revise a window you already completed.

Once you have completed all the windows, the Save button on the toolbar is enabled. You must click Save in order to correctly configure your CAD services. If you do not click Save, but opt to cancel the configuration setup process, the next time you start the tool you will have to repeat the configuration process and complete all windows.

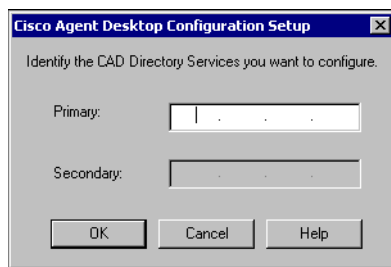
Entering Configuration Data in Initial Mode

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

To enter configuration data in Initial Mode on the primary Directory Services computer:

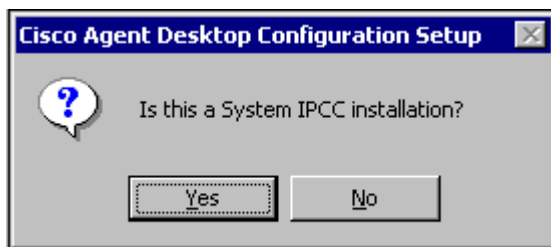
1. Configuration Setup starts automatically and displays the CAD Directory Services dialog box (see [Figure 5](#)).

Figure 5. CAD Directory Services dialog box.



2. Enter the IP address of the primary Directory Services and then click **OK**. The System IPCC dialog box appears (see [Figure 6](#)).

Figure 6. System IPCC dialog box.



3. Identify if this is a System IPCC installation.
 - If you answer **Yes**, then default peripheral IDs are automatically 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 remain at the default 5000 and agents and supervisors can log in by login name or login ID, as configured in Cisco Desktop Administrator.

The Configuration Setup tool appears, with the CallManager node selected (see [Figure 10](#)).

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 itself automatically.

NOTE: The save process may take several minutes.

To enter configuration data in Initial Mode on the secondary Directory 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 asking you if you want to set up Directory Services replication appears (see [Figure 7](#)).

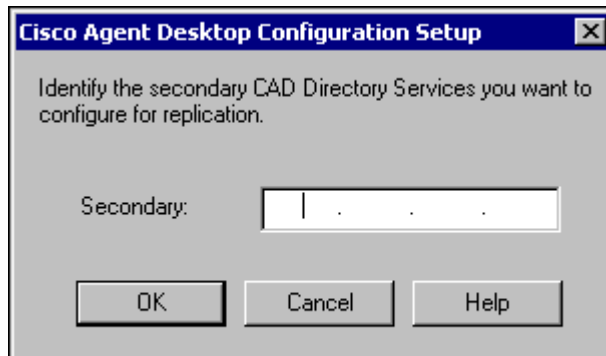
Figure 7. Directory Services Replication question dialog box.



3. Click **Yes**.

The Secondary Directory Services dialog box appears (see [Figure 8](#)).

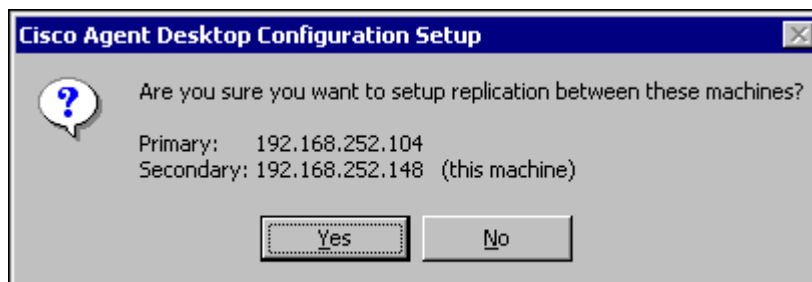
Figure 8. Secondary Directory Services dialog box.



4. Enter the IP address of the secondary Directory Services, and then click **OK**.

A confirmation dialog box appears (see [Figure 9](#)).

Figure 9. Confirmation dialog box



5. Click **Yes** to set up replication.

When replication is done, the Configuration Setup tool appears, with the CallManager node selected (see [Figure 10](#)).

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 itself automatically.

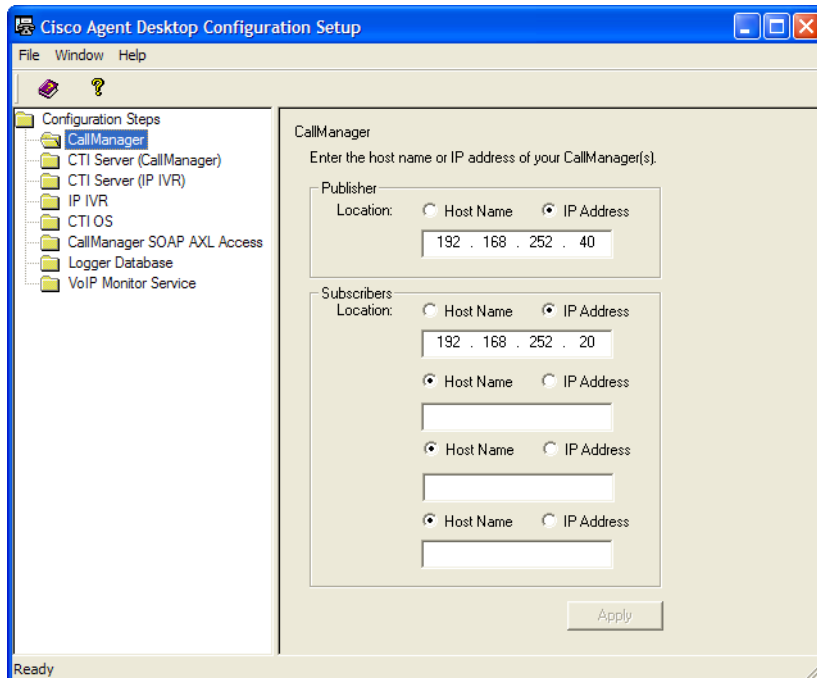
NOTE: The save process may take several minutes.

Configuration Setup Windows

The following are the windows you may see in the CAD Configuration Setup application. Which windows you see depends on how your system is set up.

CallManager Window

Figure 10. CallManager window.

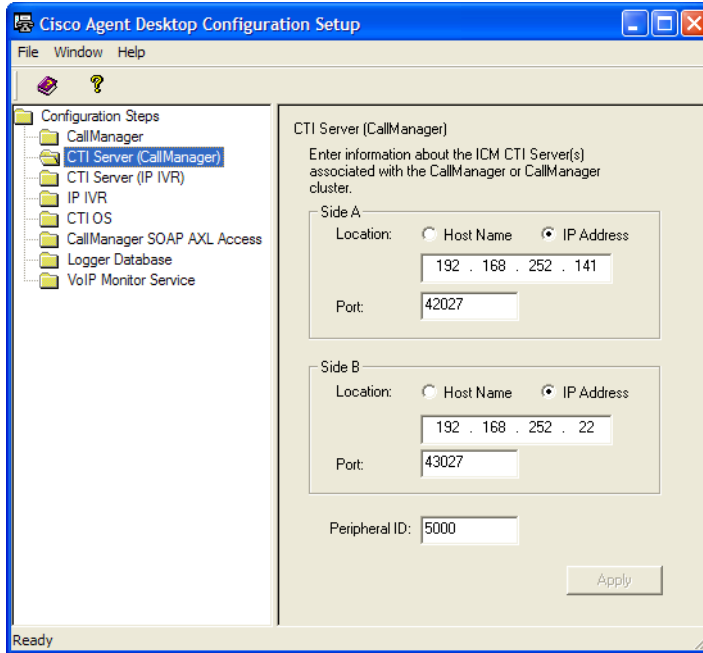


Enter the host name or IP address of your CallManager.

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

CTI Server (CallManager) Window

Figure 11. CTI Server (CallManager) window.

