Installation Guide
Cisco Desktop Product Suite 4.6 (IPCC)

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: XX-XXXX-XX
# Contents

1 Before You Install Cisco Desktop Product Suite

- Overview ................................................................................. 1-1
- Elements of the Product Suite .............................................. 1-2
  - Desktop Administrator ...................................................... 1-2
  - Agent Desktop ................................................................. 1-3
  - Supervisor Desktop .......................................................... 1-3
  - Call/Chat ............................................................................. 1-3
  - Enterprise Data ................................................................. 1-3
  - Servers ............................................................................... 1-4
- System Configurations .......................................................... 1-6
  - Recommended Configuration ............................................. 1-6
  - Alternate Configuration A .................................................. 1-7
  - Alternate Configuration B ................................................... 1-8
- Sharing Configuration Files .................................................. 1-10
- System Requirements .......................................................... 1-13
  - Desktop Monitoring Requirements .................................... 1-14
  - Recording and Statistics Server Requirements .................... 1-14
- Prerequisites ......................................................................... 1-15
  - Required Software ........................................................... 1-15
  - Required Microsoft SQL Server Licenses ............................. 1-15
  - Required SQL Account for Database Synchronization ........ 1-15
  - Required Tomcat Webserver and JRE ................................. 1-15
  - Setting Up Agents in ICM .................................................... 1-16
- Voice-Over IP Monitor Server Installation Notes ...................... 1-17
  - General Installation Guidelines .......................................... 1-18
  - Specific Configuration Examples ........................................ 1-19
- Upgrading From a Previous Version ....................................... 1-22
- Saving Data From a Previous Version ..................................... 1-23
  - Backing Up Your Data ....................................................... 1-23
- Preinstallation Considerations .............................................. 1-24
  - Configuration Files ........................................................... 1-24
  - File Sharing ........................................................................ 1-24
Contents

- Installation-Related Configuration ........................................... 1-25
- Preinstallation Survey ............................................................. 1-27

2 Installation
- Overview ................................................................................. 2-1
- Installation Procedure ............................................................. 2-2
  Starting Install Manager ............................................................ 2-2
  Installing Servers ..................................................................... 2-3
  Other Information Required During Server Installation ........... 2-21
  Installing Desktop Applications ............................................. 2-29
  Saving a Personal Phone Book ................................................. 2-36
  Post-Install Tools .................................................................... 2-37
- Licensing Cisco Desktop Product Suite ....................................... 2-38
- Configuring Cisco CallManager IP Phones to Work With IP Phone Agent ....................................................... 2-40
  Creating an IP Phone Service .................................................. 2-40
  Assigning the IP Phone Service to IP Agent Phones ............ 2-41
  Creating the “telecaster” User ..................................................... 2-41
  Changing the Default URL Authentication Parameter ........ 2-42
  Configuring a Media Termination Phone ............................... 2-43

3 Removal
- Removing Cisco Desktop Product Suite Applications ............... 3-1
Before You Install Cisco Desktop Product Suite

Overview

Install Manager guides you through the Cisco Desktop Product Suite installation process. Starting with the Select Options window (see Figure 2 on page 2-3), Install Manager allows you to select one or more packages to install, making sure that each package is installed in the correct order.

Install Manager lets you choose either of two installation modes:

- **Novice Mode.** The novice installation mode walks you through the entire installation process. You see every window in the installation sequence, even if the window collects information that the system already has. (The window displays the information, autofilled in the appropriate fields.) The novice mode is ideal for installers who do not install elements of the Cisco Desktop Product Suite on a regular basis.

- **Expert Mode.** The expert installation mode is for installers who are familiar with installing elements of the Cisco Desktop Product Suite. Expert mode skips the windows in the installation sequence that ask for information the system already has. You see only the windows needed to collect the information the system does not have. Expert mode is faster and more convenient for installers who install elements of the Cisco Desktop Product Suite frequently.

During the installation process you are warned if you attempt to install options that are not intended to be installed on the same computer. Once all the data is collected, Install Manager installs the packages you selected in the proper order.

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

The Cisco Desktop Product Suite includes the following elements:

Desktop Administrator

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

Desktop Administrator includes the following components:

Enterprise Data Configuration. Enterprise Data Configuration is used to perform the following functions:

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

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

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

IPCC Configuration. IPCC Configuration enables you to use the IPCC component administrative applications. From this tool you can:

- Launch your web browser to access the Cisco CallManager Administration website
- Launch your web browser to access the Cisco Customer Response Application (CRA) or Cisco Customer Response Solution (CRS) Administration website

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

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

Agent Desktop screen pops caller information to the agent’s 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. It includes a soft phone that allows agents to control calls from the PC. The soft phone toolbar automates common telephony functions. The toolbar includes a task bar which can launch applications based on telephony and/or data events.

Media Termination

Media Termination 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.

See the Cisco Agent Desktop 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 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 unsave recorded agent calls.

See the Cisco Supervisor Desktop User Guide for more information.

Call/Chat

Call/Chat enables agents to communicate in writing among themselves during conference calls or with their supervisors at any time to allow them to more efficiently handle a call. 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, calls display the additional enterprise data associated with them. Enterprise Data also displays call activity information for the active call.
Servers

Directory Services Server
All other Cisco Desktop servers register with the Directory Services server at startup. Clients use the Directory Services server to determine how to connect to the other servers.

You can install an optional secondary Directory Services server to provide redundancy for the primary Directory Services server.

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

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

Replication Server
The Replication server is installed only if the configuration includes a secondary Directory Services server. It handles the communication between the primary and secondary Directory Services servers so that the information contained in them is identical.

Call/Chat Server
The Call/Chat server is a CORBA server program that acts as a message broker between the Call/Chat clients and the Supervisor Desktop program. 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 IVR-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. The server accomplishes this by “sniffing” network traffic for voice packets.

Multiple Voice-Over IP Monitor servers can be installed in one logical contact center to ensure there is enough capacity to handle the number of agents in the contact center.

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. Through the supervisor log viewer, supervisors can play back recorded agent calls. It also maintains a 7-day history of agent and team statistics such as average time an agent is in a 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 ICM, change agent states, and enter wrapup data and reason codes without having the Agent Desktop software.

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

Recommended Configuration

Figure 1.1 depicts the recommended configuration for the Cisco Desktop Product Suite.

Figure 1-1. Recommended Configuration.

Key Points

Key points of this configuration are:

- The Cisco Desktop (CAD) servers are installed on the same hardware as the ICM Peripheral Gateway (PG).
- Desktop Administrator, Desktop Supervisor, and Desktop Agent are installed on machines in the corporate domain.
- Global configuration files and the installation files for Desktop Agent and Desktop Supervisor are placed on a networked file server in the corporate domain.

Advantages

The advantages of this configuration are:

- Minimal network administration is required to support the product suite.
- Minimal network security issues arise.
- Administrators, supervisors, and agents are able to fully use all of the functionality provided by the product suite without any additional setup.
Assumptions

This configuration assumes that:

■ All product suite software running in the corporate domain accesses the ICM PG and the CAD servers via TCP/IP addresses.
■ The customer already has an existing corporate domain.

Alternate Configuration A

Figure 1-2. Alternate Configuration A.

