Cisco CAD Installation Guide

Cisco Unified Contact Center Enterprise Release 7.5

First Published: July 2008
Last Modified: August 8, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Contents

Contents

Contents

Contents

Contents

Contents

Introduction

1

Overview

Installing CAD 7.5 consists of the following tasks.

1. Verify that software and hardware requirements are met. For instructions, see Chapter 2, "Requirements".
2. Complete preinstallation configuration, which includes the following tasks. For instructions, see Chapter 3, "Before You Install CAD 7.5".
   a. Configure agents in Unified ICM.
   b. Prepare user accounts and permissions.
3. Install and configure the CAD services and desktops, which includes the following steps. For instructions, see Chapter 4, "Installing CAD 7.5 Applications".
   a. Install the CAD services.
   b. Configure CAD using the CAD Configuration Setup utility.
   c. License CAD using Unified CCE License Administration.
   d. Install Desktop Administrator on the CAD administrator(s) desktop.
   e. Install client desktops.
      - Install Agent Desktop on agent desktops.
      - Install Supervisor Desktop on supervisor desktops.
      - Install the Java Runtime Environment (JRE) browser plug-in on CAD-BE agents' desktops.
   f. Modify the registry on the peripheral gateway (PG) computer.

After you have completed these steps, the basic functionality of CAD is ready to use with no further configuration required.

Related CAD Documentation

The following documents contain additional information about CAD 7.5:

- *Cisco Agent Desktop User Guide*
- *Cisco Agent Desktop—Browser Edition User Guide*
- *Cisco Supervisor Desktop User Guide*
- *Cisco IP Phone Agent User Guide*
- *Cisco Desktop Administrator User Guide*
- *Mobile Agent Guide for Cisco Unified CC Enterprise*
- *Cisco CAD Troubleshooting Guide*
- *Integrating CAD with Citrix Presentation Server or Microsoft Terminal Services*

CAD 7.5 Feature Levels

There are three feature levels of CAD 7.5: Standard, Enhanced, and Premium. The following tables list the features available in Cisco Agent Desktop (Agent Desktop), Cisco Agent Desktop--Browser Edition (CAD-BE), Cisco IP Phone Agent, Cisco Supervisor Desktop (Supervisor Desktop), and Cisco Desktop Administrator (Desktop Administrator).

Agent Desktop

The following table lists the features available in each feature level of Agent Desktop. Features that are not listed here are in all three feature levels.

Table 1. Agent Desktop features

Feature	Standard	Enhanced	Premium
Agent-initiated call recording		●	●
Agent-initiated chat	●	●	●
Cisco IP Communicator support	●	●	●
Cisco Unified Mobile Agent support	●	●	●
Cisco Unified Outbound Dialer		●	●
Cisco Unified Presence Server integration	●	●	●
Enterprise data thresholds		●	●
Event-triggered workflows		●	●
HTTP Post/Get action			●
Integrated browser with multiple tabs			●
IPC Receive action			●
Reason codes	●	●	●
Task buttons		●	●
Timer action		●	●
Wrapup data	●	●	●

CAD-BE

The following table lists the features that are available in each feature level of CAD-BE. Features that are not listed here are in all three feature levels.

Table 2. CAD-BE features

Feature	Standard	Enhanced	Premium
Agent-initiated call recording		●	●
Cisco IP Communicator support	●	●	●
Cisco Unified Mobile Agent support	●	●	●
Enterprise data thresholds		●	●
Event-triggered work flows		●	●
HTTP Get action		●	●
Integrated browser		●	●
Reason codes	●	●	●
Task buttons		●	●
Wrapup data	●	●	●

IP Phone Agent

The following table lists the features that are available in each feature level of IP Phone Agent. Features that are not listed here are in all three feature levels.

Table 3. IP Phone Agent features

Feature	Standard	Enhanced	Premium
Agent-initiated recording		●	●
Enterprise data	●	●	●
Reason codes	●	●	●
Skill group data	●	●	●
Wrap-up data	●	●	●

Supervisor Desktop

The following table lists the features that are available in each feature level of Supervisor Desktop. Features that are not listed here are in all three feature levels.

Table 4. Supervisor Desktop features

Feature	Standard	Enhanced	Premium
Barge-in	●	●	●
Cisco Mobile Agent support	●	●	●
Cisco Unified Presence Server integration	●	●	●
Integrated browser	●	●	●
Intercept	●	●	●
Real-time displays (charts)			●
Real-time displays (text)	●	●	●
Recording		●	●
Silent monitoring	●	●	●
Skill statistics	●	●	●
Supervisor work flows—all actions except threshold alerts for tree control actions only			●
Supervisor work flows—threshold alerts for tree control actions only		●	●
Team messages	●	●	●
Web page push to agents			●

Desktop Administrator

The following table lists the features that are available in each feature level of Desktop Administrator. Features that are not listed here are in all three feature levels.

Table 5. Desktop Administrator features

Feature	Standard	Enhanced	Premium
Cisco Unified Presence integration	●	●	●
Configuration of Agent Desktop integrated browser			●
Configuration of Agent Desktop, IP Phone Agent, and CAD-BE interfaces		●	●
Configuration of CAD-BE integrated browser		●	●
Configuration of work flows		●	●
HTTP Get work flow action for CAD-BE		●	●
HTTP Post and Get work flow actions for Agent Desktop			●
IPC Receive action event			●
Time of day event and data condition			●
Timer action		●	●

What's New in This Version

CAD 7.5 includes these new features.

- Integration with Unified Presence
- Administration of integrated Unified Presence features through a new browser-based interface named Cisco Desktop Presence Administrator
- Enhanced accessibility through shortcut keys
- Multiple tabs in the integrated browser in Supervisor Desktop
- Additional localization in French Canadian and Norwegian
- Support for automated updates with Windows Vista

CAD 7.5 Components

CAD 7.5 is a suite of applications and services consisting of the following elements.

Desktop Applications

Desktop Administrator

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

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

Agent Desktop

Agent Desktop is an application that provides agents with call control capabilities, such as call answer, hold, conference, and transfer, as well as ACD state control (ready/not ready, wrap-up, etc.). Agent Desktop helps agents manage their customer contacts by presenting customer information to the agents through an enterprise data window, which includes enterprise data, call activity information, and reports. Agent Desktop provides a chat client for chatting with other agents and supervisors and an integrated browser window so agents can view intranet, internet, and web application pages as needed. Agents can use a hard IP phone or the IP Communicator soft phone with Agent Desktop.

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

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

CAD-BE

CAD-BE is a Java applet version of Agent Desktop that runs in Internet Explorer and Mozilla Firefox web browsers.

CAD-BE is an application that provides agents with call control capabilities, such as call answer, hold, conference, and transfer, as well as ACD state control (ready/not ready, wrap-up, etc.). CAD-BE helps agents manage their customer contacts by presenting customer information to the agents through an enterprise data window, which includes enterprise data, call activity information, and reports. Agent Desktop also provides an integrated browser window so agents can view intranet, internet, and web application pages as needed.

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

IP Phone Agent

IP Phone Agent is a service that runs on the agent's IP phone that enables agents to manage their customer contacts without requiring the use of a computer. IP Phone Agent includes enterprise data, agent states, wrap-up data, reason codes, and skill statistics. See the *Cisco IP Phone Agent User Guide* for more information.

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, and push web pages to the agent to assist the agent in serving the customer. They can also silently monitor and record customer calls and, if necessary, conference in or take over those calls using the barge-in and intercept features. Through the Supervisor Record Viewer, supervisors can play back and save recorded agent calls.

Desktop Monitoring Console

The Desktop Monitoring Console is a Java application that allows you to monitor the status of the CAD services and the LDAP Directory Services. It is installed automatically when the CAD base services are installed. For more information, see "Desktop Monitoring Console" on page 71.

Services

CAD base services are installed on a single server and include the following services:

- Cisco Browser and IP Phone Agent Service (BIPPA service)
- Cisco Chat Service (Chat service)
- Cisco Enterprise Service (Enterprise service)
- Directory Services
- Cisco LDAP Monitor Service (LDAP Monitor service)
- Cisco Licensing and Resource Manager Service (LRM service)
- Cisco Recording and Statistics Service (Recording and Statistics service)
- Cisco Sync Service (Sync service)
- Tomcat service

CAD includes two other services that can be installed on the same server as the base services or on different servers. These services are the following:

- Cisco Recording & Playback Service (Recording & Playback service)
- Cisco VoIP Monitor Service (VoIP Monitor service)

A set of the base services plus the additional services is a logical contact center, or LCC. For LCC capacities and other CAD system capacities see Table 7 on page 22.

The CAD base services and additional services are described alphabetically below.

BIPPA Service

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

This service works in conjunction with the services feature of Unified CM and IP phones.

Chat Service

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

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

Directory Services

The LDAP Monitor service and the LRM service register with Directory Services at startup. All other services use the LRM service to determine how to connect to each other.

The majority of the agent, supervisor, team, and skill information is kept in Directory Services. Most of this information is imported from the Cisco Unified Intelligent Contact Management (Unified ICM) logger and kept synchronized by the Sync service. It is also used to hold the configuration information administered via Desktop Administrator.

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. The Enterprise service interacts with the CTI server, which typically runs on a peripheral gateway (PG).

LDAP Monitor Service

The LDAP Monitor service starts Directory Services and then monitors the services to ensure that they keep running.

LRM Service

The 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. All other CAD services, except the LDAP Monitor service, register themselves with the LRM service so that clients can locate them.

Recording & Playback Service

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

Recording and Statistics Service

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

Sync Service

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

The Sync service also monitors the Unified ICM LDAP for changes to contact information and contact lists. When this information changes, the Sync service notifies the CAD LDAP of the changes.

Tomcat Service

Tomcat is a Java-based webserver. Tomcat is required for IP Phone Agent to work with the XML pages displayed by IP phones. Tomcat is also used for CAD-BE, Desktop Management Console, and desktop installations.

VoIP Monitor Service

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

> **NOTE:** The VoIP Monitor service is not used with Unified CM-based monitoring.

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

Localization

Supported Languages

In CAD 7.5, the CAD desktop applications (except for Desktop Administrator, which is available in English only) are localized in the languages displayed in Table 6.

Table 6. Supported languages and CAD desktop application availability

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

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

Installation in Localized Contact Centers

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

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

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

System Capacity

CAD 7.5 supports the following system capacities.

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

Table 7. CAD 7.5 system capacity

Description	Capacity
Maximum number of CAD agents per peripheral gateway (PG)*	1000
Maximum number of CAD agents per PG when using Microsoft SQL Server	1000
Maximum number of IP phone agents per server	1000
Maximum number of CAD-BE agents per server	1000
Maximum number of agents per team	100
Maximum number of skills per agent (for real-time reporting)†	52
Maximum number of supervisors per site	100
Maximum number of supervisors per team	20
Average number of agents per supervisor	10
Maximum number of agents per monitor domain‡	1000
Maximum number of simultaneous recordings per contact center**	Enhanced 32 Premium 80
Maximum number of simultaneous playbacks per Recording & Playback service	8
Maximum number of CAD agents per outbound PG††	200
Maximum number of off-board VoIP Monitor services	5
Maximum number of simultaneous monitoring sessions per VoIP Monitor service	64
Maximum number of off-board Recording & Playback services	2

* Capacities are reduced when using the mobile agent feature. In call-by-call mode, capacity is reduced to approximately 70%; in nailed-up mode, capacity is reduced to approximately 50%.

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

‡ A system with more than 100 agents requires an off-board VoIP Monitor service. A system with more than 400 agents requires a VoIP Monitor service server with a 1 GB NIC.

**An off-board Recording & Playback service is required to support more than 32 simultaneous recording/playback sessions.

††PG dedicated to outbound agents coresident with dialer and media routing.

Requirements

2

System Configurations

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

Citrix and Microsoft Terminal Services Environments

CAD is supported in Citrix and Microsoft Terminal Services environments. For more information, see the document, *Integrating CAD with Citrix MetaFrame Server or Microsoft Terminal Services*.

System Requirements

CAD 7.5 is integrated into the following Unified Contact Center Enterprise and Hosted environment:

CAD Version	Unified CM Version	Unified ICM Version	CTI Server
7.5(1)	4.1, 4.2, 5.0, 6.0	7.5(1)	CTI OS 7.5

Consult the following documents for the most current compatibility information:

Cisco Unified CallManager Compatibility Matrix
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm

Cisco IP Contact Center Enterprise Edition Software Compatibility Guide
http://www.cisco.com/application/pdf/en/us/guest/products/ps1844/c1609/ccmigration_09186a008031a0a7.pdf

Operating Environment

CAD 7.5 desktop applications run on the following operating systems and hardware.

Table 8. Desktop minimum operating systems and hardware

Operating System	Desktop Applications
Windows XP Professional Edition Service Pack 2	All Desktops: • 500 MHz processor • 128 MB RAM • 800 × 600 screen resolution • 100 Mbit NIC supporting Ethernet 2 Agent, Supervisor, and Admin Desktops: • 650 MB free space
Windows Vista Business or Ultimate	All Desktops: • 500 MHz processor • 512 MB RAM • 800 × 600 screen resolution • 100 Mbit NIC supporting Ethernet 2 Agent, Supervisor, and Admin Desktops: • 650 MB free space
Red Hat Enterprise Linux v4, v5	CAD-BE Desktop only: • 1 GHz processor • 256 MB RAM • 1 GB free space (for logging) • 100 Mbit NIC supporting Ethernet 2 • 800 by 600 screen resolution

Table 8. Desktop minimum operating systems and hardware — *Continued*

Operating System	Desktop Applications
Citrix MetaFrame Presentation Server Full window mode	Agent Desktop only: For minimum software and hardware requirements, see *Integrating CAD with Citrix Presentation Server or Microsoft Terminal Services* and your Citrix documentation.
Microsoft Terminal Services for Windows	Agent Desktop only: For minimum software and hardware requirements, see *Integrating CAD with Citrix Presentation Server or Microsoft Terminal Services* and your Microsoft Terminal Services documentation.

CAD 7.5 services run on the following operating systems and hardware.

Table 9. Server minimum operating systems and hardware

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

Operating Environment Language Requirements

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

- Agent Desktop
- CAD-BE
- Supervisor Desktop

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

A site cannot support more than one localized language. All agents and supervisors must use the same language—there cannot be some agents and supervisors using one language and other agents and supervisors using another language.

For a list of supported languages, see Table 6 on page 20.

VPN and NAT Requirements

Virtual private networks (VPNs) provide a more secure connection. Connections over a VPN are supported by the CAD clients (Agent Desktop, Supervisor Desktop, and CAD-BE).

Cisco VPN 3000 Concentrator and Cisco VPN Client have been formally verified to work correctly with CAD clients, and are supported for access. VPN solutions from other vendors may work correctly, but since they have not been formally verified, they are not supported. If you want an alternative VPN solution to be verified, please contact your Cisco distributor.

