Cisco CAD Installation Guide

CAD 8.0 for Cisco Unified Contact Center Express Release 8.0
Cisco Unified Communications Manager Edition
revised March 2012

Contents

Contents

3   Installation 29

Contents

Contents

Introduction

1

Overview

This manual guides you through the process of installing the CAD client applications: Cisco Agent Desktop, Cisco Agent Desktop—Browser Edition, Cisco Supervisor Desktop, and Cisco Desktop Administrator.

The CAD services are integrated into the Cisco Unified Contact Center Express (Unified CCX) installation program. See the *Cisco Unified Contact Center Express Installation Guide* for information on installing Unified CCX.

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

Related CAD Documentation

- *Cisco Agent Desktop User Guide*

- *Cisco Agent Desktop—Browser Edition User Guide*

- *Cisco Supervisor Desktop User Guide*

- *Cisco IP Phone Agent User Guide*

- *Cisco Desktop Administrator User Guide*

  The user documents are available at:
  http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_user_guide_list.html

- *Cisco CAD Troubleshooting Guide*

- *Configuring and Troubleshooting VoIP Monitoring*

  The troubleshooting documents are available at:
  http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_troubleshooting_guides_list.html

■ *Integrating CAD with a Thin Client Environment* available at: http://www.cisco.com/en/US/products/sw/custcosw/ps427/products_ implementation_design_guides_list.html

■ *Cisco CAD Error Code Dictionary* available at: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_ technical_reference_list.html

What's New In This Release

CAD 8.0 includes the following new features:

- Support for Cisco Unified Communications Manager 8.0

- Port CAD services to the Cisco Linux platform (Unified Communications Operating System (UCOS) based on RedHat Linux AS4.0 with kernel version 2.6)

- Supports upgrades from Customer Response Solution 5.0(2) and Unified CCX 7.0(1), including all service releases

- Support for High Availability over WAN

- Support for Round Table/Round Table Lite phones as both agent and caller devices

- Support for Windows XP SP3 and Vista SP1

- Support for Window Server 2008

- Support for Windows Internet Explorer 8 and Mozilla Firefox 3.0

- Support for localization in Turkish, Polish, and Canadian French

CAD 8.0 Elements

CAD 8.0 includes the following client applications and services.

Client Applications

Cisco Desktop Administrator

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

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

Cisco Agent Desktop

Cisco Agent Desktop is an application that helps agents manage their customer contacts. It includes enterprise data, call activity information, reports, a Call/Chat client for chatting with other agents and supervisors, and an integrated browser window.

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

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

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

Cisco IP Phone Agent

Cisco IP Phone Agent is a service that runs on the agent's Cisco IP phone. It enables agents to manage their customer contacts without the need of a computer. It includes enterprise data, agent states, reason codes, and contact service queue (CSQ) statistics.

See the *Cisco IP Phone Agent User Guide* for more information.

Cisco Supervisor Desktop

Cisco Supervisor Desktop allows contact center supervisors to manage agent teams in real time. They can observe, coach, and view agent status details, as well as view conference information. Without the caller's knowledge, supervisors can initiate chat sessions with agents to help them handle calls. They can also silently monitor and record customer calls and, if necessary, conference in or take over those calls using

the barge-in and intercept features. Through the Supervisor Record Viewer, supervisors can play back and save recorded agent calls.

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

Cisco Agent Desktop–Browser Edition

Cisco Agent Desktop—Browser Edition (CAD-BE) is a Java applet version of Cisco Agent Desktop that runs in the Internet Explorer or Firefox web browser.

CAD-BE provides call control capabilities—such as call answer, hold, conference, and transfer, and ACD state control—ready/not ready, wrap-up, and so on. Customer information is presented to the agent through an enterprise data window. CAD-BE also provides an integrated browser window so agents can view intranet, internet, and web application pages as needed.

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

Services

The following are the individual CAD services that are installed on the Unified CCX server as part of the Unified CCX installation.

The group of services referred to as the "CAD Base services", which are always installed on the Unified CCX server, include the following:

- Cisco Browser and IP Phone Agent Service (BIPPA service)
- Cisco Desktop Agent E-Mail Service (Agent E-Mail service)
- Cisco Desktop Call/Chat Service (Call/Chat service)
- Cisco Desktop Enterprise Service (Enterprise service)
- Cisco Desktop LDAP Monitor Service (LDAP Monitor service)
- Cisco Desktop Licensing and Resource Manager Service (LRM service)
- Cisco Desktop Recording and Statistics Service (Recording and Statistics service)
- Cisco Desktop Recording Service (Recording service)
- Cisco Desktop Sync Service (Sync service)
- Cisco Desktop VoIP Monitor Service (VoIP Monitor service)
- Cisco Desktop Administrator Service
- Directory Services

Agent E-Mail Service

The Agent E-Mail service supports the handling and managing of e-mails for a contact center's agents and supervisors. It provides the basic set of features for receiving e-mails from customers, distributing them to agents to service customer requests, sending responses from the contact center to the customer, and reporting on e-mail activity.

Call/Chat Service

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

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

Directory Services

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

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

Enterprise Service

The Enterprise service tracks calls in the system. It is used to attach IVR-collected data to a call in order to make it available at the Agent Desktop. It also provides real-time call history.

BIPPA Service

The BIPPA service enables IP phone agents to log in and out of Unified CCX, change agent states, and enter reason codes and wrap-up data without having the Agent Desktop software.

This service works in conjunction with the Services feature of Unified CME and supported Cisco IP phones. It is also used to hold the configuration information administered via Desktop Administrator. CAD-BE agents use this service to interact with the other services.

LDAP Monitor Service

The LDAP Monitor service starts Directory Services and then monitors it to ensure that it keeps running. It also sets up the configuration for LDAP replication, and resynchronizes LDAP data.

LRM Service

The LRM service distributes licenses to clients and oversees the health of the CAD services. All other CAD services, except the LDAP Monitor service, register themselves with the LRM service so that clients can locate them.

Recording Service

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

Recording and Statistics Service

The Recording and Statistics service maintains a 1-day history of agent and team statistics, such as average time an agent is in a particular agent state, last login time, number of calls an agent has received. It maintains a rolling 7-day history of recordings (unless they are saved, in which case they are saved for 30 days).

Sync Service

The Sync service connects to Unified CCX via ACMI and retrieves agent, supervisor, team, and skill information. It then compares the information with the information in Directory Services and adds, updates, or deletes entries as needed to stay consistent with the Unified CCX configuration.

Voice over IP Monitor Service

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

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

CAD Feature Levels

There are three feature levels of CAD: Standard, Enhanced, and Premium. Table 1 outlines the features available at each level. All features not listed here are present in all three levels.

Table 1. CAD Feature Levels

	Standard	Enhanced	Premium
Cisco Agent Desktop (not available in Standard bundle)			
Agent-initiated chat		×	×
Automated recording (workflow action)		×	×
Email integration			×
Enterprise data thresholds		×	×
Event-triggered work flows		×	×
HTTP Post/Get Action			×
Integrated browser			×
Reason codes		×	×
Task buttons		×	×
Unified CCX Outbound Dialer			×
Unified Presence integration		×	×
Wrap-up data		×	×
Cisco Agent Desktop Browser Edition (not available in Standard Bundle)			
Agent-initiated high priority chat		×	×
Enterprise data thresholds		×	×
Event-triggered workflows		×	×
HTTP Get action		×	×
Integrated browser		×	×
Reason codes		×	×
Task buttons		×	×
Wrap-up data		×	×
Cisco IP Phone Agent			

Table 1.   CAD Feature Levels

	Standard	Enhanced	Premium
Agent states		×	×
Agent-initiated recording		×	×
Caller data	×	×	×
CSQ statistics	×	×	×
Reason codes	×	×	×
Wrap-up data		×	×
Cisco Supervisor Desktop			
Barge-in		×	×
CSQ statistics	×	×	×
Intercept		×	×
Recording (up to <n> simultaneous recordings/playbacks)		32	64
Real time displays	×	×	×
Silent monitoring		×	×
Supervisor workflow (tree control)		×	×
Supervisor workflow all			×
Team messages		×	×
Unified Presence integration	×	×	×
Cisco Desktop Administrator			
Configure Agent E-Mail			×
Configure Enterprise data	×	×	×
Configure silent monitoring		×	×
Configure Unified Presence	×	×	×
Configure workflow groups	×	×	×
Cisco Workflow Administrator			
Configure agent interface		×	×
Configure integrated browser		×[*]	×
Unified CCX Outbound Dialer			×

Table 1. CAD Feature Levels

	Standard	Enhanced	Premium
Configure workflows		×	×
Configure wrap-up data		×	×

* CAD-BE only

Localization

The CAD desktop applications are localized in the languages displayed in Table 2.

Table 2.   CAD desktop applications and supported languages

Language	Agent Desktop	CAD-BE	Supervisor Desktop	IP Phone Agent	Desktop Administrator
Chinese (Simplified)	×	×	×	×[*]	
Chinese (Traditional)	×	×	×	×[*]	
Danish	×	×	×	×	
Dutch	×	×	×	×	
English (US)	×	×	×	×	×
Finnish	×	×	×	×	
French	×	×	×	×	
French (Canadian)	×	×	×	×	
German	×	×	×	×	
Italian	×	×	×	×	
Japanese (Kanji)	×	×	×	×[*]	
Japanese (Katakana)	×	×	×	×[†]	
Korean	×	×	×	×[*]	
Norwegian[‡]	×	×	×	×	
Polish	×	×	×	×[*]	
Portuguese (Brazilian)	×	×	×	×	
Russian	×	×	×	×[*]	
Spanish	×	×	×	×	
Swedish	×	×	×	×	
Turkish	×	×	×	×[*]	

* Requires phones with UTF-8 support. For Russian, the phones with out UTF-8 support require ISO-8859-1 without Unicode escapes for reason code, wrap-up data, and enterprise data.

† Requires phones with Shift-JIS support. The reason code, wrap-up data and enterprise data must be in Katakana half-width in Shift-JIS format.

‡ User Interface only.

Before You Install CAD 8.0

2

System Configurations

Supported system configurations are documented in the *Cisco Unified Contact Center Express 8.0 Solution Reference Network Design (SRND)*, available at:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products _implementation_design_guides_list.html

Thin Client Environments

Agent Desktop and Supervisor Desktop are supported in Citrix/XenApp and Microsoft Terminal Services thin client environments. For more information, see *Integrating CAD with a Thin Client Environment*, available at:

http://www.cisco.com/en/US/products/sw/custcosw/ps427/products_ implementation_design_guides_list.html

System Requirements

CAD 8.0 is integrated into the Unified Contact Center 8.0 environment.

Consult the following documents for the most current compatibility information:

- Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix is available at:

  http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_device_support_tables_list.html

- Cisco Unified Contact Center Express (Cisco Unified CCX) Software and Hardware Compatibility Guide is available at:

  http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_device_support_tables_list.html

Operating Environment

> **NOTE:** CAD does not support 64-bit operating systems.

The most current hardware and system software compatibility information are documented in the Cisco Unified Contact Center Express (Cisco Unified CCX) Software and Hardware Compatibility Guide, available at:

> http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_device_support_tables_list.html

Operating Environment Language Requirements

Agent Desktop, CAD-BE, and Supervisor Desktop can be installed on machines running localized operating systems. For a list of supported languages, see "Localization" on page 17.

In a non-English language environment, it is necessary to install Desktop Administrator on a machine with a localized operating system so that Call/Chat messages, tooltips, enterprise data names, and other communications within the contact center are in the local language.

> **NOTE:** When you change the language for a contact center, the data in LDAP is completely wiped out. As a result, CAD client desktops must be configured again in Desktop Administrator. In other instances when you run the Cisco Unified CCX Desktop Client Configuration tool, the data in LDAP is preserved. See "Configuring CAD Desktop Client MSI Files" on page 31 for more information.

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

> NOTE: After changing a contact centers language, it might take several minutes for changes to take effect and the servers to complete restarting.

VPN and NAT Requirements

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

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

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

Using NAT With IP Phone Agent

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

> NOTE: Recording and monitoring do not work with IP Phone Agent when it is used with NAT.

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

http://www.cisco.com/en/US/tech/tk648/tk361/tech_tech_notes_list.html

Third Party Software Environment

CAD 8.0 requires the following software applications to run successfully.

Microsoft Internet Explorer

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

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

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

- If a page that contains a JavaScript error is opened from the CAD integrated browser and script error notification is disabled in IE (the default), the CAD integrated browser will not display any information about the error. To see detailed information about the error, you must open the page from IE with script debugged enabled.

- The CAD integrated browser does not support the more advanced features of Internet Explorer, including the pop-up blocker, the phishing filter, and Internet Explorer 7-style tabs.

- Compatibility Mode should be enabled for the Unified CCX server site in Internet Explorer to prevent potential issues with the Agent E-Mail feature.

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

   NOTE: For technical reference information about the WebBrowser control, see the MSDN article available at:

   http://msdn2.microsoft.com/en-us/library/42h6dke4(VS.80).aspx

Mozilla Firefox

Mozilla Firefox 3.0 is a supported browser for use with CAD-BE.

   NOTE: For information on supported versions of Internet Explorer and Mozilla Firefox, see the Cisco Unified Contact Center Express (Cisco Unified CCX) Software and Hardware Compatibility Guide (see "Operating Environment" on page 20 for the document URL).

Java Runtime Environment (JRE)

JRE 1.6.0_12 is required to run the Java applets and JavaServer pages (JSP) used by IP Phone Agent, Agent Desktop, and CAD-BE. JRE is shipped with CAD 8.0. It is installed automatically with the client desktops.

Monitoring and Recording Requirements

For information about recording requirements, see *Configuring and Troubleshooting VoIP Monitoring*.

The space requirements for the Recording service and the Recording and Statistics service depend on the size of the contact center as described below.

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

Agent Data Store Database

The Agent Data Store database (the IBM Informix Database (IDS) version 11.5 is associated with the Recording and Statistics service) requires 1.2 GB to store agent state and call activity records for a 7 days per week/10 hours per day, with calls that last 1 minute each. This assumes that the contact center has the maximum configuration of 300 agents and 64 simultaneous recordings.

Recording Service

The Recording service requires the following space.

- ~800 kB for each minute of a recorded G.711 voice call

- ~200 kB for each minute of a recorded G.729 voice call

- 2.6 GB to store voice calls assuming that there are 32 supervisors, each supervisor recording 10 G.711 calls per day, each call lasting 5 minutes. The space requirement is divided among all recording servers, because the recording load is balanced.

Setting Up Agents in Unified CCX

For CAD 8.0 applications to work properly, your agents must be organized into teams and some must be designated as supervisors. This is accomplished in Unified CCX. See your Unified CCX documentation for information on how to do this is available at:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

NOTE: User IDs used for logging into Cisco Agent Desktop and Cisco Supervisor Desktop can have a maximum length of 31 alphanumeric characters. Unified CCX allows IDs that are longer. Make sure that any IDs you configure in Unified CCX are no longer than 31 characters in order for agents and supervisors to log in successfully.

System Capacity

CAD 8.0 supports the system capacities displayed in Table 3.

Table 3.   Unified CM system capacity

Description	Capacity
Maximum number of agents per site	300
Maximum number of agents per team	300
Maximum number of skills per agent (for real-time reporting)	50
Maximum number of CSQs per agent (for real-time reporting)	25
Maximum number of supervisors per site	32
Maximum number of supervisors per team	32
Maximum number of simultaneous recordings/playbacks per Recording service	32 Enhanced 64 Premium
Average agents per supervisor	10:1
Maximum number of agents per monitor domain	300
Maximum number of simultaneous monitoring sessions	32

Supported IP Phones

For a list of supported IP phones, see the Cisco Unified Contact Center Express (Cisco Unified CCX) Software and Hardware Compatibility Guide. This document is available at:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_ device_support_tables_list.html

Caveats on Using a Cisco 7920 Wireless Phone

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

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

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

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

Installation

3

Upgrade Notes

Upgrading from CAD 8.0(1)

- After upgrading from CAD 8.0(1) to the next software release, you must reboot both high availability servers.

- If you upgrade CAD 8.0(1) to a higher software release, and then roll back to the original software release, all e-mail historical data is lost.

- When upgrading from CAD 8.0(1) to the higher software release and switching over between the active node and the standby node is in progress, you must not run the Cisco Unified CCX Desktop Client Configuration tool. If you try running the Unified CCX Desktop Client Configuration tool, CAD desktop applications will not be automatically updated and thus they are not configured correctly until the standby node is ready.

  If the standby node fails to upgrade, run the Unified CCX Desktop Client Configuration tool so that it configures CAD desktop applications with the active node IP address. When the standby node is ready, run the Unified CCX Desktop Client Configuration tool again. This might force you to uninstall and reinstall CAD desktop applications to correct registry entries.

Upgrading from CAD 6.6(1)

- If reason code 0 is defined in CAD 6.6(1), it automatically changes to 1001 when upgraded to CAD 8.0(1).

Upgrading from CAD 6.4(2)

- When you upgrade from CAD 6.4(2) to CAD 8.0(1), the selections made in Supervisor Desktop to generate the following real time displays will be lost:

  — Voice CSQ – Summary

  — E-Mail CSQ – Summary

  — Team Agent Statistics report

  — Team Agent State report

  You must manually select them to restore the previous selections to generate these reports.

- When you upgrade from CAD 6.4(2) to CAD 8.0(1), you must select again the Enable Integrated browser and Enable Movable Windows check boxes and reconfigure the settings in Supervisor Desktop.

- If a scalar and an array expanded call contact (ECC) variable have the same field name, one of them must be renamed before an upgrade. If you do not modify the variables so they have unique field names, they will be lost in the upgrade and you will have to recreate them.

Standard Bundle Customers

It is important to remember that if you are upgrading to CAD 8.0, the 8.0 Standard bundle does not support Agent Desktop. It supports IP Phone Agent only. Contact your Cisco partner account team for further details on how to obtain Agent Desktop.

Configuring CAD Desktop Client MSI Files

Because the CAD services are installed on a Linux platform, it is necessary to run the the Unified CCX Desktop Client Configuration tool in order to configure the Windows-based CAD client MSIs with the correct configuration information.