Key Points

Key points of this configuration are:

■ The CAD servers are installed on the same hardware as the ICM PG.
■ Desktop Administration is installed on the ICM PG.
■ Global configuration files and the installation files for Desktop Agent and Desktop Supervisor are placed on a networked file server in the corporate domain.

Advantages

Advantages of this configuration are:

■ Desktop Administrator is co-resident with the ICM PG.
■ Supervisors and agents are able to fully use all the functionality provided by the product suite without any additional setup.

Considerations

Things to consider with this configuration are:

■ Administrators must log into the corporate domain before running Desktop Administrator. Domain trust relationships are required to avoid this problem.
This configuration is best implemented with a trust relationship in which the corporate domain trusts the ICM domain.

Administrator user accounts must exist and must be kept synchronized across both domains.

**Assumptions**

This configuration assumes that:

- The administrator requires read/write access to the global configurations in the corporate domain.
- All product suite software running in the corporate domain accesses the ICM PG and the CAD servers via TCP/IP addresses.
- The customer already has an existing corporate domain.

**Alternate Configuration B**

**Figure 1-3. Alternate Configuration B.**

<table>
<thead>
<tr>
<th>ICM NT Domain</th>
<th>Corporate NT Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP IVR</td>
<td>Desktop Supervisor</td>
</tr>
<tr>
<td>ICM PG</td>
<td>Desktop Agent</td>
</tr>
<tr>
<td>CallManager</td>
<td></td>
</tr>
</tbody>
</table>

**Key Points**

Key points of this configuration are:

- The CAD servers are installed on the same hardware as the ICM PG.
- Global configuration files are shared from the ICM PG.
- Global configuration files and the installation files for Desktop Agent and Desktop Supervisor are placed on the ICM PG.
- Desktop Supervisor and Desktop Agent are installed on machines in the corporate domain.
Advantages
Advantages of this configuration are:

- Desktop Administrator is co-resident with the ICM PG.
- It supports the “appliance” concept of pre-loaded software at the factory.

Considerations
Things to consider with this configuration are:

- Installers must log into the ICM domain before installing Desktop Supervisor and Desktop Agent.
- Supervisors and agents must log into the ICM domain before running Desktop Administrator. Domain trust relationships are required to avoid this.
- This configuration is best implemented with a trust relationship in which the ICM domain trusts the corporate domain.
- Desktop Supervisor and Desktop Agent NT user accounts must exist and must be kept synchronized across both domains.

Assumptions
This configuration assumes that:

- Supervisors and agents require read/write access to the global configuration files in the ICM domain.
- All product suite software running in the corporate domain access the ICM PG and the CAD servers via TCP/IP addresses.
- The customer already has an existing corporate domain.
Sharing Configuration Files

The recommended and alternate configurations have configuration and licensing files installed on the computer which hosts the ICM server application. These files must be read-write accessible to Agent Desktop and Supervisor Desktop users.

NOTE: If installing subsequent instances of Desktop Administrator, those instances must use the same configuration files that the first instance of Desktop administrator does.

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 ICM server.

1. Set up an agent user account on the ICM server.
      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 ICM 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 ICM server's work group or 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:

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

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

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>drive</td>
<td>Available drive letter on the agent's PC</td>
</tr>
<tr>
<td>IPaddress</td>
<td>ICM server's IP address, followed by the shared folder name</td>
</tr>
<tr>
<td>DESKTOP_CFG</td>
<td>Name of the shared folder</td>
</tr>
<tr>
<td>password</td>
<td>User account password</td>
</tr>
</tbody>
</table>

**Example:** User account JohnK, with password 12345, maps drive f to ICM 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 ICM server. As a result, that login must be created on the ICM server.
System Requirements

The following are the minimum system requirements for running Cisco Desktop Product Suite 4.6.

**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.

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

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

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

### Required Hardware and Operating Systems

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Desktop Applications</th>
<th>Servers *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 95</td>
<td>not supported</td>
<td>not supported</td>
</tr>
<tr>
<td>Windows ME</td>
<td>not supported</td>
<td>not supported</td>
</tr>
<tr>
<td>Windows 98 OSR1, OSR2</td>
<td>233 MHz Pentium 32 MB RAM 16 MB free space NIC supporting Ethernet 2</td>
<td>not supported</td>
</tr>
<tr>
<td>Windows NT Professional 4.0 Service Pack 6</td>
<td>233 MHz Pentium 64 MB RAM 16 MB free space NIC supporting Ethernet 2</td>
<td>not supported</td>
</tr>
<tr>
<td>Windows 2000 Professional Service Pack 3</td>
<td>233 MHz Pentium 64 MB RAM 16 MB free space NIC supporting Ethernet 2</td>
<td>not supported</td>
</tr>
</tbody>
</table>
Desktop Monitoring Requirements

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

Recording and Statistics Server Requirements

The space requirements for the Recording and Statistics server depend on the size of the contact center. In general, it requires the following:

- 1 GB to store agent state and call activity records for a 7 days per week/10 hours per day contact center with 250 agents taking calls that last an average of 1 minute each.

- 1 MB hard drive space for each minute of recorded call.

- 1 GB hard drive space to store recordings, assuming 20 supervisors each of whom record ten 5-minute calls per day.

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

Required Software

Cisco Desktop Product Suite 4.6 requires Cisco ICM v4.6.2 or 5.0.

Consult the Cisco CallManager Compatibility Matrix (for IPCC Enterprise) for the appropriate versions of other applications required in your contact center environment. The compatibility matrix is located at:

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

Required Microsoft SQL Server Licenses

The Cisco Desktop servers require either one or two Microsoft SQL Server licenses, depending on where the Recording and Statistics server is installed:

- One license is required if it is installed on a separate machine from ICM.
- Two licenses are required if it is installed on the same machine as ICM.

Required SQL Account for Database Synchronization

To successfully install the Directory Services Sync server so that it will synchronize with the ICM database, you must establish an ODBC connection and SQL account.

**SQL Account.** The SQL account must have read privileges with the ICM Logger database.

**ODBC Connection.** The ODBC connection is used to communicate with the ICM Logger database. If the logger database is using the Named Pipes network library as the connection method, you must have a user account with sufficient privileges to create a named pipe on the ICM Logger server. If the ICM Logger database is using TCP/IP as the connection method, you may use the local administrator account.

For information on setting up SQL accounts and ODBC connections, consult your Microsoft documentation.

Required Tomcat Webserver and JRE

Tomcat is a Java-based webserver. If you are installing the IP Phone Agent application, it is needed to work with the XML pages displayed by IP phones. More information about Tomcat may be found at http://jakarta.apache.org.

JRE, or Java Runtime Environment, is required to run the Java applets and JavaServer Pages (JSP) used by the IP Phone Agent application.
Both Tomcat and JRE are shipped with the Cisco Desktop Product Suite and are automatically installed if the installation program does not detect an existing, current version of either program.

**Setting Up Agents in ICM**

**Setting Up Supervisors and Teams**
For Cisco Desktop Product Suite applications to work properly, your agents must be organized into teams and some must be designated as supervisors. This is accomplished in ICM. See your ICM documentation for information on how to do this.

**Skills Statistics**
The number displayed in the statistics field “Waiting” in the Skills statistics windows 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 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 skill data for a team in Supervisor Desktop.

See your Configuration Manager documentation for more information on setting up skill groups and queues.
Voice-Over IP Monitor Server Installation Notes

The VoIP Monitor server application is used to enable the silent monitoring and recording features of the Cisco Desktop Product Suite. It accomplishes this by monitoring (sniffing) network traffic to and from IP phones.