CAD does not support server-side network address translation (NAT). The CAD clients must be able to connect using the real IP addresses of the server components. When CAD client addresses are translated via NAT, VPN software must be used. If CAD clients are used in a NAT environment without VPN software, a variety of problems may occur, such as agents not being visible in Supervisor Desktop.

Using NAT With IP Phone Agent

NAT is supported with IP Phone Agent. However, it is required that you use static IP addresses for the IP Phone Agent phones as well as Static NAT. Dynamic NAT and address overloading are not supported. Recording and monitoring do not work with IP Phone Agent when it is used with NAT.

For more information on NAT, see *How NAT Works* (Cisco document ID 6450), at:

http://www.cisco.com/warp/public/556/nat-cisco.shtml

Third Party Software Requirements

CAD 7.5 requires the following software applications to run successfully.

Microsoft Internet Explorer

Microsoft Internet Explorer 6 or 7 must be installed on agent and supervisor PCs to support the integrated browser component of Agent Desktop, CAD-BE, and Supervisor Desktop. The CAD integrated browser is implemented using the Microsoft WebBrowser control (Shdocvw.dll), which provides a window in which the user can navigate websites and files using hyperlinks and URLs.

Differences between the CAD integrated browser and Internet Explorer include the following:

- If a third-party web application attempts to launch a new browser window, the CAD integrated browser will open a new tab instead.

- If a page that contains a JavaScript error is opened from the CAD integrated browser and script error notification is disabled in IE (the default), the CAD integrated browser will not display any information about the error. To see detailed information about the error, you must open the page from IE with script debugged enabled.
- The CAD integrated browser does not support the more advanced features of Internet Explorer, including the pop-up blocker, the phishing filter, and Internet Explorer 7-style tabs.

  NOTE: The integrated browser supports only one web session at a time for web applications that use cookies for session management. For example, you cannot log into a web application that uses cookies in one tab as User A and then log into the same web application in another tab as User B. However, multiple web sessions are supported for web applications that use URL-based session management.

  NOTE: For technical reference information about the WebBrowser control, see the MSDN article available at this URL: http://msdn2.microsoft.com/en-us/library/42h6dke4(VS.80).aspx

Java Runtime Environment (JRE)

JRE 1.5.0_14 is required to run the Java applets and JavaServer pages (JSP) used by IP Phone Agent, Agent Desktop, CAD-BE, and Desktop Monitoring Console. JRE is shipped with CAD 7.5 and is installed automatically with the CAD services and the client desktops.

Mozilla Firefox

The following versions of Mozilla Firefox are supported browsers for CAD-BE:

- Firefox 1.5.0.8 on Microsoft Windows XP and Red Hat Enterprise Linux, v4 and v5
- Firefox 2.0.0.11 on Microsoft Windows XP, Microsoft Vista, and Red Hat Enterprise Linux, v4 and v5

Apache Tomcat

Apache Tomcat 5.5, a Java-based webserver, is needed to work with the XML pages displayed by IP phones. Tomcat is also used for CAD-BE, Desktop Monitoring Console, and desktop installs. More information about Tomcat may be found at http://jakarta.apache.org. Tomcat is shipped with CAD 7.5 and is installed automatically.

Microsoft SQL Server 2000 Desktop Engine

Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) with Service Pack 4 is the free, redistributable version of SQL Server used as an embedded database. It is installed automatically with the CAD services.

OpenLDAP

System configuration data is maintained using OpenLDAP V2.3.35 Directory Services on the CAD server.

CTI OS

Computer Telephony Integration Object Server (CTI OS) must be installed on the CTI server before installing the CAD services. You may want to edit several registry keys to enable Agent Desktop to receive all CTI events. See "Supported IP Phones" on page 29 for information on changing these registry keys.

Monitoring Requirements

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

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

Version	Supports CAD-based monitoring	Supports Unified CM-based monitoring
Unified CM 4.x	X	
Unified CM 5.x	X	
Unified CM 6.0	X	X

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

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

For more information about monitoring, see *Configuring and Troubleshooting VoIP Monitoring*.

Supported IP Phones

For a list of IP phones that are supported with Agent Desktop and CAD-BE, see the *Cisco IPCC Enterprise Software Compatibility Guide*. This document is available at:

http://www.cisco.com/en/US/docs/voice_ip_comm/cust_contact/contact_center/ipcc_enterprise/ipccenterprise7_2/design/guide/IPCC_Compatibility_MATRIX_6_6_07.pdf

NOTE: IP Communicator is supported for Agent Desktop and CAD-BE. It is not supported for IP Phone Agent.

Caveats on Using a Cisco 7920 Wireless Phone

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

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

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

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

IP Phones Supported with IP Phone Agent

The following phones are supported with IP Phone Agent:

- Cisco 7905
- Cisco 7910
- Cisco 7920/7921
- Cisco 7940/7941
- Cisco 7960/7961
- Cisco 7970/7970(SIP)/7971

Before You Install CAD 7.5

3

Overview

Before you install CAD 7.5, you must complete the following tasks.

- Configure agents in Unified ICM.
- Prepare user accounts and permissions for CAD to integrate with other Unified CCE components.

These tasks are described below.

Setting Up Agents in Unified ICM

Setting Up Supervisors and Teams

For CAD 7.5 applications to work properly, your agents must be organized into teams and some must be designated as supervisors. This is accomplished in Unified ICM. See your Unified ICM documentation for information on how to do this.

Skills Statistics

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

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

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

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

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

Reason Codes

Starting with version 7.1(1) of CAD, reason codes were created and maintained in Unified ICM and pulled into CAD. In previous versions of CAD, reason codes could be created and maintained in both Unified ICM and in CAD.

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

Preparing User Accounts and Permissions

Before you install CAD base services, you must complete the following tasks:

1. Make the server (both servers in an HA environment) on which you are going to install the CAD base services a member of a domain.

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

2. Create a user account (on both servers) in Windows Computer Management with the following requirements:

   - The user must have local administrator privileges.
   - The user account must have a password. If either of the servers does not have a password, replication setup will fail because the subscriber cannot connect to the publisher to configure the replication.
   - The user account must have read and write privileges.
   - The same user account must exist on the ICM Admin Workstation computer.
   - Use the format <domain>\<username> when creating the username.

Installing CAD 7.5 Applications

4

Overview

Install the CAD 7.5 applications in the following order:

1. CAD services
2. Desktop Administrator
3. Supervisor Desktop, Agent Desktop, and the JRE for CAD-BE

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

After you finish installing the CAD 7.5 applications, you must modify the registry on the peripheral gateway (PG) computer. For instructions, see "Modifying the Peripheral Gateway Registry" on page 44.

Installation Locations

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

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

Using Automated Package Distribution Tools

CAD's MSI-based desktop application installations can be deployed ("pushed") via automated package distribution tools that make use of the Microsoft Windows Installer service.

Requirements

CAD support for automated package distribution depends on compliance with the requirements listed below.

Execution

Installations must be executed on the target machine. Deployment methods that capture a snapshot of an installation and redistribute that image are not supported.

Per-Machine vs. Per-User Installation

Installations must be deployed on a per-machine basis. Per-user installations are not supported.

It may be necessary to ensure per-machine installation via command line.

Privileges

By default, Windows Installer installations run in the context of the logged-on user. CAD installations, which use Windows Installer, require either administrative or elevated (system) privileges. If the CAD installation is run in the context of an administrative account, no additional privileges are required.

If the CAD installation is run in the context of an account with reduced privileges, the Windows policy "Always Install with Elevated Privileges" must be enabled to deploy the installation with elevated privileges.

When this policy is enabled, Windows Installer installations will run in a context with elevated privileges, thus allowing the installation to successfully complete complex tasks that require a privilege level beyond that of the logged-on user.

To direct Windows Installer to use elevated privileges, launch the Microsoft Management Console (MMC) Local Computer Policy snap-in on the target machine. Enable the Windows policy "Always Install with Elevated Privileges" for both the Computer Configuration and the User Configuration nodes.

For more information about enabling this policy, see the topic "Always install with elevated privileges" at this URL:

http://msdn2.microsoft.com/en-us/library/ms813108.aspx

Automated Package Installation vs. Manual Installation

Automated installations must use the same files and meet the same installation criteria as manually-deployed installations.

CAD MSI packages are located in a specified location (the folder C:\Program Files\Cisco\Desktop\Tomcat\webapps\TUP\CAD) on a successfully-installed production server and are intended for both manual and automated deployment. Alteration of these files or the use of other MSI files included with the product at other locations is not supported.

Installation criteria such as supported operating systems, product deployment configurations, installation order, and server/client version synchronization must be met. Altering the supplied MSI packages to circumvent the installation criteria is not supported.

Multiple Software Releases

Multiple software releases must not be combined into a single deployment package. Each CAD software release is intended for distribution in its entirety as a distinct deployment. Combining multiple releases (for example, a software package's base release and a subsequent service release) into a single deployment package is not supported.

Reboots

Any reboots associated with CAD installations are required. If the installation's default reboot behavior is suppressed, the target machine must be rebooted before running the installed applications to ensure expected functionality.

Delaying a reboot is not known to be an issue at this time, as long as a reboot occurs before launching the installed applications. If it is determined in the future that delaying a reboot via command line suppression affects expected behavior, then that delayed reboot will not be supported.

Best Practices

Best practices recommendations are listed below.

Windows Installer Logging

To ensure that any loggable issues are captured efficiently, enable Window Installer logging using the following command line argument:

```
/l*v <logfile path and name>
```

NOTE: The logfile path and name must be a location to which the installation's user context has permission to write.

Deployment

Each installation package should be deployed using its own deployment package. Using separate packages offers faster isolation of potential issues than does a composite deployment package.

Installation and Uninstallation Deployment Packages

The deployment engineer should create and test both an installation and uninstallation deployment package.

This is especially important for service release installations, which must be uninstalled before upgrading the underlying software.

Recommended Deployment Preparation Model

1. Use a lab environment to model the pending deployment.
2. Install the servers to obtain valid client installation packages.
3. Manually deploy client installation packages to ensure that the installs are compatible with your environment. This will isolate product installation vs. automated deployment issues.
4. Create your deployment packages in accordance with the requirements listed in "Requirements" on page 36.
5. Test the deployment packages.
6. At deployment time modify your deployment packages, replacing the client installation packages from the lab environment with valid client installation packages from the production server.

Installing CAD Services

The CAD services installation is run from the product CD.

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

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

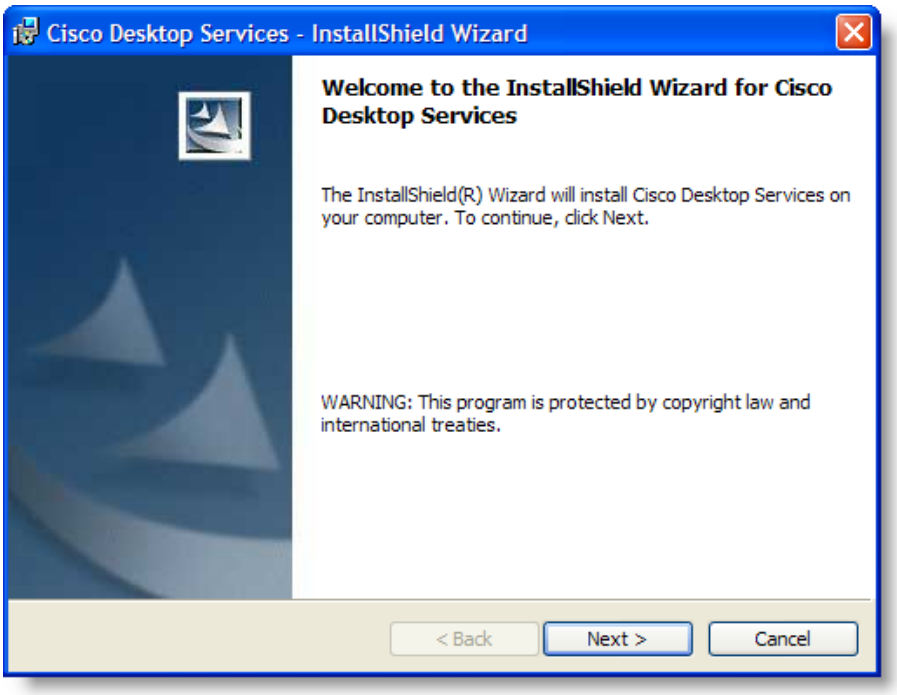
NOTE: You must install CAD base services using a local account with Administrator privileges. If you install CAD base services using a Windows Domain account, Recording and Statistics replication jobs will fail as well as Recording and Statistics clean-up jobs in SQL Server.

NOTE: The CAD services installation creates a user named CADSQLAdminUser and a group named CADSQLAdminGroup. CADSQLAdminUser has the sysadmin server role in SQL Server and is a member of CADSQLAdminGroup and Administrators. Several CAD services run under the CADSQLAdminUser user account, including MSSQL$CADSQL and SQLAgent$CADSQL. If SQL authentication is used for the ICM Admin Workstation database, then the Recording and Statistics service also runs under the CADSQLAdminUser user account. If NT authentication is used for the ICM Admin Workstation database, then the Recording and Statistics service runs under the NT user account instead.

To install the CAD services:

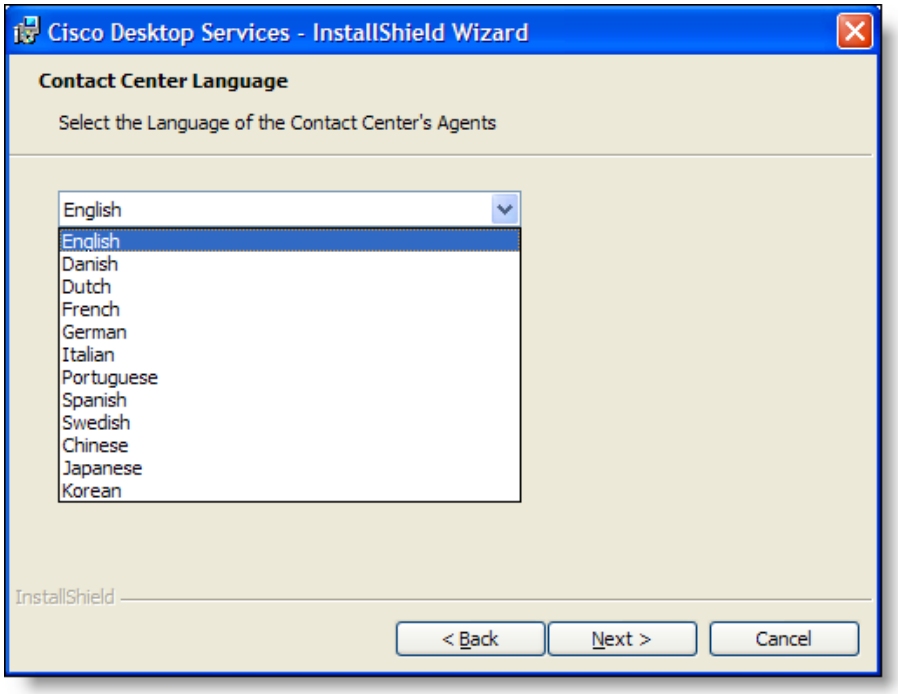
1. Launch the setup.exe file from the product CD to start the installation process (Figure 1).

