Cisco CAD Installation Guide

CAD 10.5 for Cisco Unified Contact Center Express Release 10.5

First Published: June 18, 2014
Last Modified: October 20, 2014

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco CAD Installation Guide

Introduction

1

Overview

This manual guides you through the process of installing the CAD desktop client applications: Cisco Agent Desktop, 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 client applications into a properly-configured Unified CCX environment and licensed the applications, the basic functionality of Cisco Agent Desktop, 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 Supervisor Desktop User Guide*
- *Cisco IP Phone Agent User Guide*
- *Cisco Desktop Administrator User Guide*
- *Cisco CAD Troubleshooting Guide*
- *Configuring and Troubleshooting VoIP Monitoring*
- *Integrating CAD with a Thin Client Environment*
- *Cisco CAD Error Code Dictionary*

These documents can be found online at the following location:

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Documentation Feedback

You can provide comments about this document by sending e-mail to the following address:

ccbu_docfeedback@cisco.com

We appreciate your comments.

What’s New In This Release

CAD 10.5 includes the following new features:

Release 10.5(1)

- Support for Cisco Unified Contact Center 10.5(1)
- Support for Cisco Unified Presence Server 10.5(1)
- Support for Java Runtime Environment (JRE) 1.7 Update 51
- Support for Cisco Jabber 9.7(2) with Video
- Support for Windows 8.1 (64-bit), running in 32-bit mode
- Support for Microsoft Internet Explorer 11
- Support for Cisco AnyConnect VPN 3.1.05160
- Support for Cisco Agent Desktop–Browser Edition (CAD-BE) has been discontinued

CAD 10.5 Elements

CAD 10.5 includes the following client applications and services.

Desktop Client Applications

Desktop Administrator

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.

Agent Desktop

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 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.

IP Phone Agent

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.

Supervisor Desktop

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

Services

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

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.

Agent 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 and triggers supervisor work flows.

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 CM and supported Cisco IP phones. It is also used to hold the configuration information administered via Desktop Administrator.

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. It also makes automatic nightly backups of LDAP database and checks the backup to ensure it is valid before archiving it.

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 and Playback Service

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

Recording and Statistics Service

The Recording and Statistics service maintains a 1-day history of agent and team statistics, such as average time an agent is in a particular ACD 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 protocol 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.

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
Agent Desktop (not available in Standard bundle)			
Agent-initiated chat		×	×
Automated recording (work flow action)		×	×
E-mail 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		×	×
IP Phone Agent			
Agent states	×	×	×
Agent-initiated recording		×	×
Caller data	×	×	×
CSQ statistics	×	×	×
Reason codes	×	×	×
Wrap-up data		×	×
Supervisor Desktop			
CSQ statistics	×	×	×
Barge-in		×	×
Intercept		×	×
Record and playback agent calls		×	×
Real time displays	×	×	×

Table 1. CAD Feature Levels

	Standard	Enhanced	Premium
Silent monitoring		×	×
Supervisor work flow (tree control)		×	×
Supervisor work flow (all)			×
Team messages		×	×
Unified Presence integration	×	×	×
Desktop Administrator			
Configure Agent E-Mail			×
Configure enterprise data	×	×	×
Configure silent monitoring		×	×
Configure Unified Presence	×	×	×
Desktop Work Flow Administrator			
Configure work flow groups	×	×	×
Configure agent interface		×	×
Configure integrated browser			×
Unified CCX Outbound Dialer			×
Configure work flows		×	×

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	Supervisor Desktop	IP Phone Agent	Desktop Administrator/Desktop Work Flow Administrator
Chinese (Simplified)[1]	×	×	×[2]	
Chinese (Traditional)[1]	×	×	×[2]	
Danish	×	×	×	
Dutch	×	×	×	
English (US)	×	×	×	×
Finnish[1]	×	×	×	
French	×	×	×	
French (Canadian)	×	×	×	
German	×	×	×	
Italian	×	×	×	
Japanese (Kanji)[1]	×	×	×[2]	
Japanese (Katakana)[1]	×	×	×[3]	
Korean[1]	×	×	×[2]	
Norwegian[4]	×	×	×	
Polish[1]	×	×	×[2]	
Portuguese (Brazilian)	×	×	×	
Russian	×	×	×[2]	
Spanish	×	×	×	
Swedish[1]	×	×	×	
Turkish[1]	×	×	×[2]	

[1] The spell check feature in Agent E-Mail is not supported.

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

[3] 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.

[4] User Interface only.

Configuring the CAD Environment

2

System Configurations

Supported system configurations are documented in the *Cisco Unified Contact Center Express 10.5 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 10.5 is integrated into the Unified Contact Center 10.5 environment.