By default, Ethernet switches do not deliver packets to ports other than the destination port. However, Cisco Catalyst switches have a feature called Switched Port Analyzer (SPAN) which allows copying all traffic from a list of ports or VLANs to another port.

In some cases, a single VoIP Monitor server is not able to handle the traffic in an entire contact center for these reasons:

- The VoIP Monitor server cannot see or identify the voice traffic because of the way the network is configured
- A single VoIP Monitor server cannot keep up with the amount of voice traffic in the contact center

The VoIP Monitor server identifies packets by MAC address. When a request comes in to monitor or record an agent's conversation, it retrieves the MAC address of the agent's IP phone from the Cisco CallManager.

A problem arises if the VoIP Monitor server, using SPAN, is monitoring an Ethernet port that hits a router before it reaches the IP phone. In this case, the VoIP Monitor server will not associate that packet with the IP phone because it sees the router's MAC address, not the IP phone's MAC address. For this reason, the ports that SPAN is configured to monitor must be in the same layer-2 domain (VLAN/subnet) as the IP phones to ensure that the packets it sees contain the IP phone MAC addresses.

Figure 1-4 illustrates a situation in which more than one VoIP Monitor server is required. In this figure, a central office connects two agent offices to the voice gateway. The agent offices are separated by a WAN link.

NOTE: If you install additional VoIP Monitor servers, the Recording and Statistics server must be restarted in order to recognize the additional VoIP Monitor servers added since its last restart.

A single VoIP Monitor server cannot be placed in the central office because there are routers between the central office and the agent offices. If a VoIP Monitor server were placed in the central office, it would see the MAC addresses of those routers rather than those of the IP phones it is supposed to monitor.
Cisco Desktop Product Suite 4.6 enables network architecture to include multiple VoIP Monitor servers in a single logical contact center. When this is done, IP phones are assigned to a specific VoIP Monitor server using Cisco Desktop Administrator.

Figure 1-4. System architecture that requires more than one VoIP Monitor server.

General Installation Guidelines
When setting up a network and configuring SPAN on a Catalyst switch, follow these guidelines:
- Have separate voice and data VLANs. On many switches, SPAN can be configured to monitor a VLAN. The VoIP Monitor server is only interested in voice traffic, not data, so this feature can be used to minimize the amount of extra traffic that the VoIP Monitor server will bear.

- On Catalyst 2900XL and 3500XL switches, the VoIP Monitor server and the IP phones must be in the same VLAN.

- When monitoring the entire voice VLAN on Catalyst 4000, 6000, and 6500 switches, configure SPAN to monitor only the inbound (rx) or outbound (tx) packets. Monitoring both types of packets (the default setting) can result in duplicate packets being sent to the VoIP Monitor server.

For example, if a voice VLAN setting is 10, and the VoIP Monitor server Ethernet port is 2/20, then the Catalyst SPAN command is:

```
Cat6000> (enable) set span 10 2/20 rx inpkts enable create
```

In this example, `rx` specifies inbound packets only, and `inpkts enable` allows the VoIP Monitor server connected to this port to send and receive normal network traffic in addition to the traffic that is sent to it by SPAN. By default, this option is disabled. It must be enabled for the server to function properly.

- Catalyst switches can have varying numbers of simultaneous SPAN ports, depending on the model. For example, a 3500XL can have only one SPAN port, while a 6000 can have two SPAN ports with the `inpkts enable` option.

### Specific Configuration Examples

#### Single Catalyst 3524XL

In a network configuration where:

- IP phones are on ports FastEthernet0/1 through 0/5
- VoIP Monitor server is on port FastEthernet0/10
- IP phones and VoIP Monitor server are in the same VLAN

Catalyst 3524XL SPAN commands are:

```
Cat3524XL(config)#interface FastEthernet 0/10
Cat3524XL(config-if)#port monitor FastEthernet 0/1
Cat3524XL(config-if)#port monitor FastEthernet 0/2
Cat3524XL(config-if)#port monitor FastEthernet 0/3
Cat3524XL(config-if)#port monitor FastEthernet 0/4
Cat3524XL(config-if)#port monitor FastEthernet 0/5
Cat3524XL(config-if)#exit
```
Single Catalyst 6000

In a network configuration where:
- IP phones are in VLAN 15
- VoIP Monitor server is on port 2/10

Catalyst 6000 SPAN commands are:

```
Cat6000> (enable) set span 15 2/10 rx inpkts enable create
```

Single Catalyst 6000 and Multiple Catalyst 3524XLs, with Gateway-Only Monitoring and No Agent-to-Agent Monitoring

In this configuration, the supervisors are interested only in calls going through the gateway, so that the network configuration can have a single VoIP Monitor server on the Catalyst 6000. Silent monitoring and recording of agent-to-agent calls is not required.

In this configuration, the:
- Voice gateway is directly connected to the Catalyst 6000
- Catalyst 3524XLs are directly trunked to the Catalyst 6000
- IP phones are in VLAN 15
- VoIP Monitor server is on port 2/10 on the Catalyst 6000

The Catalyst 6000 SPAN commands are:

```
Cat6000> (enable) set span 15 2/10 rx inpkts enable create
```

Single Catalyst 6000 and Multiple Catalyst 3524XLs, with Required Agent-to-Agent Monitoring

In this configuration, the supervisors must be able to monitor both gateway and agent-to-agent calls. Since agent-to-agent calls on a single 3524XL switch would not be visible on the Catalyst 6000, we need to install two VoIP Monitor servers, one for each Catalyst 3524XL.

In this configuration, the:
- Voice gateway is directly connected to the Catalyst 6000
- Catalyst 3524XLs are directly trunked to the Catalyst 6000
- IP phones are on ports FastEthernet 0/1 and 0/4
- VoIP Monitor server is on port FastEthernet 0/5
- IP phones and VoIP Monitor server are in the same VLAN
For Catalyst 3524XL Number 2:
■ IP phones are on ports FastEthernet 0/3 and 0/4
■ VoIP Monitor server is on port FastEthernet 0/6
■ IP phones and VoIP Monitor server are in the same VLAN

For Catalyst 3524XL Number 1, the SPAN commands are:
Cat3524XL1(config)#interface FastEthernet 0/5
Cat3524XL1(config-if)#port monitor FastEthernet 0/1
Cat3524XL1(config-if)#port monitor FastEthernet 0/4
Cat3524XL1(config-if)#exit

For Catalyst 3524XL Number 2, the SPAN commands are:
Cat3524XL2(config)#interface FastEthernet 0/6
Cat3524XL2(config-if)#port monitor FastEthernet 0/3
Cat3524XL2(config-if)#port monitor FastEthernet 0/4
Cat3524XL2(config-if)#exit

**Single Catalyst 6000 and Multiple Catalyst 3524XLs, with Routers Separating the Switches**

In this configuration, routers separate the various Catalyst switches. Regardless if it is necessary or not to monitor agent-to-agent calls, at least two VoIP Monitor servers are required, one for each Catalyst 3524XL switch.

Monitoring on the Catalyst 6000 is not possible because there is a router between the Catalyst 6000 and the Catalyst 3524XLs.

In this case, the implementation of the configuration is the same as for the section “Single Catalyst 6000 and Multiple Catalyst 3524XLs, with Required Agent-to-Agent Monitoring” above.

