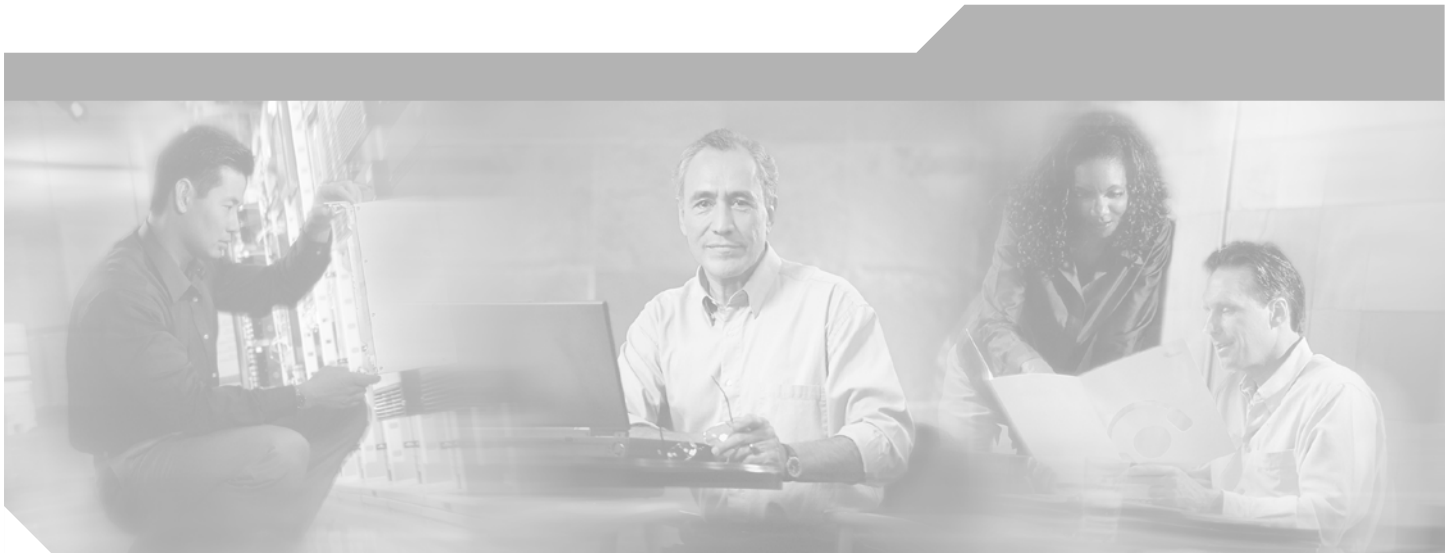


Installation Guide

Cisco Desktop Product Suite 4.3 (ICD)

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

Customer Order Number:
Text Part Number: OL-2841-01

Contents

1 Before You Install Cisco Desktop Product Suite

- Overview 1-1
  - Product Bundles 1-1
- About This Document 1-2
  - Intended Audience 1-2
  - Conventions 1-2
- Elements of the Cisco Desktop Product Suite 1-4
  - Desktop Applications 1-4
  - Servers 1-5
- CRA System Configuration 1-8
- System Requirements 1-10
- Prerequisites 1-11
  - Required SPAN Port Configuration 1-11
- Preinstallation Considerations 1-13
  - Sharing Configuration Files 1-13
  - Windows NT and Windows 2000 Platforms 1-17
  - Queue Statistics 1-17

2 Installing Desktop Applications

- Overview 2-1
- Installing Agent Desktop 2-2
  - Overview 2-2
  - Before You Install 2-2
  - Installation Procedure 2-2
- Installing Supervisor Desktop 2-4
  - Overview 2-4
  - Before You Install 2-5
  - Installation Procedure 2-5
- Installing Desktop Administrator 2-7
  - Overview 2-7
  - Before You Install 2-7
  - Installation Procedure 2-7

Contents

- Configuring Cisco CallManager IP Phones to Work With IP Phone Agent2-10
  - Creating an IP Phone Service 2-10
  - Assigning the IP Phone Service to IP Agent Phones 2-11
  - Creating the “telecaster” User 2-11
  - Configuring a Media Termination Phone 2-12

3 Removing Applications

- Removing Cisco Desktop Product Suite Applications 3-1

Before You Install Cisco Desktop Product Suite

1

Overview

This document tells you how to install Cisco Agent Desktop, Cisco Supervisor Desktop, and Cisco Desktop Administrator in your contact center after the Customer Response (CRA) platform is installed and configured.

Upon successful installation into a properly-configured ICD environment, the basic functionality of Agent Desktop and Supervisor Desktop are ready to use with no further configuration required.