Consult the following documents for the most current compatibility information:

- *Cisco Unified CM and Cisco IOS Software Version Compatibility Matrix* at:

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html

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

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

Operating Environment

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* at:

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

Minimum Hardware and OS Requirements for Desktops

CAD 10.5 runs on the following minimum hardware and operating systems.

Table 3. Desktop application minimum operating systems and hardware

Operating System	Hardware
Windows 7 Enterprise, Professional, and Ultimate Edition, Service Pack 1, 32-bit and 64-bit	*All desktops*: 500 MHz processor 1 GB RAM (32-bit) 2 GB RAM (64-bit) 100 Mbit NIC supporting Ethernet 2 *Agent, Supervisor, and Admin Desktops:* 650 MB free space

Table 3. Desktop application minimum operating systems and hardware — *Continued*

Operating System	Hardware
Windows 8.1 64 bit	*All desktops*: 1 GHz processor with support for PAE, NX, and SSE2 2 GB RAM 100 Mbit NIC supporting Ethernet 2 Microsoft DirectX 9 graphics card with WDDM driver *Agent, Supervisor, and Admin Desktops:* 1 GB free space
Microsoft Exchange 2007 Microsoft Exchange 2010 Microsoft Exchange 2013[1]	*Agent E-Mail*: Exchange 2007: 4 GB RAM Exchange 2010: 8 GB RAM Exchange 2013: 12 GB RAM 100 Mbit NIC supporting Ethernet 2
Microsoft Terminal Server	For minimum hardware requirements, see *Integrating CAD with Thin Client and Virtual Desktop Environments*
Citrix XenApp	

[1] For more information on Exchange OS, CPU, hard disk, and NIC minimum requirements, consult your Exchange documentation or refer to the Exchange Server TechCenter website (http://technet.microsoft.com/en-us/exchange/).

Operating Environment Language Requirements

Agent Desktop 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 107 for more information.

A CAD deployment 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 center's 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 and Supervisor Desktop).

Cisco AnyConnect Secure Mobility Client is verified to work properly and are supported for access with the CAD clients.

NOTE: After installing Cisco AnyConnect Secure Mobility Client, you must restart your computer. If you do not restart, monitoring and recording will not work.

VPN solutions from other vendors might result in feature loss. Because they have not been formally verified, they are not supported.

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. Recording and monitoring do not work with IP Phone Agent when used with NAT.

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

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

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

Third Party Software Environment

CAD 10.5 requires the following software applications to run successfully.

Microsoft Exchange

Microsoft Exchange is required for the operation of Agent E-Mail. CAD supports the following versions of Exchange:

- Exchange 2007

- Exchange 2010
- Exchange 2013

Microsoft Internet Explorer

Microsoft Internet Explorer must be installed on agent and supervisor PCs to support the integrated browser component of Agent Desktop and Supervisor Desktop. The Agent Desktop and Supervisor Desktop integrated browser is implemented using the Microsoft WebBrowser control (Shdocvw.dll) that is distributed by Internet Explorer. This library provides a window in which the user can navigate to websites and files using hyperlinks and URLs. However, it does not represent the full implementation of Internet Explorer. Consequently, differences exist between the behavior of the Agent Desktop and Supervisor Desktop integrated browser and Internet Explorer. Web pages might render correctly in Microsoft Internet Explorer but not render correctly, or not render at all, in the Agent Desktop and Supervisor Desktop integrated browser.

Differences between the Agent Desktop and Supervisor Desktop integrated browser and Internet Explorer include the following:

- If a third-party web application attempts to launch a new browser window, the Agent Desktop and Supervisor Desktop integrated browser will open a new tab instead.
- If a page that contains a JavaScript error is opened from the Agent Desktop and Supervisor Desktop integrated browser and script error notification is disabled in Internet Explorer (the default), the Agent Desktop and Supervisor Desktop integrated browser does not display any information about the error. To see detailed information about the error, you must open the page from Internet Explorer with script debugging enabled.
- The Agent Desktop and Supervisor Desktop integrated browser does not support the more advanced features of Internet Explorer, including the popup blocker and the phishing filters.
- Compatibility Mode should be enabled for the Unified CCX server site in Internet Explorer to prevent potential issues with Agent E-Mail.

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: The integrated browser uses Internet Explorer 9 Compatibility Mode if the agent desktop has a newer version of Internet Explorer installed.

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

NOTE: For information on supported versions of Internet Explorer, 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 1.7 Update 51 is required to run the Java applets used by IP Phone Agent, Agent Desktop, and Supervisor Desktop. Agent Desktop and Supervisor Desktop use the applet in conjunction with Agent E-Mail.