Figure 1. Desktop Services - InstallShield Wizard Welcome window.



2. Click Next to display the Contact Center Language dialog box (Figure 2).

Figure 2. Contact Center Language window.

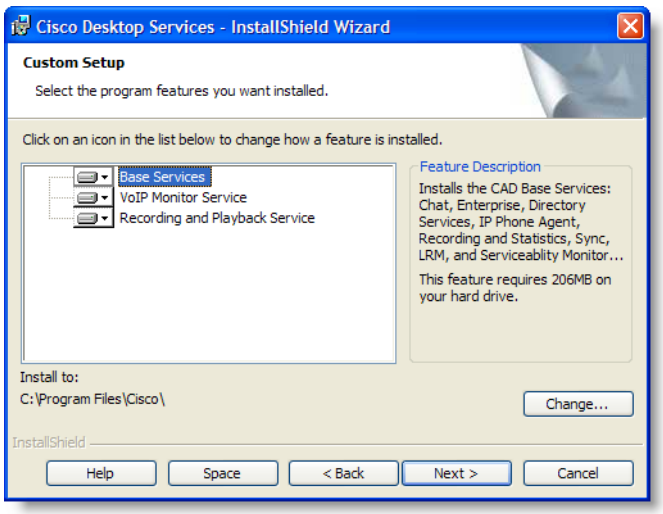


3. From the drop-down list, select the language for contact center agents to use.

   This selection determines which localized version of the desktop applications will be installed on agents' and supervisors' desktops. See "Operating Environment Language Requirements" on page 25 for more information.

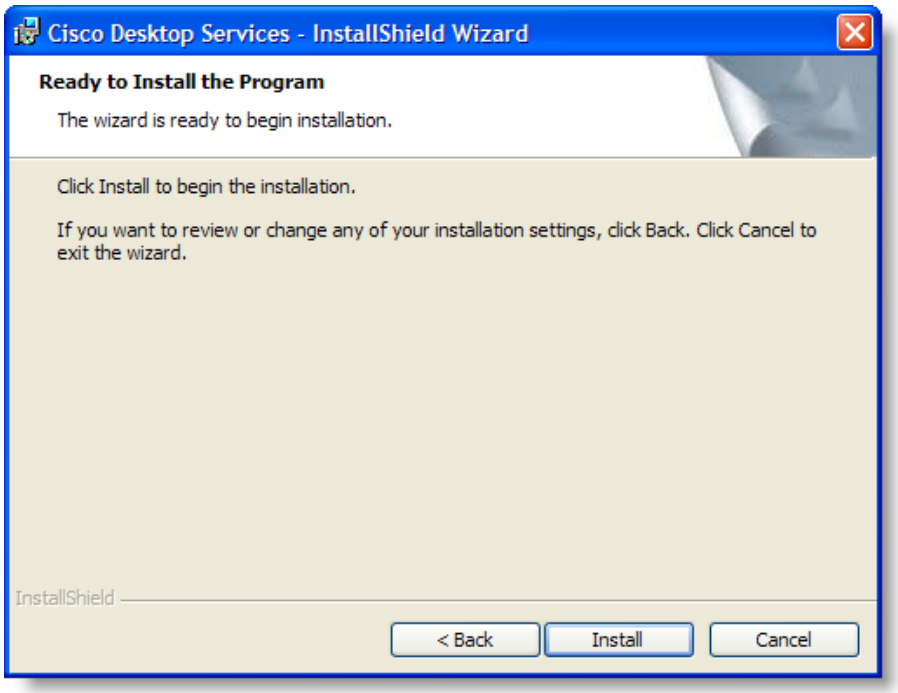
4. Click Next to display the Custom Setup dialog box (Figure 3).

Figure 3. Custom Setup dialog box



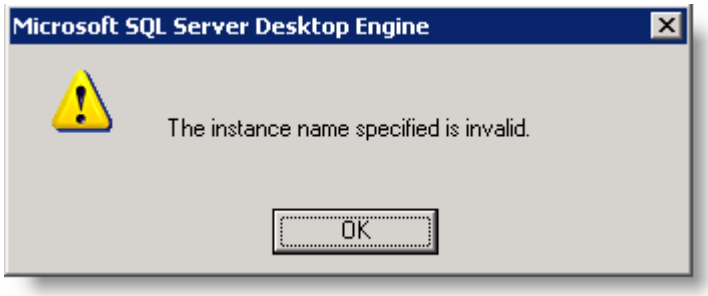
5. Click the down arrow next to the feature to add or remove it from the list of features to be installed.
6. Click Next to display the Ready to Install the Program window (Figure 4).

Figure 4. Ready to Install the Program window



7. Click Install to start the installation.

   NOTE: If you previously created a SQL Server named instance, the following warning message will appear. This is expected behavior. Click OK to continue with the installation.



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

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

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

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

8. When the installation is completed, the CAD Configuration Setup tool starts. See "CAD Configuration Setup Utility" on page 45 for instructions on configuring your system using this tool.

Modifying the Peripheral Gateway Registry

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

You must complete this modification after the CAD services and desktops have been installed.

To modify the PG computer registry key:

1. On the PG computer, open the Windows Registry Editor (regedit).
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.

CAD Configuration Setup Utility

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

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

- In Desktop Administrator, choose Setup > Configure Systems.
- On any CAD computer, run postinstall.exe, located in the folder C:\Program Files\Cisco\Desktop\bin.

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

- The host computer on which you launched CAD Configuration Setup
- The mode in which CAD Configuration Setup is running
- The services and applications that are running on the computer on which you launched CAD Configuration Setup

Table 10 lists all of the windows that are part of CAD Configuration Setup in alphabetical order. For each window, the table indicates whether that window appears when CAD Configuration Setup is run on the computer that hosts the named application or service. If you need to change a configuration setting, use the table to determine the computer on which you must run CAD Configuration Setup.

The table has the following columns:

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

Table 10. CAD Configuration Setup windows

Window Title	Mode	Base	VoIP	Rec	CAD CSD	CDA
CAD-BE Servers (page 51)	Update	×				
Unified Communications Manager (page 53)	Both	×	×			×

Table 10. CAD Configuration Setup windows

Window Title	Mode	Base	VoIP	Rec	CAD CSD	CDA
Unified CM SOAP AXL Access (page 55)	Both	×	×			×
CTI OS (page 56)	Both	×				×
CTI OS Security Setup (page 57)	Both				×	
CTI Server (Unified CM) (page 58)	Both	×				×
ICM Admin Workstation Database (page 60)	Both	×				
ICM Admin Workstation Distributor (page 62)	Both	×				
Recording and Statistics Service Database (page 64)	Both	×				
Replication Setup (page 65)	Both	×				
Restore Backup Data (page 66)	Both	×				
Services Configuration (page 67)	Update	×	×	×		
SNMP Configuration (page 68)	Update	×	×	×		
Terminal Services (page 69)	Both				×	
VoIP Monitor Service (page 70)	Update	×	×		×	

Entering Configuration Data in Initial Mode

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

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

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

> **NOTE:** Directory Services replication can be set up at a later time by running CAD Configuration Setup in update mode on the secondary base services computer and entering information in the Replication Setup window.

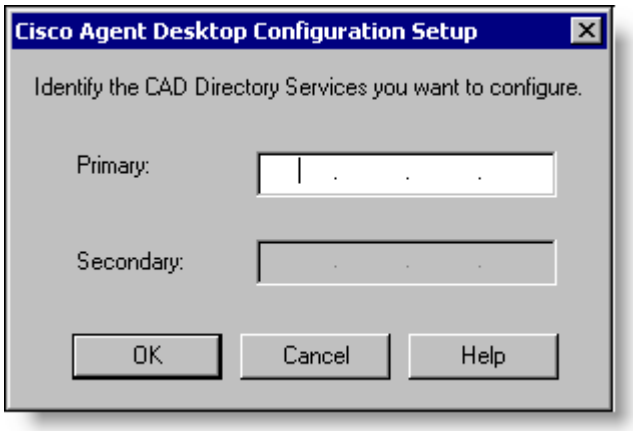
Configuring a Single or Primary Server in a Replicated System

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

To enter configuration data in initial mode on the primary base services computer:

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

Figure 5. CAD Directory Services dialog box



2. Enter the IP address of the primary Directory Services and then click OK.

3. If Configuration Setup does not detect that it is installed in a Unified System Contact Center (Unified SCC) Environment, a dialog box appears, prompting you to indicate whether this is a Unified SCC installation.
   - If you answer Yes, then default peripheral IDs are set to 1000, and agents and supervisor login by name becomes the only login option (login by login ID is disabled).
   - If you answer No, then peripheral IDs are set to 5000 and agents and supervisors can log in by login name or login ID. This option is configured later in Desktop Administrator.

   The Configuration Setup tool appears, with the Unified Communications Manager node selected.
4. Complete the fields in each window, using the right arrow on the toolbar to move forward to the next window.
   - You cannot move forward until all required information is entered.
   - You cannot skip a window.
   - You can go backwards at any time to revisit a previous window.
   - The Save button is not enabled until all windows are completed.
5. When you have completed all windows in the tool, click Save on the toolbar or choose File > Save.

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

   NOTE: The save process can take several minutes.

Configuring a Secondary Server in a Replicated System

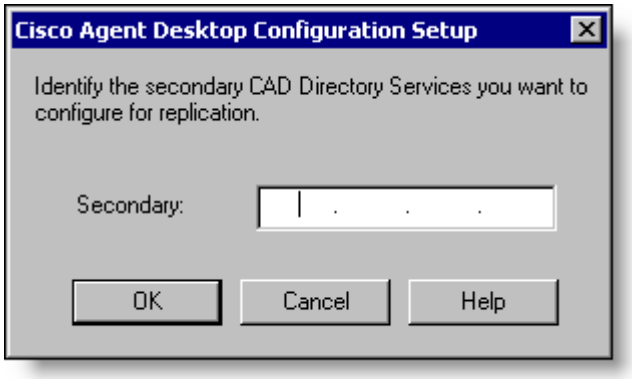
Complete the following procedure if you are running CAD Configuration Setup in initial mode on the secondary server in a replicated system.

To enter configuration data in initial mode on the secondary base services computer:

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

3. Click Yes. The Secondary Directory Services dialog box appears (Figure 6).

Figure 6. Secondary Directory Services dialog box



4. Enter the IP address of the secondary Directory Services, and then click OK. A confirmation dialog box appears, prompting you to indicate whether the primary and secondary IP addresses are correct.
5. Click Yes to set up replication. When replication is done, CAD Configuration Setup launches, with the Unified CM node selected.
6. Complete the fields in each window, using the right arrow on the toolbar to move forward to the next window.
   - You cannot move forward until all required information is entered.
   - You cannot skip a window.
   - You can go backwards at any time to revisit a previous window.
   - The Save button is not enabled until all windows are completed.
7. When you have completed all windows in the tool, click Save on the toolbar or choose File > Save. When the data is successfully saved, the program ends automatically.

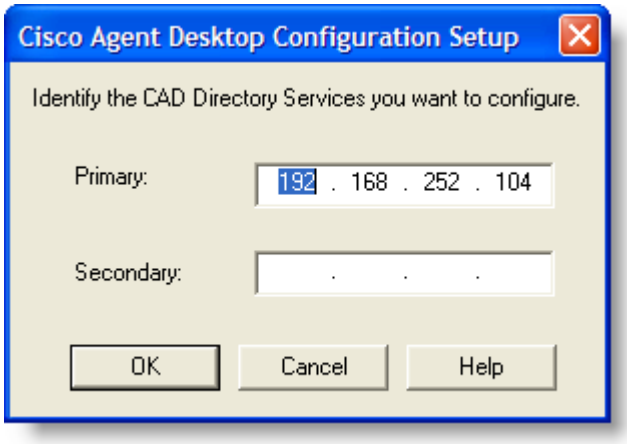
   NOTE: The save process might take several minutes.

Entering Configuration Data in Update Mode

To modify CAD configuration settings:

1. Start CAD Configuration Setup. CAD Configuration Setup starts and displays the CAD Directory Services dialog box.
   - In Desktop Administrator, select the logical contact center node in the left pane and then choose Setup > Configure Systems from the menu bar.
   - On another CAD host computer, navigate to the folder ...\Program Files\Cisco\Desktop\bin and double-click postinstall.exe.

Figure 7. CAD Directory Services dialog box



2. Verify that the primary (and optional secondary) IP addresses for Directory Services are correct, then click OK. CAD Configuration Setup launches with the Unified CM node selected.

   NOTE: To switch between the left and right pane, press F6. To move up and down the left pane, use the up and down arrows.

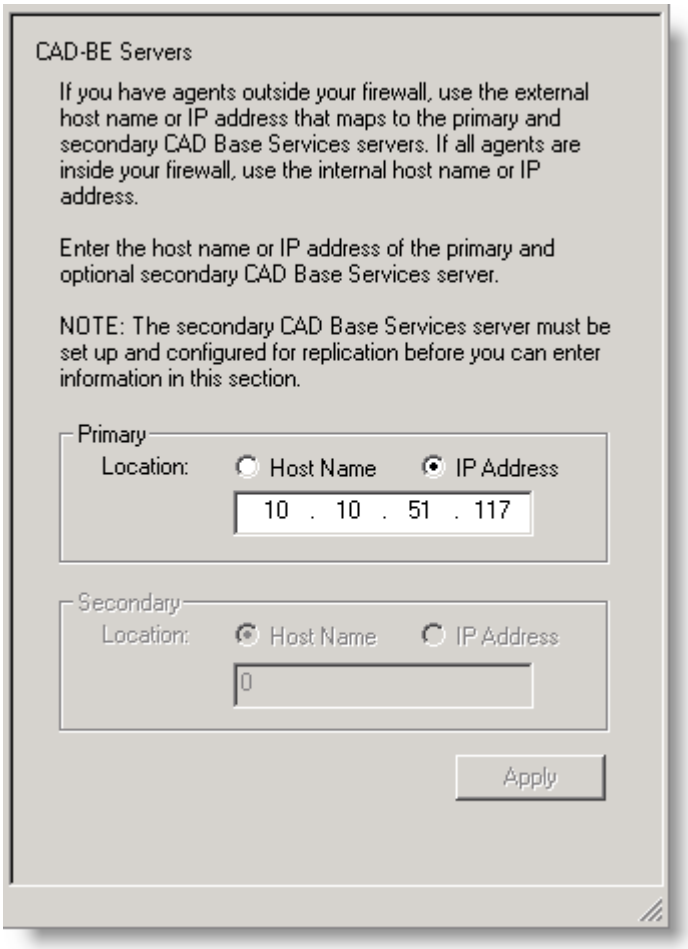
3. Select the node you want to modify from the left pane, enter the new data in the right pane, then click Apply.
   - You can display the nodes in any order you wish.
   - If you modify something in a node, you must click Apply to save your changes before you move on to another node.
4. When you are done making your changes, choose File > Exit or click Close. CAD Configuration Setup closes.
5. Restart the CAD services and all desktops for the change to go into effect.