**NOTE:** 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).
Upgrading From a Previous Version

The following versions of Cisco Desktop Product Suite can be upgraded to version 4.6 by installing version 4.6 over them:

- 4.2.0
- 4.2.1
- 4.4.0

If you have any other version of Cisco Desktop Product Suite, it must be uninstalled before version 4.6 can be installed.

Hot Fixes

If you have any CAD hot fixes installed, uninstall them before upgrading to version 4.6. 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)]

For instance:

Hot Fix 01 for: Servers, Admin
Saving Data From a Previous Version

If you are upgrading your software from versions 4.0 or 4.1, you can save your configuration files and settings for Desktop Administrator, the Enterprise server, and the Voice-Over IP Monitor server by using the UpdateUtil program (included on the installation CD).

When you install version 4.6, saved data can be automatically restored at the end of the installation of the Primary Directory Services and Directory Services Sync server applications, Voice-Over IP Monitor server application, and Desktop Administrator. You will be asked if you want to do this. If you answer Yes and enter the path to the Backup folder, the data will be restored.

Backing Up Your Data

To back up your data, follow these steps:

1. Locate the file UpdateUtil.exe on the installation CD.
2. Double-click the file to run the program.
3. The program locates the files on your PC that can be backed up. For example, in Figure 1-5 the program has located Administrator files. You could also see entries for Enterprise Server and/or VoIP Monitor Server.
4. Choose a location for the backup folder.
5. Click Backup. The program backs up those files in a subfolder under the Backup folder—one for Enterprise, one for VoIP Monitor, and one for Administrator.

Figure 1-5. UpdateUtil program window.
Preinstallation Considerations

Configuration Files

When installing the Cisco Desktop Product Suite, it is recommended that the configuration files be installed on a network drive or other accessible location. This location should:

- be a public network drive or a local shared folder that all agents can access at all times.
- allow write access to all agents. (See “Permission Requirements” in Chapter 3 of the Service Information manual for more information.)

File Sharing

If you plan to install the configuration files locally (on the administrator’s PC), the administrator’s PC must have file sharing enabled. File sharing allows users to access files and folders on the administrator’s PC.

**NOTE:** This configuration is not recommended. If file sharing is enabled on the administrator’s PC, it allows Desktop Administrator to share a local configuration with all agents. It is recommended that the administrator’s PC be a Windows NT platform, because that does not restrict the number of users that can connect to the computer at any one time.


When installing the Cisco Desktop Product Suite on Windows NT Workstation, Windows 2000, and Windows XP Professional Edition platforms, 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.
Installation-Related Configuration

Figure 1-6 displays the installation-related configuration of the IPCC bundle. Use this diagram to understand what data is requested in the installation procedure. Refer to this diagram when completing the Preinstallation Survey on page 1-27.

Figure 1-6. Installation-related configuration with one logical contact center
Figure 1-7 illustrates the configuration of a system with multiple logical contact centers. Note the use of multiple Voice-Over IP Monitor servers within each logical contact center.

Figure 1-7. System architecture with multiple logical contact centers
Preinstallation Survey

Use the following worksheet to make sure you have assembled the information necessary to successfully install the Cisco Desktop Product Suite. Refer to Figure 1-6 on page 1-25 and Figure 1-7 on page 1-26 to assist in completing the worksheets.

NOTE: This worksheet collects all information that might possibly be required when installing the Cisco Desktop Product Suite. Depending on your system configuration, you may not need to complete every section of the worksheet.

Information Required for Installing Cisco Desktop Product Suite

<table>
<thead>
<tr>
<th>Primary Directory Services server, Directory Services Sync server, and Replication server</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Sync server uses an ODBC connection to communicate with the ICM Logger’s database. If you are using the Named Pipes network library as the connection method, you must enter a user account with privileges capable of creating a named pipe on the ICM Logger server. If you are using TCP/IP, you may use the local administrator account. The Replication server application is installed automatically when installing the primary Directory Services server application, if you have provided the location of a secondary Directory Services server application.</td>
</tr>
<tr>
<td>Hostname or IP address:</td>
</tr>
<tr>
<td>Sync server application user name:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secondary Directory Services server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname or IP address:</td>
</tr>
</tbody>
</table>
Information Required for Installing Cisco Desktop Product Suite — Continued

<table>
<thead>
<tr>
<th><strong>Cisco CallManager</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>If there is more than one CallManager, use the information for the Publisher CallManager.</td>
<td></td>
</tr>
<tr>
<td>Hostname or IP address:</td>
<td></td>
</tr>
<tr>
<td>Peripheral ID:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Primary Cisco CallManager CTI server</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname or IP address:</td>
<td></td>
</tr>
<tr>
<td>Port ID:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Secondary Cisco CallManager CTI server</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname or IP address:</td>
<td></td>
</tr>
<tr>
<td>Port ID:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Cisco IP IVR</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname or IP address:</td>
<td></td>
</tr>
<tr>
<td>Peripheral ID:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Primary Cisco IP IVR CTI server</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname or IP address:</td>
<td></td>
</tr>
<tr>
<td>Peripheral ID:</td>
<td></td>
</tr>
</tbody>
</table>
### Information Required for Installing Cisco Desktop Product Suite – Continued

<table>
<thead>
<tr>
<th><strong>Secondary Cisco IP IVR CTI server</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname or IP address:</td>
<td></td>
</tr>
<tr>
<td>Port ID:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Cisco ICM Logger</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname or IP address:</td>
<td></td>
</tr>
<tr>
<td>ICM SQL Logger database login:</td>
<td></td>
</tr>
<tr>
<td>ICM SQL Logger database password:</td>
<td></td>
</tr>
<tr>
<td>ICM instance:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Call/Chat server and Enterprise server</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>IP Phone Agent server</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The user account needs read/write privileges to the location where the shared configuration files are stored.</td>
<td></td>
</tr>
<tr>
<td>IP address:</td>
<td></td>
</tr>
<tr>
<td>Server application user account user name:</td>
<td></td>
</tr>
<tr>
<td>Server application user account password:</td>
<td></td>
</tr>
</tbody>
</table>
### Information Required for Installing Cisco Desktop Product Suite — Continued

<table>
<thead>
<tr>
<th><strong>Recording and Statistics server</strong></th>
<th>The user account needs read/write privileges to the location where the shared configuration files are stored.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname or IP address:</td>
<td></td>
</tr>
<tr>
<td>Server application user account user name:</td>
<td></td>
</tr>
<tr>
<td>Server application user account password:</td>
<td></td>
</tr>
<tr>
<td>Database login:</td>
<td></td>
</tr>
<tr>
<td>Database password:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Voice-Over IP Monitor server 1</strong></th>
<th>There can be more than one VoIP Monitor server per logical contact center. Make sure you know this information for the other server installations.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname or IP address:</td>
<td></td>
</tr>
<tr>
<td>Database login (default = CiscoCCMReader):</td>
<td></td>
</tr>
<tr>
<td>Database password:</td>
<td></td>
</tr>
<tr>
<td>Packet sniffer IP address:</td>
<td></td>
</tr>
</tbody>
</table>

### Notes:

- All servers should be given static IP addresses. An IP address provided by DHCP could change in the future, possibly rendering agent desktops unusable.
- The Recording and Statistics server uses an SQL database to store data. If there is no SQL server database engine already installed on the PC where this server is installed, it will install MSDE. If an MSDE or SQL server database engine already exists, the server will attach its database to the database engine.
Installation

Overview

Install the Cisco Desktop Product Suite according to the configuration you have chosen for your contact center (see "System Configurations" on page 1-6 for three configuration scenarios).