These MSIs must be preconfigured with language and IP addresses based on the system configuration, using Windows-based libraries and runtime DLLs to perform the configuration.

The Unified CCX Desktop Client Configuration tool configures the CAD client MSIs and, depending on when the tool is run, either saves them to the local machine or uploads them to the Unified CCX server.

> **NOTE:** In a high availability environment, the Unified CCX Desktop Client Configuration tool needs to configure the IP address of only one server. Through this IP address, it will determine the IP address of the second server and upload the MSI files to both servers.

Run the Unified CCX Desktop Client Configuration tool in these scenarios:

- Whenever CAD is installed
- When the Unified CCX server is upgraded with new builds and patches
- The Unified CCX server IP address changes
- The language changes
- A High Availability system is set up or torn down
- A High Availability node is replaced
- Whenever Disaster Recovery Framework (DRF) restore procedure is performed

Running the Unified CCX Desktop Client Configuration Tool

The Unified CCX Desktop Client Configuration tool can be used either before or after the Unified CCX server is installed or upgraded.

> **NOTE:** If you use automated deployment tools, you can use the configured MSIs in the creation and testing of push packages.

After you successfully run the Unified CCX Desktop Client Configuration tool, create the automated deployment packages in accordance with the requirements listed in the section, "Using Automated Package Distribution Tools" on page 42.

Before Installing/Upgrading the Unified CCX Server

The Unified CCX Desktop Client Configuration tool that is shipped with CAD 8.0 in the CAD_Client_Config_Pkg_801_B73.zip file is labelled as the Preconfiguration tool. The CAD_Client_Config_Pkg_801_B73.zip file can be obtained from the product DVD or as a download from the Cisco website.

To unzip and run the Preconfiguration tool before the Unified CCX server is installed or upgraded:

1. Copy the CAD_Client_Config_Pkg_801_B73.zip file to a Windows PC.

2. Open the zip file and extract ConfigureMsi.exe to any location on the PC.

3. Double-click ConfigureMsi.exe. The Preconfiguration tool starts.

4. When prompted, provide the following information:

   ■ Language of the contact center

   ■ IP address of the primary Unified CCX server (server 1)

   ■ IP address of the backup Unified CCX server (server 2) (or 'none' if the system is not high availability)

   ■ Unified Communications Manager type (CM or CME)

   ■ License type (Standard, Enhanced, or Premium)

5. The Preconfiguration tool runs and puts the configured MSI files (add the exact file names here, for example, agent.msi, admin.msi, etc.) in the folder where ConfigureMsi.exe is located.

   The files are now ready to be used to install the CAD desktop client applications.

After Installing/Upgrading the Unified CCX Server

When run after the Unified CCX server is installed or upgraded, the Unified CCX Desktop Client Configuration tool configures the CAD client MSIs, uploads them to the Unified CCX server, cleans up the created temporary files, and terminates.

> **NOTE:** The Windows PC on which you run the Unified CCX Desktop Client Configuration tool must have JRE 1.6.0_12 installed.

To run the Unified CCX Desktop Client Configuration tool:

1. In the web browser, access http://<Unified CCX server>/appadmin, where <Unified CCX server> is the Unified CCX server's IP address or host name.

   The Cisco Unified CCX Administration Authentication page appears.

2. Enter your Unified CCX username and password, and then click Login. The Cisco Unified CCX Administration home page appears.

3. Choose Tools > Plug-ins. The Plug-ins page appears.

4. Click the Cisco Unified CCX Desktop Suites link. The Cisco Unified CCX page appears.

5. Click the Cisco Unified CCX Client Configuration tool link to run the Unified CCX Desktop Client Configuration tool. The File Download - Security Warning dialog box appears.

6. Click Run to run the executable, or Save to save the executable to your local computer and run it from there.

   The InstallShield Wizard starts.

   NOTE: You might see a security warning that the publisher could not be verified.

7. Click Run. The Loading CAD Client Configuration dialog box appears.

8. Enter the Unified CCX server IP address in the IP Address field and click Next.

9. The Unified CCX Desktop Client Configuration tool starts creating the client MSIs. This process might take several minutes.

10. When the process is finished, the Unified CCX Desktop Client Configuration Configuration Complete dialog box states that the clients have been configured and uploaded to the Unified CCX server. They are now ready for use.

    The Unified CCX server verifies and matches the versions of the configured MSI installers' before placing the MSI files in its location for downloading and using it at later time. Then, the Unified CCX Desktop Client Configuration tool removes its files from your machine to make sure that the old version of MSI installer is not available for re-use. In a high availability system, the Unified CCX Desktop Client Configuration tool uploads the MSI files to both the systems.

11. Click OK.

Installing CAD Desktop Applications

Before you install a CAD desktop application, you need to know:

- The IP address of the Unified CCX server

- The Unified CCX server user ID and password to access the Unified CCX Administration web application

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

Before agents can access CAD-BE or Agent Desktop's Agent E-Mail feature, you must ensure that the correct version of Java Runtime Environment (JRE) is installed on those agents' PCs.

If the incorrect version of JRE is installed, or if JRE is not present, CAD-BE will not start. Agent Desktop will function normally except for the Agent E-Mail feature, which will be disabled until the correct version of JRE is installed.

Upgrading From an Earlier Version

Over-the-top upgrades (installing the new version over the older version) from CAD 6.3(1), 6.4(2), and 6.6(1) to CAD 8.0 is supported.

Upgrading from any other version of CAD requires that the older version of CAD is uninstalled before CAD 8.0 is installed.

Adding Desktop Applications After Initial Setup

You can install additional CAD desktop applications on a client desktop that already hosts a CAD desktop application. However, if the client desktop has had one or more service releases installed, you must follow these steps.

1. Uninstall all CAD service releases from the client desktop. See "Rolling Back Client-Side Service Releases" on page 112.

2. Install the desired additional CAD desktop applications. See "Installing CAD Desktop Applications" on page 35.

3. Reapply the service releases via the automated update feature. See "Automated Updates" on page 45.

Methods for Installing CAD Desktop Applications

The CAD desktop applications can be installed one of two ways:

- The desktop applications can be "pushed" to the Agent Desktops using an automated package distribution tool.

■ The agent can install the application from the Unified CCX Administration web application.

The desktop user must have either administrator or elevated privileges to install the CAD desktop applications. This applies to installations pushed to the desktop via an automated package distribution tool or manual installation.

Installing CAD Desktop Applications

The Unified CCX Administrator download page includes installation files for all CAD desktop applications. The Unified CCX Administrator web page, when accessed using a supervisor username and password, contains only the installation file for Supervisor Desktop. The Unified CCX User Options web page contains only the installation file for Agent Desktop.

If you do not want agents and supervisors to access the Unified CCX Administration web application as administrators, direct them to one of the alternatives given in the following procedure.

When you install Supervisor Desktop, Agent Desktop is also automatically installed.

> NOTE: If you already have Agent Desktop installed on a PC and want to install Supervisor Desktop, you must first uninstall the existing instance of Agent Desktop.

To install a CAD desktop application:

1. Open your web browser and enter http://<Unified CCX server>/appadmin, where <Unified CCX server> is the Unified CCX server's IP address or host name.

   ■ If you are an administrator, complete the following steps:

      a. Access http://<Unified CCX server>/appadmin. The Cisco Unified CCX Administration Authentication page appears.

      b. Type your Unified CCX username and password.

      c. Click Login. The Cisco Unified CCX Administration home page appears.

      d. Choose Tools > Plug-ins. The Plug-ins page appears.

      e. Click the Cisco Unified CCX Desktop Suites link. The Cisco Unified CCX page appears.

      f. Go to step 2 to complete the application installation process.

   ■ If you are a supervisor, complete the following steps:

a. Access http://<Unified CCX server>/appadmin. The Cisco Unified CCX Administration Authentication page appears.

b. Type Supervisor Desktop username and password.

c. Click Login. The Cisco Unified CCX Supervision page appears

d. Choose Tools > Plug-ins. The Plug-ins page appears.

e. Click the Cisco Unified CCX Desktop Suites link. The Cisco Unified CCX page appears.

f. Go to step 2 to complete the application installation process.

■ If you are an agent, complete the following steps:

a. Access http://<Unified CCX server>/appuser. The Cisco Unified CCX User Options Authentication page appears.

b. Type Agent Desktop username and password.

c. Click Login. The Cisco Unified CCX User Options home page appears.

d. Choose User Options > Cisco Unified CCX Downloads. Download Page appears.

e. Go to step 2 to complete the application installation process.

2. Click the link for the application you want to install. The File Download - Security Warning dialog box appears.

3. Click Run to run the installation program. You can also click Save to save the installation program to your local computer and run it from there.

   The InstallShield Wizard starts.

   NOTE: You might see a security warning that the publisher could not be verified. Do not click Don't Run. If you click Don't Run, then application will not install.

4. Click Run.

5. Follow the instructions in the InstallShield Wizard to complete installing the selected application.

   NOTE: After installation finishes, a dialog box might appear, stating that you must reboot your computer to complete the installation. If this message appears, click OK, exit all running applications, then restart your computer.

Installing the JRE Plug-in for CAD-BE

Before an agent can access the CAD-BE Java applet, you must install the correct version of the JRE plug-in for Internet Explorer or Firefox on that agent's PC. Both browsers require version 1.6.0 of the JRE plug-in, build 12. CAD-BE runs in the following web browsers:

Operating System	Supported Browsers
Microsoft Windows XP Professional with Service Pack 2 and 3	Microsoft Internet Explorer 7 and 8 Mozilla Firefox 3.0
Microsoft Windows Vista Business, Enterprise, and Ultimate Editions	Microsoft Internet Explorer 7 and 8 Mozilla Firefox 3.0
Red Hat Enterprise Linux 4 and 5	Mozilla Firefox 3.0

See "Internet Explorer Settings for CAD-BE" on page 39 and "Firefox Settings for CAD-BE" on page 40 for information on how to configure your web browser to run CAD-BE. In addition, all popup blockers must be disabled. Consult your administrator for instructions on disabling your popup blockers, if any.

To install the JRE plug-in on Microsoft Windows:

1. From the agent's PC on which you want to install the JRE plug-in, start your web browser.

2. Type https://<Unified CCX server>/cadbe/CAD-BE.jsp in the address field, where <Unified CCX server> is the IP address or hostname of the server that is hosting CAD.

3. Press Enter.

   NOTE: A warning might appear, stating that this website's certificate cannot be verified. To prevent this warning from displaying again, select the check box Always trust content from this publisher, then click Yes to launch CAD-BE. Do not click No. If you click no, then CAD-BE will not launch.

   ■   If the CAD-BE Login dialog appears, the agent's PC already has the correct version of JRE installed. You can skip the rest of this procedure.

   ■   If a page with an error message appears, the agent's PC does not have the correct version of JRE installed. Continue to the next step.

4. Click the hyperlink that corresponds to the operating system of the PC on which you are installing the plug-in. The browser might display a security warning.

5. Click Run to run the installation program. You can also click Save to save the installation program to your local computer and run it from there. The installation program starts up.

6. Follow the instructions in the Windows Installer to install the selected application.

To install the JRE plug-in on Red Hat Linux:

1. From the agent's PC on which you want to install the JRE plug-in, start your web browser.

2. Type the following address in the address field, where <Unified CCX server> is the IP address or hostname of the server that is hosting CAD.

   `https://<Unified CCX server>/cadbe/CAD-BE.jsp`

3. Press Enter.

   If the CAD-BE Login dialog appears, the agent's PC already has the correct version of JRE installed. You can skip the rest of this procedure. If a page with an error message appears, the agent's PC does not have the correct version of JRE installed. Continue to the next step.

4. Click the hyperlink that corresponds to the operating system of the PC on which you are installing the plug-in. The browser might display a security warning.

5. Click Save to save the installation program to your local computer

6. At the terminal, type: **su**

7. Enter the root password.

   NOTE: To install JRE in a systemwide location such as /usr/local, you must log in as the root user to gain the necessary permissions. If you do not have root access, install the JRE in your home directory or a subdirectory for which you have write permissions.

8. Change to the directory where you want to install JRE by typing the following command.

   `cd <directory path>`

9. Change the permission of the file you downloaded to be executable by typing the following command.

   `chmod a+x jre-1_6_0_12-linux-i586.bin`

10. Verify that you have permission to execute the file by typing the following command.

    `ls -l`

11. Start the installation process by typing the following command. A binary license agreement is displayed.

    ```
    ./jre-1_6_0_12-linux-i586.bin
    ```

12. Press the spacebar to display the next page.

13. At the end, type **Yes** to proceed with the installation. JRE is installed into its own directory. When the installation finishes, the word Done appears.

To enable the Firefox JRE plug-in on Linux:

1. Go to the plug-ins subdirectory under the Firefox installation directory by typing the following command, where <Firefox directory> is the directory in which Firefox is installed.

    ```
    cd <Firefox directory>/plugins
    ```

2. Create a symbolic link to the JRE ns7/libjavaplugin_oji.so file by typing the following command, where <JRE directory> is the directory in which JRE is installed.

    ```
    ln -s <JRE directory>/plugin/i386/ns7/libjavaplugin_oji.so
    ```

3. Start the Firefox browser. If it is already running, restart it.

    NOTE: If there are other Firefox components running (such as Messenger or Composer), you must restart them as well.

4. Choose Edit > Preferences. Under the Content category, select Enable Java.

Internet Explorer Settings for CAD-BE

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

Popup Blocker

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

1. Choose Tools > Internet Options and select the Security tab.

2. Click Custom Level.

3. In the Settings pane, Under the Miscellaneous section, set Use Pop-up Blocker to Disable.

    OR

1. Choose Tools > Internet Options and select the Security tab.

2. Select the Trusted sites icon and click Sites, and then add the CAD-BE IP address(es) to the list of allowed sites.

NOTE: If you are using the Microsoft Windows Vista Business operating system, you must add the Unified CCX server IP address to the list of allowed sites in order to be able to generating the CAD BE logs.

Internet Options

Set the following internet options:

1. Choose Tools > Internet Options and select the Security tab.

2. Click Custom Level.

3. In the Settings pane, set the following options:

   ■ Under the ActiveX controls and plug-ins section, set Run ActiveX controls and plug-ins to Enable.

   ■ Under the Miscellaneous section, set Launching programs and files in an IFRAME to Prompt or Enable.

   ■ Under the Scripting section, set Active Scripting to Enable.

Firefox Settings for CAD-BE

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

Popup Blocker

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

1. Choose Tools > Options > Content.

2. Clear the Block Pop-up Windows check box.

   OR

1. Choose Tools > Options > Content.

2. Select the Block Pop-up Windows check box.

3. Click Exceptions and add the CAD-BE IP address(es) to the list of allowed sites.

   NOTE: If you are using the Microsoft Windows Vista Business operating system, you must add the Unified CCX server IP address to the list of allowed sites in order to be able to generating the CAD BE logs.

Content Settings

Configure the following settings:

1. Choose Tools > Options > Content, and select the following check boxes:

- Enable Java

- Enable JavaScript

2. Next to the Enable JavaScript check box, click Advanced and select these check boxes in the Advanced JavaScript Settings dialog box:

- Raise or lower windows

- Disable or replace context menus

3. In the browser address field, type the following:

   `about:config`

4. Locate the preference dom.allow_scripts_to_close_windows.

5. Right-click the preference and select Toggle to set the value to True.

Using Automated Package Distribution Tools

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

If you need to create MSIs before the CAD services are installed, see "Running the Unified CCX Desktop Client Configuration Tool" on page 31.

Requirements

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

Execution

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

Per-Machine vs. Per-User Installation

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

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

Privileges

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

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

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

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

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

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

Automated Package Installation vs. Manual Installation

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

CAD MSI packages are located in a specified location on a successfully-installed production server and are intended for both manual and automated deployment. Alteration of these files or the use of other MSI files included with the product at other locations is not supported.

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

Multiple Software Releases

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

Reboots

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

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

Best Practices

Best practices recommendations are listed below.

Windows Installer Logging

Window Installer logging should be enabled. The installations should be run with the following command line argument:

/l*v <logfile path and name>

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

This ensures that any loggable issues are captured efficiently.

Deployment

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

Installation and Uninstallation Deployment Packages

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

Recommended Deployment Preparation Model

1. Use a lab environment to model the pending deployment.

2. Install the servers to obtain valid client installation packages.

3. Manually deploy client installation packages to ensure that the installs are compatible with your environment. This will isolate product installation vs. automated deployment issues.

4. Create your deployment packages in accordance with the requirements listed in "Requirements" on page 42.

5. Test the deployment packages.

6. At deployment time modify your deployment packages, replacing the client installation packages from the lab environment with valid client installation packages from the production server.

Automated Updates

CAD automatically updates all instances of the CAD desktop applications to a newer version if the services have been updated.

CAD Desktop Applications

Every time a client desktop application is launched, the software checks to see if there is an updated version available, or if there was a system configuration change that requires a Windows registry change. If either of these conditions are true, the software automatically runs the update process.

When an update is available, the user sees a dialog box notifying the user that the desktop application will be updated. The uses clicks OK to proceed with the update.

A progress bar is displayed to show the status of the download.

When the update is finished, the user will see a final dialog box that the update is complete, and which applications were updated. If the user has more than one CAD desktop application installed, they will all have been updated.

> NOTE: Because Agent Desktop is automatically installed when Supervisor Desktop is installed, only Supervisor Desktop will be listed as having been updated in the final dialog box, even though Agent Desktop was also updated. Agent Desktop will be listed only if Supervisor Desktop is not present on the desktop.

When the user clicks OK to close the dialog box, any CAD desktop application that had been running on the desktop restarts automatically.

> NOTE: To ensure that automated updates function correctly, Internet Explorer must be configured so that it checks for newer versions of stored pages. In Internet Explorer, choose Tools > Internet Options. In the Browsing history section on the General tab, click Settings. Select the option labeled Every time I visit the web page.

> NOTE: If the system is configured with two Unified CCX servers, and one server is upgraded while the user's instance of CAD is connected to the older Unified CCX, and the user's system administrator performs a failover to switch all agents to the upgraded server, the user's CAD desktop applications will not automatically upgrade when the user logs into the new server. The user must shut down CAD desktop applications and start them again for the automatic upgrade to take place.