Monitoring and Recording Requirements

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

The space requirements for the Recording and Playback 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.

> **NOTE:** CAD cannot handle duplicate packets.

Agent Data Store Database

The Agent Data Store database reserves 2.4 GB to store agent state and call activity records. In a High Availability environment, the 2.4 GB is split between the primary and secondary servers so that each reserves 1.2 GB of space.

Recording Service

The Unified CCX platform reserves 2.6 GB of hard drive space per server for recordings.

Space required for recordings can be calculated based on the following:

- ~800 KB for each minute of a recorded G.711 voice call
- ~200 KB for each minute of a recorded G.729 voice call

Setting Up Agents in Unified CCX

For CAD 10.5 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 Agent Desktop and Supervisor Desktop can have a maximum length of 31 alphanumeric characters. Chinese, Japanese, Korean, Russian have a maximum length of 15 characters. Unified CCX allows IDs that are longer. Make sure that any IDs you configure in Unified CCX do not exceed the character limit in order for agents and supervisors to log in successfully.

System Capacity

Table 4 displays select system capacities supported by CAD 10.5. Additional sizing considerations appear in the *Cisco Unified Contact Center Express 10.5 Data Sheet* available at:

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

Table 4. Unified system capacity

Description	Capacity
Maximum number of agents per system	400
Maximum number of agents per team	100
Maximum number of skills/CSQs per agent (for real-time reporting)	50
Maximum number of supervisors per system	40
Maximum number of simultaneous recordings/playbacks	32 Enhanced 80 Premium
Maximum number of agents per monitor domain	300
Maximum number of Agent E-Mail agents (Exchange 2007, 2010)	120
Maximum number of Agent E-Mail agents (Exchange 2013)	30
Maximum number of simultaneous monitoring sessions	40
Maximum number of Agent E-Mail CSQs (Exchange 2013)	30

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* at:

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

> **NOTE:** The Unified CCX does not support Internet Protocol version 6 (IPv6) agent phones and requires agents to use IPv4 phones only.

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.

Configuring Agent E-Mail

3

Introduction

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

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

Application	Configure
Microsoft (MS) 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 42 for procedures.
Cisco Unified CCX Application Administration	• Set up CSQs • Set up skills See the *Cisco Unified Contact Center Express Administration Guide, Release 10.5(1)* for procedures.
Desktop Administrator	• Set up Exchange server information • Map CSQs to e-mail addresses See the *Cisco Desktop Administrator User Guide* for procedures.

Security and Certificate Warnings

While logging in to Agent Desktop with Agent E-mail enabled, an agent might receive multiple security and certificate warnings. The Information bar displays warning messages such as the hostname does not match the certificate, the content is blocked due to certificate errors, or the publisher is not trusted. These warnings appear while Agent E-Mail is loaded in the integrated browser. In order for Agent E-Mail to function normally, all certificate errors must be ignored, required certificates must be installed, publishers must be trusted, hostnames must match, and content must be unblocked.

The agent can click the security warning displayed on the Information bar in the browser, and select an appropriate action depending on the available options in the popup menu to unblock the content or trust the publisher. You can configure Internet Explorer settings to trust the certificate publisher to suppress these warnings.

> **NOTE:** You must run Internet Explorer as an administrator for the following procedure.

To trust a certificate publisher:

1. Open Internet Explorer.
2. From the menu bar, choose Tools > Internet Options. The Internet Options dialog box appears.
3. Select the Content tab, and then click Publishers. The Certificates dialog box appears.
4. Select the Untrusted Publishers tab.
5. Select the publisher you want to trust, click Remove, and then click Yes to confirm that you want to trust that publisher.
6. Click Close to save the changes in the Certificates dialog box.
7. Click OK to save the changes in the Internet Options dialog box.

Supported Unicode Encoding

Client systems using Agent E-Mail must be configured for UTF-8–compatible input only. Client systems using input that is not UTF-8–compatible is unsupported and unexpected results might occur.

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. It is enabled by default when used by the CAD Integrated Browser. See the *Cisco CAD Troubleshooting Guide* for more information on Compatibility Mode and how it interacts with CAD.