In the recommended configuration (Scenario 1):

- The Directory Services server and the Directory Services Sync server are installed on the same machine that hosts the ICM Peripheral Gateway
- The optional servers are installed on the same machine as the Directory Services server and Directory Services Sync server or on other machines, depending on space and load requirements
- Global configuration files and the installation files for Agent Desktop and Supervisor Desktop are placed on a networked file server

We recommend that you install Desktop Product Suite applications in this order:
1. Primary Directory Services server and Directory Services Sync server
2. Other servers
3. Desktop Administrator
4. Supervisor Desktop and Agent Desktop

NOTE: It is highly recommended that you complete the preinstallation survey (see "Preinstallation Survey" on page 1-27) so that you have all the relevant installation information at hand while you run Install Manager.
Installation Procedure

Starting Install Manager

Install Manager (InstallManager.exe) is the program that assists in installing the components of the Cisco Desktop Product Suite.

To start Install Manager:

1. In Windows Explorer, browse to the Desktop Product Suite CD.
2. Double-click **InstallManager.exe**.

Install Manager starts, and the Welcome window appears. (See Figure 2.)

**NOTE:** All Install Manager windows are depicted here in expanded mode, with the Info pane open.

---

**Figure 2-1. Welcome window.**
Installing Servers

Once Install Manager is started, follow these steps to install Cisco Desktop Product Suite servers.

**NOTE:** If you press Esc during the install process, the installation program closes and all entered information is lost.

1. On the Welcome window, click **Next**.

   The Options window appears.

   **Figure 2-2. Options window.**

   ![Options window](image)

   - **Cisco Desktop Product Suite for IPCC**
     - **Servers**
       - Primary Directory Services Server and Sync Server
       - Desktop Base Server
       - Voice Over IP Monitor Server
       - Recording and Statistics Server
       - Secondary LDAP Server
     - **Desktop Administrator**
     - **Supervisor Desktop**
       - On-Site Supervisor Desktop
       - On-Site Supervisor Desktop with Media Termination
       - Remote Supervisor Desktop
     - **Agent Desktop**
       - Agent Desktop
       - Agent Desktop with Media Termination
     - **Documentation**
       - Desktop Product Suite Documentation (PDF format)
   - **Post-Install Tools**
     - Reload LDAP Settings

2. Check the check box next to the server applications you want to install.

   You may install more than one server application at a time. Install Manager will make sure that the applications do not conflict with one another and that the packages are installed in the correct order.

   **NOTE:** You cannot install the Primary Directory Services and Secondary Directory Services server applications on the same PC.
3. Click **Next**.

The License Agreement window appears. (See Figure 2-3.)

**Figure 2-3. License Agreement window.**

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

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

   **NOTE:** There might be more than one License Agreement window, depending on the components you checked in the Options window.

   The Install Manager Mode window appears. (See Figure 2-4.)
5. Choose the installation mode you want to use during the installation.

The possible installation modes are:

- **Novice Mode** steps you through the install process, and provides help for determining the information you must enter for a successful install. You will see every window in the install process, even if the system already has the information requested in the window. This mode is best for installers who do not install these applications very often.

- **Expert Mode** displays only the windows needed for a successful installation and skips windows asking for information the system already has. Help is available, but not automatically displayed. This mode is best for experienced installers.

Depending on your install mode choice, all or some of the following windows appear. This procedure describes the windows that appear during a Novice Mode installation.

6. Click **Next**.

The Language window appears. (See Figure 2-5.)
7. Choose the appropriate language for your contact center, and then click Next.

The Restore Backup Data window appears. (See Figure 2-6.)
8. If you want to restore data saved from versions 4.0 or 4.1 of Cisco Desktop Product Suite, click **Yes**. If not, click **No**.

   If you are upgrading from versions 4.0 or 4.1, the UpdateUtil program (available on the installation CD) saves the configuration files and setting for Desktop Administrator, the Enterprise server application, and the Voice-Over IP Monitor server application.

   If you are upgrading from versions after 4.1, it is not necessary to restore data. You can install version 4.6 over your version, and the configuration files and settings are preserved.

   See "Saving Data From a Previous Version" on page 1-23 for more information on how to use the UpdateUtil program.

9. Click **Next**.

   The Machine IP Address window appears. (See Figure 2-7.)
10. From the IP Address drop-down list, choose the IP address of the PC on which you are installing the selected server application(s).

The server applications must register their IP address with the Directory Services server. If the PC on which they are being installed has more than one network card, it will have more than one IP address. The IP address you select should be the address associated with the card being used to connect to the LAN.

11. Click **Next**.

The Directory Services Server: Location window appears. (See Figure 2-8.)
12. Enter the following information:

- Host name or IP address of the Primary Directory Services server application
- Host name or IP address of the optional Secondary Directory Services server application, if you are installing a backup Directory Services server

The Primary and Secondary Directory Services server applications must be installed on different computers, so that if the Primary fails, the Secondary can take over.

**NOTE:** You must enter the location of the Secondary Directory Services server application at this time so that the Primary Directory Services server application will be configured to replicate its data correctly. You will actually install the Secondary Directory Services server application when you run Install Manager on that particular PC.

13. Click **Next**.

The Directory Services Server: Logical Contact Center window appears. (See Figure 2-9.)
14. Choose an existing logical contact center from the drop-down list, or type the name of a new one in the Logical Contact Center field.

The logical contact center is the root of the Directory Services tree where Cisco Desktop applications query for information.

Your contact center can have multiple logical contact centers. Each desktop and server in your contact center belongs to only one logical contact center, with the exception of the Primary and Secondary Directory Services and Directory Services Sync server applications. (See Figure 1-7 on page 1-26 for an illustration of a contact center with multiple logical contact centers.)

If you create a new logical contact center here, it will be created in the Directory Services server application.

15. Click Next.

The Desktop Version window appears. (See Figure 2-10.)
Figure 2-10. Desktop Version window.

16. Select the Cisco Desktop application version you are installing in your contact center. When you select the enhanced version, Agent Desktop and Desktop Administrator include the following features:

   - Enhanced Agent Desktop includes administrator-configured task buttons and the Work Ready and Work Not Ready agent states.
   - Enhanced Desktop Administrator enables administrators to customize the Agent Desktop interface and to automate work flows.

   See the Cisco Agent Desktop User Guide and Cisco Desktop Administrator User Guide for more information about the enhanced version features.

17. Click Next.

   The Destination Folder window appears. (See Figure 2-11.)
18. Choose the destination folder where Install Manager will install the applications you selected.

You can accept the default folder location or click **Browse** to navigate to a different folder.

Install Manager will create any needed subfolders under the folder you select here.

**WARNING**: If you are upgrading from a previous version, do not change the destination folder location. If you do so, the uninstall process will not function correctly.

19. Click **Next**.

The Cisco CallManager window appears. (See Figure 2-12.)
20. Enter the host name or IP address of the computer where the Cisco CallManager is installed.

   If you are installing into a CallManager Cluster, use the host name or IP address of the Publisher CallManager.