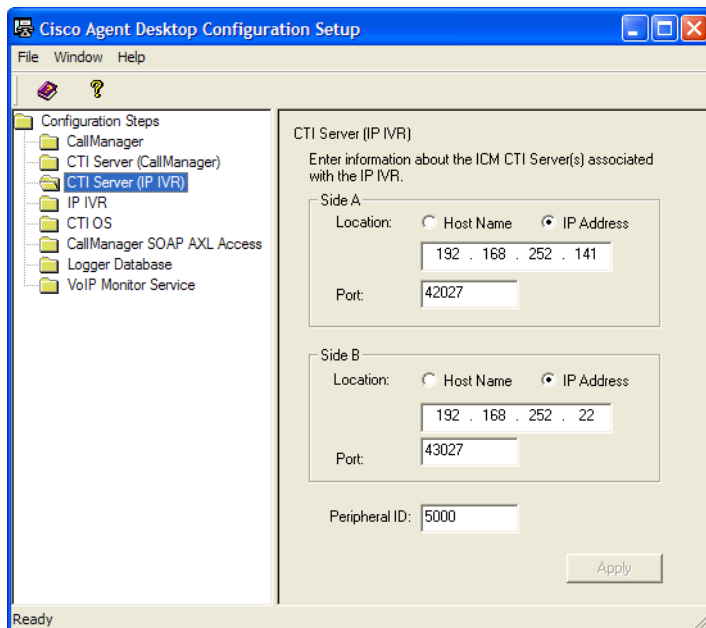


Enter the host name or IP address, port number, and peripheral ID of the ICM CTI Server associated with the CallManager or CallManager cluster.

- 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.

CTI Server (IP IVR) Window

Figure 12. CTI Server (IP IVR) window.



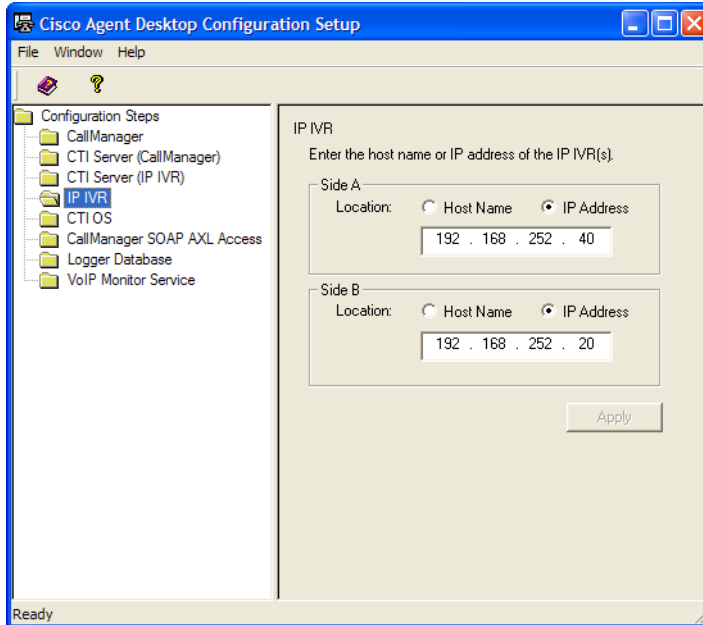
NOTE: This window is autofilled with the information from the CTI (CallManager) window. In most cases it will not be necessary to change anything. However, if you have a system that has multiple CTI servers, you may have to update the information entered here.

Enter the host name or IP address, port number, and peripheral ID of the ICM CTI server associated with IP IVR. It may be the same ICM CTI server that is associated with the CallManager, or it may be a separate service.

- 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.

IP IVR Window

Figure 13. IP IVR window.

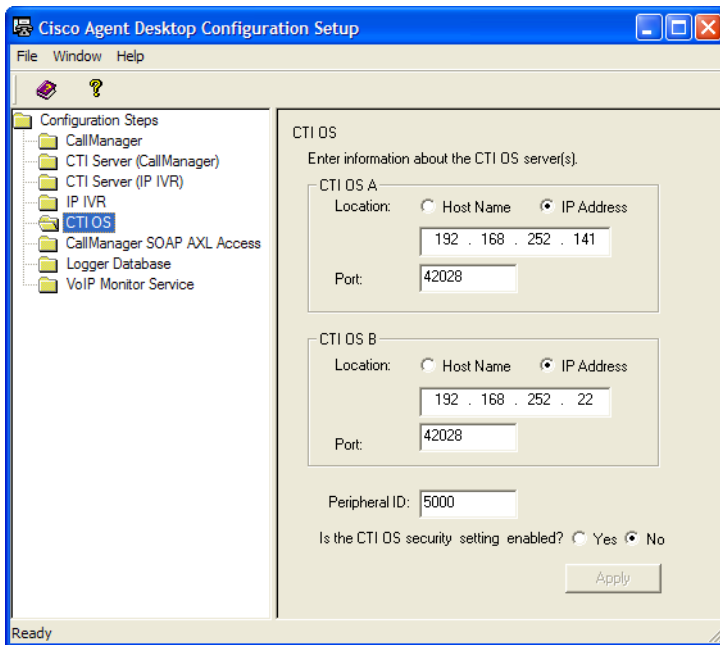


Enter the host name or IP address of the IP IVR.

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

CTI OS Window

Figure 14. CTI OS window.



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

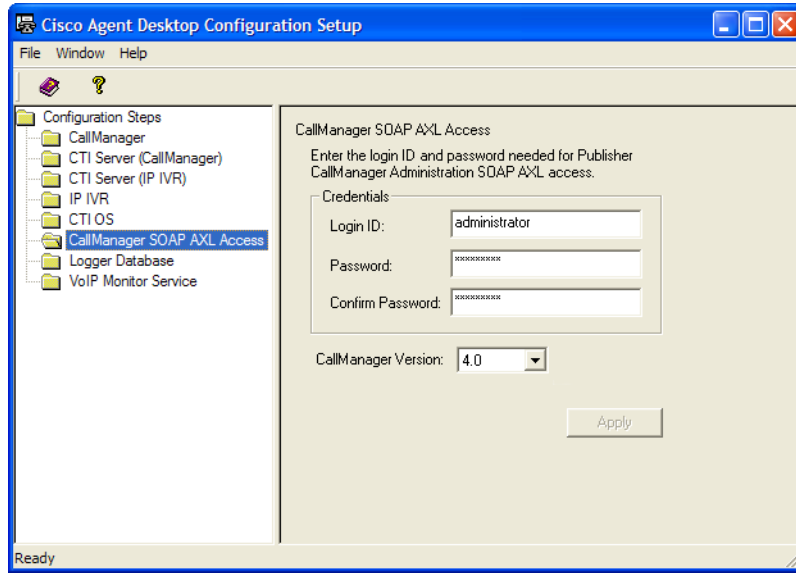
- If you have only one CTI OS, enter the information in the CTI OS A section.
- If you are also using a redundant CTI OS in a duplexed environment, enter the location of the redundant CTI OS in the CTI OS B section.
- The peripheral ID is used by services to filter information such as agents and skills. You can find the peripheral ID by using PG Explorer in the ICM Configuration Manager.

Check **Yes** or **No** to indicate if the CTI OS security setting is enabled.

If you choose Yes, ensure that CTI OS security is enabled on the CTI OS server, and then follow the procedures for enabling security on each agent desktop (see "[Setting Up CTI OS Security](#)" on page 66).

CallManager SOAP AXL Access Window

Figure 15. CallManager SOAP AXL Access window.

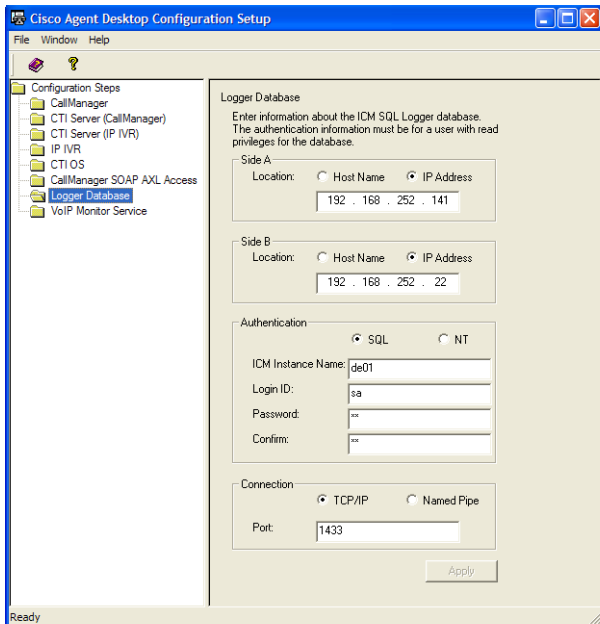


Enter the login ID and password required for the Publisher CallManager Administration to access SOAP AXL (Simple Object Access Protocol Administrative XML Layer), and select the CallManager version.