Product Bundles

Cisco Desktop Product Suite 4.3 offers four different bundles:

- Standard Bundle
- Standard Bundle with Media Termination
- Enhanced Bundle
- Enhanced Bundle with Media Termination

Media Termination enables the Agent Desktop soft phone to perform call functions, so that no hard IP phone is needed.

The Enhanced Bundle, with or without Media Termination, offers the full range of functionality described in the section “Elements of the Cisco Desktop Product Suite” on page 1-4.

The Standard Bundle, with or without Media Termination, offers the same basic functionality, with these exceptions:

- Agent Desktop–No task buttons (no work flow automation).
- Supervisor Desktop–No call monitoring, recording, barge-in, or intercept.
- Desktop Administrator–No work flow automation or Agent Desktop interface customization.

About This Document

Intended Audience

This document is written for personnel who install the desktop applications of the Cisco Desktop Product Suite.

Conventions

In this document, terminology and typographic conventions are as follows.

Terminology

- The word *enter* means to press the sequence of keys specified. For example, an instruction to enter the letter “y” is shown as

  Enter **y** to continue.

- The word *click* means to use your mouse to execute the action represented by a button. For example, an instruction to click the Next button is shown as

  Click **Next**.

- The words *check* and *uncheck* mean to activate or deactivate a check box. For example, an instruction to deactivate the Dial Number as Entered check box is shown as

  Uncheck the **Dial Number as Entered** check box.

- The word *choose* means to pick an option from a menu or submenu. For example, an instruction to choose the Desktop option from a series of submenus is shown as

  Choose **Start > Programs > Cisco > Desktop**.

- The word *select* means to mark text or other elements to be copied or cut. For example, an instruction to select text is shown as

  Select an entry from the list to edit.

- Simultaneous keystrokes (as when you hold down the first key, then press the second and third keys) are represented as a series of bolded key names joined by hyphens. For example, an instruction to press and hold the Alt key while pressing the letter “d” is shown as

  Press **Alt-d**

- Function keys are represented by the letter F followed by the function key number. For example, an instruction to press function key 3 is shown as

  Press **F3**.

Typography

- Commands and text you type, the names of windows, buttons, menus, and menu options appear in bold type:

  From the **Options** menu, choose **Local Admin**.

- Variables you must enter appear in italics:

  http://*servername*/appadmin

- Terms that are being defined appear in italics:

  Actions are commands that perform a task.

- Menu paths appear in bold type with menu options separated by right angle brackets:

  Choose **Options > Status Bar**.

Elements of the Cisco Desktop Product Suite

The Cisco Desktop Product Suite includes the following elements:

Desktop Applications

Desktop Administrator

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

Desktop Administrator includes the following components:

Enterprise Configuration. Enterprise Configuration is used to define the fields for displaying the data collected by the CallManager or the ICD and stored on the Enterprise server.

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

- Dial Strings: format how phone numbers are displayed
- Phone Book: create and administer global phone books
- Reason Codes: create and administer reason codes
- Work Flow Groups: create and administer work flows, customize the Agent Desktop interface, and administer enterprise data

ICD Configuration. ICD Configuration enables you to use the ICD component administrative applications. From this tool you can launch your web browser to access these websites:

- Cisco CallManager Administration
- Cisco Customer Response Application Administration
- Client AW application on your PC (if you have ICM installed)

Personnel Configuration. Personnel Configuration enables you to view and extend the attributes for the contact center's resources beyond their definitions in ICD. You can view the attributes for agents, and create, modify, and delete supervisors and teams.

Agent Desktop

Agent Desktop screen pops caller information to the agent desktop along with the call. It can populate any sort of third-party application based on the calling number, called number, or other telephone identifier.

Agent Desktop includes a soft phone that allows agents to control calls from the PC. The optional Media Termination feature enables Agent Desktop to function as an IP phone, so no actual phone is needed at an agent's workstation. (For Media Termination to function, a sound card in the agent's PC is required.)

Agent Desktop's toolbar automates common telephony functions. The toolbar includes a task bar which can launch applications based on telephony and/or data events.

Supervisor Desktop

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

Call/Chat

Call/Chat enables agents to communicate in writing among themselves or with their supervisors so they can handle calls more efficiently. It also provides a marquee message function that allows supervisors to send important messages to some or all agents on their teams.

Enterprise Data

Enterprise Data is a server-based data management system. Used in conjunction with Agent Desktop, it displays the additional enterprise data associated with a call. Enterprise Data also displays call activity information for the active call.