Java Runtime Environment

Every time a CAD desktop application is launched, it checks to see if the correct version of JRE is installed. If the correct version is not detected, the user is notified, and it prompts the user to install the correct JRE.

Repairing CAD

Client Applications

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

To repair a CAD client application:

1. On the client desktop, in Windows Control Panel, start the Add or Remove Programs tool.

2. In the list of currently installed programs, locate the CAD desktop application you want to repair. CAD client applications are repaired using the listing for the specific application (for example, "Cisco Desktop Administrator").

3. Click the Click here for support information link to display the Support Info dialog box (Figure 1).

Figure 1.   Support Info dialog box
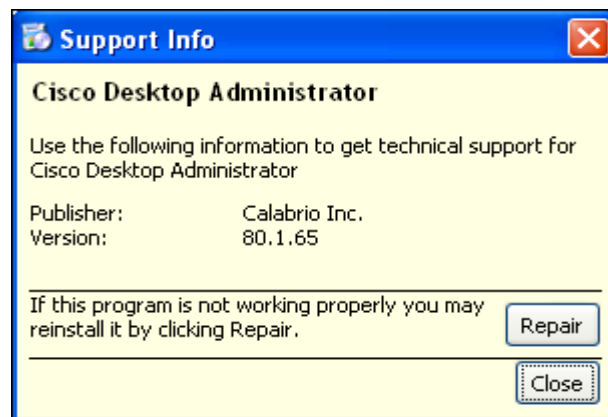
4. Click Repair. The program reinstalls and displays the Location of Unified CCX server(s) dialog box (Figure 2 on page 50).

5. Ensure that the correct primary (and optional secondary) Unified CCX server IP address is entered, and then click OK.

   NOTE: If you are running CAD Configuration Setup on a PC that hosts Desktop Administrator and no other CAD desktop application, after you close this dialog box, CAD Configuration Setup closes because there is nothing else to configure on this PC.

The CAD Configuration Setup window appears (Figure 3 on page 51).

6. Verify the settings are correct and choose File > Exit from the menu or click X to close the window.

7. Click Close after the CAD desktop application repair completes.

8. Repeat Steps 2 through 7 on the CAD service release, if one has been installed.

CAD Configuration Setup

The CAD Configuration Setup utility is used to configure the following settings on CAD client desktops:

- Location of the primary (and optional secondary) Cisco Unified CCX server

- This is the NIC used for end point sniffing

- Whether or not the client desktop application is running in a thin client environment

After initial installation, you can launch CAD Configuration Setup:

- From Desktop Work flow Administrator or running PostInstall.exe (located in the folder C:\Program Files\Cisco\Desktop\bin folder on any CAD computer).

- From Desktop Administrator. See the Accessing Desktop Administrator section in the *Cisco Desktop Administrator User Guide*.

In most instances, the default settings in CAD Configuration Setup are correct and there is no need to run it after the client desktop is installed. You should run CAD Configuration Setup in the following instances:

- There is only one Unified CCX server and its IP address changes

- There is a primary and secondary Unified CCX server, and both server IP addresses change

  If either the primary or secondary Unified CCX server IP address changes, but not both, there is no need to run CAD Configuration Setup. The next time a client desktop is started, the automated update feature will reinstall the client desktop and make the necessary change.

  However, if both the primary and secondary Unified CCX server IP addresses change, the client will be unable to start because it cannot communicate with either server. In that case, you must run CAD Configuration Setup and change the Unified CCX server IP addresses.

- There is more than one NIC in the client PC

- The client desktop application is running in a thin client environment

To modify configuration data in client:

1. Start CAD Configuration Setup.

   - In Desktop Work Flow Administrator, select the Call Center 1 node in the left pane and then choose Setup > Configure Systems from the menu bar.

   - On a PC having CAD desktop applications installed, navigate to the C:\Program Files\Cisco\Desktop\bin folder and double-click PostInstall.exe.

Configuration Setup starts and displays the Location of Unified CCX server(s) dialog box (Figure 2).

Figure 2.   Cisco Agent Desktop Directory Services dialog box
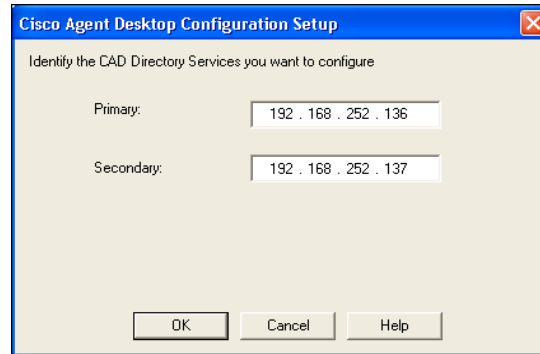
2. Ensure that the correct primary (and optional secondary) Unified CCX server IP address is entered, and then click OK.

   NOTE: If you are making changes in CAD Configuration Setup from Desktop Work Flow Administrator, choose File > Exit from the menu or click Close for changes to take effect.

   NOTE: If you are running CAD Configuration Setup on a PC that hosts Desktop Administrator and no other CAD desktop application, after you close this dialog box, CAD Configuration Setup closes because there is nothing else to configure on this PC.

The CAD Configuration Setup window appears (Figure 3).

Figure 3.   CAD Configuration Setup

[
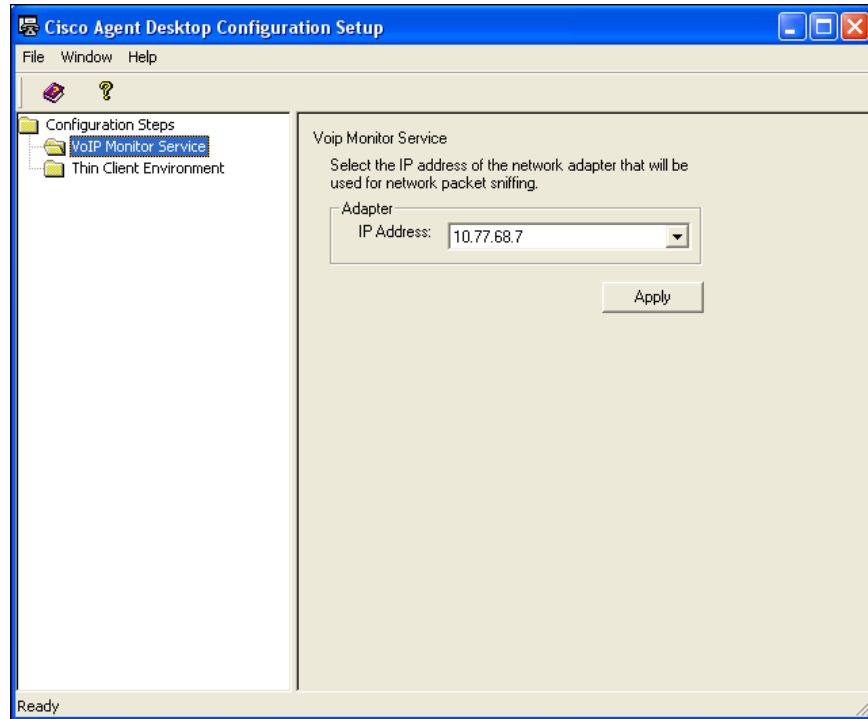
3. Select the step you want to modify from the left pane, enter the new data in the right pane, and then click Apply.

   ■   You can display the steps in any order you want.

   ■   If you modify a step, you must click Apply to save your changes before you move on to another step.

   ■   You can press F6 to switch between the left and right pane, and use the up and down arrows to move up and down the navigation tree in the left pane.

4. When you are done making your changes, choose File > Exit from the menu or click X to close the window.

   CAD Configuration Setup closes.

5. Stop and restart the desktop application for the change to go into effect.

Configuring CAD Configuration Setup

Table1 lists where you must configure CAD Configuration Setup to change the desired configuration setting.

Table 4.   CAD Configuration Setup configured as per host computer

Step Name	CAD and CSD[1]	CDA
Thin Client Environment (page 52)	×	
VoIP Monitor Service (page 53)	×	
CAD-BE Servers (page 54)		×
Services IP Address (page 55)		×
BIPPA User Login (page 55)		×

1 CAD—Cisco Agent Desktop, CSD—Cisco Supervisor Desktop, and CDA—Cisco Desktop Administrator

Thin Client Environment

Figure 4.   Thin Client Environment

Select Yes if CAD is installed in a thin client environment (for example, Microsoft Terminal Services, Citrix, or VMWare). The default setting is No.

VoIP Monitor Service

Figure 5.   VoIP Monitor Service

Select the IP address of the network adaptor to which voice packets are sent to be sniffed by the VoIP Monitor service on the client desktop. It is the NIC on which the computer is daisy-chained to the IP phone.

CAD-BE Servers

Figure 6.   CAD-BE Servers

From Desktop Administrator, choose CAD Configuration Setup > in the CAD-BE Servers section (Figure 6):

1. Enter the host name or IP address of the CAD Base Services server in the Primary Location field. Apache Tomcat, which is required to run CAD-BE, is installed on this server.

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

2. Enter the host name or IP address of a second server in the Secondary Location field. The secondary server hosts the CAD Base Services and you must have configured replication between the primary and secondary server.

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

   NOTE: The Secondary Location field is not enabled until you configure the second CAD Base Services server and establish replication.

3. Click Save to save your changes.

Services IP Address

Figure 7. Services IP Address

From Desktop Administrator, choose CAD Configuration Setup >In the Services IP Address section (Figure 7):

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

- Click Save to save your changes.

BIPPA User Login

Figure 8. BIPPA User Login

In order to connect to the Unified CM, the BIPPA service must have a login ID and password. This login ID and password are also set up in Unified CM (see "Configuring IP Phones for Cisco IP Phone Agent" on page 57). You can complete these fields in the BIPPA User Login section (**Figure 8**) before setting up the user in Unified CM, but the login ID and password must be identical in both places. If they are changed in this window or in Unified CM, they must be changed in both.

> **NOTE:** If Directory Services is not running when you view this section, the BIPPA login information cannot be changed.

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

Changing Unified CCX Cluster IP Addresses

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

For this procedure, see the *Cisco Unified Contact Center Express Administration Guide*, available at:

> http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Configuring IP Phones for Cisco IP Phone Agent

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

1. Create an IP phone service.

2. Assign the IP phone service to each IP agent phone.

3. Create an application user named "telecaster" with "telecaster" as the password (or whatever BIPPA user ID and password was specified in the CAD Configuration Setup utility).

4. Assign the telecaster application user to all the IP agent phones.

5. Change the default URL Authentication parameter.

These procedures can be done before or after CAD has been installed on your system.

Passwords and User Names

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

Creating an IP Phone Service

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

If you have a high availability system, you should create two IP Phone services, one for each Unified CCX engine server IP address.

> **NOTE:** At any point, only one BIPPA service is active. If the primary service fails, you are automatically logged out and you must manually log in to the secondary service.

To create a new IP phone service:

1. From the menu at the top of the page, choose Device > Device Settings > Phone Services.

2. On the Find and List IP Phone Services page, click Add New.

3. On the Cisco IP Phone Services Configuration page, enter the following information:

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

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

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

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

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

where:

■ 192.168.252.44 is the IP address of the machine on which the BIPPA service is loaded

■ 6293 is the Tomcat webserver port (if 6293 is not the port number, check the port parameter in the Tomcat server file for the correct value)

■ ipphone/jsp/... is the path to the jsp page under Tomcat on the machine on which the BIPPA service is loaded

NOTE: You will not find a file called IPAgentInitial.jsp at this location; there will be a file called IPAgentInitial.class, which contains the implementation of the .jsp file.

NOTE: The Tomcat webserver is included with the installation.

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

Assigning the IP Phone Service to IP Agent Phones

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

From the Unified CM Administration web-based application, complete the following steps to configure each IP phone.

To assign the IP phone service to IP agent phones:

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

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

3. Locate the phone in the list of results and click the hyperlink. The Phone Configuration page appears.

4. In the upper right corner of the page, select Subscribe/Unsubscribe Services from the Related Links drop-down list, and then click Go. A popup window for subscribing to services for that device appears.

5. From the Select a Service drop-down list, choose the new service, and then click Next. A popup window showing the new service appears.

6. Click Subscribe. The service is added to the Subscribed Service section of the popup window.

7. Click Save, and then close the popup window.

Configuring IP Phones for use with a Localized BIPPA Service

If a contact center is using a non-English language version of CAD, the BIPPA service will be displayed on the agent's IP phone in that non-English language (see "Localization" on page 17 for a list of supported languages). The phone does not need to be configured for the chosen locale. However, in this situation, the IP phone itself will display in English, the default locale for the phone, while the BIPPA service displays in the non-English language.

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

- On the enterprise level, so that all IP phones controlled by that Unified CM display in the selected language

- On the phone device level, so that individual IP phones can display in a language that is not the default language

To assign a locale at the enterprise level:

1. On the System menu, choose Enterprise Parameters. The Enterprise Parameters Configuration page appears.

2. In the Localization Parameters section, select the appropriate language from the drop-down lists in the Default Network Locale and Default User Locale fields.

3. Click Save.

To assign a locale at the phone device level:

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

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

3. Locate the phone in the list of results and click the hyperlink. The Phone Configuration page appears.

4. In the User Locale field, select the appropriate language from the drop-down list.

5. Click Save.

Creating a Unified CM User

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

> **NOTE:** The Unified CM user ID and password are also entered in CAD Configuration Setup and must match what is configured in Unified CM. If you change them in Unified CM, you must also change them in CAD Configuration Setup. See "Services IP Address" on page 55 for more information.

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

To create the Unified CM user:

1. From the User Management menu, choose Application User. The Find and Add Users page appears.

2. Click Add New. The Application User Configuration page appears.

3. In the Application User Information section, enter a user ID and password for the new user. Entries are case sensitive. If your system is set up to require password complexity, be sure to choose a password that satisfies those requirements.

4. In the Device Information section, use the arrows to move phones from the Available Devices pane to the Controlled Devices pane and move profiles from the Available Profiles pane to the CTI Controlled Device Profiles pane.

5. When you are done, click Save at the bottom of the page.

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

1. From the User Management menu, choose User Group. The Find and List User Groups page appears.

2. Click Find to display a list of all user groups.

3. From the list of search results, click Standard CTI Enabled. The User Group Configuration page appears.

4. Click Add App Users to Group. The Find and List Application Users window appears.

5. Select telecaster from the search results and then click Add Selected. The window closes and the Unified CM user is added to the Standard CTI Enabled group.

Configuring a One-Button Login for IP Phone Agents

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

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

> http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_
> tech_note09186a008029e6d5.shtml#proc

URL Authentication Parameter

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

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

> http://<Unified CM IP address>:8080/ccmcip/authenticate.jsp

> **NOTE:** You must use the IP address, not the host name, for Unified CM.

Configuring an IP Communicator Phone

From the Unified CM Administration web-based application, follow these steps to configure a IP Communicator soft phone.

1. Choose Device > Phone. The Find and List Phones page appears.

2. Click Add New. The Add a New Phone page appears.

3. From the Phone Type drop-down list, select Cisco IP Communicator, and then click Next. The Phone Configuration page appears.

4. From the Select the device protocol drop-down list, select the device protocol, and then click Next.

5. Complete the fields in the Phone Configuration page, and then click Save.

   The IP Communicator phone is inserted into the Unified CM database.

   NOTE: In the Device Name field, enter the MAC address of the computer on which the IP Communicator phone is installed, prefaced by SEP (for example, SEP01123FF8AA84).

Configuring Agent E-Mail

This section provides information on what must be done in order for the Agent E-Mail feature to function correctly.

> **NOTE:** The Agent E-Mail feature is not supported for the following languages: Chinese (Traditional and Simplified), Japanese, Korean, and Russian.

Overview

The Agent E-Mail feature requires configuration in the following applications before it will function.

Application	Configure
Microsoft Exchange	• Set up Agent E-Mail e-mail account • Set up Agent E-Mail distribution lists • Set up Agent E-Mail mailboxes See "Configuring Microsoft Exchange for Agent E-Mail" on page 72 for procedures.
Cisco Unified CCX Application Administration	• Set up CSQs • Set up skills See the *Cisco Unified Contact Center Express Administration Guide, Release 8.0(1)* for procedures.
Cisco Desktop Administrator	• Set up Exchange server information • Map CSQs to e-mail addresses See the *Cisco Desktop Administrator User Guide* for procedures.

Routing Rules

The Agent E-Mail feature manages the distribution of e-mails to agents based on the date the e-mail is received. The oldest e-mail is distributed first using a first-in-first-out (FIFO) distribution method.

If an agent supports multiple e-mail CSQs, the oldest e-mail in those CSQs is routed to the agent.

> NOTE: The agent's skill competency level is not taken into
> consideration for e-mail distribution.

Compatibility Mode

In order to prevent possible issues with Agent E-Mail, Internet Explorer's Compatibility Mode should be enabled for the Unified CCX server site.

Agent E-Mail Mailbox Folder Management

Messages received from and sent to customers are stored in the enterprise mail store in the Agent E-Mail mailbox.

By default, a new user's mailbox contains a standard set of folders, one of which is the Inbox. The Agent E-Mail service monitors this folder for incoming e-mails and automatically creates additional folders as needed at runtime.

A typical folder layout is illustrated in Figure 9.