NOTE: If you are using CallManager 4.2, you must select 4.1 from the CallManager Version drop-down list.

Logger Database Window

Figure 16. Logger Database window.



Enter the host name or IP address of the ICM SQL Logger database.

- If you have only one ICM SQL Logger database, enter the information in the Side A section.
- If you are also using a redundant Logger database in a duplexed environment, enter the location of the redundant Logger database in the Side B section.

Select if the database is SQL or NT.

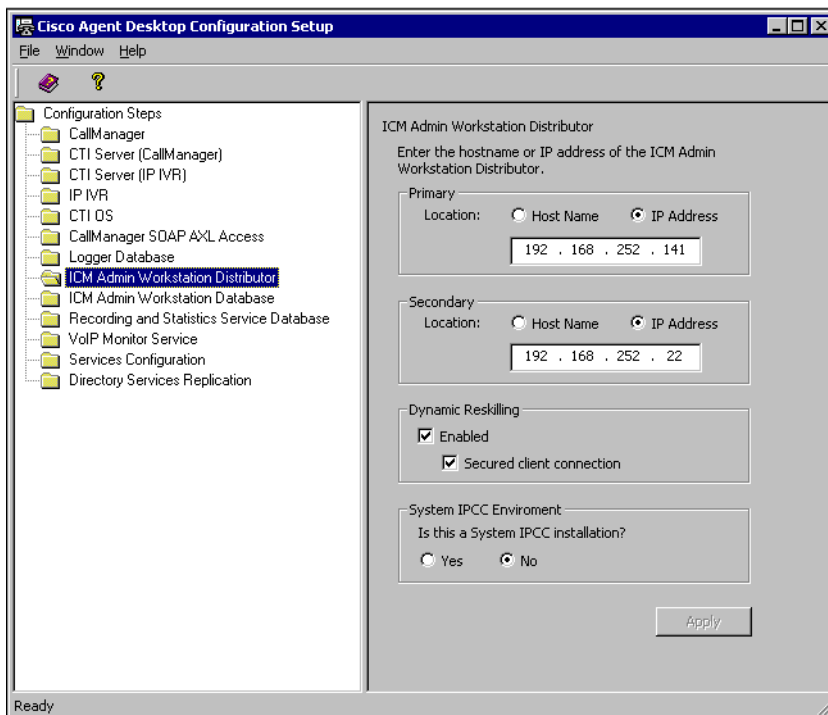
- If you select SQL, enter the ICM instance name, login ID, and password of a user who has read privileges for the ICM Logger database.
- If you select NT, enter the ICM instance name, login ID, and password of a user who can log into the ICM Logger computer and who has read privileges for the ICM Logger database. The login ID is of the format <domain>\<username> or .\<username>.

Enter the type of connection, TCP/IP or Named Pipes.

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

ICM Admin Workstation Distributor Window

Figure 17. ICM Admin Workstation Distributor window.



Enter the host name or IP address of the ICM Admin Workstation (AW) Distributor.

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

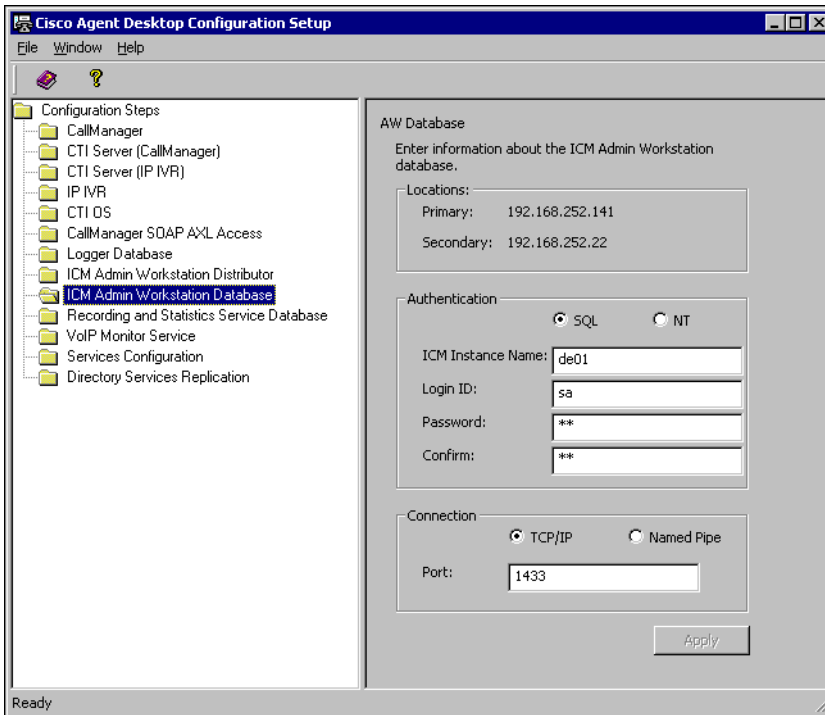
To enable supervisors to dynamically re-skill agents on their teams using the Cisco IPCC Agent Re-skilling Tool, check the **Enabled** check box in the Dynamic Re-skilling section. This tool is a web-based application. If it is located on a secured server and requires an https URL, check the **Secured client connection** check box. If you leave this box unchecked, the URL will use the http prefix.

In the System IPCC Environment section, select **Yes** or **No** to indicate whether or not your configuration is running in a System IPCC environment.

NOTE: This section is enabled only in update mode. When CAD Configuration Setup runs in initial mode, this question is asked in a popup dialog box.

ICM Admin Workstation Database

Figure 18. ICM Admin Workstation Database window.



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

Select if the database is SQL or NT.

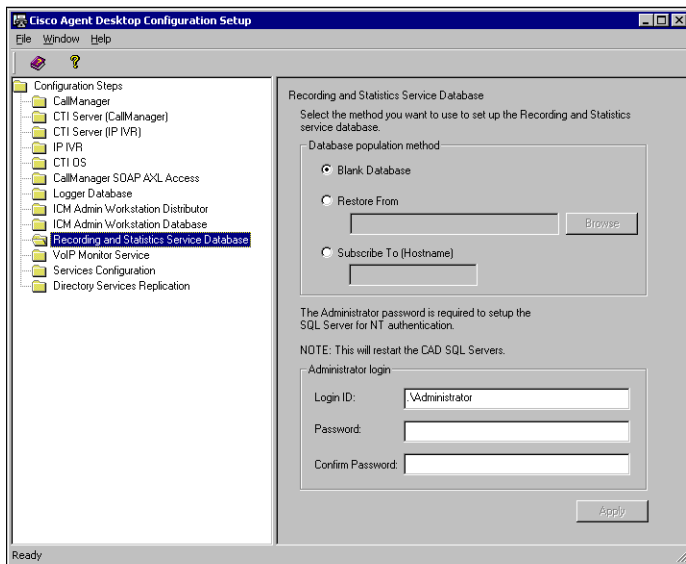
- If you select SQL, enter the ICM instance name, login ID, and password of a user who has read privileges for the Admin Workstation database.
- If you select NT, enter the ICM instance name, login ID, and password of a user who can log into the ICM Admin Workstation computer and who has read privileges for the ICM Admin Workstation database. The login ID is of the format <domain>\<username> or .\<username>.

Enter the type of connection, TCP/IP or Named Pipes.

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

Recording and Statistics Service Database Window

Figure 19. Recording and Statistics Service Database window.