Servers

Directory Services Server

The Directory Services server is an LDAP server. All other Cisco Desktop servers register with this server at startup. Clients use the Directory Services server to determine how to connect to the other servers.

The majority of the agent, supervisor, team, and skill information is also kept on the Directory Services server. Agent and skill information is imported from ICD and kept synchronized by the Directory Services Sync (Synchronization) server. Supervisor and team information is configured in Desktop Administrator.

The Cisco Desktop Product Suite is capable of working with four different Directory Services servers. They are:

- DC Directory
- Microsoft Active Directory
- Netscape iPlanet
- OpenLDAP

Directory Services Sync Server

The Directory Services Sync server connects to the ICD database via an ODBC connection and retrieves agent information. It then compares the information with the information in the Directory Services server and adds, updates, or deletes LDAP entries as needed to stay consistent with the ICD configuration.

Call/Chat Server

The Call/Chat server is a CORBA server program that acts as a message broker between the Call/Chat clients and Supervisor Desktop. The Call/Chat server is in constant communication with all agent and supervisor desktops.

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

Enterprise Server

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

Voice-Over IP Monitor Server

The Voice-Over IP Monitor server is a CORBA server program that is used to enable supervisors to silently monitor agents.

Recording and Statistics Server

The Recording and Statistics server is a CORBA server program that extends the capabilities of the Voice-Over IP Monitor server by allowing supervisors and agents to record calls. Supervisors can play back recorded agent calls through the Supervisor Log Viewer. The Log Viewer also 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, and many more statistics.

IP Phone Agent Server

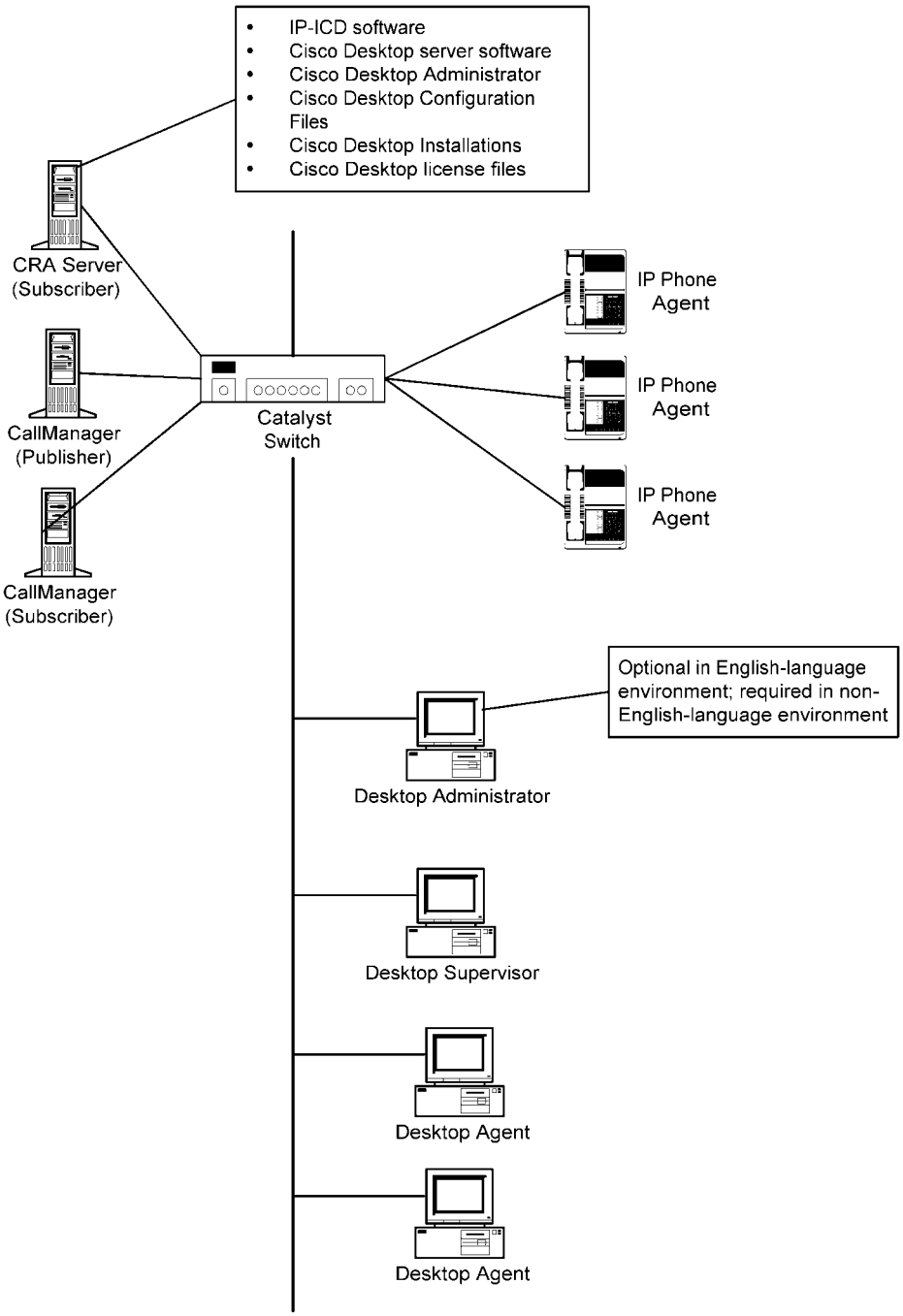
The IP Phone Agent server enables IP phone agents to log in and out of ICD, change agent states, and enter reason codes without having the Agent Desktop software.