Figure 9.   **Typical Agent E-Mail mailbox folder layout**
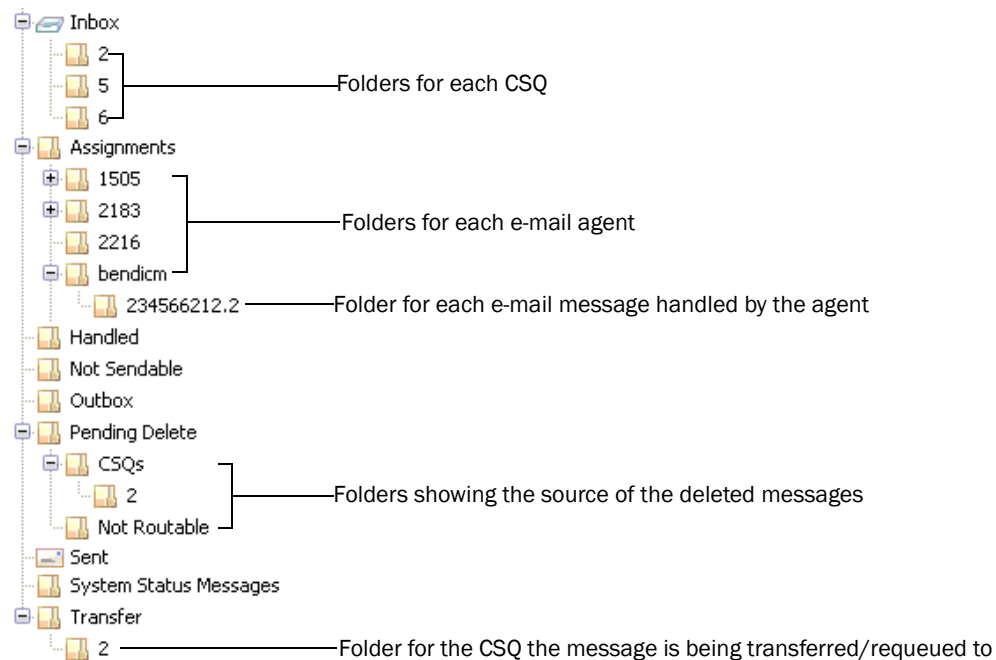
E-mail flow is illustrated in the flowchart in Figure 10 and Figure 11.

Figure 10.   Customer e-mail flowchart (incoming e-mail)
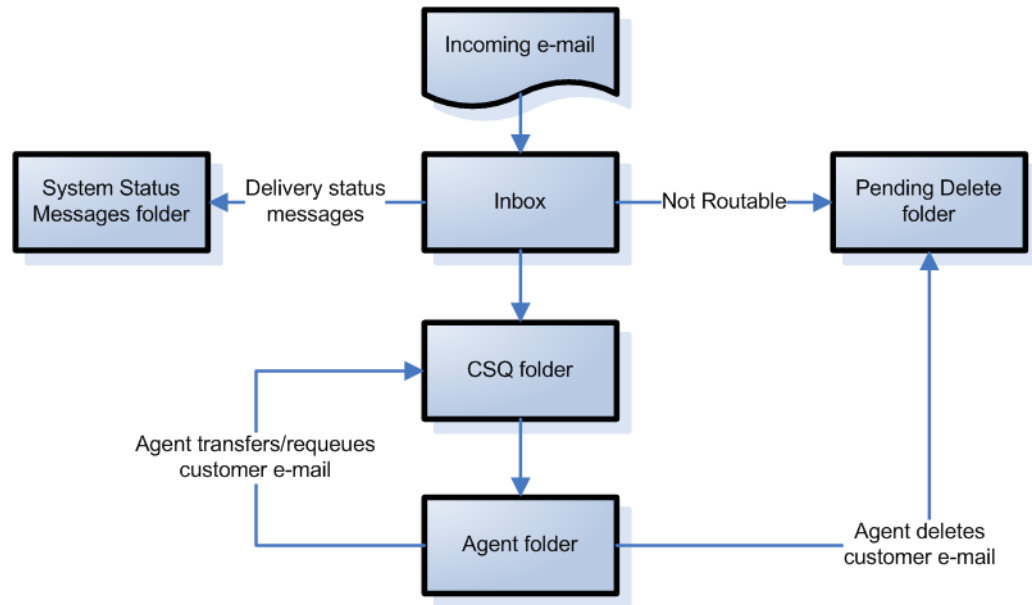
Figure 11.   Agent reply e-mail flowchart (outgoing e-mail)
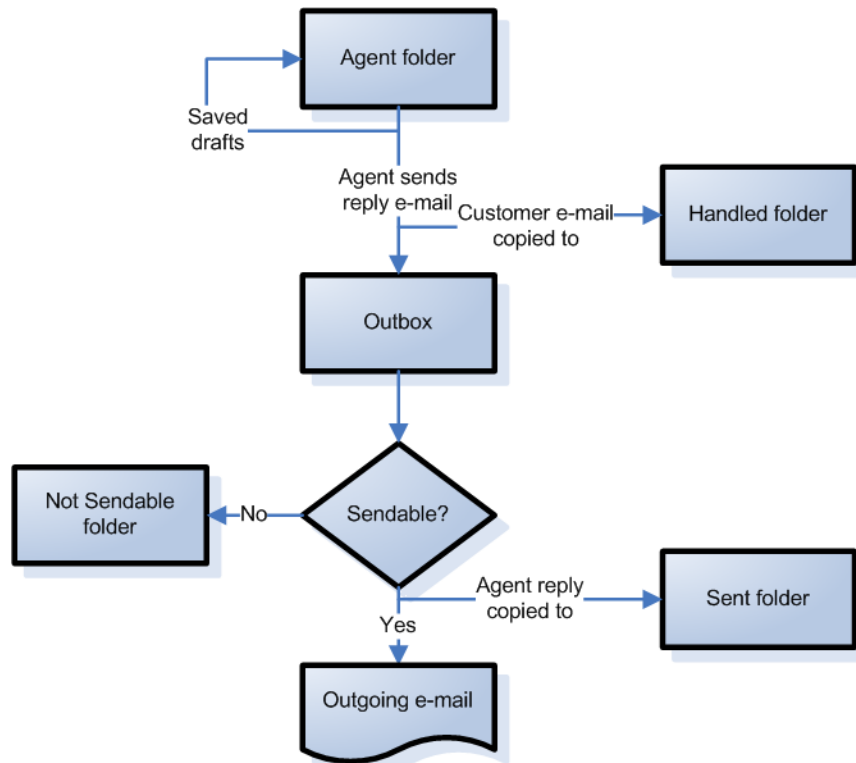
Agent E-Mail Mailbox Folders

The following folders, with the exception of the Inbox folder, are created by the Agent E-Mail service at runtime.

Inbox Folder

Initially, all inbound e-mails sent to the e-mail addresses associated with the Agent E-Mail user appear in the Inbox folder.

The Agent E-Mail service periodically checks the Inbox folder for new messages and moves them to the appropriate subfolder based on the routing rules (configured in Cisco Desktop Administrator) and agent availability. If an e-mail agent is in the E-Mail Ready state and is assigned to the appropriate CSQ, the e-mail is routed to that agent's subfolder under the Assignments folder. If there are no agents in the E-Mail Ready state, the e-mail is routed to the e-mail CSQ subfolder to wait for an agent to become available to handle that e-mail. The e-mail CSQ ID is used as the folder name.

Normally, it is not necessary to manipulate the messages located in the Inbox folder. A possible exception to this is if the Agent E-Mail service is unable to process a message in the Inbox folder and an error occurs. If this happens, you can use any IMAP client to move the message out of the Inbox and into another folder.

Assignments Folder

The Assignments folder contains subfolders, one for every agent who is assigned to an e-mail CSQ. The agent ID is used as the folder name. The Agent E-Mail service creates these folders when agents are assigned to an e-mail CSQ.

Whenever an e-mail is assigned to an agent, a subfolder is created below the agent's folder. The name of the e-mail subfolder follows the format:

> <unique e-mail ID>.<CSQ>

This message subfolder contains the customer e-mail and any saved draft response to that e-mail. When the agent clicks the Send button, the message subfolder is deleted.

Handled Folder

The Handled folder contains customer e-mails that have been answered by agents. When the agent clicks the Send button, the reply is sent and the original customer e-mailed is moved to this folder.

Periodically, the messages in the Handled folder are deleted by the Agent E-Mail service. The cleanup interval is configured in Cisco Desktop Administrator.

Not Sendable Folder

If an error occurs when sending a reply to a customer e-mail, that reply e-mail is moved to the Not Sendable folder. Errors can occur if the Exchange server is not configured to permit the Agent E-Mail account to send responses using the e-mail

addresses set up in Cisco Desktop Administrator. Once this issue is resolved, you can use a third party IMAP client to move the unsent message back into the Outbox folder for processing.

Outbox Folder

The Outbox folder contains reply messages waiting to be sent to customers. Cisco Agent Desktop moves messages to this folder so that Agent Desktop avoids using SMTP directly (SMTP typically is disabled by virus checkers). The Agent E-Mail service periodically checks this folder and sends any message it finds using SMTP. If the message is not sendable for some reason, it is moved to the Not Sendable folder.

Pending Delete Folder

The Pending Delete folder contains customer e-mails that were marked for deletion, either manually by an agent or automatically by the Agent E-Mail service if the message was determined to be non-routable when it arrived in the Inbox. Messages deleted by agents are in CSQ subfolders, and those deleted by the Agent E-Mail service are in the Not Routable folder.

In the case of messages in the Not Routable folder, it might be desirable to move those messages back into the Inbox if they were sent to a valid e-mail address that was not configured in Cisco Desktop Administrator when they arrived. After configuring the e-mail address, you can use a third-party IMAP client to move the messages from the Not Routable folder back into the Inbox so that they can be processed.

Periodically, the messages in the Pending Delete folder are deleted by the Agent E-Mail service. The cleanup interval is configured in Cisco Desktop Administrator.

Sent Folder

The Sent folder contains copies of e-mails sent by agents in response to customer e-mails. When the agent clicks the Send button, the reply is sent to the Outbox and a copy of it is moved to this folder.

It is possible that this folder contains e-mails that were not sendable. Sendability is determined when the e-mail reaches the Outbox.

Periodically, the messages in the Sent folder are deleted by the Agent E-Mail service. The cleanup interval is configured in Cisco Desktop Administrator.

System Status Messages Folder

System status or delivery status messages are usually error messages that indicate a problem with e-mail delivery. An example of an error message is the automatically-generated message received when an agent's reply to a customer e-mail is undeliverable because the customer's inbox is full. These error messages are initially delivered to the Inbox, where the Agent E-Mail service finds and moves them to the System Status Messages folder. They are never delivered to the agents.

Periodically, the messages in the System Status Messages folder are deleted by the Agent E-Mail service. The cleanup interval is configured in Cisco Desktop Administrator.

transfer folder

The Transfer folder is used by Cisco Agent Desktop in its transfer/requeue logic. It contains subfolders for the CSQs to which the e-mail messages are being transferred or requeued. Messages are moved to the subfolders and then periodically processed by the Agent E-Mail service for reassignment to the new CSQ.

Agent E-Mail Best Practices

To maximize the efficiency of Agent E-Mail, consider the following best practices recommendations when configuring and maintaining your system.

Microsoft Exchange Server

- If MS Exchange is replicated, use the most powerful and fastest of the two physical servers as the primary Mailbox node.

- Consider running all Exchange servers on physical servers instead of on virtual servers.

- The OS Event Viewer can provide information on Exchange performance monitoring, if logging for such tasks is enabled. For more information on Exchange debugging, see:

- http://www.msexchange.org/articles_tutorials/exchange-server-2007/management-administration/managing-exchange-server-2007-log-files-part1.html

Regarding the Exchange CAS/Hub and Mailbox servers, the following can contribute to poor Exchange performance:

- Low disk space on the CAS server: what is the disk space utilization?

- Severe file fragmentation: has the disk been defragmented recently? Is this monitored?

- Other processes running in the background: are there known periodic processes such as backups, software updates, or virus checking that run?

- Network connectivity between the server and the corporate network: is the connection good? Is DNS working correctly for the server? Is other network traffic affecting the processing between the Exchange server and the Unified CCX server? Are the two servers across the WAN from one another?

- Hardware: is a hardware component, such as the hard disk or network card, failing?

- VMWare: if provisioned on VMWare, is the VM image healthy? Is the VM host provisioned correctly?

Wide Area Network

Deploy the Exchange CAS/Hub and Mailbox server closer to the Unified CCX server in order to improve network traffic from the Exchange IMAP server to the Agent E-Mail server process.

Microsoft Exchange Server Management

Periodically check the following folders for backlogs of e-mails:

- Sent
- Sent Items
- Handled
- Not Sendable
- Not Routable
- Trash
- Deleted

The Agent E-Mail service does not maintain these folders. A large number of e-mails (10,000 or more) stored in these folders can cause delays in Agent E-Mail. Empty them to improve Exchange performance.

Configuring Java for Agent E-Mail

It is possible that some e-mails will be too large to be readily displayed in Cisco Agent Desktop. In general, e-mails over 1 MB in size can take a long time to download and display, or might not display at all. The reason for this is that the default maximum heap size for the Java applet used for the Agent E-Mail feature is too small to handle larger messages well.

To improve the handling of large e-mail messages, you can increase the maximum heap size in the Java applet.

To increase the maximum heap size in the Java applet:

1. On the agent's PC, make sure that all browsers are closed.

2. Open the Windows Control Panel.

3. Double-click the Java (or Java Plug-In) icon to display the Java Control Panel.

4. Select the Java tab (Figure 12).

Figure 12.   Java Control Panel
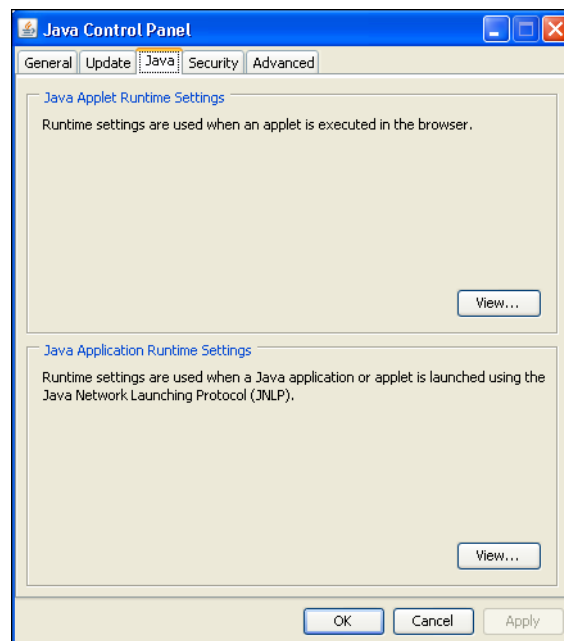
5. In the Java Applet Runtime Settings section, click View. The Java Runtime Settings dialog box appears (Figure 13).

Figure 13. Java Runtime Settings dialog box
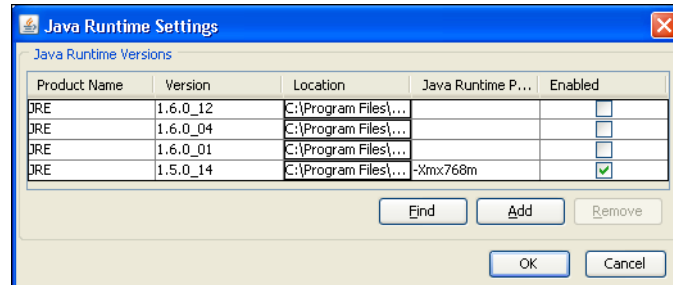
6. On the row for the most recent JRE version supported by CAD (JRE 1.6.0_12), double-click the Java Runtime Parameters field and enter the following parameter:

-Xmx768m

NOTE: The value 768m has been tested and found to improve performance so that e-mail up to 2 MB are displayed easily. However, if the agent's PC does not have enough memory to accommodate this value, lower values (such as 512m or 300m) can be used.

7. Click OK to close the dialog box, and then click OK again to save your changes and close the Java Control Panel.

8. Exit Windows Control Panel.

The next time the agent starts Agent Desktop, the new setting will be in effect.

Configuring Microsoft Exchange for Agent E-Mail

This section describes how to configure Microsoft (MS) Exchange so that it supports the Agent E-Mail feature.

CAD supports MS Exchange 2003 and MS Exchange 2007.

CAD connects to a single mail store account for all agents and for the Agent E-Mail service. This account must be created by the mail store administrator. CAD is configured to use this account via Cisco Desktop Administrator (see the *Cisco Desktop Administrator User Guide* for more information).

CAD uses the following protocols:

■ IMAP4 for retrieving messages. IMAP4 is used to communicate to the MS Exchange server from the Unified CCX servers and all e-mail agent desktops.

■ SMTP for sending messages. SMTP is used to communicate with the MS Exchange server from the Unified CCX servers only. SMTP is not used from agent desktops for the Agent E-mail feature.

These protocols must be enabled in MS Exchange. Note that these protocols are not typically enabled by default.

> NOTE: Make sure that the Agent E-Mail service can use the SMTP protocol to communicate with the mail store. SMTP is sometimes blocked by firewalls and virus protection software.

CAD uses a single e-mail account. However, it can (and typically will) have multiple distribution group addresses that direct e-mails to specific users. This e-mail account and the corresponding distribution lists must be configured manually by the mail store administrator. Routing information for the distribution list addresses can then be specified in Desktop Administrator.

General Process for Configuring MS Exchange for Agent E-Mail

The following is the general procedure for configuring Agent E-Mail.

To configure Agent E-Mail:

1. Configure a single e-mail account for Microsoft Exchange. This is typically performed using Active Directory tools.

2. Create one or more distribution groups with the new e-mail account as the only member. These distribution groups can then be published by the company for external use by customers. E-mail sent to these groups is routed to the Agent E-Mail e-mail account. Examples of distribution lists are:

   ■   sales@example.com

   ■   marketing@example.com

   ■   support@example.com

3. Create one or more E-Mail CSQs in CCX Administrator.

4. Associate the E-Mail CSQs with the appropriate e-mail agents in CCX Administrator.

5. Configure CAD's connection to the mail store (IMAP and SMTP) using Desktop Administrator.

6. Associate the distribution group e-mail addresses with the E-Mail CSQs.

Configuring MS Exchange 2003

Use the following procedures as a guideline for configuring MS Exchange 2003.

> NOTE: Since installations of MS Exchange 2003 can be configured differently, the location of some nodes might be different than what is displayed in these procedures. It is recommended that you consult your MS Exchange 2003 documentation for more complete and up-to-date instructions.

Configuring IMAP and SMTP

MS Exchange enables you to set up virtual IMAP and SMTP servers. The EEM product makes use of these virtual servers to ensure that the connection to the mail store uses the appropriate settings.