In the Database population method section, select the method you want to use to set up the Recording & 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 & Statistics service schema.
- Select **Restore From** if you are restoring a previously backed-up database, and then use the Browse button to navigate to the location of the database backup file.
- Select **Subscribe To (Hostname)** when installing a secondary Recording & Statistics service in a replicated environment. You must enter the host name (not the IP address) of the location of the primary service. This option creates the Recording & Statistics service schema and creates a replication relationship between the secondary and primary services.

NOTE: Make sure that Cisco Security Agent is stopped on both the primary and secondary Recording & Statistics servers if you select Subscribe To (Hostname).

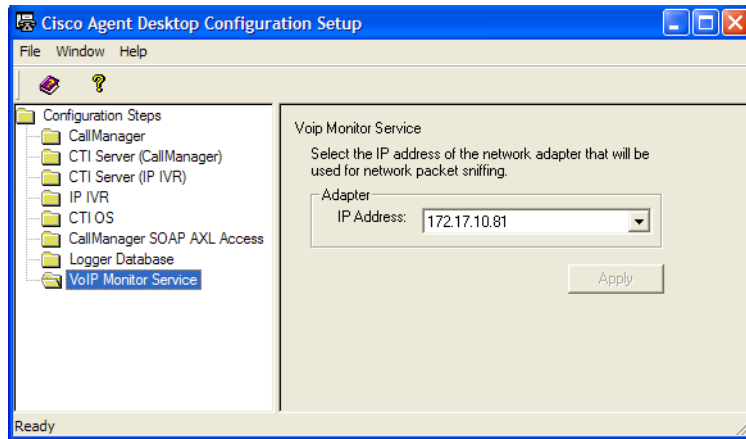
In order for the Recording & Statistics service to replicate databases, NT authentication must be used. In the Administrator login section, enter the Login ID and password of a user with NT authentication for both machines.

NOTE: Whenever you modify anything on this window, you must enter the Administrator Login ID and password. This account can be any account that belongs to the Administrators group.

NOTE: If you are installing on a Windows 2003 Server machine, the Administrator account cannot have a blank password. The server has the security option “Accounts: Limit local account use of blank passwords to console only” enabled by default. Create a password or disable this option.

VoIP Monitor Service Window

Figure 20. VoIP Monitor Service window.

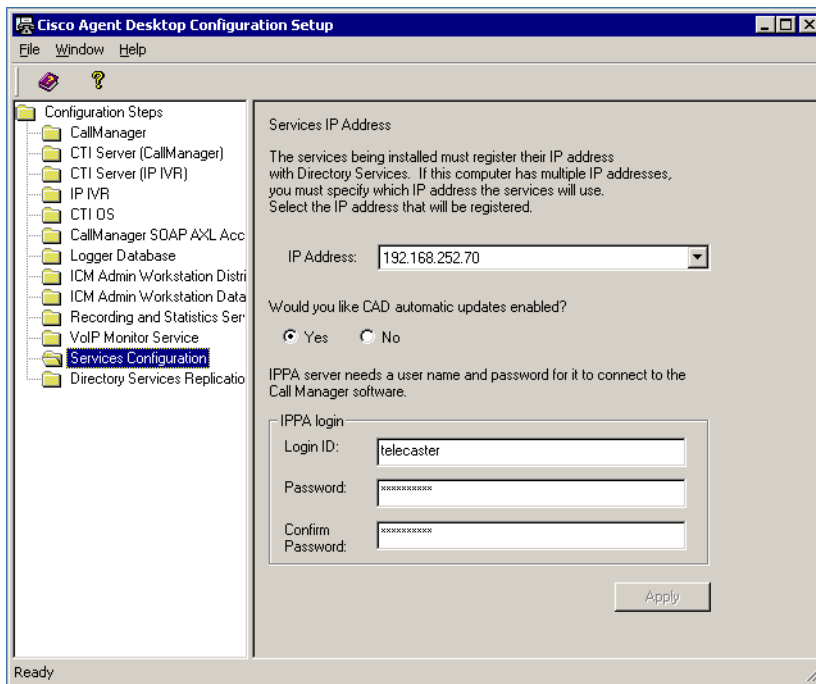


Select the IP address of the network adaptor to which voice packets are sent to be sniffed by the VoIP Monitor service (if this is a server box) or the desktop monitor (if this is an agent desktop).

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

Services Configuration Window

Figure 21. Services Configuration window.



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

Services must register their IP address with LDAP 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.

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

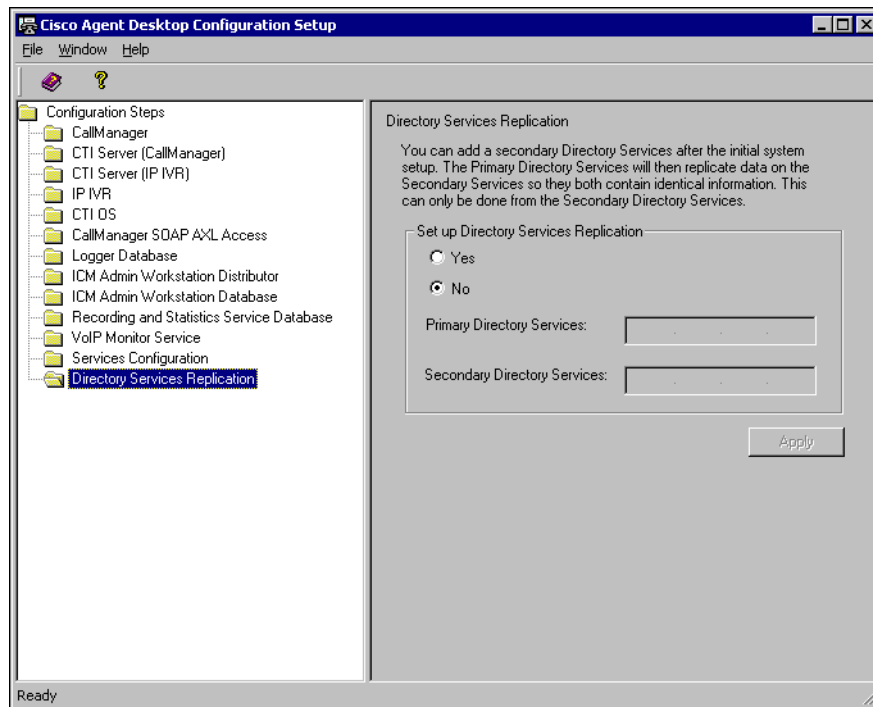
If you enable automated CAD updates, every time a user starts Agent Desktop, Supervisor Desktop, or Desktop Administrator the system checks if there is a newer version available. If there is, it automatically runs the update process.

In the IPPA Login section, enter a login ID, password, and confirm the password to enter into LDAP 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, and they must be identical to what is entered in CallManager.

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

Directory Services Replication Window

Figure 22. Directory Services Replication window.



This window is displayed when you run CAD Configuration Setup in Update mode.

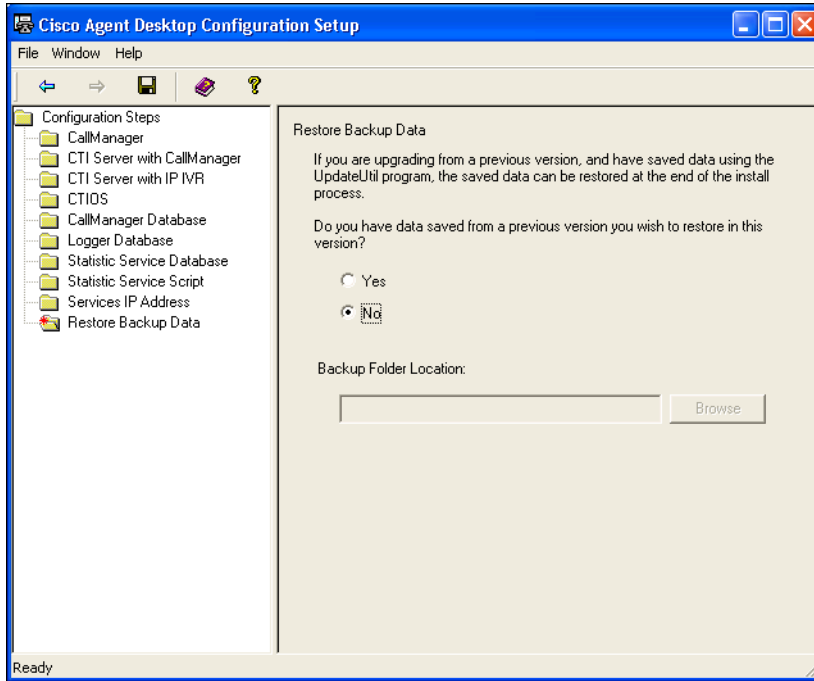
Use the Directory Services Replication window to add a secondary Directory Services service after the initial system setup. The primary Directory Services will then replicate data on the secondary Directory Services so that they both contain identical information.