This server works with the Services feature of CallManager and model 7940/7960 Cisco IP phones.

CRA System Configuration

Figure 1.1 depicts the standard CRA system configuration for a contact center.

Figure 1-1. Standard ICD configuration.



NOTE: Desktop Administrator is always installed on the CRA server. However, in a non-English-language environment, it is necessary to run a second instance of Desktop Administrator on a machine with a local-language operating system so that chat messages, tooltips, enterprise data names, and other communication within the contact center is in the local language.

System Requirements

The following are the minimum system requirements for running Cisco Desktop Product Suite.

NOTE: It is recommended that desktops running Media Termination have more memory and faster processors than the minimums listed below.

NOTE: Cisco Desktop servers and applications require significant system resources. Running other resource-intensive applications at the same time may adversely affect their performance.

Desktop Client Applications	
Operating System	• Windows 98 OSR 1 or greater • Windows 2000 Professional, Service Pack 2 or greater • Windows XP Professional • Windows NT Workstation, Service Pack 6a or greater
Hardware	• 350 MHz Pentium II processor • 32 MB RAM (Windows 98) • 64 MB RAM (Windows NT, Windows XP) • 16 MB free hard disk space • NIC supporting Ethernet 2 • Sound card for supervisor and media termination agent

Prerequisites

Required SPAN Port Configuration

The Voice-Over IP (VoIP) Monitor server accomplishes voice monitoring and recording functions by “sniffing” voice packets to and from IP phones.

Because network switches do not normally deliver packets to Ethernet ports other than the destination port (in this case, an IP phone), the switch must be configured to do this. To accomplish this, the Ethernet port for the VoIP Monitor server must be configured to monitor the Ethernet ports for all agent IP phones. If the voice packets going to and from an agent’s IP phone are not sent to the VoIP Monitor server’s port for any reason, that conversation will not be available to the supervisor.

Having the VoIP Monitor server monitor a port that all voice traffic goes through (for instance, the Ethernet port to which a gateway to the PSTN is connected) is not sufficient. It must monitor the Ethernet ports to which the IP phones are directly connected. The reason for this is that the server identifies packets by the IP phone’s MAC (medium access control) address. The packet’s MAC address changes as the packet moves around the network. There must not be a router between the IP phone and the port the server is monitoring.

The server sniffs packets on a single network interface card (NIC) and thus a single Ethernet port. This is the port that must be configured. This does not necessarily require that the server and the IP phones be connected to the same network switch. That depends on the switch’s monitoring capabilities.

The port monitoring feature on Cisco Catalyst switches is called Switched Port Analyzer (SPAN). For detailed information on SPAN, see “Configuring the Catalyst Switched Port Analyzer (SPAN) Feature” on the Cisco website in the Tech Notes section (www.cisco.com/warp/public/473/41.html).

Switch Capabilities and Restrictions

The following capabilities and restrictions are from the above-mentioned document. Refer to Cisco documentation for more details.

Catalyst 2900XL and 3500XL Switches

A monitor port:

- Cannot be in a Fast EtherChannel or Gigbit EtherChannel port group
- Cannot be enabled for port security
- Cannot be a multi-VLAN port

- Must be a member of the same VLAN as the port monitored. VLAN membership changes are disallowed on monitor ports and ports being monitored
- Cannot be a dynamic-access port or a trunk port. However, a static-access port can monitor a VLAN on a trunk, a multi-VLAN, or a dynamic-access port. The VLAN monitored is the one associated with the static-access port
- Port monitoring does not work if both the monitor and monitored ports are protected ports

Catalyst 4000, 5000, and 6000 Series Switches

4000, 5000, and 6000 series switches are able to monitor ports belonging to multiple VLANs.