To set up an IMAP virtual server:

1. Launch Microsoft Exchange System Manager.

2. In the left navigation pane, select the Servers > Protocols > IMAPV4 node.

3. From the menu, choose Action > New > IMAPV4 Virtual Server. The New IMAPV4 Virtual Server Wizard appears.

4. Enter the information requested by the wizard to create the new virtual server. When you click Finish, the new virtual server is listed in the navigation pane under Servers > Protocols > IMAPV4.

5. Right-click the server name and choose Properties. The server properties window appears.

6. Select the Access tab, and click Authentication. The Authentication window appears (Figure 14).

Figure 14.   Authentication window
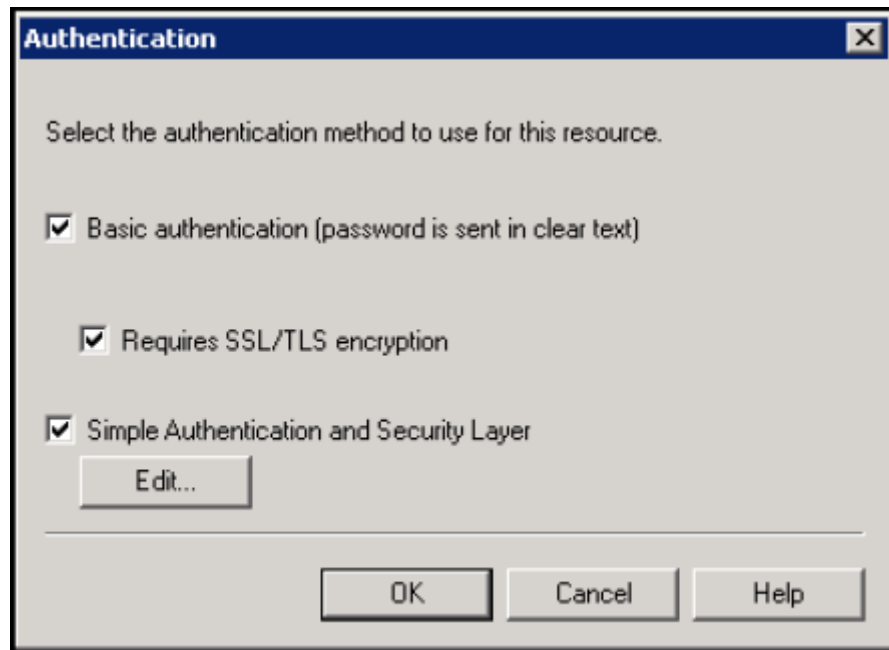
7. Configure the window as shown in Figure 14.

   ■ Basic authentication with and without SSL/TLS encryption is supported.

   ■ Simple authentication and security layer is supported.

   If you choose to use SSL/TLS encryption, you must have a valid security certificate configured.

   a. Click OK to close the Authentication window.

   b. Select the Access tab. If the Communication button is disabled, a certificate has not yet been configured.

   c. To configure a certificate, click Certificate. The Web Server Certificate Wizard appears.

   d. Complete the wizard. For more information on security certificates, consult your Microsoft Exchange 2003 documentation.

8. Select the Message Format tab, and complete the tab as shown in Figure 15.

Figure 15.   Message Format tab
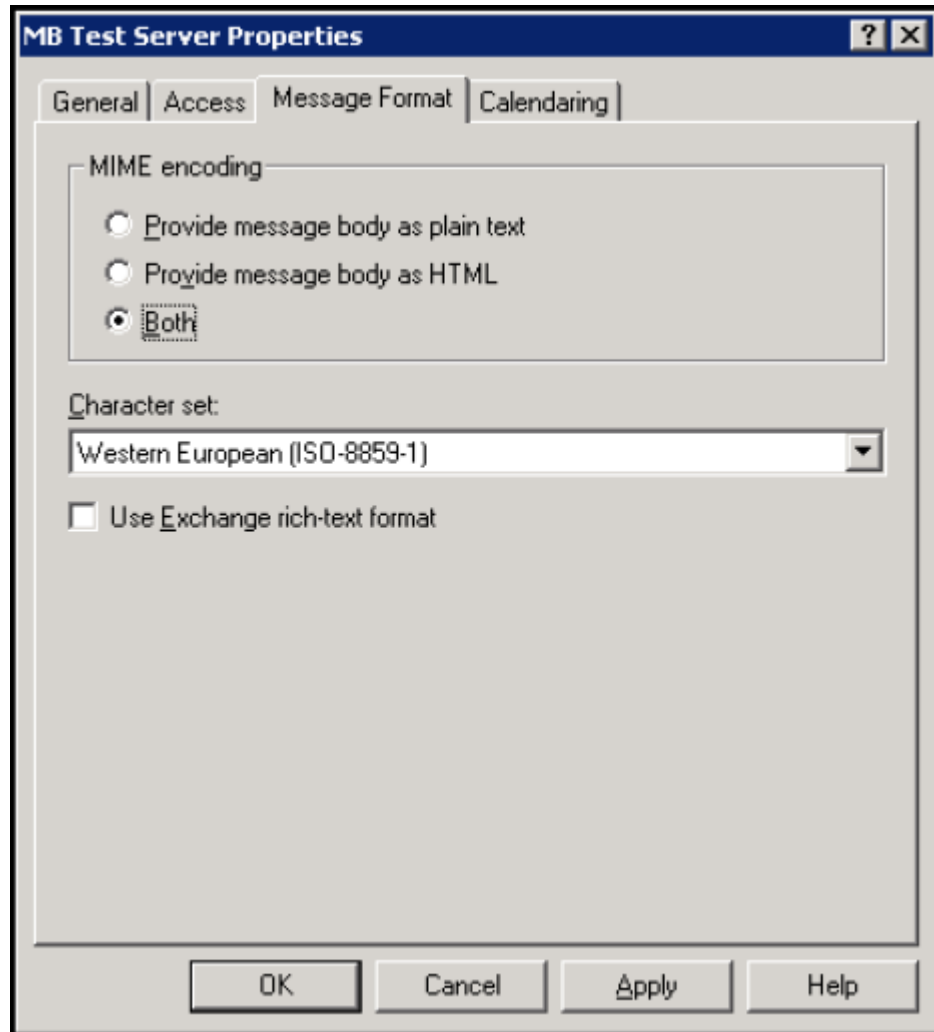
9. Click OK to save your changes and close the window.

10. The new virtual server should be running. Right-click the server name to view a menu that includes the options Start and Stop. Click Start if the server is not already running.

11. If you are unable to start the server, select Start > Control Panel > Administrative Tools > Services and ensure that the Microsoft Exchange IMAP4 service is started.

> **NOTE:** If you make any changes while the service is running, you must restart the IMAP4 service to ensure the changes go into effect.

To set up an SMTP virtual server:

1. Launch Microsoft Exchange System Manager.

2. In the left navigation pane, select the Servers > Protocols > SMTP node.

3. From the menu, choose Action > New > SMTP Virtual Server. The New SMTP Virtual Server Wizard appears.

4. Enter the information requested by the wizard to create the new virtual server. When you click Finish, the new virtual server is listed in the navigation pane under Servers > Protocols > SMTP.

5. Right-click the server name and choose Properties. The server properties window appears.

6. Select the Access tab, and click Authentication. The Authentication window appears (Figure 16).

Figure 16. **Authentication window**
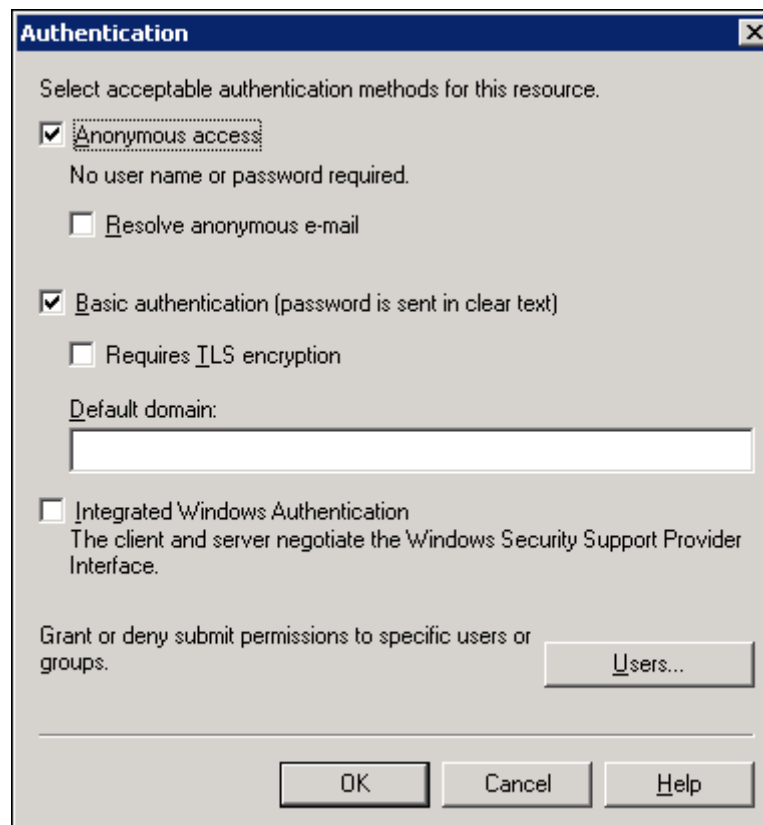
7. Configure the window as shown in Figure 16.

   ■ Anonymous access (open relay) and basic authentication (clear text) are supported.

   ■ TLS encryption for basic authentication and Integrated Windows Authentication are supported.

8. Click OK.

9. The new virtual server should be running. In the navigation pane. Right-click the server name to view a menu that includes the options Start and Stop. Start is disabled and Stop is enabled if the server is running.

10. If you are unable to start the server, select Start > Control Panel > Administrative Tools > Services and ensure that the Microsoft Exchange SMTP service is started.

   NOTE: If you make any changes while the service is running, you must restart the SMTP service to ensure the changes go into effect.

Creating a User
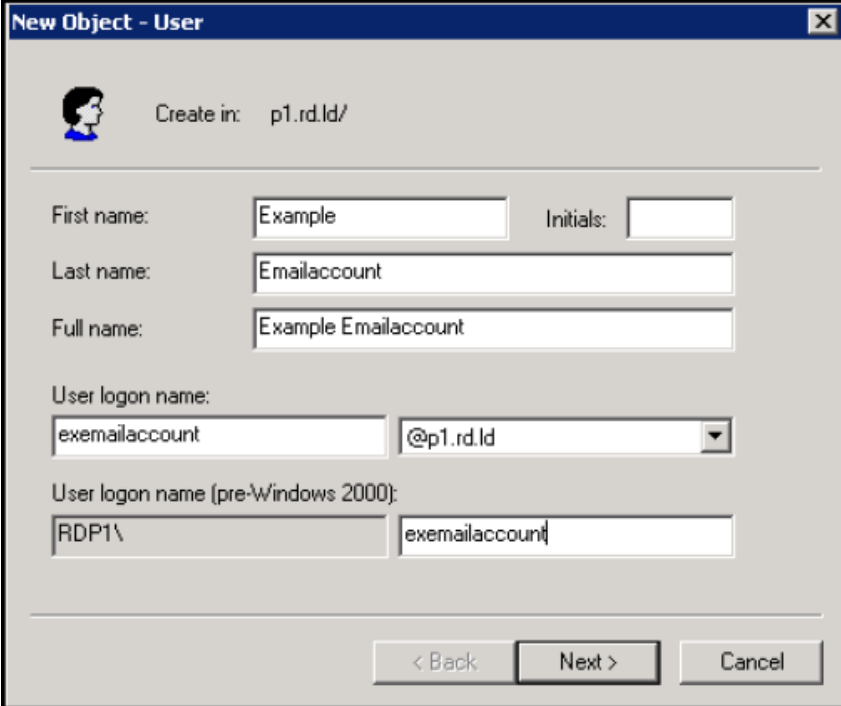
Follow these steps to create the Active Directory user account that is used to receive customer e-mails.

To create a user:

1. Launch Active Directory Users and Computers.

2. In the left navigation pane, right-click the appropriate domain and choose New > User. The New Object - User wizard appears (Figure 17).

Figure 17.   New Object - User window 1

3. Complete the name information for the new user, and then click Next. The next window in the wizard appears (Figure 18).
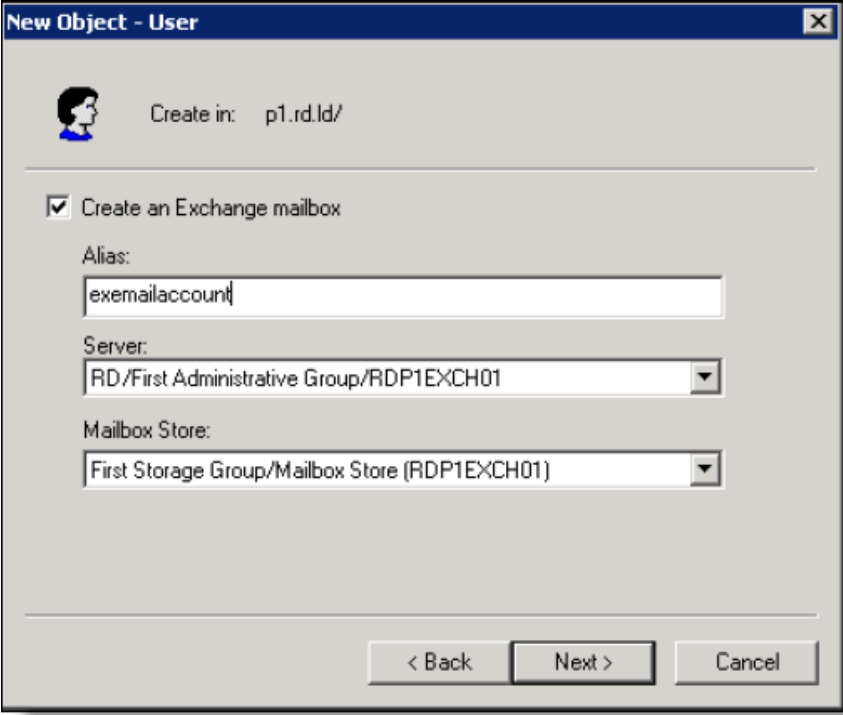
Figure 18.   New Object - User window 2

4. Create a password for the new user, and then click Next. The next window in the wizard appears (Figure 19).

Figure 19.   New Object - User window 3

5. Select the Create an Exchange mailbox check box, complete the rest of the fields, and then click Next. The final window in the wizard appears (Figure 20).

Figure 20.   New Object - User window 4
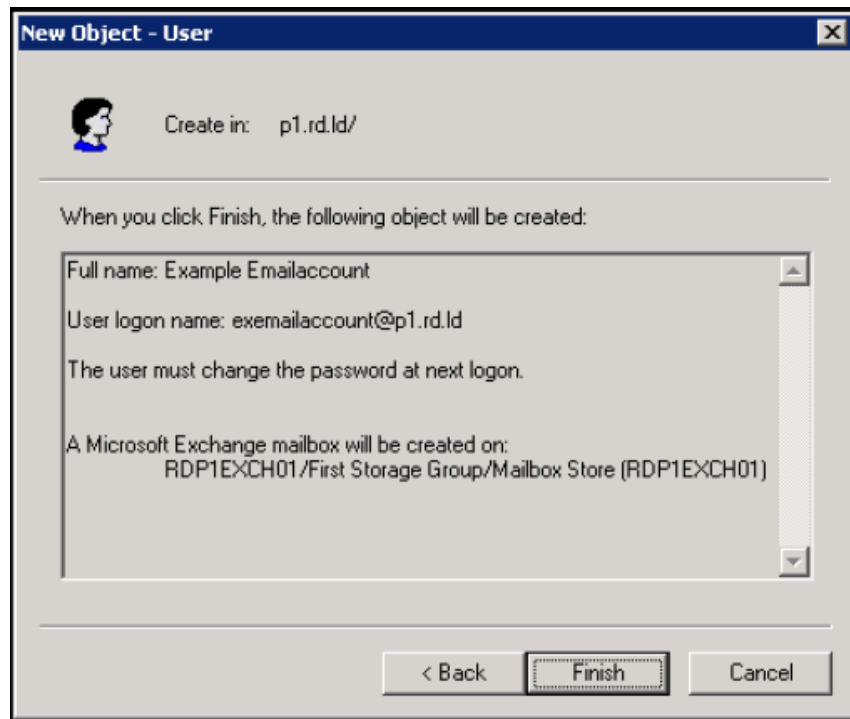
6. If all the information in the window is correct, click Finish. If you want to change anything, click Back to the appropriate window and enter your corrections. After you click Finish, the new user is listed under the Users node in the navigation pane.

Creating Distribution Groups
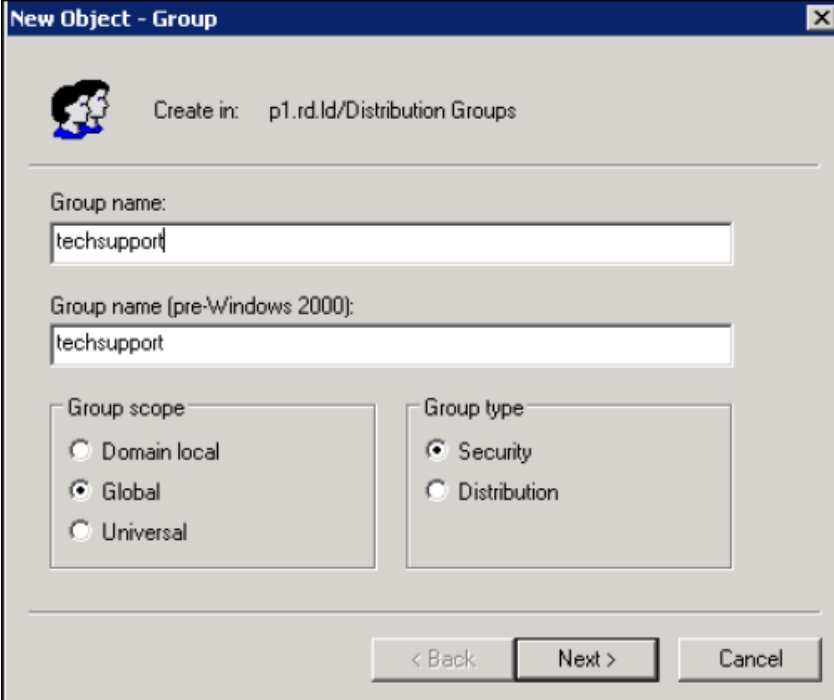
Follow these steps to create the distribution groups that will be used to route customer e-mails to the appropriate agent contact service queues. Each distribution group you create will contain only one user, the user you created in the previous section.