CAD Configuration Setup Windows

This section describes the CAD Configuration Setup windows in alphabetical order.

CAD-BE Servers

Figure 8. CAD-BE Servers



The CAD-BE Servers window only appears in update mode.

In the Primary Location field, type the hostname or IP address of the CAD base services server. Tomcat, which is required to run CAD-BE, is installed on this server.

If some of your agents are outside your firewall, use the external hostname/IP address that maps to the servers. If all of your agents are inside your firewall, use the internal hostname/IP address.

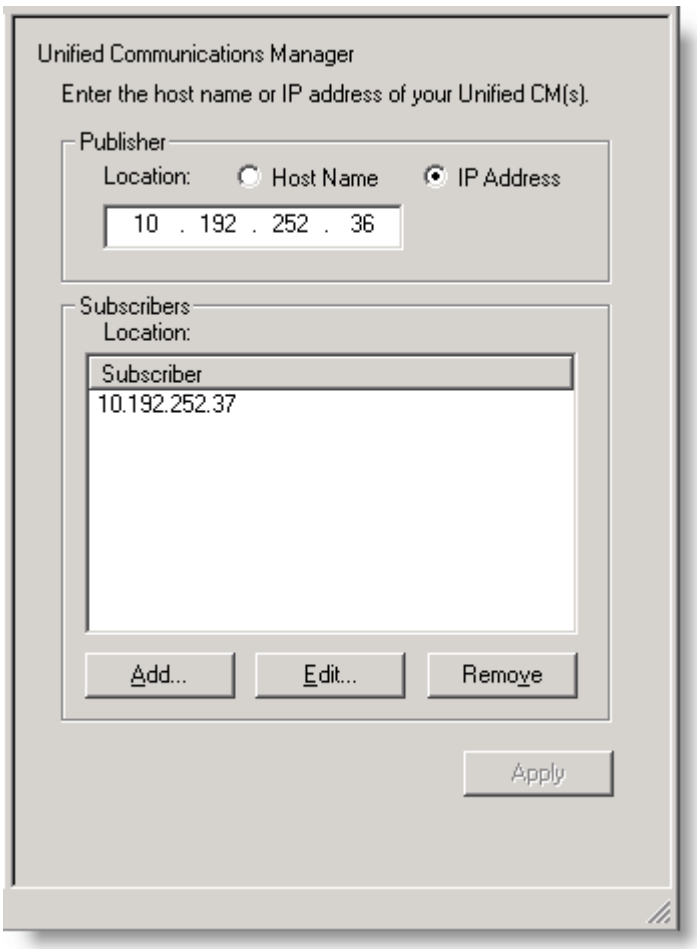
If your configuration includes a second server hosting the CAD base services, and you have configured replication between the two servers, type the location of the second server in the Secondary Location field.

NOTE: If you established replication in initial mode, the Secondary Location field is filled automatically.

NOTE: The Secondary Location is not enabled until you configure the second CAD base services server and establish replication.

Unified Communications Manager

Figure 9. Unified Communications Manager



The Unified Communications Manager window has two sections: the Publisher section and the Subscriber section. If you have only one Unified CM server, complete the Publisher section and leave the Subscriber section blank. If you have a Unified CM cluster, which consists of one publisher Unified CM server and one or more subscriber Unified CM servers, complete both sections.

To complete the Publisher section, select Hostname or IP Address. Then type the location of the Unified CM server (the publisher Unified CM server if you have a Unified CM cluster).

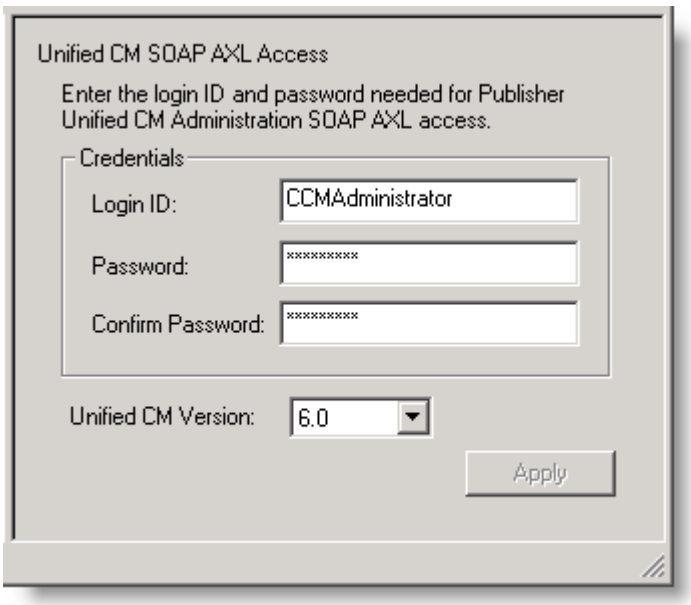
If you have a Unified CM cluster, add the locations of all of the subscriber Unified CM servers in the Subscribers section. To add a subscriber location, click Add. The Add/Edit Host dialog box appears. Enter the location of the subscriber Unified CM server in one of the following ways, then click Apply.

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

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

Unified CM SOAP AXL Access

Figure 10. Unified CM SOAP AXL Access

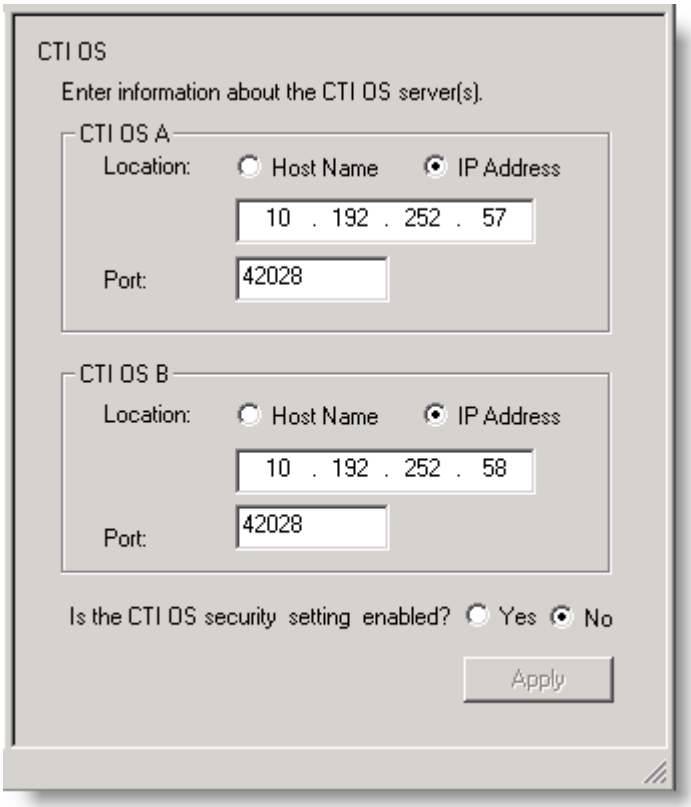


Enter the login ID and password required for the Publisher Unified CM Administration to access Unified CM SOAP AXL (Simple Object Access Protocol Administrative XML Layer). The login ID and password are the same used to access the Publisher Unified CM. Select the Unified CM version from the drop-down list.

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

CTI OS

Figure 11. CTI OS



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

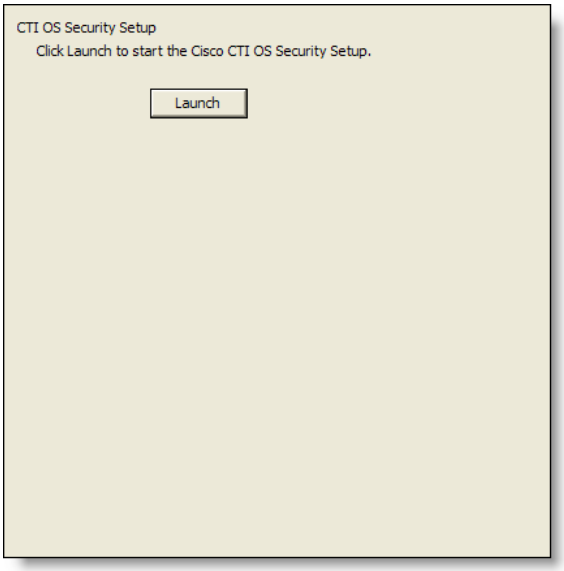
- If you have only one CTI OS, enter the information in the CTI OS A section.
- If you are also using a redundant CTI OS in a duplexed environment, enter the location of the redundant CTI OS in the CTI OS B section.

If you are running CAD Configuration Setup in upgrade mode, the following question appears: “Is the CTI OS Security Setting Enabled.” Select Yes or No. If you choose Yes, ensure that CTI OS security is enabled on the CTI OS server. Then follow the procedures in "Setting Up CTI OS Security" on page 107.

> **NOTE:** If you are running CAD Configuration Setup in initial mode (immediately after installation), the question does not appear.

CTI OS Security Setup

Figure 12. CTI OS Security Setup

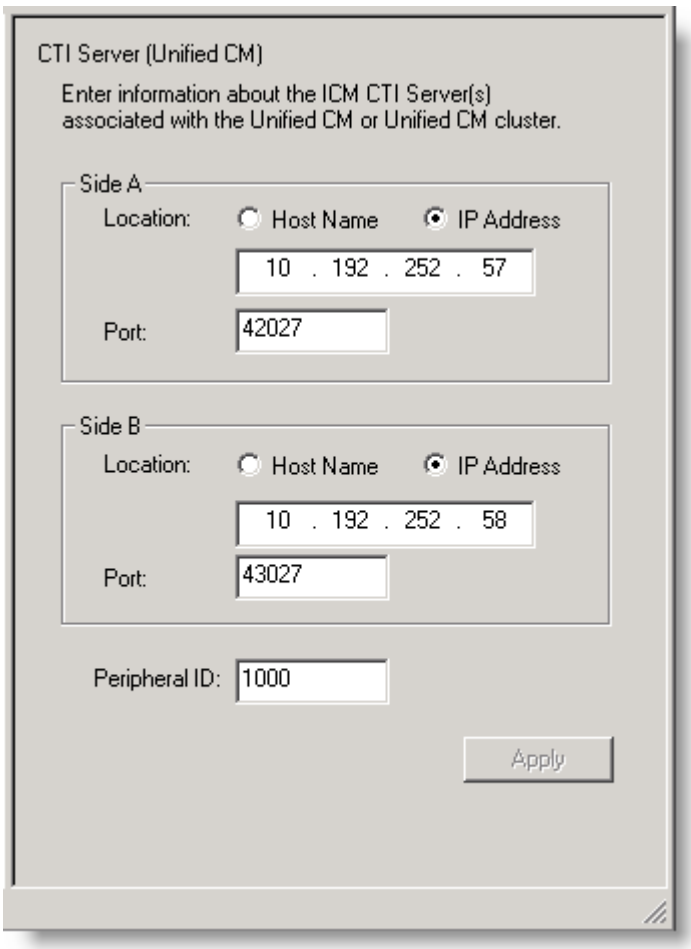


Click Launch to start the CTI OS Security Setup installation program and install the CTI OS Security client on the PC.

This window appears only if CTI OS Security is enabled for your system. For more information, see "Setting Up CTI OS Security" on page 107.

CTI Server (Unified CM)

Figure 13. CTI Server (Unified CM)



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

- If the CTI Server is entered with a hostname in Unified ICM, enter a hostname. If it is entered as an IP address, enter an IP address. Mixing hostname and IP address between Unified ICM and Configuration Setup can result in failing to display enterprise data in desktop applications.
- If you have only one Unified ICM CTI server, enter the information in the Side A section.
- If you are also using a redundant Unified ICM CTI server in a duplexed environment, enter the location of the redundant Unified ICM CTI server in the Side B section.

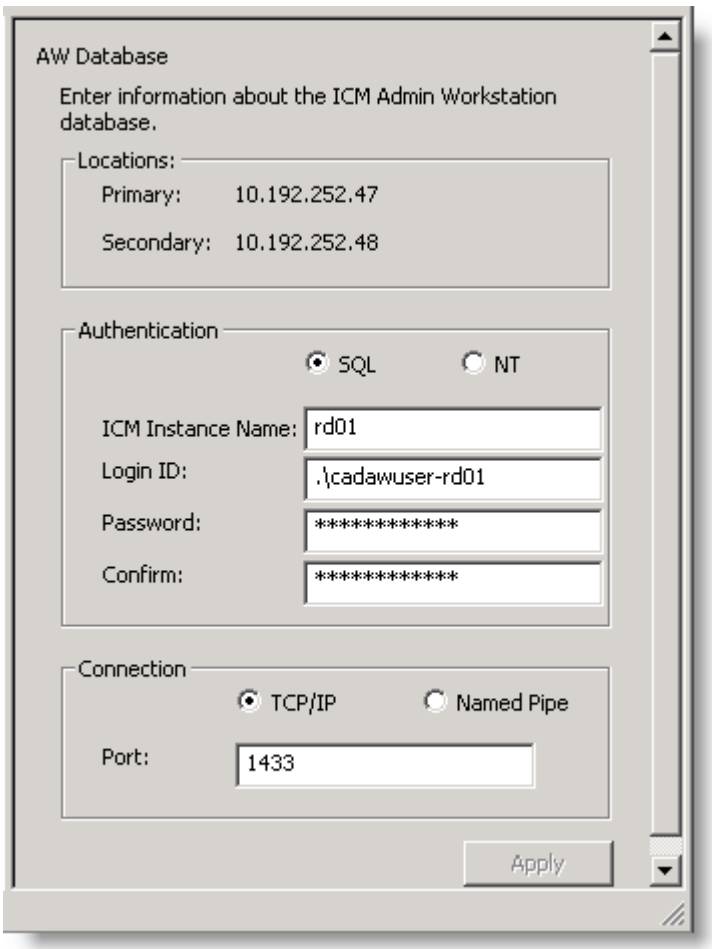
- The peripheral ID is used by services to filter information such as agents and skills. You can find the peripheral ID by using PG Explorer in the Unified ICM Configuration Manager.

  NOTE: If you change the peripheral ID, you must restart the Sync service, the Enterprise service, and the BIPPA service to ensure that the change is registered with them properly.