21. Click **Next**.

   The Cisco CallManager Peripheral ID window appears. (See Figure 2-13.)
22. Enter the peripheral ID assigned to the Cisco CallManager in Intelligent Contact Management (ICM).

   The peripheral ID is used by the applications you are installing to filter information such as agents and skills.

   The peripheral ID number can be found using PG Explorer in the ICM Configuration Manager (ICM version 4.6.2).

23. Click Next.

   The Cisco CallManager CTI Server window appears.
24. Enter the following information:
   - Host name or IP address and port number of the Side A (primary) ICM CTI server application
   - Host name or IP address and port number of the Side B (secondary) optional ICM CTI server application

   The ICM CTI server communicates with the CallManager or CallManager cluster.

   The Side B information is optional. It is needed only if you are using a duplexed environment, in which case the Side B server application is the backup for the Side A server application.

25. Click **Next**.

   The Installation Environment Question dialog box appears. (See Figure 2-16.)
26. Indicate if there is a separate CTI server for the Cisco IP IVR server:

- If you click **Yes**, the Cisco IP IVR CTI Server window appears. (See Figure 2-17.)
- If you click **No**, the next Installation Environment Question dialog box appears. (See Figure 2-18.)
27. Enter the following information:
   - Host name or IP address and port number of the Side A (primary) IP IVR CTI server application
   - Host name or IP address and port number of the Side B (secondary) optional IP IVR CTI server application

   The IP IVR CTI server communicates with the Cisco IP IVR server.
   The Side B information is optional. It is needed only if you are using a duplexed environment, in which case the Side B server application is the backup for the Side A server application.

28. Click **Next**.

   The next Installation Environment Question dialog box appears. (See Figure 2-18.)
29. Indicate if the ICM Logger is located on the same computer as the Cisco CallManager CTI server:
   - If you click Yes, the Start Copying Files window appears. (See Figure 2-20.)
   - If you click No, the Cisco ICM Logger window appears. (See Figure 2-19.)
30. Enter the following information:
   - Host name or IP address of the Side A ICM Logger
   - Host name or IP address of the Side B optional ICM Logger

This information is required if the ICM Logger is not located on the same computer as the Cisco CallManager CTI server application.

The Side B information is optional. It is needed only if you are using a duplexed environment, in which case the Side B ICM Logger is the backup for the Side A ICM Logger.

31. Click Next.

The Start Copying Files window appears. (See Figure 2-20.)
32. The settings you have entered are listed in the Current Settings pane.
   a. Review the settings for accuracy.
   b. If any are incorrect, click **Back** until you reach the window on which the information was entered.
   c. Correct the information, and then click **Next** until you return to the Start Copying Files window.

33. Click **Next**.
    Install Manager installs the selected applications. When the installation is completed, the Installation Results window appears.

34. Click **Finish** to complete the installation process.
    If you wish to install more applications, start Install Manager and proceed through the installation process again.
Other Information Required During Server Installation

When installing the Recording and Statistics, Voice-Over IP Monitor, Directory Services Sync, and IP Phone Agent server applications, you will be asked for information needed for accessing various databases and shared configuration files.

**NOTE:** If your configuration is set up so that it spans two domains (for example, the ICM is in one domain and the VoIP Monitor server is in another), the user name and password you enter in the following windows must be identical across the two domains and in a trusted relationship. Install Manager does not validate user names and passwords to ensure they are in trusted domain relationships, so you must make sure they are correct.
Directory Services Sync Server Setup

The Sync server uses an ODBC connection to communicate with the ICM Logger’s database. If the logger’s database is using the Named Pipes network library as the connection method, you must enter a user account with sufficient privileges to create a named pipe on the ICM Logger server. If the logger’s database is using TCP/IP, you may use the local administrator account.

Figure 2-21. Directory Services Sync Server Setup User Account window.

In the Directory Services Sync Server Setup User Account window, select an existing user from the drop-down list or create a new user on the local machine.
Installation Procedure

Figure 2-22. Directory Services Sync Server ICM SQL Logger Database Information window.

Enter the ICM instance, login, and password of a user who has read privileges for the ICM SQL Logger database.

**NOTE:** There is no password validation, so if you enter an incorrect password the installation proceeds without problems. However, the server will not be able to synchronize with the Logger database because the password is invalid. The password cannot be corrected in the registry because it is encrypted. To correct this problem, you must remove and reinstall the Directory Services Sync server.

**Recording and Statistics Server Setup**

When installing the Recording and Statistics server application, the user must have sufficient privileges to manage audio files located in the shared configuration folder and to access and make changes in the Recording and Statistics (RASCAL) database.
In the Recording and Statistics Server Setup User Account window, select an existing user from the drop-down list or create a new user on the local machine.
Enter the Login and password for the Recording and Statistics (RASCAL) database. The user must have the rights to create a new Recording and Statistics database on the existing SQL Server.

This window appears only if an existing MSDE or SQL Server database is found on the computer.

If no database is detected, MSDE is automatically installed and this window does not appear. (The installation knows the login and password for the database it creates.)
Voice-Over IP Monitor Server Setup

When installing the VoIP Monitor server application, the system needs to know the location of the VoIP packet sniffer. The user also must be able to access the publisher CallManager database.

Figure 2-25.  VoIP Monitor Server Setup Packet Sniffer window.

Enter the IP address of the network adaptor to which packets are sent to be sniffed.
Figure 2-26. VoIP Monitor Server Setup Database Login Information window.

Accept the default login (CiscoCCMReader) and password (cowboys). This login is needed to enable the VoIP Monitor server to read the publisher CallManager database.

**NOTE:** This default login and password belong to a default user created in the CallManager database when CallManager is installed. The default login should be valid, but it is possible that it has been changed. It is a good idea to check your CallManager setup to ensure it is valid.
IP Phone Agent Interface Setup

When installing the IP Phone Agent server application, the user must have sufficient privileges to read the license files located in the shared configuration folder.

Figure 2-27. IP Phone Agent Interface Setup User Account window.

In the IP Phone Agent Server Setup User Account window, select an existing user from the drop-down list or create a new user on the local machine.
Installing Desktop Applications

Desktop Administrator

When Desktop Administrator is installed for the first time from the installation CD, the files necessary to install subsequent instances of Desktop Administrator are copied from the installation CD to the location you choose during the installation for the shared configuration files. Therefore, subsequent instances of Desktop Administrator can be installed from either the installation CD or from the shared file location.

NOTE: All instances of Desktop Administrator should be installed on a PC with a local-language operating system, so that chat messages, tooltips, and other communication within the contact center are in the local language.

To install Cisco Desktop Administrator, follow these steps.

1. Start Install Manager. (See "Starting Install Manager" on page 2-2.)

   **NOTE:** If this is the first time Desktop Administrator is being installed, Install Manager is located on the installation CD. If this is a subsequent installation, you can install from either the installation CD or from the shared files location.

2. On the Welcome window, click **Next**.
   The Options window appears. (See Figure 2-2 on page 2-3.)

3. Check the check box next to Desktop Administrator, and then click **Next**.
   The License Agreement window appears. (See Figure 2-3 on page 2-4.)

4. Click **Yes** to accept the End User License Agreement.
   The installation quits if you do not agree to the End User License Agreement.