To create a distribution group:

1. Launch Active Directory Users and Computers.

2. In the left navigation pane, right-click the Distribution Groups node and choose New > Group. The New Object - Group wizard appears (Figure 21).

Figure 21.   New Object - Group window 1

3. Enter a name for your distribution group and click Next. The next window in the wizard appears (Figure 22).

Figure 22.   New Object - Group window 2
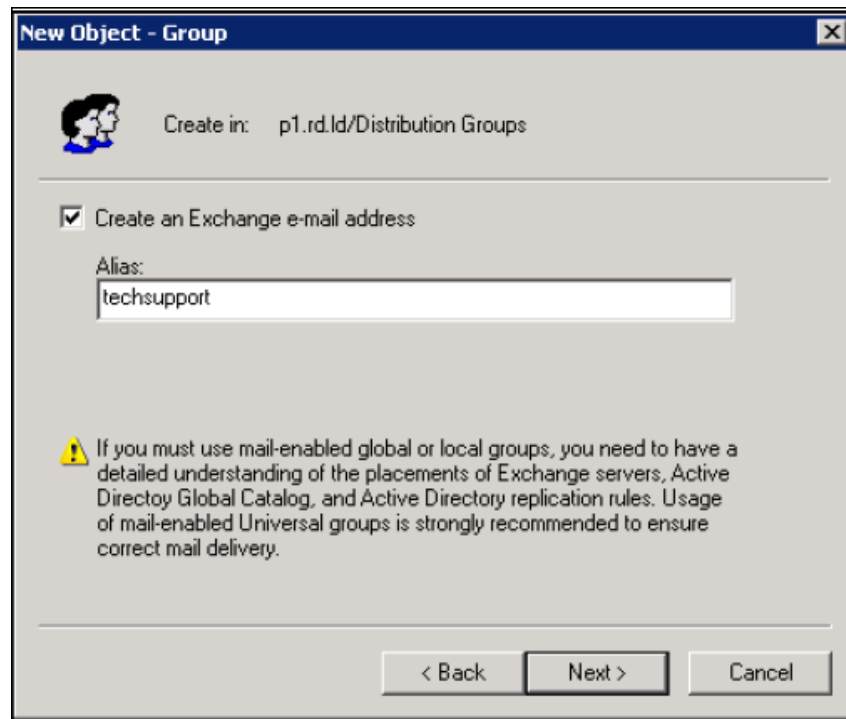
4. Select the Create an Exchange e-mail address check box, enter an alias for the distribution group, and click Next. The final windows of the wizard appears (Figure 23).

Figure 23.   New Object - Group window 3
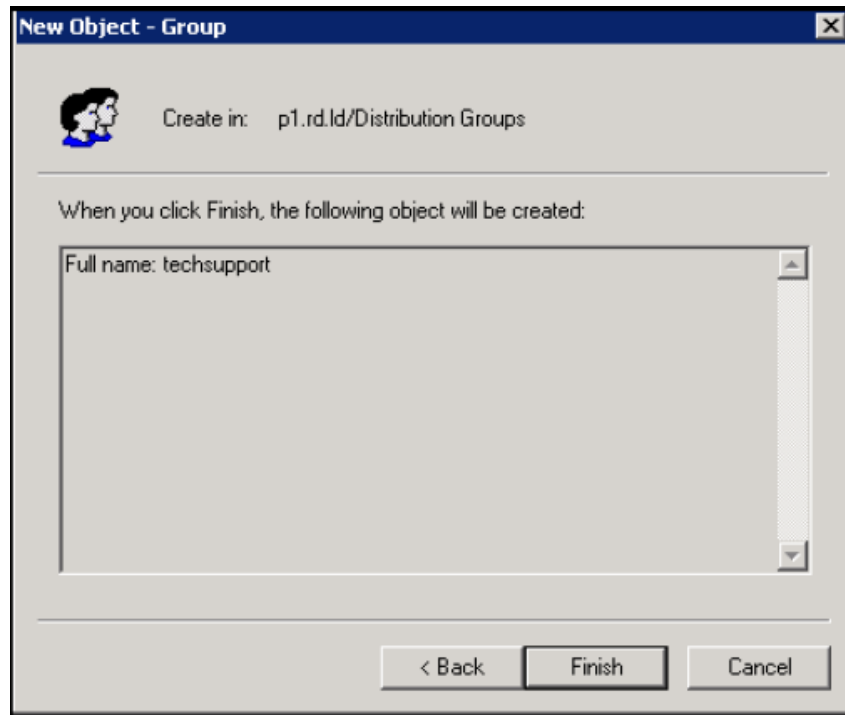
5. If all the information in the window is correct, click Finish. If you want to change anything, click Back to the appropriate window and enter your corrections. After you click Finish, the new distribution group is listed under the Distribution Groups node in the navigation pane.

To add the user to the new distribution group:

1. Select the Distribution Groups node in the left navigation pane, and then right-click the distribution group name in the right pane. Select Properties from the popup menu. The Properties window appears.

2. Select the Members tab, and click Add. The Select Users, Contacts, Computers, or Groups dialog box appears (Figure 24).

Figure 24.   Select Users, Contacts, Computers, or Groups dialog box
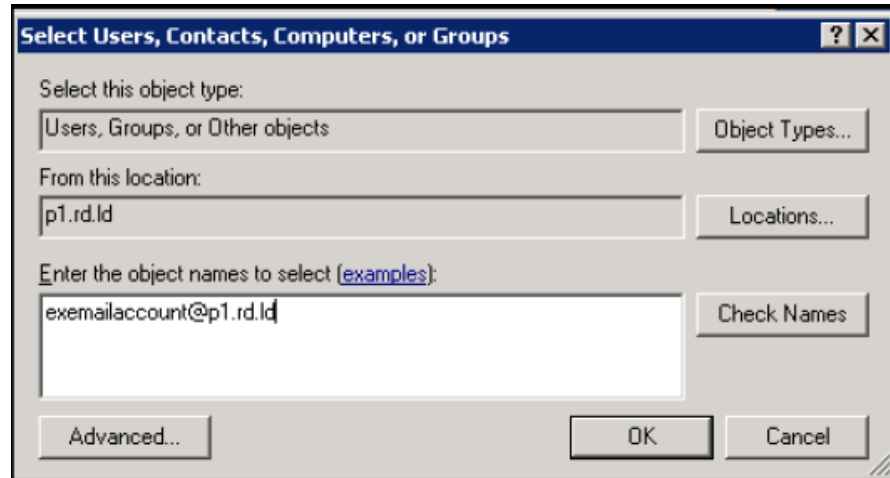
3. Enter the e-mail address of the user and then click OK. The user is now listed on the Properties window's Members tab (Figure 25). Click OK again to close the window.

Figure 25.   Distribution Group Properties window
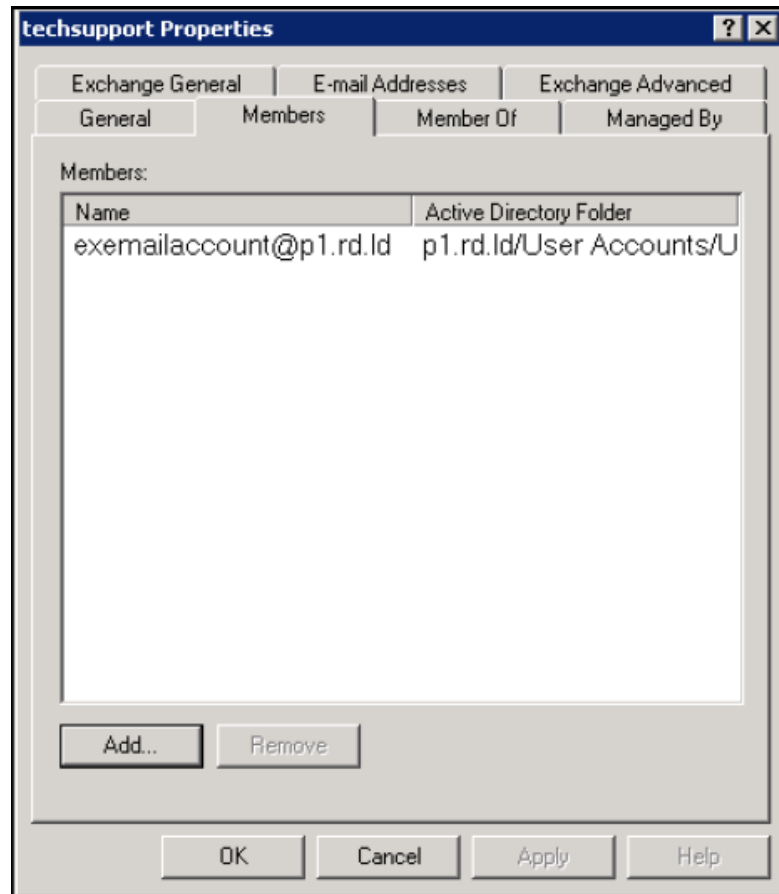
4. Repeat steps 1–3 for each distribution group you created.

Once the distribution groups are configured, you can associate them with e-mail CSQs using Desktop Administrator. See the *Cisco Desktop Administrator User Guide* for more information on this process.

Configuring MS Exchange 2007

Use the following procedures as a guideline for configuring MS Exchange 2007.

> **NOTE:** Since installations of MS Exchange 2007 can be configured differently, it is recommended that you consult your MS Exchange 2007 documentation for more complete and up-to-date instructions.

Configuring IMAP and SMTP

MS Exchange enables you to set up virtual IMAP and SMTP servers. The Agent E-Mail feature makes use of these virtual servers to ensure that the connection to the mail store uses the appropriate settings.

It is recommended that you have your MS Exchange administrator set up IMAP and SMTP virtual servers.

IMAP Connections per User

By default, the maximum number of IMAP connections per user in MS Exchange 2007 is 10. Every agent and the E-mail Service uses the same user ID, so this number is far too low. It is recommended that the number of IMAP connections per user is increased to 1,000.

To increase the maximum number of connections per IMAP user:

1. Launch the Exchange Management Console.

2. Under the Server Configuration node, select Client Access.

3. On the POP3 and IMAP4 tab, right-click IMAP4 and select Properties. The IMAP4 Properties dialog box appears.

4. On the Connection tab, change the value for Maximum connections from a single user to 1000.

5. Click Apply, and then click OK.

Configuring Security Settings

The following section contains information on how to configure IMAP4 and SMTP security settings for use with Agent E-Mail.

To configure IMAP security settings:

1. Launch the Exchange Management Console.

2. In the left navigation pane, select Server Configuration > Client Access.

3. In the middle pane, select the POP3 and IMAP4 tab.

4. Right-click IMAP4 and choose Properties from the popup menu. The Properties window appears (Figure 26).

Figure 26.   IMAP4 Properties window.
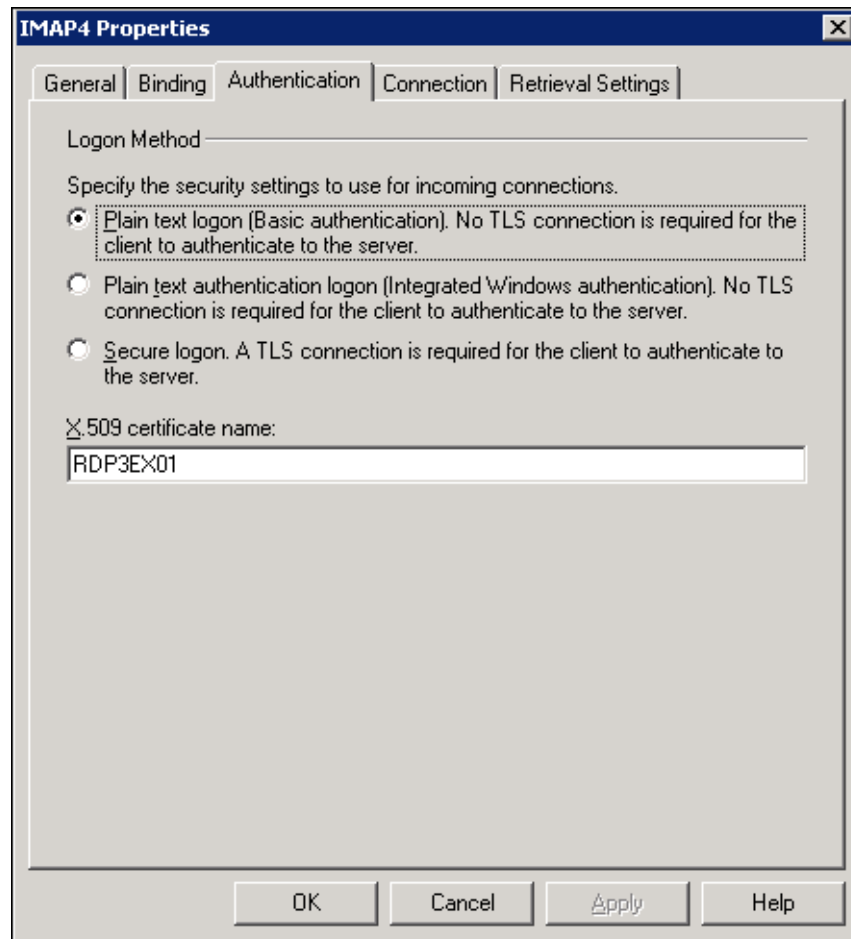
5. Select the Authentication tab, and configure the tab as shown in Figure 26.

    ■   Plain text logon (basic authentication) is supported.

    ■   Secure logon is supported.

    ■   Plain text authentication logon (Integrated Windows authentication) is not supported.

        If you choose secure logon, you must configure a valid security certificate. See your Microsoft Exchange 2007 documentation for further details.

6. Click Apply and then OK to save your changes and dismiss the window.

7. Restart the IMAP server after you have made your changes.

To configure SMTP security settings:

1. Launch the Exchange Management Console.

2. In the left navigation pane, select Hub Transport.

3. In the middle pane, right-click the appropriate SMTP connector in the Receive Connectors tab, and choose Properties from the popup menu. The Properties window appears (Figure 27).

Figure 27. Properties window (Authentication tab)
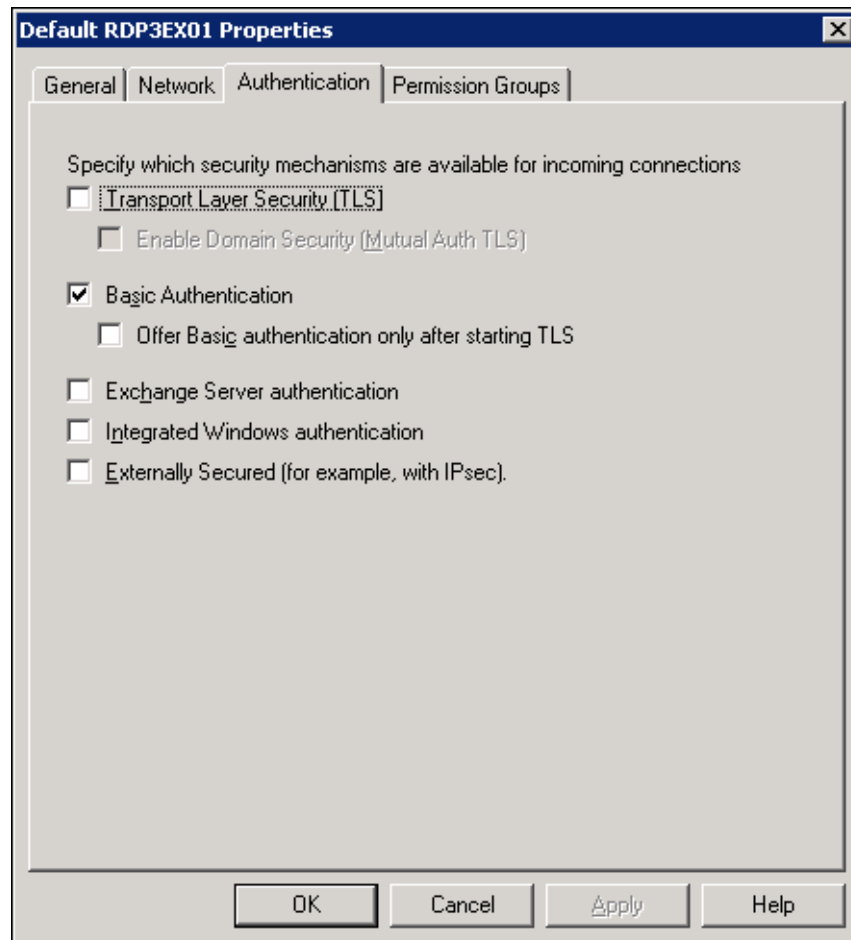
4. On the Authentication tab, select the Basic Authentication check box.

   NOTE: No other security methods are supported.

5. Click Apply and then OK to save your changes and dismiss the window.

6. Restart the SMTP server after you have made your changes.

Creating a User

The following procedure is an example of how to create a user in MS Exchange 2007. For more in-depth information, see this page of the Microsoft Exchange Team Blog:

http://msexchangeteam.com/archive/2006/09/05/428833.aspx

To create a user:

1. Launch the Exchange Management Console.

2. In the left navigation tree pane, select the Recipient Configuration > Mailbox node (Figure 28)..

Figure 28.   Exchange Management Console

When you select the Mailbox node, three panes are displayed. The center pane lists all existing accounts for both MS Exchange 2003 and MS Exchange 2007. The Recipient Type Details column indicates the type of account:

■ Legacy = MS Exchange 2003

■ User = MS Exchange 2007

You cannot share accounts between the Exchange 2003 and 2007 servers. You must setup a separate account for each server, and the account must have a unique name across both servers.