Click **Yes** if you want to set up replication, and then enter the IP address of the primary and secondary Directory Services.

NOTE: Make sure that Cisco Security Agent is stopped on both the primary and secondary Directory Services servers if you opt to set up replication.

Restore Backup Data Window

Figure 23. The Restore Backup Data window.



NOTE: This window appears only in Initial Mode.

If you want to restore data saved by using the DABackupTool.exe utility or the CDBRTTool.exe utility, click **Yes**.

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 view a list of the running services.
7. Select **SNMP Service** from the list of services, right-click, and select **Properties**.
8. In the SNMP Service Properties window, select the Security tab.
 - In the Accepted community names pane, verify that Public with READ-ONLY rights is displayed.
 - Select the **Accept SNMP packets from any host** option.
9. Click **Apply** to save your changes, and then **OK** to close the window.

Licensing CAD 7.0

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 the CAD software will run.

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**.

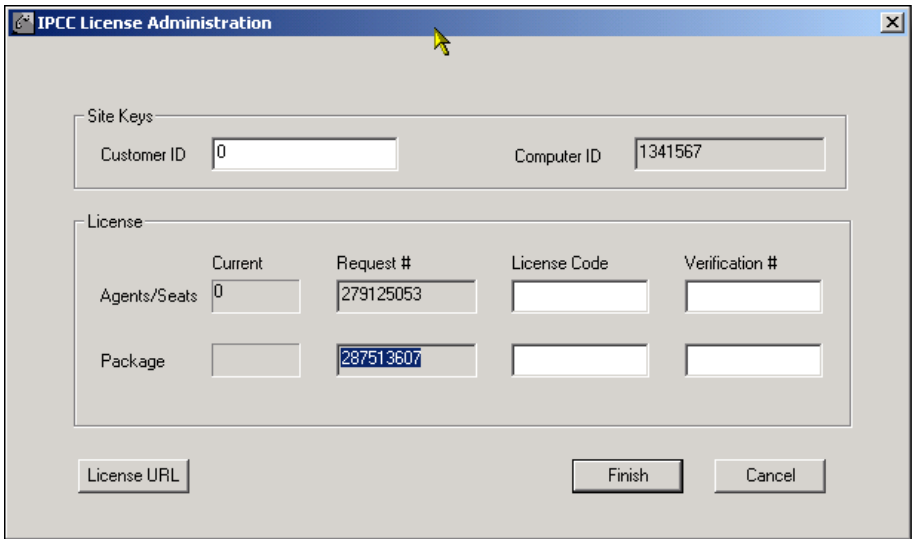
To start IPCC License Administration:

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 24](#).)

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

Figure 24. IPCC License Administration window.



To license CAD 7.0:

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 25](#).)

Figure 25. Web page showing returned license codes and verification numbers.

| 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:1 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:

- an agent or supervisor will not be able to record a call
- a supervisor will be able to open Supervisor Record Viewer, but no recordings will be listed in the application and an error message will be 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.

NOTE: You cannot install any of the desktop applications on a server.

If you want users with limited privileges to their computer to be able to install a desktop application (for example, an agent installing his or her own instance of 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, the installation process changes the user privilege to administrator level during the installation and restores it to the lower level at the end of the installation.

Using Automated Package Distribution Tools

Cisco Agent Desktop and Cisco Supervisor Desktop can be installed or upgraded on multiple desktops ("pushed") through the use of an automated package distribution tool. Consult the distribution tool's documentation for information on how to do this.

Cisco Desktop Administrator

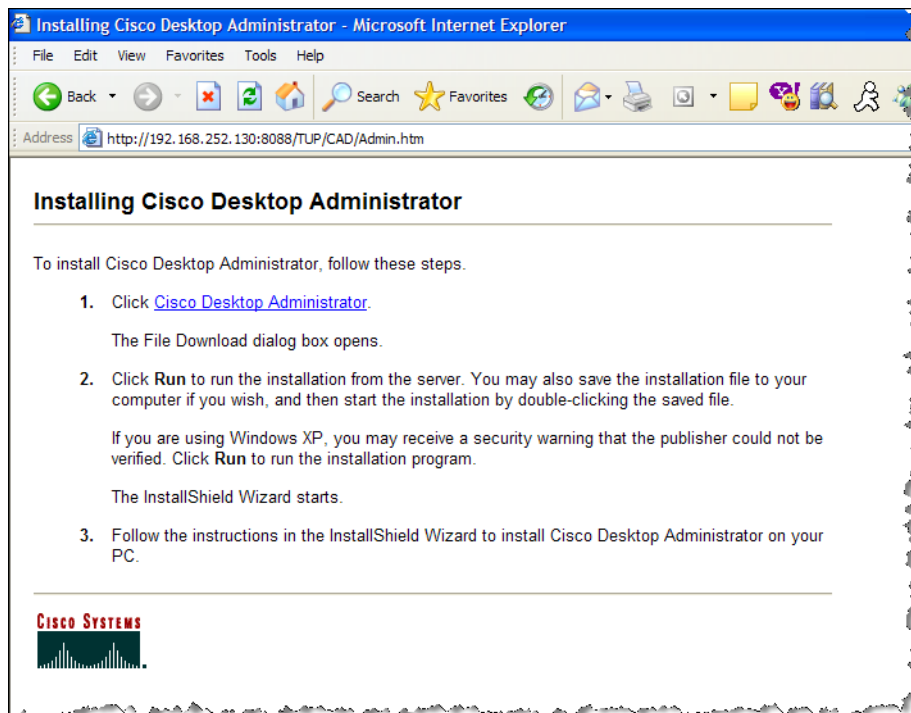
To install Desktop Administrator:

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 26. Cisco Desktop Administrator Installation web page



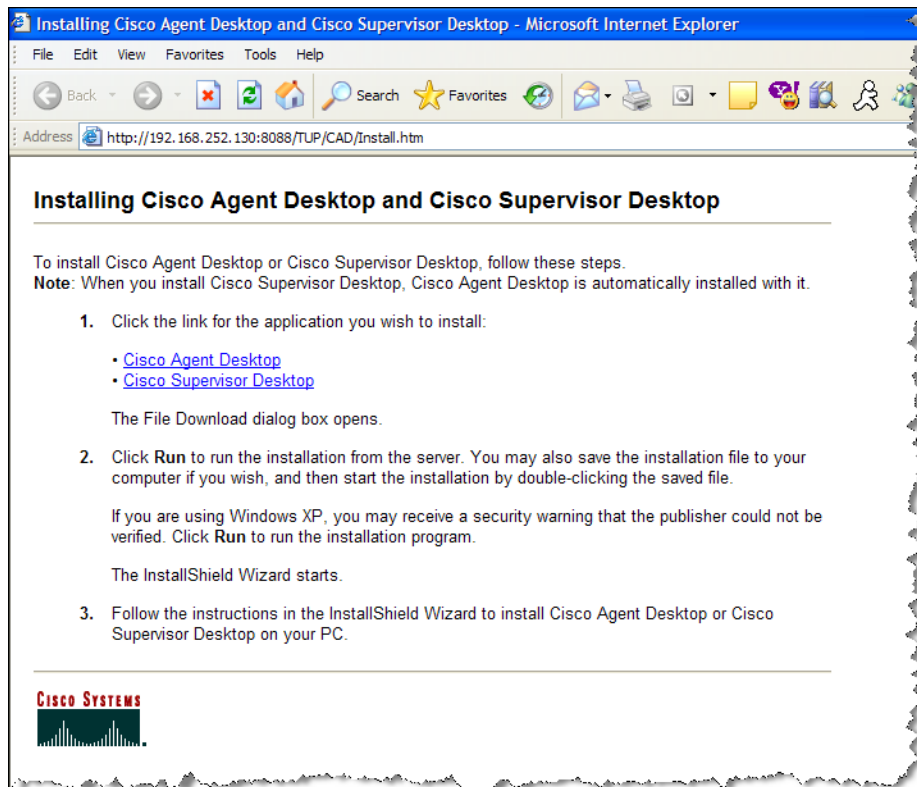
Follow the instructions on the web page to install the application.