Preinstallation Considerations

Sharing Configuration Files

Configuration and licensing files are installed on the CRA server. They must be read-write accessible to Agent Desktop and Supervisor Desktop users.

NOTE: If installing a second instance of Desktop Administrator, that instance must use the configuration files on the CRA server.

NOTE: Windows 2000 Professional machines have a built-in limitation of ten shared sessions. Take this into consideration if you intend to install the shared configuration files on this type of platform.

There are a number of ways to ensure that the configuration files are accessible to all agents. among these methods are:

- Using a login script to establish the shared configuration location
- Manually mapping the shared configuration location
- Automatically mapping the shared configuration location

Login Script Method

In this method, agents use an agent user account to connect to the CRA server.

1. Set up an agent user account on the CRA server.
    a. Choose **Start > Control Panel > Performance & Maintenance > Administrative Tools > Computer Management**.

    The Computer Management window appears.

    b. Choose **Action > New User**.

    The New User dialog box appears.

    c. Enter user name **Agent** and password **agent**, uncheck all check boxes, and then check the **Password Never Expires** check box.

    d. Click **Create**.

    The new user “Agent” is created as a member of the Users group, and appears in the navigation pane under the Users folder.
2. Find out the CRA server’s NT domain or NT work group.
    a. Right-click **My Computer**, and then choose **Properties**.

    The System Properties dialog box appears.

b. Select the Network Identification tab.

The CRA server's NT work group or NT domain name is shown on the tab.

3. Add the following net use command to the agent PC's login script or autoexec.bat file.

For Windows NT and Windows 2000:

`net use` *`drive`*`: \\`*`IPaddress`*`\DESKTOP_CFG /USER:`*`workgroup or domain\account password`*

where:

drive	Available drive letter on the agent's PC
IPaddress	CRA server's IP address
DESKTOP_CFG	Name of the shared folder
/USER:	Optional net use parameter that allows you to specify which account to use when logging in
workgroup or domain	CRA server's NT work group or NT domain name
account	The user account used when logging in
password	User account's password

Example 1: User account JohnK, with password 12345, maps drive f to the shared folder DESKTOP_CFG on CRA server 192.168.252.46. The user account is in the same domain as the CRA server.

```
net use f: \\192.168.252.46\DESKTOP_CFG /user:
JohnK 12345
```

Example 2: User account JohnK, with password 12345, maps drive f to the shared folder DESKTOP_CFG on CRA server 192.168.252.46. The CRA server is in the CALLCENTER domain; the user account is in another domain.

```
net use f: \\192.168.252.46\DESKTOP_CFG /user:
CALLCENTER\JohnK 12345
```

For Windows 98:

`net use` *`drive`*`: \\`*`IPaddress`*`\DESKTOP_CFG` *`password`*

where:

drive	Available drive letter on the agent's PC
IPaddress	CRA server's IP address, followed by the shared folder name
DESKTOP_CFG	Name of the shared folder
password	User account password

Example: User account JohnK, with password 12345, maps drive f to CRA server 192.168.252.46.

```
net use f: \\192.168.252.46\DESKTOP_CFG 12345
```

NOTE: On a Windows 98 platform, the login used by the agent is the same login that is used by net use to gain access to the CRA server. As a result, that login must be created on the CRA server.

Manual Mapping Method

Follow these steps to manually map the shared drive to the agent's PC:

1. Double-click **Network Neighborhood** on your Windows desktop.

   The Network Neighborhood window appears.

2. Double-click the host on which the Cisco Desktop Administrator configuration files are located.

   The host's window appears.

   Explore it to find the directory in which the configuration files are stored.

3. Select the directory, and then click **File > Map Network Drive…**.

   The Map Network Drive dialog box appears.

4. Map the drive to a drive letter on your local PC, check the **Reconnect at Logon** check box to ensure you will have access to the mapped drive, and then click **OK**.

   The agent PC is now mapped to the network drive.

   NOTE: When you map a drive using manual mapping, the user is prompted for his or her password every time the drive is mapped to the PC, once per logon process.

Automatic Mapping Method

If a trust relationship is established between the Cisco and corporate domains, it is possible to create a script that will map the drive when an agent logs into his or her PC.

A sample script is as follows:

```
rem login.bat--simple login script for mapping drives
if exists drive:\nul net use drive: /del
if exists path\*.* net use drive: path
```

where:

drive	Available drive letter
path	Path to the Customer Response Applications (CRA) folder

The first line of the script (after the comment line) unmaps the drive letter you need if the user has manually mapped it. The second line of the script maps the drive if it is available.