3. Right-click the Mailbox node and from the popup menu, choose New Mailbox. The New Mailbox wizard appears (Figure 29).

Figure 29.   New Mailbox wizard window 1
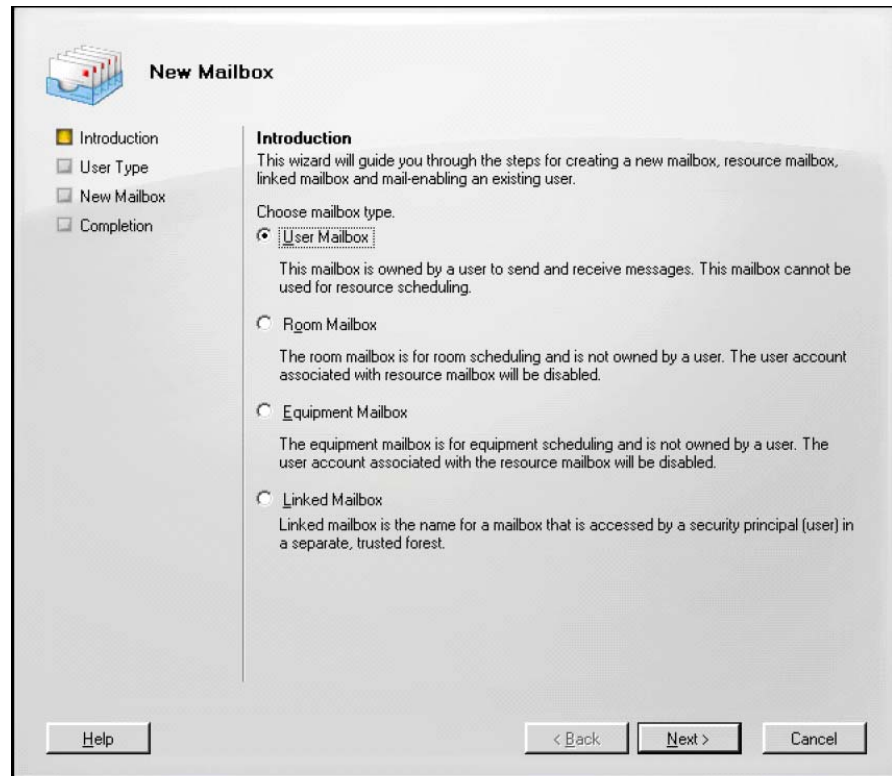
4. Select New User and click Next.

Figure 30.   New Mailbox wizard window 2
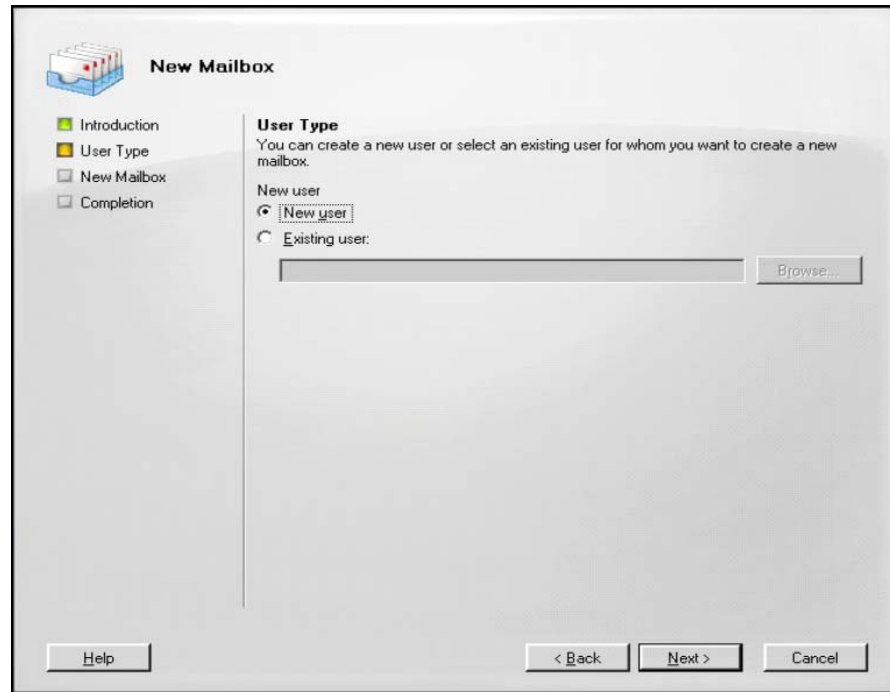
5. New User is selected. If you want to migrate an account from MS Exchange 2003, select Existing User and then browse to the account name. Bear in mind that if you do this, the account will no longer be available in MS Exchange 2003.

6. Click Next. The User Information window of the wizard appears (Figure 31).

Figure 31.   New Mailbox wizard window 3

7. Enter the user information for the new account and click Next. The Mailbox Settings window of the wizard appears (Figure 32).

Figure 32.   New Mailbox wizard window 4

8. Accept the defaults, or configure the mailbox settings as desired, and then click Next. A window containing the summary of the new mailbox settings appears (Figure 33).

Figure 33.   New Mailbox wizard window 5
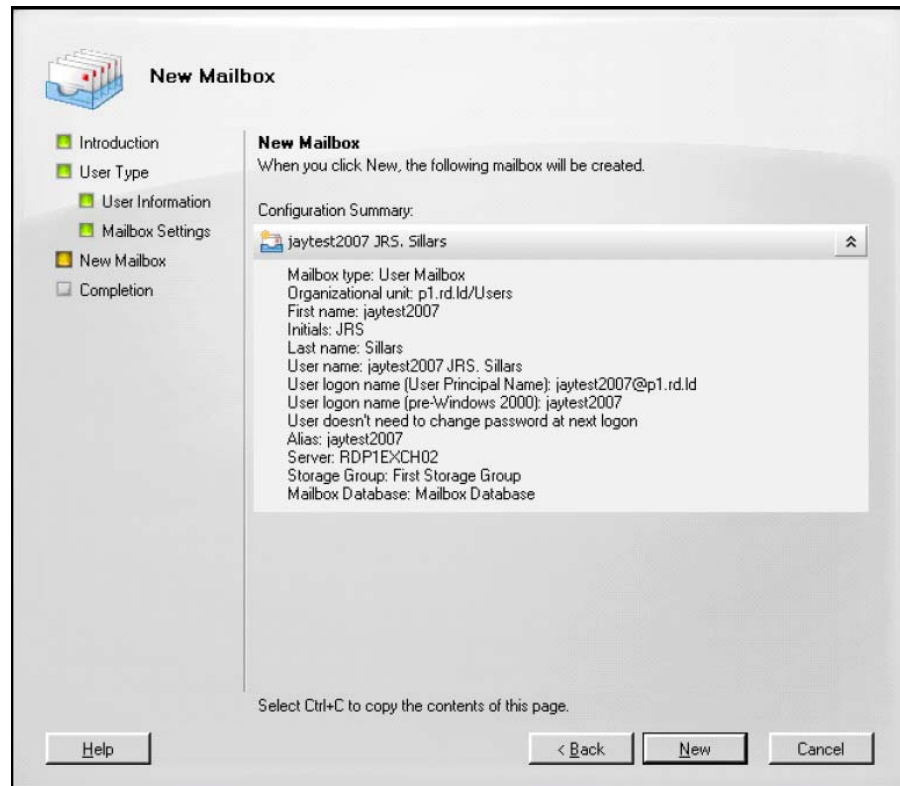
9. If the settings are not correct, click Back and correct the errors. If the settings are as you desire, click New. The final window of the wizard appears (Figure 34).

Figure 34.   New Mailbox wizard window 6
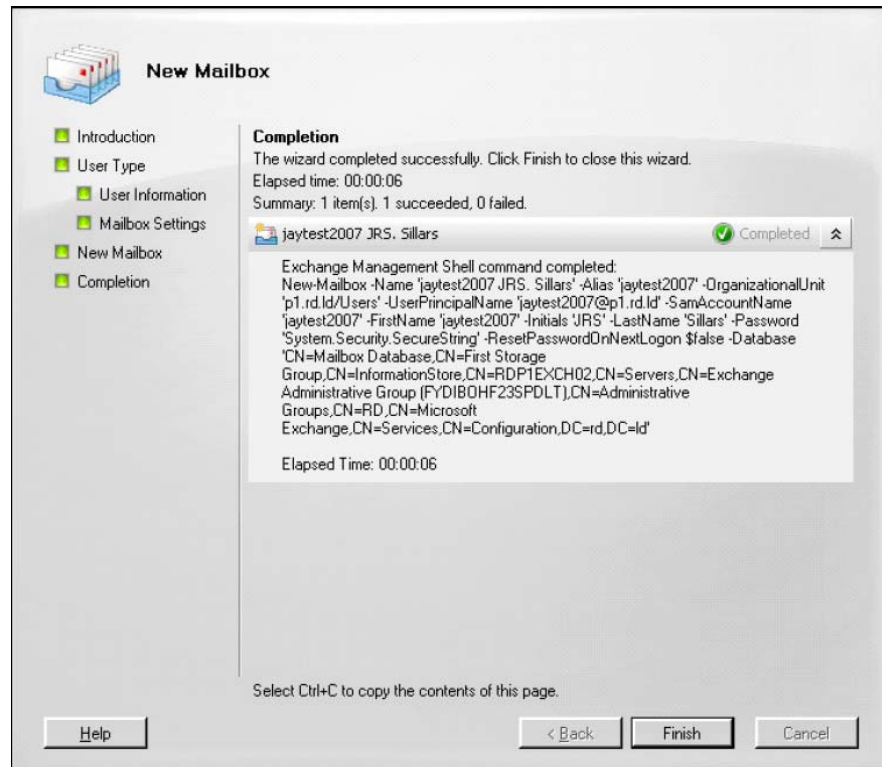
10. Click Finish to close the wizard and create the new mailbox.

Creating Distribution Groups

By default, MS Exchange 2007 rewrites the recipient address (SMTP to) in incoming e-mail to the primary e-mail address for the account. This does not work well with Agent E-Mail because this feature keys off the recipient address for its routing decisions.

As a workaround, distribution groups can be used instead of e-mail address aliases. Customers then send e-mail to a distribution group, which then gets routed to the Agent E-Mail e-mail account. The address of the distribution group is preserved in the To field of the e-mail, so routing can be based on that.

In Cisco Desktop Administrator, use the distribution group address to associate e-mails with an e-mail CSQ.
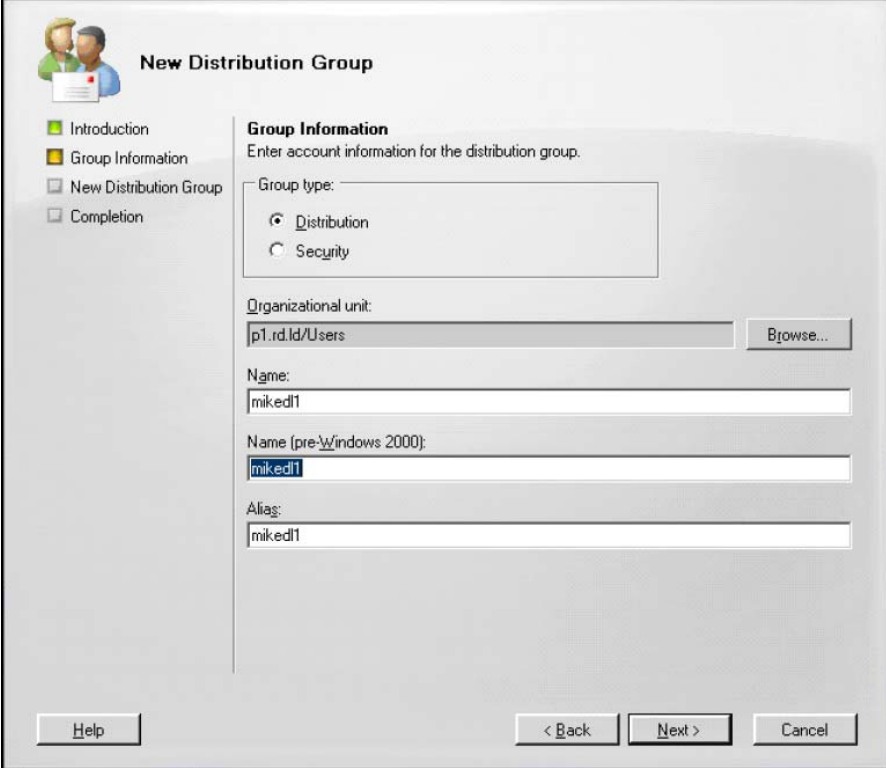
To create a distribution group:

1. Launch Exchange Management Console.

2. In the left navigation pane, select the Distribution Group node.

3. Right-click the Distribution Group node and select New Distribution Group from the popup menu. The New Distribution Group wizard appears (Figure 35).

Figure 35.   New Distribution Group wizard window 1

4. Select New Group and then click Next. The Group Information window appears (Figure 36).

Figure 36.   New Distribution Group wizard window 2

5. Select Distribution as the group type, complete the required information for the new group, and then click Next. The final window in the wizard appears (Figure 37).

Figure 37. New Distribution Group wizard window 3
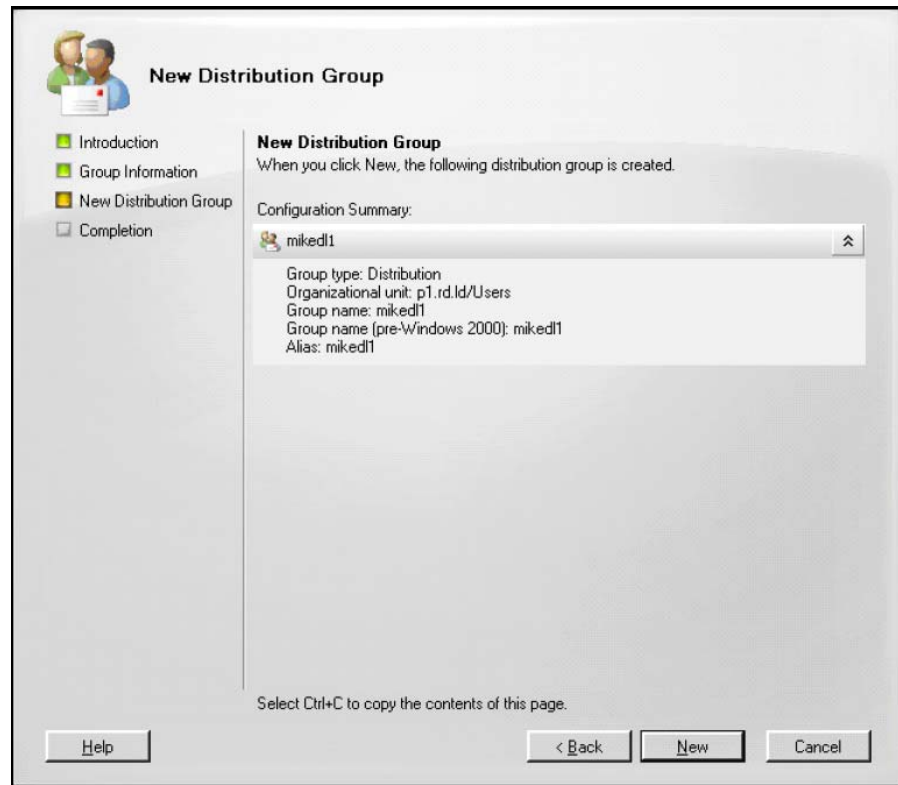
6. If the settings are not correct, click Back and correct the errors. If the settings are as you desire, click New. The final window of the wizard appears (Figure 38).

Figure 38.   New Distribution Group wizard window 4

7. Click Finish to create the new distribution group and close the wizard. The new distribution group is now listed under the Distribution Group node.

To add the Agent E-Mail e-mail address to the new distribution group:

1. Launch Exchange Management Console.

2. In the left navigation pane, select the Distribution Group node. The distribution groups are listed in the center pane.

3. Double-click the distribution group. The Properties window appears. Select the Members tab.

4. Click Add and select the Agent E-Mail e-mail account. The account is added to the distribution group (Figure 39)..

Figure 39. Distribution Group Properties window
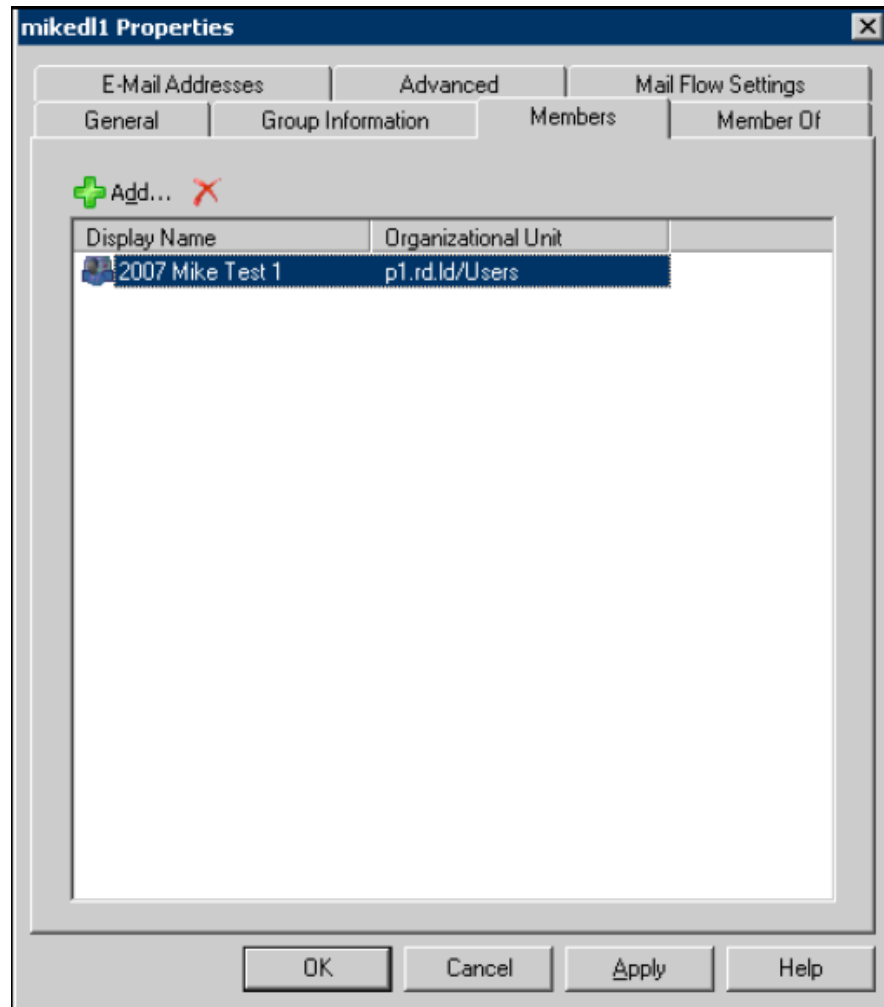
5. Click Apply to save your changes, and then OK to close the Properties window.