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 Installation web page appears (see [Figure 27](#)).

Figure 27. Cisco Agent Desktop and Cisco Supervisor Desktop installation web page



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

NOTE: 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.

NOTE: Do not install Agent Desktop and then attempt to install Supervisor Desktop on the same machine, or errors may result. To install Supervisor Desktop on a machine where Agent Desktop has already been installed, you must first uninstall Agent Desktop.

Upgrading From a Previous Version

Previous versions of CAD must be uninstalled before installing CAD 7.0. You can back up your configuration data before uninstalling the old version with various utilities provided on the installation CD, and then restore the data to CAD 7.0 during the installation process.

You can upgrade CAD 7.0 to a newer version of CAD 7.0 by installing the newer version over the older version. In this situation, it is not necessary to back up and restore your configuration data. That is done automatically during the upgrade.

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

The backup and restore utilities used in the following upgrade procedures are described in detail in the section ["Backup and Restore Utilities" on page 56](#).

Hot Fixes and Service Releases for Previous Versions

If you have any CAD hot fixes or service releases for previous versions installed, uninstall them before upgrading to CAD 7.0. They 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]

Upgrading from CAD 4.6

Follow these steps to upgrade CAD 4.6 to CAD 7.0.

1. Run the following utilities to back up CAD 4.6 data:
 - DABackupTool to back up configuration data
 - BackupDB to back up the Recording & Statistics database
 - RecordingBackup to save recording metadata and recordings and make them available through a web page

NOTE: You must obtain the most recent version of DABackupTool from the Cisco Software Center Downloads page for Cisco Agent Desktop. The version on your CAD 4.6 installation CD is no longer valid.

2. Uninstall CAD 4.6.
3. Install CAD 7.0.

The backed-up data is restored through the CAD Configuration Setup tool:

- The configuration files backed up with DABackupTool are restored by entering the location of the backup file in the Restore Backup Data window.
- The Recording & Statistics database backed up with BackupDB is restored by selecting “Restore From” and entering the location of the backup file in the Recording & Statistics Service Database window.

Upgrading from CAD 6.0

Follow these steps to upgrade CAD 6.0 to CAD 7.0.

1. Run the following utilities to back up CAD 6.0 data:
 - CFBRTool to back up configuration data and recordings. You must run this utility twice: once to back up the configuration data, and once to back up recordings. Save each backup to a different location.
 - BackupDB to back up the Recording & Statistics database.
2. Uninstall CAD 6.0.
3. Install CAD 7.0.

The backed-up data is restored through the CAD Configuration Setup tool:

- The configuration data backed up with CDBRTool is restored by entering the location of the backup file in the Restore Backup Data window.
 - The Recording & Statistics database backed up with BackupDB is restored by selecting “Restore From” and entering the location of the backup file in the Recording & Statistics Service Database window.
4. Run CDBRTool and restore the recordings you backed up in Step 1.

Upgrading CAD 7.0 to a Newer Version

CAD 7.0 can be upgraded to a newer version of CAD 7.0 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: If you repair your current version or upgrade to a newer version of any of the desktop applications, and if 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.

Rolling Back CAD 7.0 to an Earlier CAD Version

If you need to uninstall CAD 7.0 and revert to an earlier version of CAD, follow these steps.

NOTE: It is assumed that you backed up your original version of CAD before installing CAD 7.0.

1. Uninstall CAD 7.0.
2. Install your previous CAD version according to the product documentation.
3. 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 & Statistics database backed up with BackupDB is restored by selecting "Restore From" and entering the location of the backup file in the Recording & Statistics Service Database window.

Backup and Restore Utilities

This section describes how to use the CAD backup and restore utilities.

BackupDB Utility

To preserve the Recording & Statistics service database, use the BackupDB utility. This utility saves the information in the database except recording metadata and the recordings themselves. Recording metadata is the information saved about a recording—time and date of recording, the agent recorded, and so on.

The Recordings themselves are preserved using the Bulk Export utility—see ["RecordingBackup \(Bulk Export\) Utility" on page 60](#) for more information.

The backed up data is imported into CAD 7.0 through the Configuration Setup tool during the installation process.

The BackupDB file is located on the CAD 7.0 installation CD.

To run BackupDB.bat:

1. On the server hosting the CAD Recording & Statistics service, open a command window.
2. Navigate to the folder where BackupDB is located.
3. On the command line, type:

```
BackupDB.bat "<userID>" "<password>" "<dbserver>" "<destination folder>"
```

where:

<userID> User ID needed to access the old database

<password>. Password needed to access the old database

<dbserver>. Hostname of the server where the database is located

<destination folder> Location where the backup file is saved

4. Press **Enter**.

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

5. Install CAD 7.0. When CAD Configuration Setup runs, select the **Restore From** option on the Recording & Statistics Service Database window and specify the location of the cadbkp.dat file.

CDBRTool Utility

The CDBRTool utility backs up phone books, work flows, enterprise data, the default dial plan, and recordings.

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

NOTE: The CDRBTool utility cannot be used if the primary Directory Services is down and only the secondary Directory Services is running. In this case, use the backup and restore functionality built into Cisco Desktop Administrator.

To run CDBRTool.exe:

1. On the computer where Desktop Administrator is located, open a command window.
2. Navigate to the folder where CDBRTool is located.
3. On a command line, type:

```
CDBRTool <switches> "<pathname>" "<LCC ID>"
```

where <pathname> is the folder where the backup files are to be saved, and <LCC ID> is the name of the logical contact center.

The syntax includes the following switches:

Table 1. CDBRTool switches

| Switch | Description |
|--------|--|
| /B | Back up configuration data. You must use this in conjunction with one of the switches that specify the type of data to back up: /C, /D, /L, or /A. |
| /R | Restore configuration data. Use this to restore data if the old LCC and the new LCC have the same name. You must include the LCC ID in the command line. |
| /C | Company data (all). This backs up all data in LDAP: company data and LCC data. |
| /L | Specific LCC. This backs up data in a specific logical contact center. You must include the LCC ID in the command line. |
| /A | Audio files. This backs up existing recordings. |
| /P | Merge data with the current Directory Services. |

4. Uninstall the older CAD version.
5. Install CAD 7.0. When CAD Configuration Setup runs, on the Restore Backup Data window, click **Yes** and browse to the location of the backup folder.

When you save your Configuration Setup settings, the configuration data is imported to CAD 7.0.

6. To restore recordings, run CDBRTool and specify the location of the folder where you saved the backed-up recordings.

DABackupTool Utility

The DABackupTool utility is used only when backing up CAD 4.6 configuration data. It is not used with newer versions of CAD.

NOTE: You must obtain the most recent version of DABackupTool from the Cisco Software Center Downloads page for Cisco Agent Desktop. The version on your CAD 4.6 installation CDs is no longer valid.

DABackupTool preserves the following settings:

- Logical contact centers
- Enterprise data fields and layouts
- Monitored devices
- Agents
- Work flow groups
- Work flows
- Dial plans
- Macros
- Reason codes
- VoIP Monitor/Desktop Monitor settings
- User interface settings
- Global phone books

NOTE: Default work flow groups are overwritten when CAD is upgraded. As a result, any settings made in the Default work flow group are lost. Customized work flow groups (new work flow groups with names other than “Default”) are preserved in an upgrade.

NOTE: Supervisors, teams, skill groups, and employee phone books are not preserved. They must be set up again in the upgraded version of CAD.