Windows NT and Windows 2000 Platforms

When installing a Desktop application on a Windows NT and Windows 2000 platform, the user must have administrator privileges.

Desktop Administrator users must also have Administrator or Power User privileges on these platforms. The reason for this is that the user must have sufficient rights to update registry settings.

Queue Statistics

The number displayed in the statistics field “Waiting” in the Queues statistics windows in Agent Desktop and Supervisor Desktop is dependent on how you configure skill groups and set up queues in 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.

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

Installing Desktop Applications

2

Overview

In a typical configuration, all server software, global configuration files, and Desktop Administrator are installed on the CRA server prior to the installation of the desktop applications.

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

Installing Agent Desktop

Overview

You can choose to install either Agent Desktop, or Agent Desktop with Media Termination.

> **NOTE:** It is recommended that you not install Agent Desktop on the CRA server. However, if you do so, ensure that Agent Desktop's LDAP registry information does not point to your production CRA server.

If you install Agent Desktop with Media Termination, the agent can use Agent Desktop's soft IP phone for call control. A hard IP phone is not necessary.

> **NOTE:** If Media Termination is installed, the Media Termination phone must be set up in Cisco CallManager as phone type 30 SP+. The Media Termination phone does not support auto-registration with the CallManager. Therefore, the device DN should be set up in the CallManager using the MAC address of the PC where the Media Termination phone is installed.

Before You Install

Before you install Agent Desktop, you need to know:

- The IP address of the CRA server
- The user ID and password to access the CRA User Options web page (the same user ID and password used to access Cisco Agent Desktop)
- The destination folder on the user's PC in which you will install the application
- The extension of the user's ICD phone

Installation Procedure

▶ **To install Agent Desktop, follow these steps:**

1. Open your web browser and access the Cisco CRA User web page at http://*servername*/appuser.

   Replace *servername* with the IP address of the Cisco CRA server.

   The CRA User Options Authentication window appears.

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

   The Welcome window appears.

3. Click **ICD Downloads**.

   The Download Cisco IP ICD Agent Desktop window appears.

4. Use the Windows Copy function to copy the following command line from the Download Cisco IP ICD Agent Desktop window. (*Servername* is the IP address of your CRA server.)

   \\Servername\DESKTOP_CFG\desktop\InstallManager

5. From the Windows taskbar, choose **Start > Run**.

   The Run dialog box appears.

6. In the Open field in the Run dialog box, use the Windows Paste command to paste the command line that you copied in Step 4, and then click **OK**.

   The Enter Network Password dialog box appears.

7. Enter your user name and password, and then click **OK**.

   The Welcome dialog box appears.

8. Click **Next**.

   The Select Options dialog box appears.

9. Check the version of Agent Desktop you wish to install, and then click **Next**.

   The Choose Destination Location dialog box appears.

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

    The Telephone Extension dialog box appears.

11. Enter the extension of the ICD telephone used with this installation, and then click **Next**.

    The Start Copying Files dialog box appears.

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

    Installation Manager installs the application you chose.

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

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

Installing Supervisor Desktop

Overview

There are five versions of Supervisor Desktop available. They are:

- On-Site Enhanced Supervisor Desktop

  This version includes all available functionality.

- On-Site Enhanced Supervisor Desktop with Media Termination

  This version includes all available functionality, with the addition of Media Termination. Media Termination enables the supervisor to use Agent Desktop's soft IP phone for call control. A hard IP phone is not necessary.

- On-Site Supervisor Desktop

  This version does not include call monitoring, recording, barge-in, or intercept features.

- On-Site Supervisor Desktop with Media Termination

  This version does not include call monitoring, recording, barge-in, or intercept features. It includes Media Termination, which enables the agent to use Agent Desktop's soft IP phone for call control. A hard IP phone is not necessary.

- Remote Supervisor Desktop

  This version enables a supervisor to monitor agents from outside of the local contact center, but not to intervene (barge-in, intercept, or record conversations, or change agent states) in any way.

When you install any version of Supervisor Desktop, Agent Desktop is automatically installed at the same time.

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

NOTE: If Media Termination is installed, the Media Termination phone must be set up in Cisco CallManager as phone type 30 SP+. The Media Termination phone does not support auto-registration with the CallManager. Therefore, the device DN should be set up in the CallManager using the MAC address of the PC where the Media Termination phone is installed.