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

ICM Admin Workstation Database

Figure 14. ICM Admin Workstation Database



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

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

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

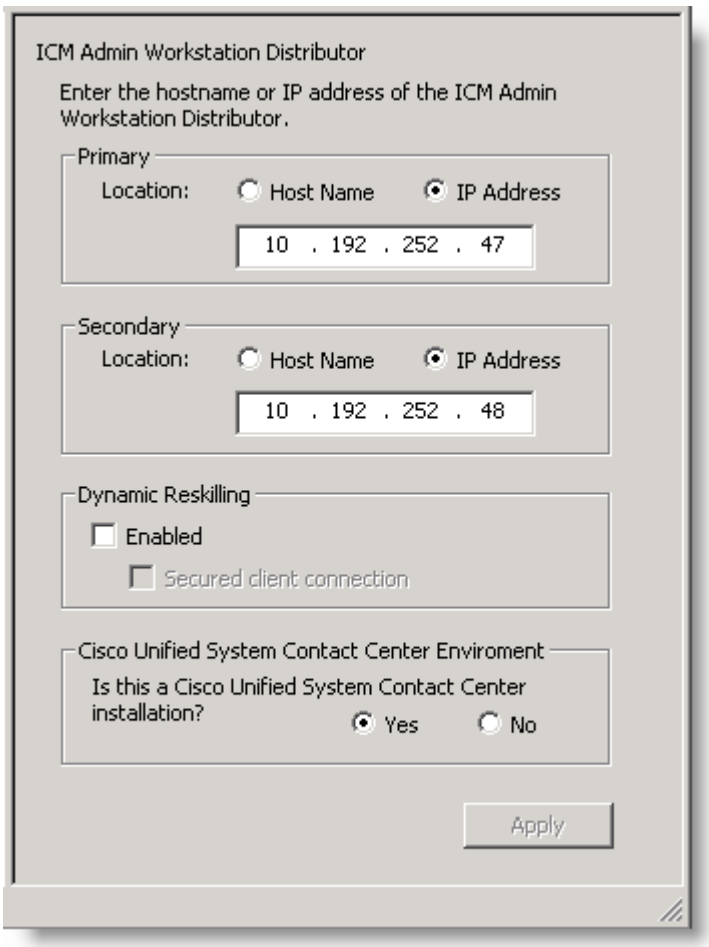
Select the connection type, TCP/IP or Named Pipes.

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

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

ICM Admin Workstation Distributor

Figure 15. ICM Admin Workstation Distributor



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

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

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

The Dynamic Reskilling and Cisco Unified System Contact Center Environment sections appear only if you are running CAD Configuration Setup in update mode.

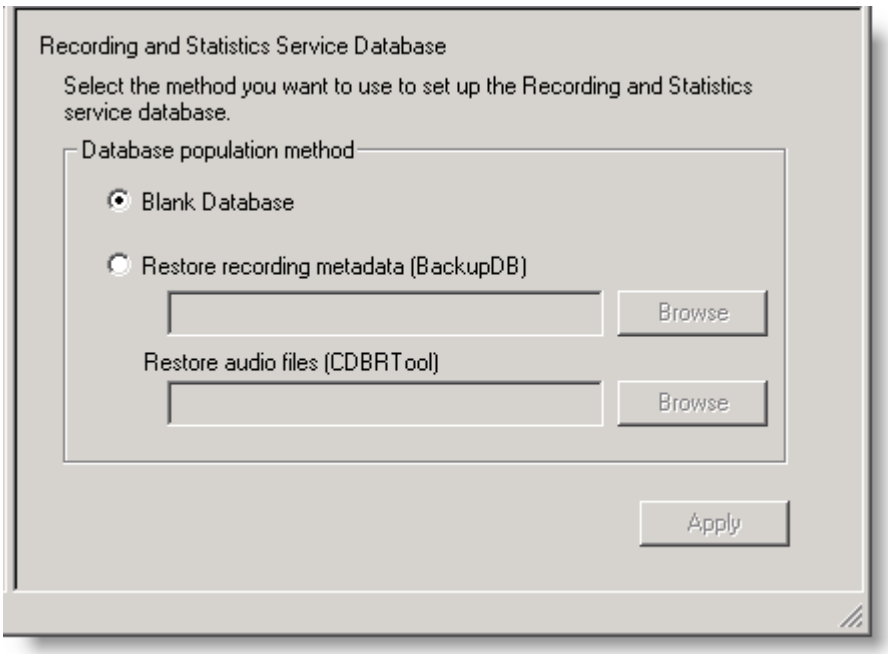
In the Dynamic Reskilling section, select the Enabled check box to enable supervisors to dynamically re-skill agents on their teams using the Unified Contact Center Enterprise Web Administration Agent Re-skilling tool. This tool is a web-based application. If it is located on a secured server and requires a secure socket URL (https), select the Secured client connection check box. If you leave this box unchecked, the URL will use the http prefix.

In the Cisco Unified System Contact Center Environment section, select Yes or No to indicate whether or not your configuration is running in a Unified System Contact Center (SCC) environment.

> **NOTE:** If CAD Configuration Setup does not detect that it is installed in a Unified SCC environment, a dialog box appears in initial mode, prompting you to indicate whether it is a Unified SCC environment.

Recording and Statistics Service Database

Figure 16. Recording and Statistics Service Database



This window appears in both initial and update modes. If you are running CAD Configuration Setup on the secondary server in a replicated system, this window does not appear, because the information was already entered on the primary system.

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

Select a method to set up the Recording and Statistics service database.

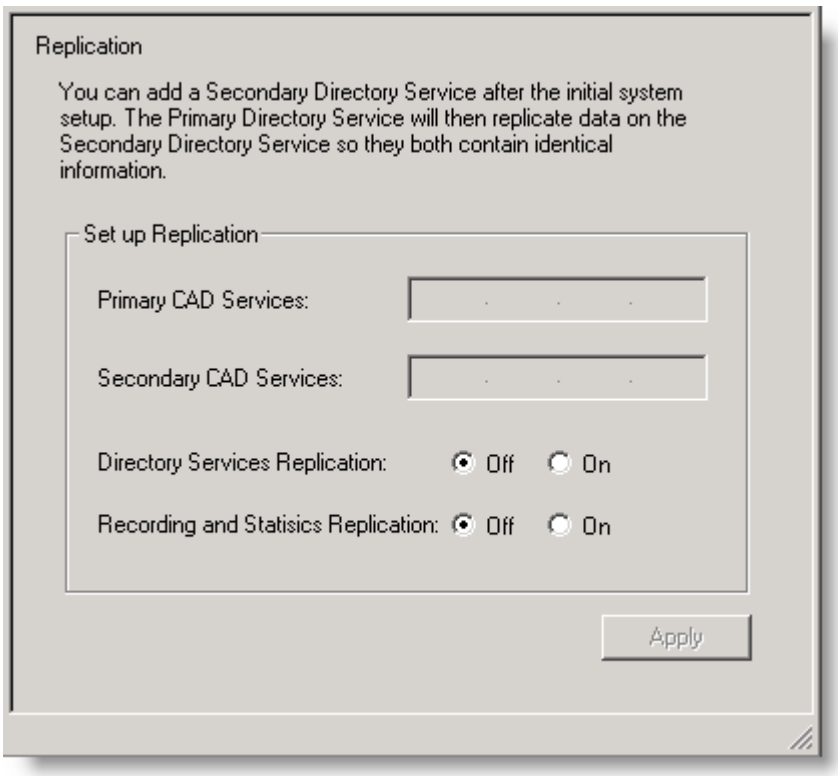
- Select Blank Database (default) if installing one service or a primary service in a replicated environment. This option creates the database schema.

  Select Restore From if you are restoring a previously backed-up database. If you are running CAD in a replicated environment, a message appears, reminding you to shut down replication before restoring data. After dismissing the dialog box, click Browse to navigate to the backup database created with the BackupDB and CDBRTool utilities. When you go to the next window, a message appears, reminding you to re-establish replication after the restore. For more information, see "Backup and Restore (BARS)" on page 90.

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

Replication Setup

Figure 17. Replication Setup



This window appears only when you run CAD Configuration Setup in update mode on the secondary CAD services server.

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

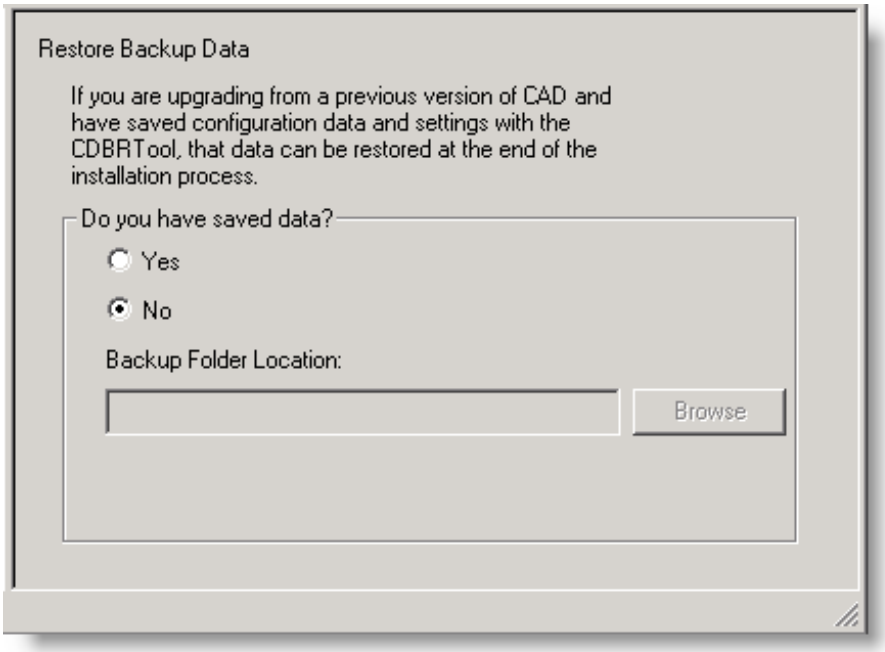
> **NOTE:** If you are setting up replication for Directory Services and/or the Recording and Statistics service, stop CSA on both computers.

To set up Directory Services replication, select On for Directory Services Replication, type the primary and secondary server IP addresses in the fields, then click Apply.

To set up Recording and Statistics replication, select On for Recording and Statistics Replication, type the primary and secondary server IP addresses in the fields, then click Apply. A dialog box appears, prompting you to type the primary server hostname for Recording and Statistics replication. Type the hostname, then click OK. Another dialog box appears, prompting you to type the secondary server hostname for Recording and Statistics replication. Type the hostname, then click OK.

Restore Backup Data

Figure 18. Restore Backup Data



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

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

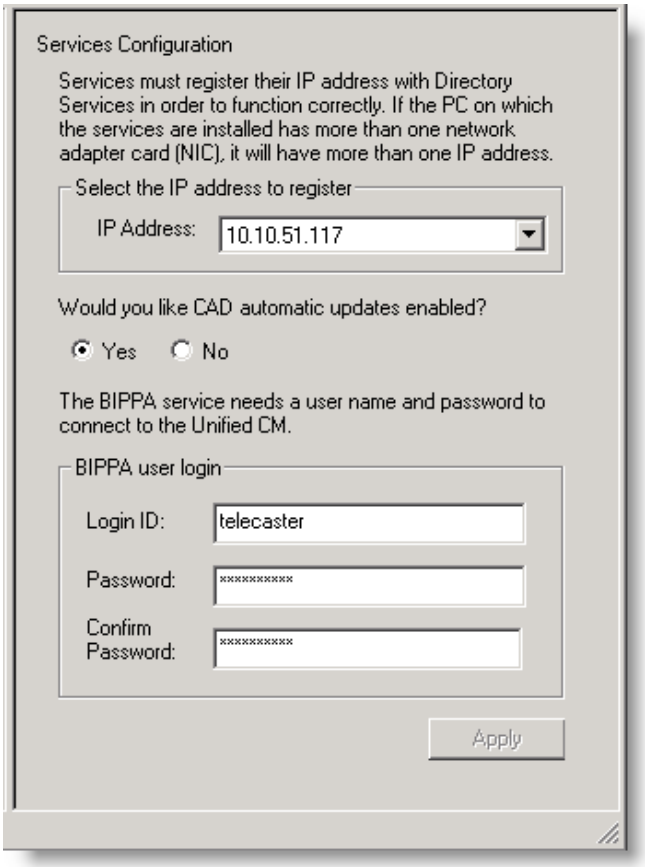
> **NOTE:** If you do not shut down replication before restoring your data, your database can become corrupted.

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

The tool used to save data is the CDBRTool utility. For information about using these tools, see "Upgrading From a Previous Version" on page 83.

Services Configuration

Figure 19. Services Configuration



The Services Configuration window only appears during update mode.

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

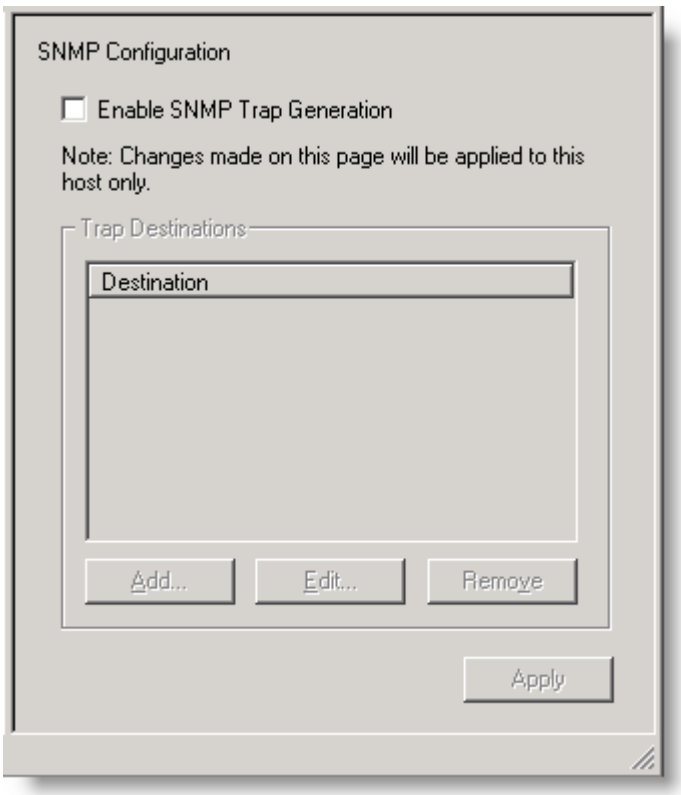
To enable CAD automated updates, select Yes. Automated updates cause Agent Desktop, Supervisor Desktop, and Desktop Administrator to look for newer versions every time they start. If one is found, the update process is run automatically.