Testing Access to the Agent E-Mail Account

The new e-mail account can be accessed using an IMAPv4-capable e-mail client, such as Microsoft Outlook 2003. Follow these steps to test access to the account.

To test access to the Agent E-Mail e-mail account:

1. In Control Panel, start the Mail utility. The Mail Setup—Outlook window appears.

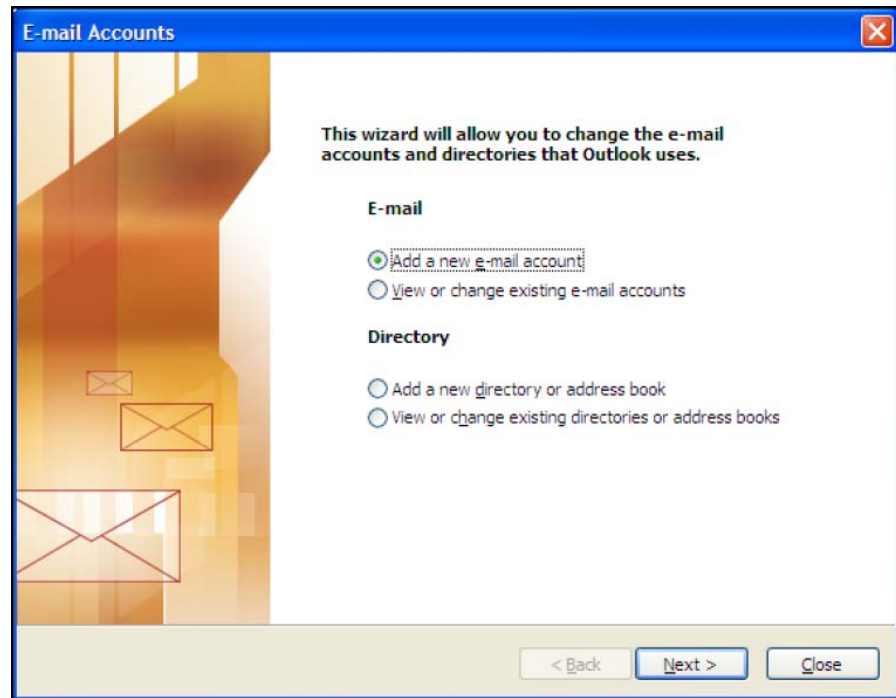2. Click Show Profiles. The Profiles window appears (Figure 40).

Figure 40.   Mail Profiles window
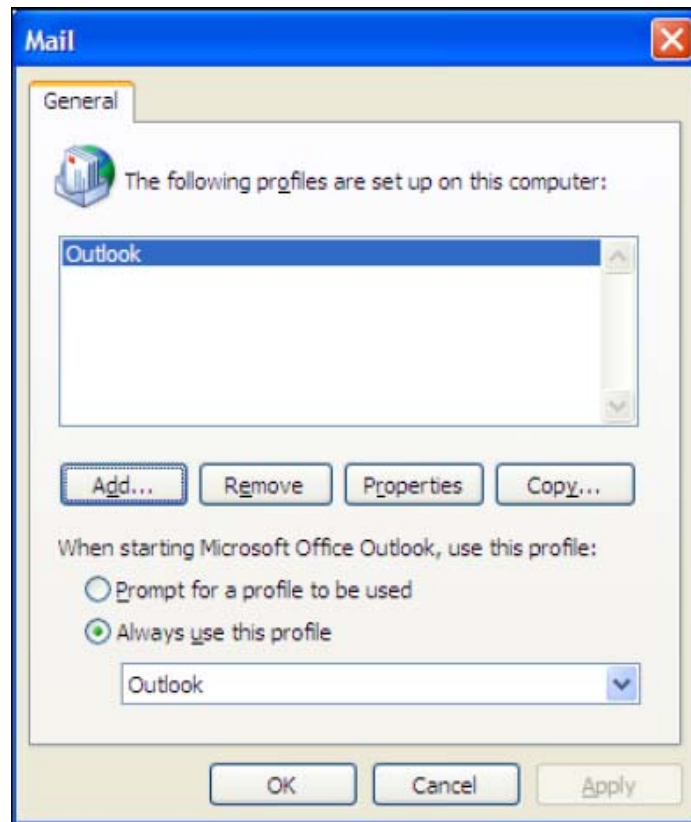
3. Click Add.The New Profile dialog box appears (Figure 41).
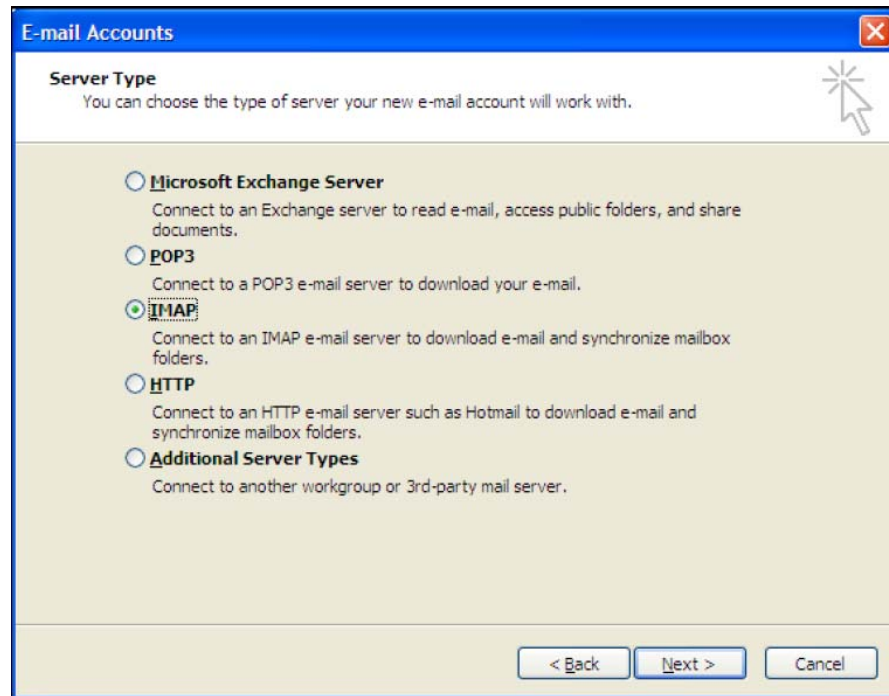
Figure 41.   New Profile dialog box
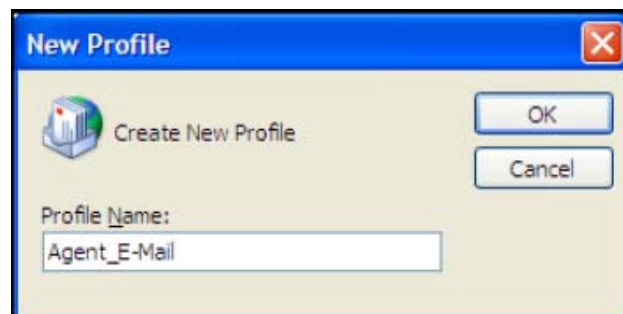
4. Enter the name of the Agent E-Mail account and click OK. The E-Mail Accounts wizard appears (Figure 42)..

Figure 42.   E-Mail Accounts wizard window 1

5. Select Add a new e-mail account and then click Next. The Server Type window appears (Figure 43).

Figure 43. E-Mail Accounts wizard window 2

6. Select IMAP and then click Next. The Internet E-Mail Settings (IMAP) window appears (Figure 44).

Figure 44.   E-Mail Accounts wizard window 3

7. Enter the required information for the Agent E-Mail account. If you have changed the SMTP and/or IMAP port numbers to something other than the defaults, click More Settings and configure the information on the Advanced tab.

8. Click Next and then Finish to create the new e-mail account profile. The new profile is now listed on the Mail Profiles window (Figure 45).

Figure 45.   Mail Profiles window displaying the new profile
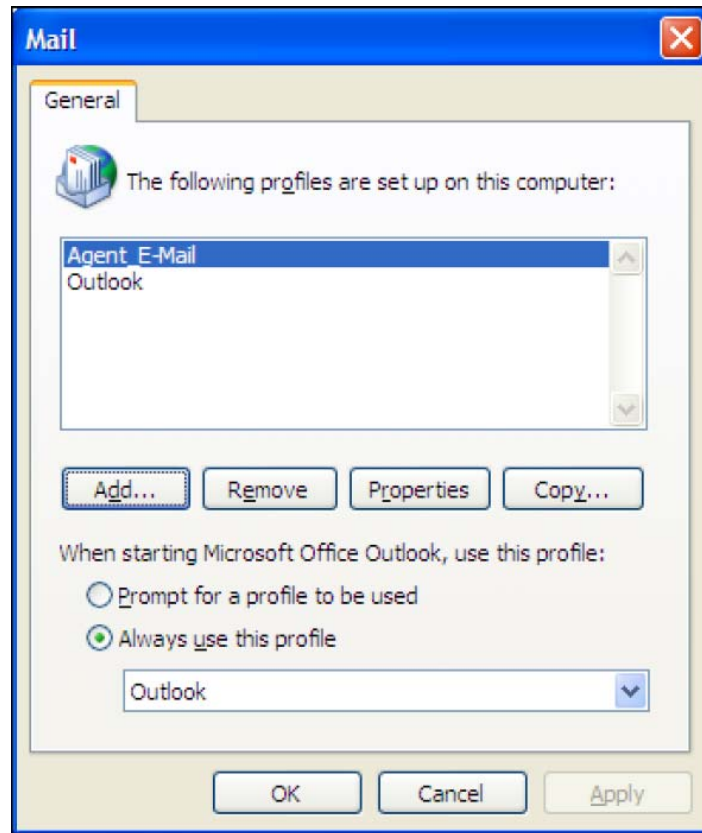
9. When you launch MS Outlook, you will be prompted for a profile to use. Select your new profile from the Choose Profile dialog box and click OK.

10. The Outlook inbox is displayed. Note that by default the Agent E-Mail account has two folders, Inbox and Junk E-Mail (Figure 46).

Figure 46.   MS Outlook Inbox

Converting Recordings from RAW to WAV Format

Recordings made by supervisors are archived as RAW voice data packets; they can only be reviewed using the Supervisor Record Viewer. However, if you want to permanently save selected recordings as WAV files, you can use either of two methods:
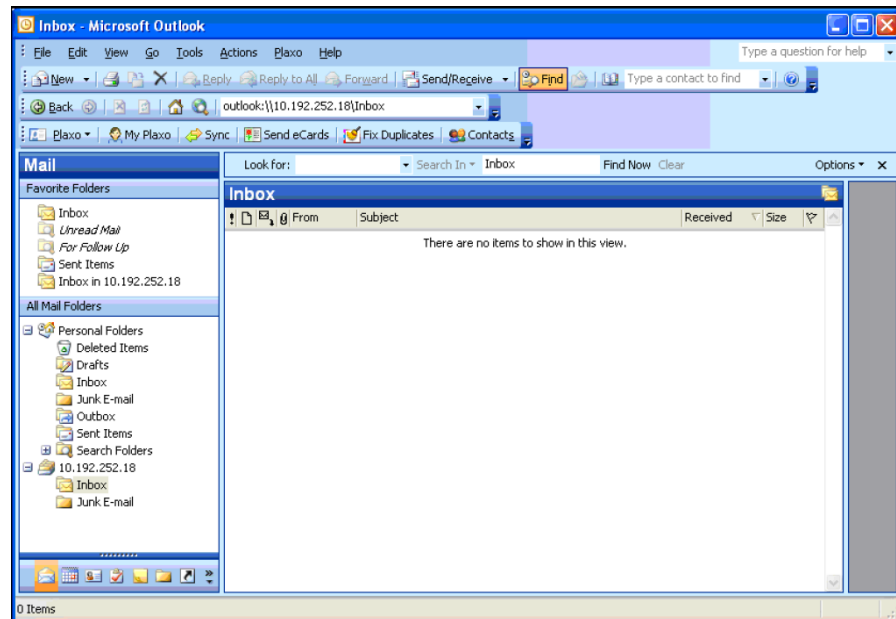
- Using the "Play and Save" button in Supervisor Record Viewer and saving the recording to a selected folder
- Using the Unified CCX Raw2Wav.exe command line utility

See the *Cisco Supervisor Desktop User Guide* for information on saving recordings as WAV files through Supervisor Record Viewer.

Using the Unified CCX raw2wav Utility

This utility is located in the C:\Program Files\Cisco\Desktop\bin folder. It must be run from this location in a command window on the computer that has Cisco Desktop Work Flow Administrator installed.

Each RAW format recording is comprised of the following files:

- <name>.to.raw, containing data sent to the agent phone
- <name>.from.raw, containing data sent from the agent phone

You need use only one of the file pair when running the utility. The utility finds the other file and combines the two files into one WAV file named <name>.wav.

The naming convention used for <name> is as follows:

<YYYYMMDD>_<HHMMSS>_<counter>_<extension>_<agent ID>

where:

<YYYYMMDD>	Date the file was recorded
<HHMMSS>	Time the file was recorded
<counter>	Counter that is reset every time the agent logs in. It is incremented sequentially starting from 00000 every time a recording of that agent is made during that session.
<extension>	The extension of the agent recorded
<agent ID>	The ID of the agent recorded

The utility looks in the registry to find the location of the RAW files. If this information is not in the registry, the utility assumes that the location is the folder C:\Program Files\Cisco\Desktop_Audio. The utility writes the converted WAV files to a folder it creates located at C:\Program Files\Cisco\Desktop_wav.

The utility syntax is:

```
Raw2Wav.exe <filename> [path]
```

where:

- <filename> is either the <name>.to.raw or <name>.from.raw file.
- <path> is optional. The location of the unconverted audio (*.RAW) files, if other than the default location.

Running Unified CCX raw2wav in a Batch File

You can use the Unified CCX raw2wav utility from a batch file that iterates through a wildcard-specified set of source files.

If the utility finds a WAV file with a name identical to one that is about to be created, the conversion is not executed.

> **NOTE:** If the utility is halted prematurely, the WAV file being written at that time might be corrupted.

A batch file is a text file with a BAT extension. You can put DOS commands into this file and then run the file as if it were an executable.

For example, the following series of DOS commands can be put into a batch file called convert.bat:

```
c:\
cd c:\program files\cisco\desktop\bin
for %%c in (..\..\desktop_audio\*.raw) do Unified CCX raw2wav
"%%~nc%%~xc"
```

These DOS commands cause all the RAW files in the folder C:\Program Files\Cisco\Desktop_audio to be converted to WAV format and placed in the folder C:\Program files\Cisco\Desktop_wav, leaving the original RAW files in the Desktop_audio folder.

Additional lines can be added to the batch file to copy the files to another folder or file server.

> **NOTE:** The utility has a feature that prevents it from reconverting files that are already present in the Desktop_wav directory, so the batch

file does not have to explicitly check to see if the files have already been converted.

If you want the batch file to run automatically on specific days at a specific time, the Windows "at" command can be used.

For example, if you want convert.bat to run automatically every 13th and 23rd day of the month at 1:46 pm, do the following:

1. Put convert.bat in the C:\Program Files\Cisco\Desktop\bin folder.

2. Open a command window and enter the following DOS command:

```
at 1:46p /every:13,23 cmd /c "c:\program
files\cisco\desktop\bin\convert.bat" ^> c:\splkconvert.txt
```

Removal

4

Removing CAD 8.0 Desktops

To remove a CAD 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 want to remove and click Add/Remove. The application is removed.

Rolling Back Client-Side Service Releases

The update that can be applied to the Unified CCX server and the CAD clients is the engineering special (ES). When an ES is applied to the Unified CCX server, the CAD clients are updated only if there is a higher software release for CAD.

The following chart illustrates a hypothetical series of service releases (SRs) and ESs applied to a configuration.

Unified CCX Server	CAD Clients	Description
Main Release	Main Release	
ES1		First Cisco ES
ES2	SR1	First CAD SR
ES3	SR1	No changes made to SR1 for CAD
ES4	SR2	Second CAD SR
ES5	SR2	No changes made to SR2 for CAD
ES6	SR2	No changes made to SR2 for CAD
ES7	SR3	Third CAD SR

If any ES is removed from the Unified CCX server, that server reverts to the main release level. (ESs are cumulative, so when ES2 is removed, so is ES1.) Similarly, the CAD clients cannot roll back from SR2 (the equivalent to ES4 on the server) to SR1. Instead, SR2 must be removed from the CAD clients so that they revert to the main release, and then SR1 applied again.

> NOTE: If the client desktop is not rolled back to the server SR level, the user sees an error message that the client and server are running incompatible versions and will not start.

The client-side SR1 can be applied via True Update the next time the client application is started, or installed individually on each client desktop.

To roll back a CAD client-side SR:

1. Roll back the SR on the Unified CCX server to the desired SR or ES. See your Unified CCX documentation for this procedure.

> NOTE: It is recommended that SRs are rolled back on the Unified CCX server first in order to avoid True Update issues.

2. On the client computers, use the Windows Add or Remove Programs Control Panel to remove the client-side SR. The SR is removed and the client applications are rolled back to the main release version. The next time the client application is started, True Update detects that an SR is present on the Unified CCX server and automatically updates the client application to the current SR.