To run DABackupTool:

1. On the computer where Desktop Administrator is located, open a command window.
2. Navigate to the folder where the DABackupTool utility is located.
3. On the command line, type:
dabackuptool “<destination folder>”
where <destination folder> is the folder where the backup file will be saved.
For example:
dabackuptool “C:/Backup/”
The program backs up the configuration data to your destination folder.
4. Uninstall the previous version of CAD.
5. Install CAD 7.0. When CAD Configuration Setup runs, on the Restore Backup Data window, click **Yes** and browse to the location of the backup folder.

When you save your Configuration Setup settings, the configuration data is imported to CAD 7.0.

- Restart the CAD services after the restore is completed.

RecordingBackup (Bulk Export) Utility

CAD 7.0 archives recordings differently than it did in CAD 4.6. If you want to be able to review recordings made with CAD 4.6, you must export them from the Recording & Statistics service database using RecordingBackup (also known as the Bulk Export utility).

The Bulk Export Utility creates an HTML page you can use to view the recording files you previously viewed using the Supervisor Log Viewer. Like Supervisor Log Viewer, the HTML gives you access to recordings made in the last seven days plus those that are marked to be saved for 30 days.

NOTE: CAD no longer manages these recording files. All file management must be handled manually.

The file RecordingBackup is found on the CAD 7.0 installation CD.

To run RecordingBackup.exe:

- Ensure that the Recording & Statistics service is running.
- Open a command window on the machine where the Recording & Statistics service is running.
- Navigate to the folder where RecordingBackup is located.
- On a command line, type:

```
RecordingBackup.exe
```

The utility copies files to your AudioFiles folder, including one named RecordLogView.html (see [Figure 28](#)). View this file using your web browser.

Figure 28. Sample RecordLogView.html.

The screenshot shows a web interface for viewing recordings. At the top, there is a section titled "Select a Day:" with a row of buttons for each day of the week: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. The "Wednesday" button is highlighted. Below this, there is a section titled "Recordings for Wednesday:". Underneath is a table with the following columns: Agent, Team, Date, Start, Stop, and File. The table contains three rows of recording 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 | 17:36:00 | 2004100817302112101.wav |

Configuring Cisco CallManager IP Phones for Cisco IP Phone Agent

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

1. Create an IP phone service.
2. Assign the IP phone service to each IP agent phone.
3. Create an IPPA authentication user and assign to it all the IP agent phones.
4. Change the default URL Authentication parameter.

Configuration Procedure

Creating an IP Phone Service

From the Cisco CallManager 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 **Feature > IP Phone Service**.
2. On the Cisco IP Phone Services Configuration page, enter the following information:

Service Name. Enter the service name that will be shown in the IP phone Services window.

Service Description. Optional. Enter a description of the service.

Service URL. Enter the URL for the service. For example:

`http://<IP address>:8088/ipphone/jsp/sciphonexml/IPAgentInitial.jsp`

where:

- `<IP address>` is the IP address of the machine where the Agent State service is loaded
- 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 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.

3. Click **Insert** to create the new IP phone service. The new service is now listed in the shaded box at the left of the 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. User 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 red hyperlink.
The Phone Configuration window appears.
4. Click **Subscribe/Unsubscribe Services** in the upper right corner of the window.
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 **Continue**.
The Service Subscription popup window showing the new service appears.
6. Click **Subscribe**.
The new service is listed in the shaded box at the left of the page.
7. Close the popup window.

Creating the CallManager IPPA Authentication User

The next task to accomplish is to create a CallManager IPPA authentication user.

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 Configuration Window](#)" on page 44 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 menu, choose **Add a New User**.

The User Configuration window appears.

2. Enter the following information.

Entries are case sensitive. Enter them exactly as shown.

| | |
|---------------|---|
| First Name | telecaster |
| Last Name | telecaster |
| UserID | <the user ID set up in CAD Configuration Setup on the Services Configuration window> |
| User Password | <the password set up in CAD Configuration Setup on the Services Configuration window> |
| PIN | 12345 |
| Confirm PIN | 12345 |

3. Check the **Enable CTI Application Use** check box, and then click **Insert**.
4. Click **Device Association** in the shaded box at the left.
The Find and List Phones window appears.
5. Use the search function to locate all phones that are to be associated with the IPPA authentication user. This should be every IP phone that will be used by an IP phone agent.
6. Select the phone(s) from the search results to associate them with the IPPA authentication user, check the **No Primary Extension** check box, and then click **Update** to complete the association.

On the User Configuration window, the phones you selected are listed by their MAC addresses under Controlled Devices.

7. Continue until all appropriate IP phones are associated.

Changing the Default URL Authentication Parameter

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

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 webservice IP address:8088/ipphone/
jsp/sciphonxml/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 CallManager 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 CallManager database.

NOTE: A Cisco IP Communicator phone registers with the CallManager 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 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.

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

SecuritySetupPackage.exe can be copied from one of the client boxes, where it is installed automatically, or you can install the Win32 CTI OS Toolkit, which installs the three programs required for security. If you use the CTI OS server as the Certificate box, install this toolkit.

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 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. 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:

- 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 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 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\Desktop\bin** 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.
2. Copy the **CtiosServerKey.pem** and **CtiosServerReq.pem** files from the CTI OS server 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:\Program Files\Cisco\Desktop\bin** 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 the Server CTI OS Security Certificate on a Peer CTI OS Server

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.

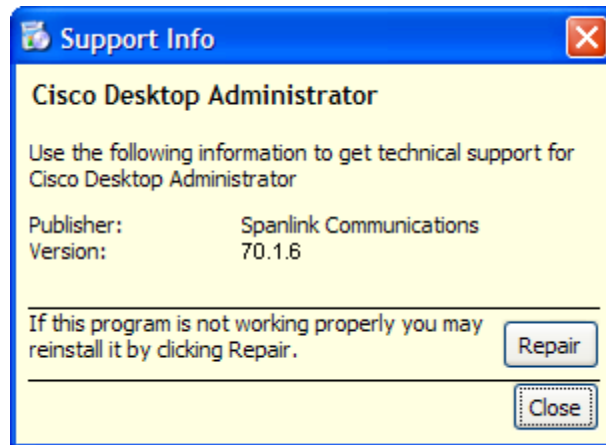
Repairing CAD

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.

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 informaton** link to display the Support Info dialog box (see Figure 29).

Figure 29. 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 7.0

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

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

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.

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 CallManager does not support two NICs, using multiple NICs works only in configurations where CallManager 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 host name> command. This ensures that the local name always resolves to the normal traffic card IP address.

Required Registry Changes

The installation process offers the user the option to choose the IP address that the VoIP Monitor Service will use for normal traffic and the IP address of the network adapter that the server will use for sniffing.

However, the installation is such that the user can only specify the IP address of the sniffing card. The IP address that the VoIP Monitor Service is receiving requests at is, by default, the first one to appear in the system-supplied enumeration.

While this works in a one-NIC scenario, it may be wrong in a two-NIC scenario. If the first IP address that appears in the enumeration is the sniffing card then the same card would be used for both sniffing and other traffic. This is the situation we are trying to avoid by making sure that the correct IP address is written in the CAD service registry settings, as outlined in the procedure below.

Second NIC is Present Before IPCC Enterprise/Hosted Installation

1. Enter the sniffing card's IP address when asked for the VoIP Monitor Service during the installation process.
2. After the installation finishes, make sure the following registry key has the normal traffic IP address value:

HKLM\SOFTWARE\Spanlink\Site Setup\IOR HOSTNAME

Second NIC is Installed After IPCC Enterprise/Hosted Installation

1. Navigate to the following registry key:
HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\
NetworkCards
2. Find the newly-inserted card entry.
3. Copy the value in ServiceName.
4. Paste this value in the following registry key:
HKLM\SOFTWARE\CAD\VoIP Monitor Server\Config\MONITOR DEVICE
5. Prefix the value with **\Device\Spkpc_**. This string is case sensitive—it must match exactly.
6. Close the Windows registry.