To connect to Unified CM, the BIPPA service must have identical user IDs and passwords configured in this window and in Unified CM. You can complete the fields in this window before configuring the user in Unified CM. To configure credentials in Unified CM, see "Creating a Unified CM User" on page 103.

> **NOTE:** If you change any of these settings, you must restart all CAD services to ensure that the change is registered with them properly.

SNMP Configuration

Figure 20. SNMP Configuration



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

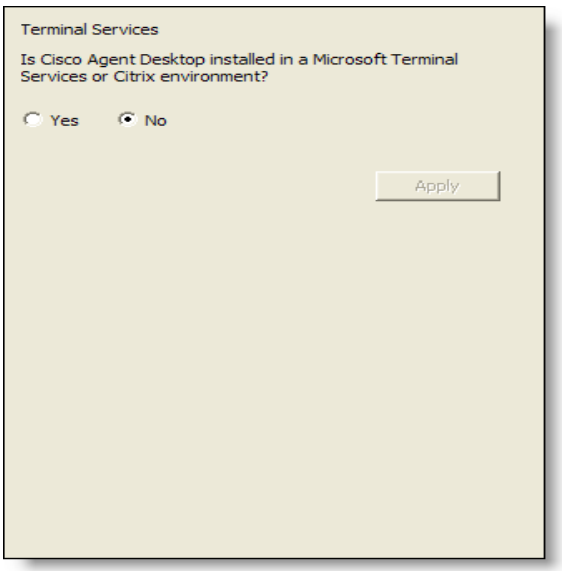
If you select the Enable SNMP Trap Generation check box, INFO and higher error messages are sent from the CAD services server to the IP addresses configured in the Destination pane. Use the Add, Edit, and Remove buttons to manage the list of destination IP addresses.

To install the SNMP service, open the Add or Remove Programs control panel, then click Add or Remove Windows Components. Select Management and Monitoring Tools from the list of components, then select Simple Network Management Protocol.

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

Terminal Services

Figure 21. Terminal Services

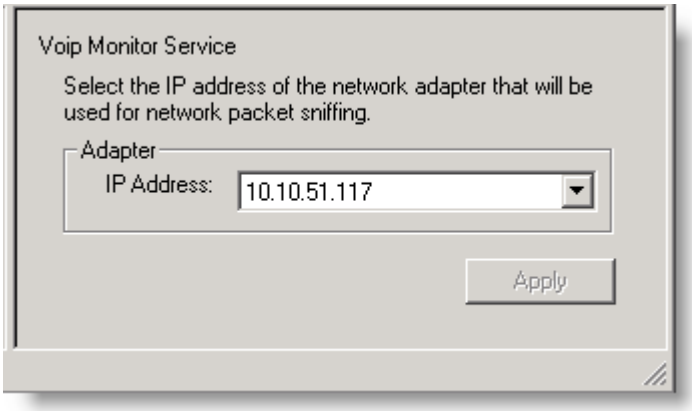


If this installation of CAD is installed in a Microsoft Terminal Services or Citrix environment, click Yes. If not, click No.

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

VoIP Monitor Service

Figure 22. VoIP Monitor Service



The VoIP Monitor service window only appears during update mode.

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

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

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

Desktop Monitoring Console

The Desktop Monitoring Console is a Java application that allows you to monitor the status of the CAD services and the LDAP Directory Services. It is installed automatically when the CAD base services are installed. To access the console, use the following URL, where <CAD server> is the IP address of the server on which the CAD services are installed.

http://<CAD server>:8088/smc/monitor.jsp

The CAD administrator can hyperlink this URL to the Unified CCE Configuration node in Desktop Administrator for easy access to Desktop Monitoring Console.

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

To install the Windows Management and Monitoring Tool component:

1. On the server where the CAD service(s) is installed, open the Windows Add or Remove Programs control panel.
2. From the button bar on the left of the Add or 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 or Remove Programs window.
6. Start the Administrative Tools control panel and select Services to display a list of available services.
7. Right-click SNMP Service and select Properties.
8. In the SNMP Service Properties window, select the Security tab.
   a. Under the Accepted Community Names section, click Add. The SNMP Service Configuration window opens.
   b. Select READ ONLY from the Community Rights drop-down list, type **public** in the Community Name field, then click Add. The public community is added to the Accepted Community Names section.

      NOTE: Community names are case sensitive. The word “public” must be all lowercase.
   c. Select one of the following SNMP options.
      — Accept SNMP Packets From Any Host

— Accept SNMP Packets From These Hosts

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

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

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

9. Click Apply to save your changes, then OK to close the window.

NOTE: After making any changes to the SNMP service, restart the service for the changes to take effect.

Licensing CAD 7.5

After you have installed and configured CAD, Unified CCE License Administration automatically starts. You can license your software at this point, or close the application and license your software later. Your CAD software will not run until you have licensed your CAD services. You can re-run Unified CCE License Administration whenever you want to update the number of seats you have purchased.

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

Obtaining a License Account

You must obtain a license account user ID and password to license your software.

To obtain a license account:

1. Open Internet Explorer.
2. Navigate to the following address:

   http://209.46.83.138/sws/WebLicensingInitial/InitialLicensePage.html
3. Click the Create a License Account hyperlink.
4. Complete the Partner License Request Form, then click E-mail Request. After your request is processed, your user ID and password will be emailed to you.

Using Unified CCE License Administration

If you are installing the CAD services on a computer running Windows Server 2003, Internet Explorer might display the following message and block you from accessing the website.

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

You must reconfigure Internet Explorer to enable access to the licensing website.

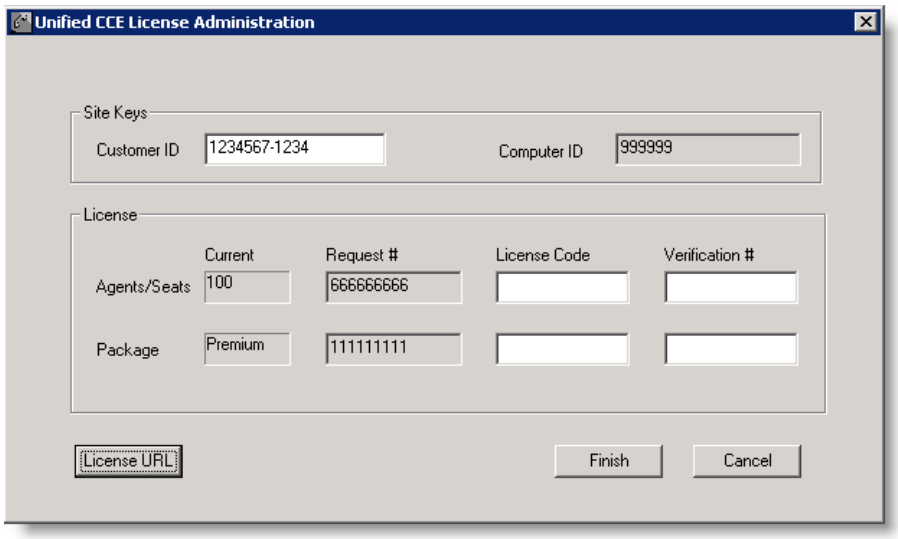
To enable access to the licensing web site:

1. Open Internet Explorer.
2. Choose Tools > Internet Options, then select the Security tab.
3. Select Trusted Sites, then click Sites.
4. Enter the URL of the licensing web site in the appropriate field, then click Add.
5. Clear the Require Server Verification (https:) For All Sites in This Zone check box, then click OK.

To license CAD 7.5:

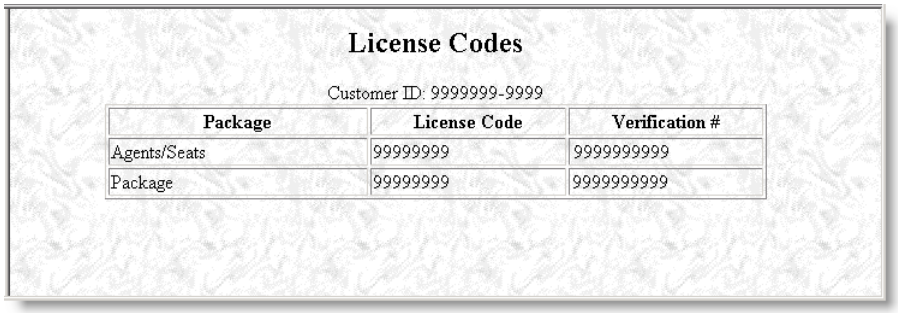
1. Launch LicenseAdmin.exe, in the folder ...\Program Files\Cisco\Desktop\bin. Unified CCE License Administration appears (Figure 23).

Figure 23. Unified CCE License Administration



2. Click License URL. Internet Explorer is launched and accesses the website at http://209.46.83.138/sws/ciscoLicense/LicenseRegister.html.
3. Follow the instructions on the website. All of the information is required.
4. Click Submit. The website displays a page listing the license codes and verification numbers you need to license your product (Figure 24).

Figure 24. License codes and verification numbers



License Codes

Customer ID: 9999999-9999

Package	License Code	Verification #
Agents/Seats	99999999	9999999999
Package	99999999	9999999999

5. Enter the License Codes and Verification numbers in Unified CCE License Administration, then click Finish. All of the licensed applications are activated.

Recording Licenses

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

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

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

If all licenses are in use:

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

Installing Desktop Applications

Desktop Administrator, Supervisor Desktop, and 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.

CAD-BE is a Java applet that runs on the server hosting the CAD base services. It is accessed by agents through their Windows Internet Explorer or Mozilla Firefox browser. The Java Runtime Environment (JRE) browser plug-in must be installed on each agent's computer.

> **NOTE:** You cannot install the desktop applications on the CAD server unless you are running CAD in a Citrix/MTS environment. For more information, see "Citrix and Microsoft Terminal Services Environments" on page 23.

Desktop users must have either administrator or elevated privileges to install the CAD desktop applications. If you want users with limited privileges to their computer to be able to install a desktop application, you must enable the Windows policy "Always Install with Elevated Privileges" on their computers. This also applies to installations pushed to the desktop via an automated package distribution tool. For more information about enabling this policy, see "Privileges" on page 36.

Client Installation Failure

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

To correct this problem, complete the following procedure.

> **NOTE:** In a redundant configuration, you must complete this procedure on the primary and secondary CAD base services servers.

To reconfigure CAD client installation programs:

1. Run CAD Configuration Setup on the CAD base services server (see "CAD Configuration Setup Utility" on page 45 for more information).
2. From the menu, choose File > Reset Client Installs. This process reconfigures the client installation programs.
3. When the process is complete, the message, "Client installs reset" is displayed. Click OK to close the message. You can now install the client applications from the installation web pages.

Error/Event and Debug Logs

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

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

Using Automated Package Distribution Tools

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

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

Installing Desktop Administrator

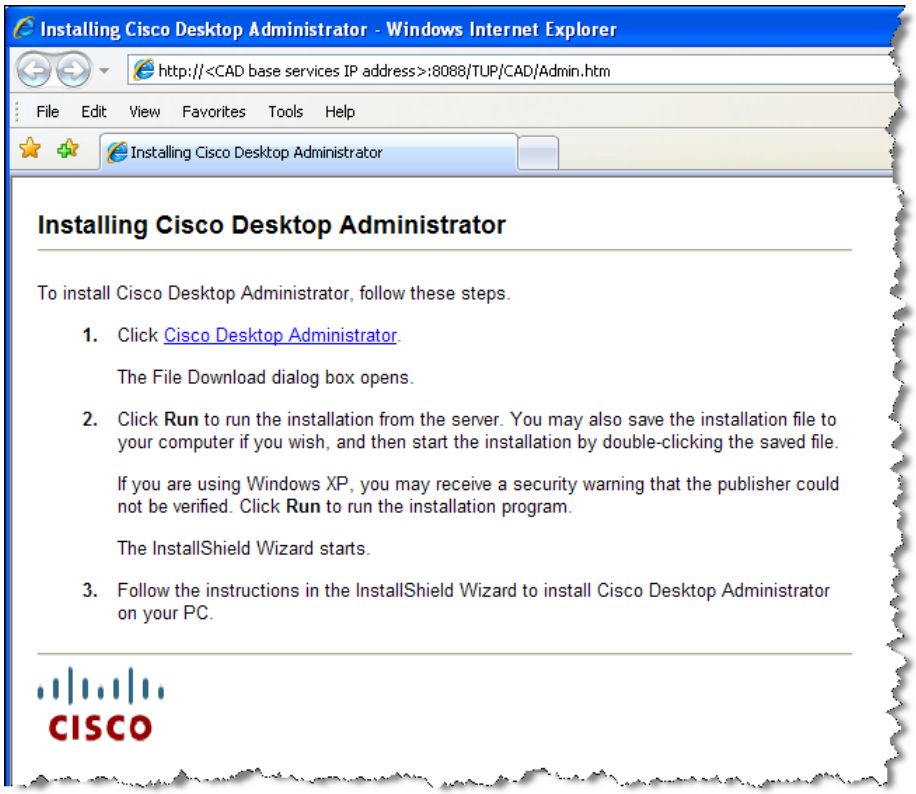
To install Desktop Administrator:

1. From the desktop on which you want to install Desktop Administrator, access the following URL, where <CAD server> is the IP address of the server on which the CAD base services are installed.

   http://<CAD server>:8088/TUP/CAD/Admin.htm

   The Cisco Desktop Administrator installation web page appears (Figure 25).

   Figure 25. Desktop Administrator Installation web page



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

Installing Agent Desktop and Supervisor Desktop

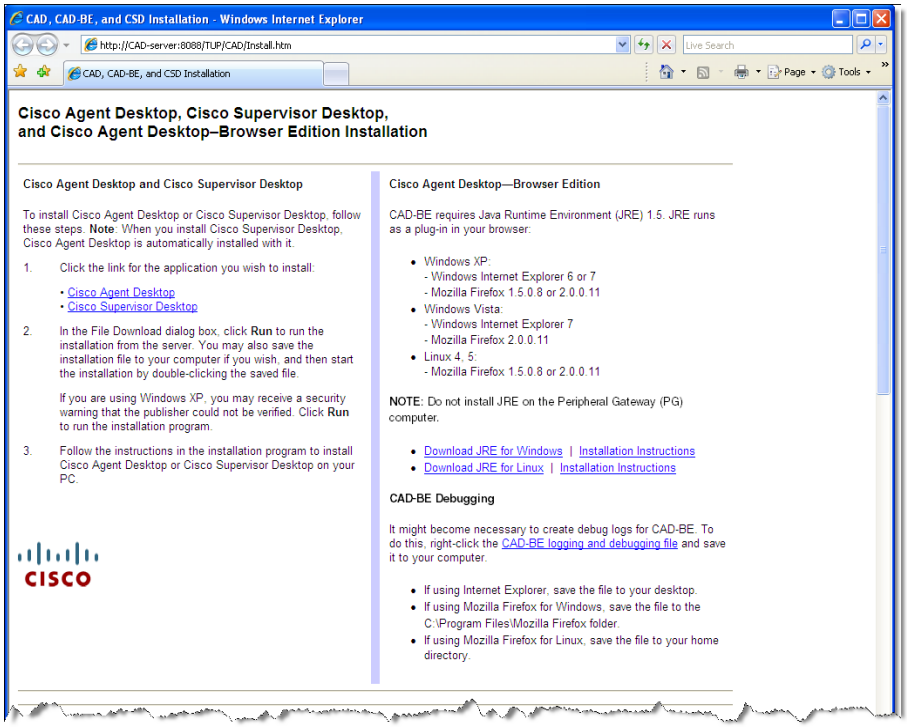
To install Agent Desktop and Supervisor Desktop:

1. From the desktop on which you want to install Agent Desktop or Supervisor Desktop, access the following URL, where <CAD server> is the IP address of the server on which the CAD base services are installed:

   http://<CAD server>:8088/TUP/CAD/Install.htm

   The Cisco Agent Desktop, Cisco Supervisor Desktop, and Cisco Agent Desktop—Browser Edition Installation web page appears (Figure 26).