5. The Install Manager Mode window appears. (See Figure 2-4 on page 2-5.)

6. Choose the installation mode you want to use during the installation.
   The possible installation modes are:
   - **Novice Mode** steps you through the install process, and provides help for determining the information you must enter for a successful install. You will see every window in the install process, even if the
system already has the information requested in the window. This mode is best for installers who do not install these applications very often.

■ **Expert Mode** displays only the windows needed for a successful installation and skips windows asking for information the system already has. Help is available, but not automatically displayed. This mode is best for experienced installers.

Depending on your install mode choice, all or some of the following windows appear. This procedure describes the windows that appear during a Novice Mode installation.

7. Click **Next**.

   The Restore Backup Data window appears. (See Figure 2-6 on page 2-7.)

8. If you want to restore data saved from a previous version of Cisco Desktop Product Suite, click **Yes**. If not, click **No**.

   The UpdateUtil program (available on the installation CD) saves the configuration files and settings for Desktop Administrator, the Enterprise server application, and the Voice-Over IP Monitor server application.

   You can save and restore data from versions 4.0 and 4.1.

   See “Saving Data From a Previous Version” on page 1-23 for more information on how to use the UpdateUtil program.

9. Click **Next**.

   The Directory Services Server: Location window appears. (See Figure 2-8 on page 2-9.)

10. Enter the following information:

    ■ Host name or IP address of the Primary Directory Services server application

    ■ Host name or IP address of the optional Secondary Directory Services server application, if there is a backup Directory Services server

11. Click **Next**.

   The Directory Services Server: Logical Contact Center window appears. (See Figure 2-9 on page 2-10.)

12. Choose a logical contact center from the drop-down list, and then click **Next**.

   The Use Previous Data dialog box appears.

13. Click **Yes** if you want to use installation information stored in the Directory Services server, or **No** if you do not.
If you choose Yes, many of the upcoming fields will be autofilled with the existing installation information. If you choose No, you will have to enter that information yourself.

14. Click **Next**.

The Destination Folder window appears. (See Figure 2-11 on page 2-12.)

15. Choose the destination folder where Install Manager will install Desktop Administrator.

You can accept the default folder location or click **Browse** to navigate to a different folder.

Install Manager will create any needed subfolders under the folder you select here.

16. Click **Next**.

17. The Configuration File Location window appears.

18. Choose the destination folder where Install Manager will install the necessary configuration files.

You can accept the default folder location or click **Browse** to navigate to a different folder.

If these configuration files are to be shared, make sure the destination folder is read/write accessible to all desktop application users. See "Sharing Configuration Files" on page 1-10 for more information.

If a previous installation of Desktop Administrator has designated a configuration file folder other than the folder you choose, you may see the warning shown in Figure 2-28.

**Figure 2-28. Configuration file location warning.**

![Configuration file location warning]

Make sure you are selecting the correct location for your configuration files, and click Yes or No accordingly.

**NOTE:** Once you pass the Choose Configuration File Location window, you cannot go back to that window to change the configuration file location. To change the configuration file location, you must cancel the installation and begin again.
19. Click **Next**.
   The Cisco CallManager window appears. (See Figure 2-12 on page 2-13.)

20. Enter the host name or IP address of the computer where the Cisco CallManager is installed.
   If you are installing into a CallManager Cluster, use the host name or IP address of the Publisher CallManager.

21. Click **Next**.
   The Start Copying Files window appears. (See Figure 2-20 on page 2-20.)

22. The settings you have entered are listed in the Current Settings pane.
   a. Review the settings for accuracy.
   b. If any are incorrect, click **Back** until you reach the window on which the information was entered.
   c. Correct the information, and then click **Next** until you return to the Start Copying Files window.

23. Click **Next**.
   Install Manager installs Desktop Administrator. When the installation is completed, the Installation Results window appears.
   During the installation, InstallShield will ask you to provide the following information:
   - Dial plan settings—the area code, outside line access numbers for local and long distance dialing, and whether or not to add a "1" when dialing long distance numbers
   - VoIP Monitor database login information (see Figure 2-26 on page 2-27)
   - Adobe Acrobat Reader (needed to view the product documentation)—if InstallShield detects that it doesn’t exist on this PC, it gives you the option of installing it now

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

After you have installed Desktop Administrator, the IPCC License Administration application starts automatically. See "Licensing Cisco Desktop Product Suite" on page 2-38 for more information.

**Supervisor Desktop and Agent Desktop**

When Desktop Administrator is installed, the files necessary to install Supervisor Desktop and Agent Desktop are copied from the installation CD to the same location you chose for the shared configuration files. As a result, you can install them from either the installation CD or from this shared location.
To install Supervisor Desktop and Agent Desktop, follow these steps. The procedure is identical for both applications.

**NOTE:** When you install Supervisor Desktop, you will also automatically install Agent Desktop.

**To install Supervisor Desktop and Agent Desktop:**

1. Start Install Manager. (See "Starting Install Manager" on page 2-2.)
2. On the Welcome window, click **Next**.
   
   The Options window appears. (See Figure 2-2 on page 2-3.)
3. Check the check box next to the application you want to install, and then click **Next**.
   
   The License Agreement window appears. (See Figure 2-3 on page 2-4.)
4. Click **Yes** to accept the End User License Agreement.
   
   The installation quits if you do not agree to the End User License Agreement.
5. The Install Manager Mode window appears. (See Figure 2-4 on page 2-5.)
6. Choose the installation mode you want to use during the installation.
   
   The possible installation modes are:
   
   ■ **Novice Mode** steps you through the install process, and provides help for determining the information you must enter for a successful install. You will see every window in the install process, even if the system already has the information requested in the window. This mode is best for installers who do not install these applications very often.
   
   ■ **Expert Mode** displays only the windows needed for a successful installation and skips windows asking for information the system already has. Help is available, but not automatically displayed. This mode is best for experienced installers.

Depending on your install mode choice, all or some of the following windows appear. This procedure describes the windows that appear during a Novice Mode installation.

7. Click **Next**.
   
   The Machine IP Address window appears. (See Figure 2-7 on page 2-8.)
8. From the IP Address drop-down list, choose the IP address of the PC on which you are installing the application.
9. Click **Next**.
The Directory Services Server: Location window appears. (See Figure 2-8 on page 2-9.)

10. Enter the following information:

   - Host name or IP address of the Primary Directory Services server application
   - Host name or IP address of the optional Secondary Directory Services server application, if there is a backup Directory Services server

11. Click **Next**.

    The Directory Services Server: Logical Contact Center window appears. (See Figure 2-9 on page 2-10.)

12. Choose a logical contact center from the drop-down list, and then click **Next**.

    The Use Previous Data dialog box appears.

13. Click **Yes** if you want to use installation information stored in the Directory Services server, or **No** if you do not.

    If you choose Yes, many of the upcoming fields will be autofilled with the existing installation information. If you choose No, you will have to enter that information yourself.

14. Click **Next**.

    The Destination Folder window appears. (See Figure 2-11 on page 2-12.)

15. Choose the destination folder where Install Manager will install the application(s).

    You can accept the default folder location or click **Browse** to navigate to a different folder.

    Install Manager will create any needed subfolders under the folder you select here.

16. Click **Next**.

    The Start Copying Files window appears. (See Figure 2-20 on page 2-20.)