Testing Ethernet Cards for Silent Monitoring

B

Overview

On a site where IP telephony is deployed, the Cisco CallManager and the IP phones are normally configured to use a Virtual Local Area Network (VLAN) so that voice is logically separated from data. Although both traffic types are carried on the same physical channel, they are transmitted on different VLAN, one for voice and another for data. This configuration allows voice to be transmitted with higher priority than data.

In a contact center that uses silent monitoring, the agent desktop system is required to be connected to the PC port on the back of the IP phone so that voice packets reaching the phone can be collected by the silent monitor subsystem and then be forwarded to the supervisor workstation. In this case, the agent desktop system will then be using one single physical channel to interact with two different VLANs.

The agent desktop system accesses the physical channel via an Ethernet Network Interface Controller (NIC). The NIC watches the channel and collects Ethernet frames addressed to the agent's computer. The NIC then runs a pre-processing step to extract IP packets from the Ethernet frames and delivers them to the TCP/IP stack on the operating system.

During internal testing, Cisco identified that some Ethernet NIC card drivers are not capable of pre-processing Ethernet frames that have an IP packet encapsulated in a VLAN frame. That is, the NIC card driver discards the Ethernet frame altogether if the IP packet is encapsulated in an 802.1Q frame. Some vendors can provide a configuration setting that allows their NIC card driver to forward VLAN traffic to the TCP/IP stack.

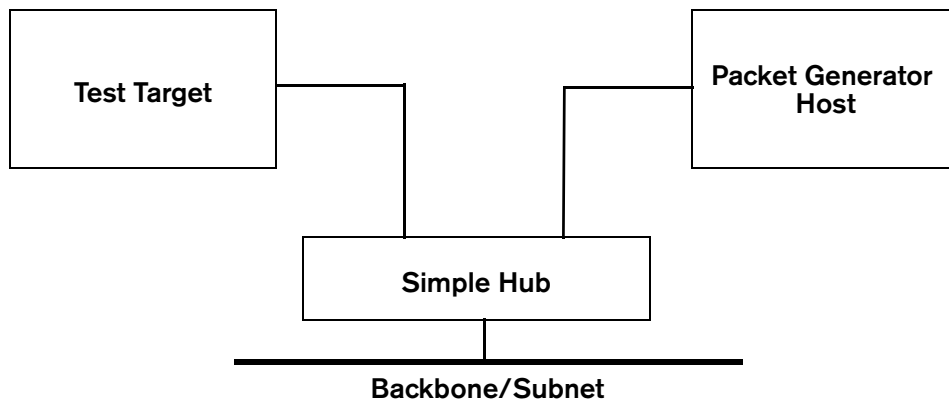
If an agent desktop's NIC card driver discards VLAN traffic, then the silent monitor subsystem on that desktop will not be able to collect and forward voice packets to the supervisor workstation and silent monitoring will not function properly.

Cisco has developed a procedure to determine if a particular Ethernet NIC card driver will work with CAD silent monitoring. The procedure is described in the following section.

Test Procedure

The test involves sending sample VLAN packets to a test target NIC card and verifying that the packets are not discarded by the pre-processing step, but are passed on to the TCP/IP stack on the operating system at the computer hosting the NIC card.

The test requires a configuration as shown in the following diagram.



The test target NIC is connected to one port of a simple hub. The hub is connected to the network backbone or subnet. You also need a packet generator host capable of generating Ethernet traffic. The packet generator host will be connected to another port on the hub.

The packet generator host equipment can be either a dedicated packet analyzer or a computer with a software-based packet analyzer capable of generating Ethernet traffic.

There are a number of software packet analyzers available that can be used for this purpose. For a comprehensive list of reliable analyzers, visit the Cooperative Association for Internet Data Analysis website at www.caida.org/tools/taxonomy/workload.xml. The following procedures use the Sniffer Pro packet analyzer.

Once the environment is set up as described above, load the software tools on the test target and packet generator host as follows.

Preparing the Test Target

Perform the following steps to prepare the test target.

1. Download and install the WinPcap utility.
2. Create a folder on the test target computer named "VLANTest".
3. Download WinDump.exe and copy it to the VLANTest folder.

4. Open a command window and navigate to the VLANTest folder.
5. Determine the MAC address of the test target NIC by executing **ipconfig /all** at the command prompt. Write down the number that appears for the Physical Address. See [Figure 1](#) for an example: the physical (MAC) address of the Intel Pro/100" NIC card is 00-D0-59-d8-f7-d9.

Figure 1. Output of the ipconfig /all command.

```

Select C:\WINNT\system32\cmd.exe
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . : cisco.com

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : cisco.com
    Description . . . . . : Cisco Systems 350 Series PCMCIA Wir
    Physical Address. . . . . : 00-09-43-74-55-94
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 10.86.165.239
    Subnet Mask . . . . . : 255.255.254.0
    Default Gateway . . . . . : 10.86.164.1
    DHCP Server . . . . . : 161.44.124.23
    DNS Servers . . . . . : 161.44.124.122
                           64.102.6.247
                           171.68.226.120
    Primary WINS Server . . . . . : 161.44.122.10
    Secondary WINS Server . . . . . : 64.102.2.51
    Lease Obtained. . . . . : Friday, August 08, 2003 5:39:41 PM
    Lease Expires . . . . . : Saturday, August 09, 2003 1:39:41 P

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : cisco.com
    Description . . . . . : Intel(R) PRO/100 UE Network Connect
    Physical Address. . . . . : 00-D0-59-D8-F7-D9
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 10.86.139.153
    Subnet Mask . . . . . : 255.255.255.128
    Default Gateway . . . . . : 10.86.139.129
  
```

6. Determine the device interface number of the test target NIC. Execute **windump -D** and write down the number of the NIC you want to test. In our example, we are interested in the interface number 1 that corresponds to the Intel Pro/100 NIC card.

NOTE: If you are not sure which number to pick, repeat the test for each card until the test succeeds for one (sufficient to pass) or this fails for all cards.

7. Start WinDump to monitor the test target NIC for incoming VLAN packets. To do this, execute **windump -i <device number> vlan**. In the following example, the device number is 1.

Figure 2. Output of the windump -i <device number> command.

```

C:\WINNT\system32\cmd.exe - windump -i vlan
D:\Development\VLAN Testing\WinDump>windump -i 1 vlan
windump: listening on \Device\NPF_{5E18F3A4-4257-46C3-9ADB-A33EBC591C3C}

```

Preparing the Packet Generator Host

Perform the following steps to prepare the packet generator host.

1. Load the packet analyzer software onto your packet generator host.
2. Obtain the sample capture file **VLANSamplePackets.cap** and load it into the packet analyzer software. The capture file was generated in a format that is used by most dedicated and software packet analyzers.
3. Select the DECODE view from the tab at the bottom of the window.

Executing the Test

The test involves sending a sample VLAN packet to a test target NIC card and verifying that the packet is not discarded by the pre-processing step, but rather is passed on to the TCP/IP stack on the computer hosting the NIC card.

The test case to determine whether or not the test target NIC is qualified to work with CAD silent monitoring is as follows.

| | | |
|------------------|--|---|
| Objective | Verify that the test target NIC is able to pre-process VLAN packets and is able to forward them to the TCP/IP stack on the test target host. | |
| Step | Party | Action |
| 1 | PA* | Select one of the loaded sample VLAN packets. |
| 2 | PA | Select or right-click Send Current Frame . |
| 3 | PA | Modify the destination MAC address to use the MAC address of the test target NIC. |
| 4 | PA | Send the new frame five times to the test target NIC. |

| | | |
|------------------------|--|--|
| 5 | WD [†] | Verify that there is activity reported on the test target NIC. |
| Expected Result | At the test target computer, WinDump will display five packets for VLAN ID = 85. If the test failed, no packets will be displayed. | |

* Packet Analyzer.

† WinDump.

If the outcome of this test is successful, then your test target NIC will work with CAD silent monitoring. Otherwise, contact your NIC card provider and ask what settings are necessary to allow your NIC card driver to forward all packets, including VLAN packets, to the TCP/IP stack on the test target host computer so that your packet analyzer tool can capture and display them.

Apply the appropriate adjustments and rerun this test procedure.