Before You Install

Before you install Supervisor Desktop, you need to know:

- The IP address of the CRA server
- The user ID and password to access the CRA User Options web page (the same user ID and password used to access Cisco Agent Desktop)
- The destination folder on the user's PC in which you will install the application
- The extension of the user's ICD phone

Installation Procedure

▶ **To install Supervisor Desktop, follow these steps:**

1. Open your web browser and access the Cisco CRA User web page at http://*servername*/appuser.

   Replace *servername* with the IP address of the Cisco CRA server.

   The CRA User Options Authentication window appears.

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

   The Welcome window appears.

3. Click **ICD Downloads**.

   The Download Cisco IP ICD Agent Desktop window appears.

4. Use the Windows Copy function to copy the following command line from the Download Cisco IP ICD Agent Desktop window. (*Servername* is the IP address of your CRA server.)

   \\Servername\DESKTOP_CFG\desktop\

5. From the Windows taskbar, choose **Start > Run**.

   The Run dialog box appears.

6. In the Open field in the Run dialog box, use the Windows Paste command to paste the command line that you copied in Step 4, and then click **OK**.

   The Enter Network Password dialog box appears.

7. Enter your user name and password, and then click **OK**.

   Your Desktop folder opens.

8. From the Windows task bar, choose **Start > Programs > Command Prompt**.

   The DOS command window appears.

9. Enter the following command in the DOS command window:

   ```
   \\servername\DESKTOP_CFG\Desktop\InstallManager.exe -f
   \\servername\DESKTOP_CFG\Desktop\AdvancedManager.cfg
   ```

   HINT: To ensure this command is entered accurately, drag the InstallManager.exe file from the Folder window to the DOS command window, type a space, **–f**, and another space, and then drag the AdvancedManager.cfg file from the Folder window to the DOS command window.

10. In the DOS command window, press **Enter**.

    The Install Manager program starts and displays the Welcome window.

11. Click **Next**.

    The Select Options dialog box appears.

12. Check the version of Supervisor Desktop you want to install, and then click **Next**.

    The Choose Destination Location dialog box appears.

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

    The Telephone Extension dialog box appears.

14. Enter the extension of the ICD telephone used with this installation, and then click **Next**.

    The Start Copying Files dialog box appears.

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

    Installation Manager installs the application you chose.

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

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

Installing Desktop Administrator

Overview

Desktop Administrator is installed with the CRA applications on the CRA server. In a non-English environment, a second instance of Desktop Administrator must be run on a machine with a local-language operating system, so that chat messages, tooltips, and other communication within the contact center is in the local language.

> **NOTE:** If Agent Desktop and/or Supervisor Desktop are installed on the same machine as the second instance of Desktop Administrator, they must be installed first. If Desktop Administrator is installed first, Install Manager will not install Java.

PDF versions of the Cisco Desktop Product Suite documentation are installed automatically when you install Desktop Administrator.

Before You Install

Before you install Desktop Administrator, you need to know:

- The URL of the Cisco Customer Response Applications (CRA) User web page on the CRA server
- The user ID and password to access the CRA User Options web page (the same user ID and password used to access Cisco Agent Desktop)
- The destination folder on the administrator's PC in which you will install the application

Installation Procedure

▶ **To install Desktop Administrator, follow these steps:**

1. Open your web browser and access the Cisco CRA User web page at http://*servername*/appuser.

   Replace *servername* with the IP address of the Cisco CRA server.

   The CRA User Options Authentication window appears.

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

   The Welcome window appears.

3. Click **ICD Downloads**.

   The Download Cisco IP ICD Agent Desktop window appears.

4. Use the Windows Copy function to copy the following command line from the Download Cisco IP ICD Agent Desktop window. (*Servername* is the IP address of your CRA server.)

   \\Servername\DESKTOP_CFG\desktop\

5. From the Windows taskbar, choose **Start > Run**.

   The Run dialog box appears.

6. In the Open field in the Run dialog box, use the Windows Paste command to paste the command line that you copied in Step 4, and then click **OK**.

   The Enter Network Password dialog box appears.

7. Enter your user name and password, and then click **OK**.

   Your Desktop folder opens.

8. From the Windows task bar, choose **Start > Programs > Command Prompt**.

   The DOS command window appears.

9. Enter the following command in the DOS command window:

   ```
   \\servername\DESKTOP_CFG\Desktop\InstallManager.exe -f
   \\servername\DESKTOP_CFG\Desktop\AdvancedManager.cfg
   ```

   HINT: To ensure this command is entered accurately, drag the InstallManager.exe file from the Folder window to the DOS command window, type a space, **–f**, and another space, and then drag the AdvancedManager.cfg file from the Folder window to the DOS command window.