17. The settings you have entered are listed in the Current Settings pane.

    a. Review the settings for accuracy.
    b. If any are incorrect, click **Back** until you reach the window on which the information was entered.
    c. Correct the information, and then click **Next** until you return to the Start Copying Files window.

18. Click **Next**.

    Install Manager installs the selected application(s).
19. During the installation of Agent Desktop, the Information window appears.  
(See Figure 2-29.)

**Figure 2-29. Information window.**

This window provides information about NIC card compatibility with the 
CSD silent monitoring feature, including potential problems and solutions.

Review the information.

20. Click **Next**.

The VoiP Packet Sniffer window appears. (See Figure 2-30.)
21. From the IP Address drop-down list, select the IP address of the network adaptor in the PC to which packets are sent for sniffing. This enables this instance of Agent Desktop to use desktop monitoring.

   When the installation is completed, the Installation Results window appears.

22. Click Finish to complete the installation process.

Saving a Personal Phone Book

You can keep a personal phone book from a previous version of Agent Desktop and use it with an upgrade of Agent Desktop.

   NOTE: You must move the personal phone book file to a new location before removing the previous version of Agent Desktop. If you don’t, the file will be removed with the rest of the application.

To save and restore a personal phone book:

1. In Windows Explorer, navigate to the …Cisco\Desktop\config folder and locate the personal.csv file.
2. Move the personal.csv file to another folder on your PC.

   **NOTE:** This folder must not be underneath the Cisco folder, or it will be removed when you uninstall the old version of Agent Desktop.

3. Install the new version of Agent Desktop. (See "To install Supervisor Desktop and Agent Desktop:" on page 2-33.)

   At the end of the install, you will see an informational dialog box that reads, "If you have saved a personal phone book, you may now restore it to the folder …\Cisco\Desktop\config."

   The exact folder location shown in the dialog box is the location to which you have installed Agent Desktop.

4. Click **OK** to close the dialog box.

5. After the installation is finished, move the personal.csv file to the config folder.

   The personal phone book is now saved to the new version of Agent Desktop.

### Post-Install Tools

You can reset your system’s Directory Services settings with the “Reload LDAP Settings” post-install tool.

This application displays all the windows you see when installing servers (see "Installing Servers" on page 2-3). This enables you to re-enter all the server information in order to update Directory Services.

   **NOTE:** The application does *not* reinstall the server applications.
Licensing Cisco Desktop Product Suite

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

Until you have licensed it, none of the Cisco Desktop software, except for Desktop Administrator, will run.

To start IPCC License Administration:

2. Navigate to the …\Cisco\Desktop\bin folder.
3. In the folder, double-click LicenseAdmin.exe.

   IPCC License Administration starts. (See Figure 2-31.)

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

Figure 2-31. IPCC License Administration window.
To license your Cisco Desktop applications:

1. In the IPCC License Administration window, click License URL.
   
   Your web browser is started and the secured licensing website at http://209.46.83.138/sws/ciscoLicense/LicenseRegister.html is accessed.

2. Follow the instructions on the website, entering installer and contact center information, and license request numbers.

3. After you submit the information, the website returns with a page listing the license codes and verification numbers you need to license the products.

   Figure 2-32. Web page showing returned license codes and verification numbers.

<table>
<thead>
<tr>
<th>Package</th>
<th>License Code</th>
<th>Verification #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>1321998</td>
<td>1376133809</td>
</tr>
<tr>
<td>Agent Media Termination</td>
<td>13285482</td>
<td>1379349041</td>
</tr>
<tr>
<td>IP Phone Agent</td>
<td>13901126</td>
<td>1109704985</td>
</tr>
<tr>
<td>IP Enhanced Supervisor</td>
<td>13768221</td>
<td>1378295857</td>
</tr>
<tr>
<td>Agent Recording</td>
<td>13002819</td>
<td>1110843953</td>
</tr>
</tbody>
</table>

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

   IPCC License Administration creates a licensing file and places it in the folder where the global configuration files are located. It then activates all the licensed applications.
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 ICM 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:
       
       \[http://192.168.252.44:8080/ipphone/jsp/sciphonexml/IPAgentInitial.jsp\]

       where:

       - 192.168.252.44 is the IP address of the machine where the Agent State service is loaded
       - 8088 is the Tomcat webserver port (if 8088 is not the port number, check the port parameter in the file C:\Program Files\wfavidi\ 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
NOTE: You will not find a file called IPAgentInitial.jsp at this location; there will be a file called IPAgentInitial.class, which contains the implementation of the .jsp file.

NOTE: The Tomcat webserver is included with the installation.

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

### Assigning the IP Phone Service to IP Agent Phones

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

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

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

1. On the Device menu, choose **Phone**.
   The Find and List Phones window appears.

2. 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 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 next 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. Use 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.

**Changing the Default URL Authentication Parameter**

The default URL Authentication parameter can be bypassed to maximize system performance. This prevents the CallManager from polling all devices in the system to authenticate a specific device every time that device pushes information to the CallManager.

1. From the Service menu, choose **Enterprise Parameters**. The Enterprise Parameters Configuration window appears.
2. Locate the URL Authentication parameter.
3. Change the default value to the following:
   
   ```
   http://Tomcat webserver IP address:8088/ippophone
   /jsp/sciphonexml/IPAgentAuthenticate.jsp
   ```

   **Note**: This URL is case sensitive.
4. Click **Update**.

5. Reset all IP Phone Agent phones by unplugging their power cords, and then plugging them in again.

**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.
Configuring Media Termination for Agents Working Over a VPN

If an agent is using Cisco Agent Desktop with Media Termination over a VPN client, you must manually change the port number used by Tomcat. If this manual change is not performed, there will be one-way audio only when CAD with Media Termination is used over a VPN client.

**To manually change the port number:**

1. On the Tomcat server, open the `server.xml` file for editing.
   
   This file is located in the `<Tomcat_Home>/conf` folder.

2. Change the http port parameter.

   Locate these lines:
   
   `<Parameter name>="port" value="8088"/>
   
   Change **8088** to **80** and then save the file.

3. Stop and then restart the Tomcat server from the Windows Services Manager.

4. In CallManager, navigate to the Cisco IP Phone Service Configuration page for the `< ? >` (Feature > Cisco IP Phone Services > Cisco IP Phone Services Configuration).

5. In the Service URL field, change the URL from:

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

   to:

   `http://<CallManager IP Address>:80/ipphone/jsp/sciphonexml/IPAgentInitial.jsp`

6. In CallManager, navigate to the `?` and change the URL authentication parameter. Change:

   `http://<CallManager IP Address>:8088/ipphone/jsp/sciphonexml/IPAgentAuthenticate.jsp`

   to:

   `http://<CallManager IP Address>:80/ipphone/jsp/sciphonexml/IPAgentAuthenticate.jsp`

7. Reset the agent’s IP phone by removing and then reinserting the power cord.
Removing Cisco Desktop Product Suite Applications

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

1. Hot fixes, if any
2. User applications (Agent Desktop, Supervisor Desktop, and Desktop Administrator)
3. Servers
4. Cisco Base

**IMPORTANT:** Always remove Base last.

To remove a Cisco Desktop application:

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

The application is removed. You may be prompted to reboot your computer. It is recommended that you do this in order to completely remove all Cisco Desktop files.

**NOTE:** You must reboot your computer before reinstalling any Cisco Desktop applications, or remnants of the previous installation may interfere with the new installation.