   Figure 26. Agent Desktop, Supervisor Desktop, and CAD-BE installation web page



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

Installation Notes

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

Configuring CAD-BE

The CAD-BE Java applet is installed when the BIPPA service is installed, on the same computer as the BIPPA service.

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

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

To install the JRE plug-in:

1. From the desktop where you wish to install the JRE plug-in, access the following URL, where <CAD server> is the IP address of the server on which the CAD base services are installed:

   http://<CAD server>:8088/TUP/CAD/Install.htm

1. The Cisco Agent Desktop, Cisco Supervisor Desktop, and Cisco Agent Desktop—Browser Edition Installation web page appears (Figure 26).
2. From the CAD-BE section, download the appropriate version of JRE for your operating system (Windows or Linux).
3. Click the appropriate installation instructions hyperlink and complete the procedure that corresponds to your operating system.

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

Internet Explorer Settings for CAD-BE

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

Pop-up Blocker

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

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

OR

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

Internet Options

Set the following internet options:

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

Internet Explorer 7 Security Feature

Internet Explorer 7 has a security feature that places a non-editable address bar directly below the title bar in the CAD-BE interface.

To remove the address bar perform the following:

1. Choose Tools > Internet Options.
2. Select the Security tab and select either the Local intranet zone or the Trusted sites zone.
3. Click Sites, then click Add. This adds the CAD-BE web site to the zone you selected. (The Local intranet and Trusted sites zones have the setting “Allow websites to open windows without address or status bars” enabled.

Firefox Settings for CAD-BE

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

> **NOTE:** The Preferences window in Firefox for Linux is the same as the Options window in Firefox for Windows. To access Preferences in Firefox for Linux, choose Edit > Preferences.

Popup Blocker

You can either disable the pop-up blocker or create an exception to enable pop-ups from the CAD server.

To disable the pop-up blocker:

1. Choose Tools > Options > Content.
2. Deselect Block Popup Windows.

To create an exception to enable pop-ups from the CAD server:

1. Choose Tools > Options > Content.
2. Click Allowed Sites and add the IP address(es) of the CAD server to the list of allowed sites.

Content Settings

Configure the following settings:

1. Choose Tools > Options > Content, and select the following check boxes:
   - Enable Java
   - Enable JavaScript
2. Next to the Enable JavaScript check box, click Advanced and select these check boxes in the Advanced JavaScript Settings dialog box:
   - Raise or lower windows
   - Disable or replace context menus
3. In the browser address field, type the following:

   ```
   about:config
   ```
4. Locate the preference dom.allow_scripts_to_close_windows.
5. Right-click the preference and select Toggle to set the value to True.

Upgrading From a Previous Version

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

If you are upgrading to CAD 7.5 from CAD 6.0(2) or higher, you must complete the following steps in the order shown.

1. Back up your configuration data using the CAD backup and restore utilities for the version you are upgrading.
2. Uninstall the previous version of CAD.
3. Install CAD 7.5 and restore the data you backed up during the installation.

If you are upgrading to CAD 7.5 from CAD 7.0, 7.1, or 7.2, you can install CAD 7.5 directly over the previous version. You can also upgrade an older version of CAD 7.5 to the current CAD 7.5 version by installing the current version over the previous version.

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

NOTE: In CAD 7.1 or higher, reason codes are created and maintained in Unified ICM. Any reason codes that you created using Desktop Administrator in previous versions of CAD will be lost in an upgrade. To continue using previously-created reason codes, re-create them in Unified ICM.

The backup and restore utilities used in the following upgrade procedures are described in detail in "Backup and Restore (BARS)" on page 90.

NOTE: You must use the utilities from the version you are backing up. For example, if you are upgrading from CAD 6.0(2) to CAD 7.5, use the CAD 6.0(2) utilities, not the CAD 7.5 utilities.

Previous Version Hot Fixes and Service Releases

If you have any CAD hot fixes or service releases for previous versions installed, uninstall them before upgrading to CAD 7.5.

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

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

For instance,

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

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

- CAD Service Release
- CAD Clients Service Release

Changing Feature Levels in an Upgrade

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

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

As a best practice, after you change feature level, back up your system at the new feature level. Then, delete any backups you made before changing the feature level.

For information on the features provided at each feature level, see "CAD 7.5 Feature Levels" on page 11.

To change feature levels in an upgrade:

1. On the computer that hosts the CAD services, navigate to the folder C:\Program Files\Cisco\Desktop\bin.
2. Run LicenseAdmin.exe to start Unified CCE License Administration.
3. In the Unified CCE License Administration window, click License URL. Your web browser starts and opens the secured licensing website at http://209.46.83.138/sws/ciscoLicense/LicenseRegister.html.

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

   NOTE: You must enter 0 in the customer ID field, even if you already have a customer ID number.

5. Enter the product information. This includes the new package (feature level) you have purchased.
6. Continue through the licensing process (see "Licensing CAD 7.5" on page 73).
7. When licensing is completed, restart the BIPPA service.

Upgrading from CAD 6.0(2) to CAD 7.5

If you are upgrading a single server:

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

If you are upgrading a replicated system:

- Shut down replication on both servers before beginning the following procedure. For instructions, see "Shutting Down Replication in CAD 7.1 and before" on page 99.
- Complete steps 1-5 on the primary server and the remaining steps on the secondary server.

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

To upgrade from CAD 6.0(2) to CAD 7.5:

1. Back up your CAD 6.0(2) LDAP configuration data, recordings, and Cisco Recording and Statistics Service database.
   a. Back up your LDAP configuration data and recordings by running CDBRTool twice. For instructions, see "CDBRTool Utility" on page 93.
   b. Back up your Recording and Statistics database using BackupDB. For instructions, see "BackupDB Utility" on page 91.

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

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

2. Uninstall CAD 6.0.
3. Install CAD 7.5. After the installation finishes, CAD Configuration Setup starts automatically.
4. In CAD Configuration Setup, complete the data entry windows as described in "Configuring a Single or Primary Server in a Replicated System" on page 47.
   a. In the Recording and Statistics Service Database window, select Restore From and enter the location to which you backed up the database in step 1b. Then click Apply to restore the database.
   b. In the Restore Backup Data window, enter the location to which you backed up the CAD services LDAP configuration data (see "Restore Backup Data" on page 66). Then, click Apply to restore the CAD services LDAP configuration data.
   c. Exit CAD Configuration Setup.
5. Restore your recording backups using CDBRTool. For instructions, see "CDBRTool Utility" on page 93.
   - If you are upgrading a single server, you have completed the upgrade.
   - If you are upgrading a replicated system, complete the remaining steps on the secondary server.
6. Log onto the secondary server.
7. Uninstall CAD 6.0.
8. Install CAD 7.5. After the installation finishes, CAD Configuration Setup starts automatically.
9. In CAD Configuration Setup, complete the data entry windows as described in "Configuring a Secondary Server in a Replicated System" on page 48.
10. After you complete all of the data entry windows and exit CAD Configuration Setup, the upgrade on both servers is done and replication is re-established.
11. After the upgrade on both servers is complete, restart the LDAP Monitor service on both servers.

Upgrading from CAD 7.0 or higher to CAD 7.5

NOTE: When you upgrade from CAD 7.0 or higher to CAD 7.5, the install process automatically backs up your CAD services LDAP configuration data. It is a good idea, however, to back up your data manually as well. For instructions, see "CDBRTool Utility" on page 93 and "BackupDB Utility" on page 91.

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

If you are upgrading a single server:

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

If you are upgrading a replicated system:

- Shut down replication on both servers before beginning the following procedure. For instructions, see "Shutting Down Replication in CAD 7.1 and before" on page 99.

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

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

To upgrade from CAD 7.0 or higher to CAD 7.5:

1. Install CAD 7.5. After the installation finishes, CAD Configuration Setup starts automatically.
2. In CAD Configuration Setup, verify that the data is correct in the data entry windows as described in "Configuring a Single or Primary Server in a Replicated System" on page 47.
   a. In the Recording and Statistics Service Database window, leave Blank Database selected. Your recording and statistics data will be restored automatically. A new database will not be configured.
   b. In the Restore Backup Data window, leave No selected. Your CAD LDAP configuration data will be restored automatically.
   c. Exit CAD Configuration Setup.
      - If you are upgrading a single server, you have completed the upgrade.
      - If you are upgrading a replicated system, complete the remaining steps on the secondary server.
3. Log onto the secondary server.
4. Install CAD 7.5. After the installation finishes, CAD Configuration Setup starts automatically.
5. In CAD Configuration Setup, complete the data entry windows as described in "Configuring a Secondary Server in a Replicated System" on page 48.
6. After you complete all of the data entry windows and exit CAD Configuration Setup, the upgrade is done and replication is re-established.
7. After the upgrade on both servers is complete, restart the LDAP Monitor service on both servers.

Upgrading CAD 7.5 to a Newer Version

CAD 7.5 can be upgraded to a newer version of CAD 7.5 by installing the new version over the old version. Configuration data and recordings are preserved during the upgrade and do not need to be backed up.

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

Rolling Back CAD 7.5 to an Earlier Version of CAD

To use the following procedure, you must have backed up your original version of CAD before installing CAD 7.5.

To uninstall CAD 7.5 and revert to an earlier version of CAD:

1. If you are rolling back CAD 7.5 on a replicated system, shut down replication now. For instructions, see "Shutting Down and Restarting Replication" on page 96.

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

2. Uninstall CAD 7.5.
3. Install your previous CAD version according to the product documentation.
4. Restore your backed-up data using the CAD Configuration Setup tool:
   - The configuration data backed up with CDBRTool or DABackupTool is restored by entering the location of the backup file in the Restore Backup Data window.
   - The Recording and Statistics database backed up with BackupDB is restored by selecting “Restore From” and entering the location of the backup file in the Recording and Statistics Service Database window.
5. If you are rolling back a replicated system, re-establish replication. For instructions, see "Shutting Down and Restarting Replication" on page 96.

Upgrade Notes

- Any work sites configured for the Agent Desktop integrated browser in CAD 6.0(2) or 7.0 will become work flow browser tabs in CAD 7.5, The first tab, which is reserved for a supervisor push page, is automatically set to www.cisco.com.
- Any reason codes created using Desktop Administrator in previous versions of CAD 7.1 or older will be lost after upgrading to CAD 7.5. All reason codes are created and maintained in Unified ICM in CAD 7.5. To continue using the reason codes created in previous versions, ensure they are set up in Unified ICM.
- All reserved reason codes are automatically enabled in CAD 7.5.
- Phone books from previous CAD versions will be saved as global phone books in CAD 7.5.
- Wrap-up data from previous CAD versions will be enabled at the work flow group level and disabled at the global level. It can be enabled later at the global level as needed.
- If you changed the IP address of any server in your configuration after you backed up data, you must run CAD Configuration Setup and enter the current IP addresses after you have restored your data, because the old IP addresses will be restored.

Backup and Restore (BARS)

This section describes how to back up and restore CAD configuration settings and recordings using the CAD backup and restore (BARS) utilities. For the most up-to-date information on BARS procedures and utilities, see the Release Notes.

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

NOTE: You must use the utilities that were provided with the version of CAD you are backing up and with the version of CAD to which you are restoring the data. For example, if you are upgrading from CAD 6.0(2) to CAD 7.5, you must use the CAD 6.0(2) utilities to back up data, and the CAD 7.5 utilities to restore data.

Backup File Location

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

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

Backing Up CAD Data

Backups are recommended to protect your CAD 7.5 configuration settings and recordings. Use the following procedures for backing up your system. Best practice is to perform backups during down times when all agents are logged out.

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

To back up CAD data:

1. On the server hosting the CAD base services, run CDBRTool to back up the configuration data and/or recordings (see "CDBRTool Utility" on page 93).
2. On the server hosting the Recording and Statistics service, run the BackupDB utility to back up recording metadata (see "BackupDB Utility" on page 91).

   NOTE: To prevent potential file permission issues upon restore, save Recording and Statistics service database backup files to a local drive. If desired, copy the backup files to a secure location elsewhere.

Restoring CAD Data

The process for restoring your CAD configuration data and recordings is outlined here. After you have upgraded or reinstalled the CAD services, CAD Configuration Setup runs. Part of CAD Configuration Setup is restoring backed-up data.

To restore CAD data if you are upgrading to CAD 7.5 or reinstalling CAD 7.5:

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

   This restores the recording metadata and recordings. See "Recording and Statistics Service Database" on page 64 for more information.
2. In the Restore Backup Data window, answer Yes and enter the path where the backup files created by the CDBRTool utility are saved.

   This restores the CAD services LDAP (Directory Services) database. (See "Restore Backup Data" on page 66 for more information.)

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

To restore CAD data if you are restoring a backup of an existing CAD 7.5 installation:

1. On the server hosting the CAD base services, run the CDBRTool utility (see "CDBRTool Utility" on page 93). The CAD services LDAP configuration data and the recordings are restored.
2. On the server hosting the Recording and Statistics service, run the InstallRestoreDB utility (see "InstallRestoreDB Utility" on page 93). The recording metadata is restored.

BackupDB Utility

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

using the CDBRTool utility. See "CDBRTool Utility" on page 93 for more information.

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

To run BackupDB:

1. Log in to the server hosting the Recording and Statistics service.

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

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

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

   Use the following values.

<dbUser>	Any value may be used.
<dbPassword>	Any value may be used.
<server>	The hostname of the server on which the database is located, or the local loopback IP address of 127.0.0.1.
<dir>	The absolute path for the directory in which the backup file is to be saved. <dir> must be a local drive. The quotation marks are necessary only if the path has spaces in it. **NOTE:** The directory must exist before you run this command or it will fail.