10. In the DOS command window, press **Enter**.

    The Install Manager program starts and displays the Welcome window.

11. Click **Next**.

    The Select Options dialog box appears.

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

    The Choose Destination Location dialog box appears.

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

    The Start Copying Files dialog box appears.

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

    The Question dialog box appears, asking if you wish to share the existing configuration with other administrators.

15. Click **Yes**.

    Installation Manager installs the application you chose.

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

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

Configuring Cisco CallManager IP Phones to Work With IP Phone Agent

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

1. Create an IP phone service.
2. Assign the IP phone service to each IP agent phone.
3. Create a user named “telecaster” and assign to it all the IP agent phones.

NOTE: Agent usernames and passwords in CallManager must be in lowercase. If uppercase is used, agents are not able to log into the ICD server when starting the IP Phone Agent service.

Creating an IP Phone Service

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

▶ **To create a new IP phone service:**

1. From the menu at the top of the page, click **Feature > IP Phone Service**.
2. On the Cisco IP Phone Services Configuration page, enter the following information:

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

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

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

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

   where:

   - 192.168.252.44 is the IP address of the machine where the Agent State service is loaded
   - 6293 is the Tomcat webserver port (if 6293 is not the port number, check the port parameter in the file C:\Program Files\wfavvid\Tomcat_appadmin\conf\server.xml for the correct value.)
   - ipphone/jsp/… is the path to the jsp page under Tomcat on the machine where the Agent State server is loaded (the CRA server)

   NOTE: The Tomcat webserver is included with the ICD installation.

3. Click **Insert** to create the new IP phone service. The new service is now listed in the shaded box at the left of the page.

Assigning the IP Phone Service to IP Agent Phones

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

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

▶ **To assign the IP phone service to IP agent phones:**

1. On the Device menu, choose **Phone**.

   The Find and List Phones window appears.

2. User the search function to find the phone. Search results are listed at the bottom of the page.

3. Locate the phone in the list of results and click the red hyperlink.

   The Phone Configuration window appears.

4. Click **Subscribe/Unsubscribe Services** in the upper right corner of the window.

   A popup window for subscribing to services for that device appears.

5. From the **Select a Service** drop-down list, choose the new service, and then click **Continue**.

   A popup window showing the new service appears.

6. Click **Subscribe**.

   The new service is listed in the shaded box at the left of the page.

7. Close the popup window.

Creating the "telecaster" User

The final task to accomplish is to create the "telecaster" user.

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

▶ **To create the "telecaster" user:**

1. From the User menu, choose **Add a New User**.

   The User Information window appears.

2. Enter the following information.

   Entries are case sensitive. Enter them exactly as shown.

   First Name . . . . . telecaster

   Last Name . . . . . telecaster

   UserID . . . . . telecaster

   User Password . . . . . telecaster

   PIN. 12345

   Confirm PIN 12345

3. Check the **Enable CTI Application Use** check box, and then click **Insert**.
4. Click **Device Association** in the shaded box at the left.

   The Find and List Phones window appears.

5. User the search function to locate all phones that are to be associated with the telecaster user. This should be every IP phone that will be used by an IP phone agent.
6. Select the phone(s) from the search results to associate them with the telecaster user, check the **No Primary Extension** check box, and then click **Update** to complete the association.

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

7. Continue until all appropriate IP phones are associated.

Configuring a Media Termination Phone

From the Cisco CallManager Administration web-based application, follow these steps to configure a Media Termination phone.

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

   The Add a New Device window appears.

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

   The Add a New Phone window appears.

3. From the Phone Type drop-down list, choose **Cisco 30 SP+**, and then click **Next**.

   The Phone Configuration window appears.

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

   In the MAC Address field, enter the MAC address of the computer on which the Media Termination phone is installed.

   The Media Termination phone is inserted into the CallManager database.

NOTE: A Media Termination phone registers with the CallManager only when Agent Desktop is running on the agent PC.

Removing Applications

3

Removing Cisco Desktop Product Suite Applications

It is recommended that you remove Cisco Desktop applications in this order:

1. User applications (for example, Agent Desktop, Supervisor Desktop, and Desktop Administrator)
2. Servers
3. Cisco Base

IMPORTANT: Always remove Base last.

▶ **To remove a Cisco Desktop application:**

1. From the Windows task bar, choose **Start > Settings > Control Panel.**

   The Control Panel appears.

2. Double-click **Add/Remove Programs**.

   The Add/Remove Properties dialog box appears.

3. Choose the application you wish to remove, and then click **Add/Remove**.

   The removal process begins.

4. Follow the instructions in the dialog boxes to remove the application from your computer.