4. Press Enter. The utility backs up the database to a file named Cadbkp.dat in the folder you specified. The results of running the utility are written to a log file named db.backup.fcrassvr.sql.log in C:\temp.

InstallRestoreDB Utility

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

To run InstallRestoreDB:

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

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

2. Navigate to the folder where InstallRestoreDB.bat is located. The default location is C:\Program Files\cisco\Desktop\DB.
3. On the command line, type:

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

   where:

   <userID> is the user ID for the destination database. The default is **sa**.

   <password> is the destination database password. The default is **sa**.

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

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

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

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

4. Press Enter. The recording metadata is restored to the specified database.

CDBRTool Utility

The CDBRTool utility backs up the following data:

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

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

NOTE: If it is a redundant system, both Directory Services sides must be running in order for the CDBRTool utility to run correctly.

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

If you are running CDBRTool on a replicated system:

- Shut down replication on both servers before beginning the following procedure. When you have completed the procedure, restart replication. For instructions, see "Shutting Down and Restarting Replication" on page 96.

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

To run CDBRTool:

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

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

   where:

   <switches> is one of the switch combinations listed in Table 11 below

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

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

Table 11 lists permissible switch combinations and their meaning.

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

Table 11. CDBRTool switches

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

BARS Notes

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

Shutting Down and Restarting Replication

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

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

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

If you are shutting down replication because you are upgrading from a version of CAD 7.1 or earlier, complete the shutdown procedure in "Shutting Down Replication in CAD 7.1 and before" on page 99.

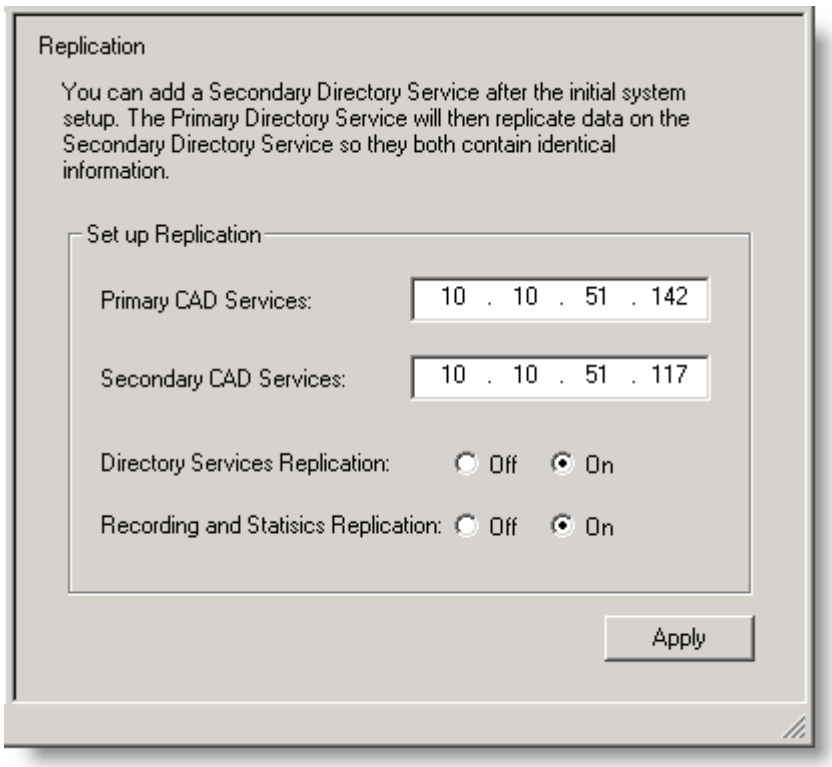
NOTE: If you are setting up replication for Directory Services and/or the Recording and Statistics service, make sure that Cisco Security Agent is stopped on both computers.

Shutting Down Replication in CAD 7.5 and 7.2

To shut down replication in CAD 7.5 and 7.2:

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

Figure 27. Replication Setup window



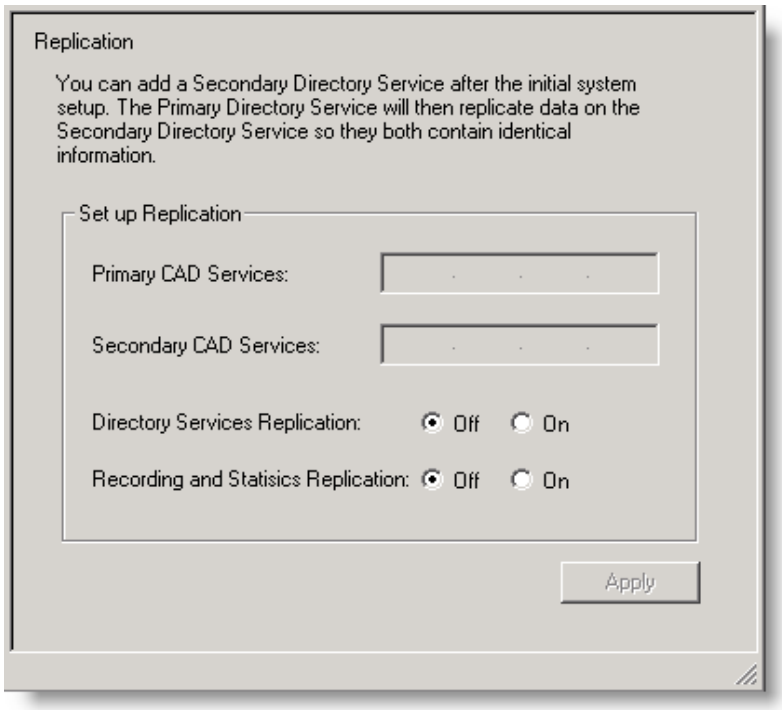
5. In the Replication Setup window, select Off for both services.
6. Click Apply and exit CAD Configuration Setup. Replication is now shut down.

Restarting Replication in CAD 7.5 and 7.2

To restart replication in CAD 7.5 and 7.2:

1. Log into either the primary or the secondary server.
2. In Windows Explorer, navigate to C:\Program Files\Cisco\Desktop\bin. This is the default location for CAD utilities.
3. Run postinstall.exe to start CAD Configuration Setup.
4. Select the Replication Setup window (Figure 28).

Figure 28. Replication Setup window



5. In the window, select On for the service(s) you want to replicate. Then enter the IP addresses of the primary and secondary servers.
6. Click Apply. Replication is now re-established between the primary and secondary servers.

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

Shutting Down Replication in CAD 7.1 and before

To shut down replication in CAD 7.1 and before:

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

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

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

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

Configuring IP Phones for IP Phone Agent

After all IP agent phones are added to Unified CM, you must complete the following tasks in Unified CM Administration. You can complete these procedures before or after CAD has been installed on your system.

1. Create an IP phone service.
2. Assign the IP phone service to each IP agent phone.
3. Create an application user and assign to it all the IP agent phones. Use the name “telecaster” with a password of “telecaster” or the BIPPA user ID and password that was specified in CAD Configuration Setup.

   NOTE: If you are using Active Directory 2003 on the machine hosting Unified CM and password complexity is enabled, the default “telecaster” password is not valid because it does not contain any capital letters or numbers. You will need to change the Unified CM user password in CAD Configuration Setup.

4. If desired, change the default URL Authentication parameter.
5. If desired, configure a one-button login for IP phone agents.

Creating an IP Phone Service

Complete the following steps to create a new IP phone service. If you have a redundant system, create two IP phone services, one for each CAD server.

To create a new IP phone service:

1. Log into Unified CM Administration.
2. Choose Device > Device Settings > Phone Services. The Find and List IP Phone Services page appears.
3. Click Add New. The IP Phone Services Configuration page appears.
4. Enter the following information:

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

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

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

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

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

where:

- 192.168.252.44 is the IP address of the machine on which the BIPPA service is installed
- 8088 is the Tomcat webserver port (if 8088 is not the port number, look in 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 on which the BIPPA service is loaded

NOTE: This folder does not contain IPAgentInitial.jsp, but rather IPAgentInitial.class, which has the implementation of the .jsp file.

NOTE: The Tomcat webserver is included with the installation.

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

Assigning the IP Phone Service to IP Agent Phones

After you create the IP phone service, you must assign it to each agent's phone.

To assign the IP phone service to an agent's phone:

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

Configuring IP Phones for Use with a Localized BIPPA Service

If a contact center is using a non-English language version of CAD, the BIPPA service will be displayed on the agent's IP phone in that non-English language (see "Localization" on page 20 for a list of supported languages). The phone does not need to be configured for the chosen locale. However, in this situation, the IP phone itself will display in English, the default locale for the phone, while the BIPPA service displays in the non-English language.

In order for the IP phone itself to display in the non-English language, you can configure the Unified CM one of two ways:

- On the enterprise level, so that all IP phones controlled by that Unified CM display in the selected language
- On the phone device level, so that individual IP phones can display in a language that is not the default language

To assign a locale at the enterprise level:

1. On the System menu, choose Enterprise Parameters. The Enterprise Parameters Configuration page appears.
2. In the Localization Parameters section, select a language from the drop-down lists in the Default Network Locale and Default User Locale fields.
3. Click Save.

To assign a locale at the phone device level:

1. On the Device menu, choose Phone. The Find and List Phones window appears.
2. Use the search function to find the phone. Search results are listed at the bottom of the page.
3. Locate the phone in the list of results and click the hyperlink. The Phone Configuration page appears.
4. In the User Locale field, select a language from the drop-down list.
5. Click Save.

Creating a Unified CM User

The next task to accomplish is to create a Unified CM user, and then add the Unified CM user to the Standard CTI Enabled group. The Unified CM user is used by the BIPPA service to push pages to agent IP phones.

> **NOTE:** The Unified CM user ID and password are also entered in CAD Configuration Setup and must match what is configured in Unified CM. If you change them in Unified CM, you must also change them in CAD Configuration Setup. See "Services Configuration" on page 67 for more information.

To create the Unified CM user:

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

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

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

Changing the Default Authentication URL

The default URL used for authentication is the best setting for most contact centers. If your contact center needs IP Phone Agent screens to be refreshed more quickly, changing the default URL to the IP Phone Agent authentication URL on the CAD server might provide better performance with IP Phone Agent. Note that improved performance is not guaranteed, however, and other applications that use this URL for authentication might even slow down.

> **NOTE:** If either the CAD server is down or the Tomcat service (which runs on the CAD server) is down, authentication will fail.

You can change the URL used for authentication either for all IP phones as a group or for one or more IP phones individually. The advantage to changing the URL for all IP phones is that you only need to make the change once. Note that a global change will affect every IP phone and application that requires authentication. The advantage to changing the URL for one or more IP phones individually is that you can choose the specific phones you want to configure. Note that you must repeat the configuration process for every IP phone separately, however.

To change the authentication URL for all IP phones as a group:

1. Log into Unified CM Administration.
2. Choose System > Enterprise Parameters. The Enterprise Parameters Configuration window appears.
3. In the Phone URL Parameters section, change the value of the URL Authentication parameter to the following, where <Tomcat> is the IP address of the CAD server on which Tomcat is running.

   http://<Tomcat>:8088/ipphone/jsp/sciphonexml/IPAgentAuthenticate.jsp

   > **NOTE:** The URL is case sensitive.

4. Click Save. A dialog box appears, telling you to click on the Reset Phone button to have the changes take effect.
5. Click OK. The dialog box closes.
6. Click Reset. The Device Reset window appears.
7. To restart the device without shutting it down, click Restart. To shut down the device and bring it back up, click Reset.

To change the authentication URL for an individual IP phone:

1. Log into Unified CM Administration.
2. Choose Device > Phone. The Find and List Phones page appears.
3. Click the Device Name of the phone that you want to configure. The Phone Configuration page appears.
4. In the External Data Locations Information section, change the value of the Authentication Server parameter to the following, where <Tomcat> is the IP address of the CAD server on which Tomcat is running.

   http://<Tomcat>:8088/ipphone/jsp/sciphonexml/IPAgentAuthenticate.jsp

   NOTE: The URL is case sensitive.

5. Click Save. A dialog box appears, telling you to click on the Reset Phone button to have the changes take effect.
6. Click OK. The dialog box closes.
7. Click Reset. The Device Reset window appears.
8. To restart the device without shutting it down, click Restart. To shut down the device and bring it back up, click Reset.

Configuring a One-Button Login for IP Phone Agents

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

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

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

Configuring an IP Communicator Phone

From Unified CM Administration, complete the following steps to configure an IP Communicator soft phone.

1. Choose Device > Add a New Device. The Add a New Device window appears.
2. In the Device Type field, select Phone, and then click Next. The Add a New Phone window appears.
3. From the Phone Type drop-down list, select IP Communicator, and then click Next. The Phone Configuration window appears.
4. Complete the fields in the Phone Configuration window, then click Insert. The IP Communicator phone is inserted into the Unified CM database.

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

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

Setting Up CTI OS Security

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

Element	Functions performed on this element
CTI OS Server	• Enable security via CTI OS setup • Automatically creates an unsigned certificate
Desktop Administrator client PC	• Run CAD Configuration Setup and enable CTI OS security, which sets a flag in the CAD services LDAP that enables the CTI OS node in the client CAD Configuration Setup
Agent Desktop client PC	• Run CAD Configuration Setup to enable CTI OS security • Automatically create an unsigned certificate
Certificate PC: can be located anywhere, best on CTI OS server	• 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. For instructions, see the *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise and Hosted Edition*. After security is enabled, SecuritySetupPackage.exe runs automatically to create two files, CtiosServerKey.pem and CtiosServerReq.pem, located in the folder C:\ICM\<instance name>\CTIOS1\security.

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

Desktop Administrator PC

After you enable security on the CTI OS servers, enable security on the CAD system.

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

This sets a flag in CAD services LDAP to display the CTI OS window whenever the CAD Configuration Setup tool is run on an 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.

Agent Desktop Client PCs

After 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 C:\Program Files\Cisco\Desktop\bin.
2. Locate and then double-click PostInstall.exe to start CAD Configuration Setup.
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.

SecuritySetupPackage.exe runs and creates two files, CtiosClientkey.pem and Ctiosclientreq.pem, located in C:\Program Files\Cisco Systems\CTIOS Client\Security. These files are used when signing the client certificate.

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

Certificate PC

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

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

Signing Client CTI OS Security Certificates

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

1. On the Certificate PC, run CreateSelfSignedCASetupPackage.exe, create a CTIOS Certificate Authority password of between 8 and 30 characters when prompted, and store the resulting files in a secure location.

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

Signing the Server CTI OS Security Certificate

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

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

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

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

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

Signing a Peer CTI OS Server Security Certificate

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

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

Repairing CAD

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

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

To repair a CAD client or server application:

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

Removal

5

Removing CAD 7.5

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

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

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

To remove a CAD application:

1. Open the Add or Remove Programs control panel.
2. Select the application you wish to remove and click Remove. The application is removed.

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