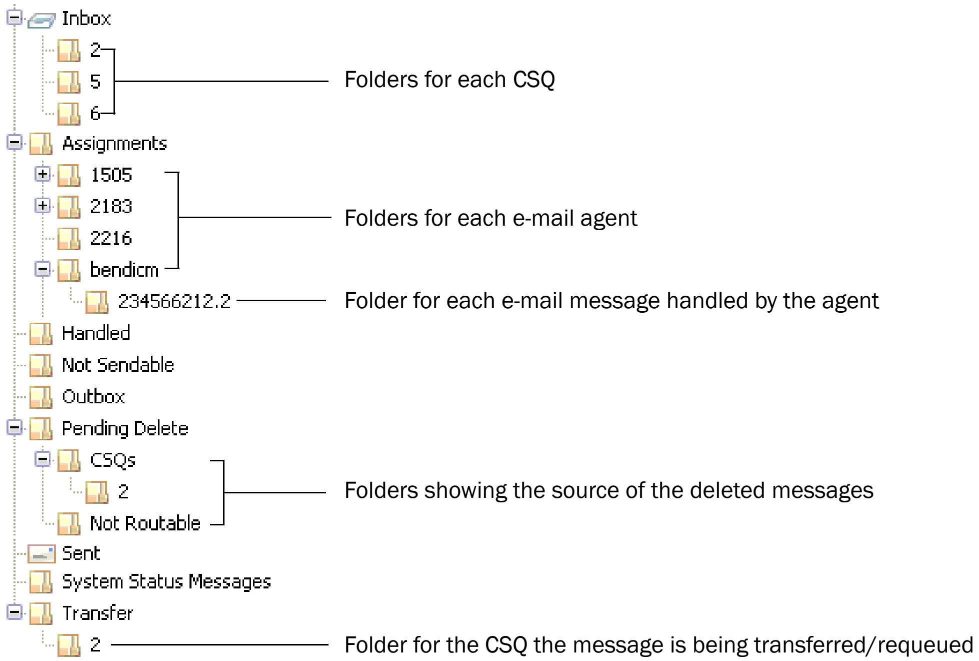
Agent E-Mail Microsoft Exchange Mailbox Folder Management

E-mails received from and sent to customers are stored in the Exchange Server's mail store.

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 the Inbox folder associated with the Agent E-Mail user for incoming e-mails and automatically creates additional folders in Exchange as needed at runtime.

A typical Exchange folder layout is illustrated in Figure 1.

Figure 1. Typical Agent E-Mail Exchange mailbox folder layout


Inbox
2
5
6
Folders for each CSQ
Assignments
1505
2183
2216
bendicm
Folders for each e-mail agent
234566212.2
Folder for each e-mail message handled by the agent
Handled
Not Sendable
Outbox
Pending Delete
CSQs
2
Not Routable
Folders showing the source of the deleted messages
Sent
System Status Messages
Transfer
2
Folder for the CSQ the message is being transferred/requeued

E-mail flow is illustrated in the flowchart in Figure 2 and Figure 3.

Figure 2. Customer e-mail flowchart (incoming e-mail)

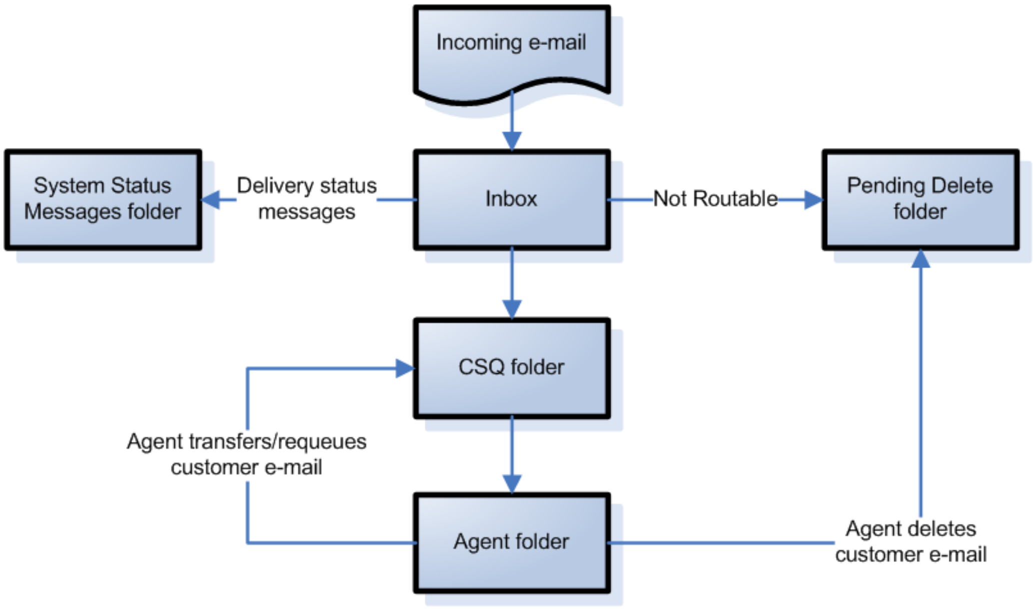
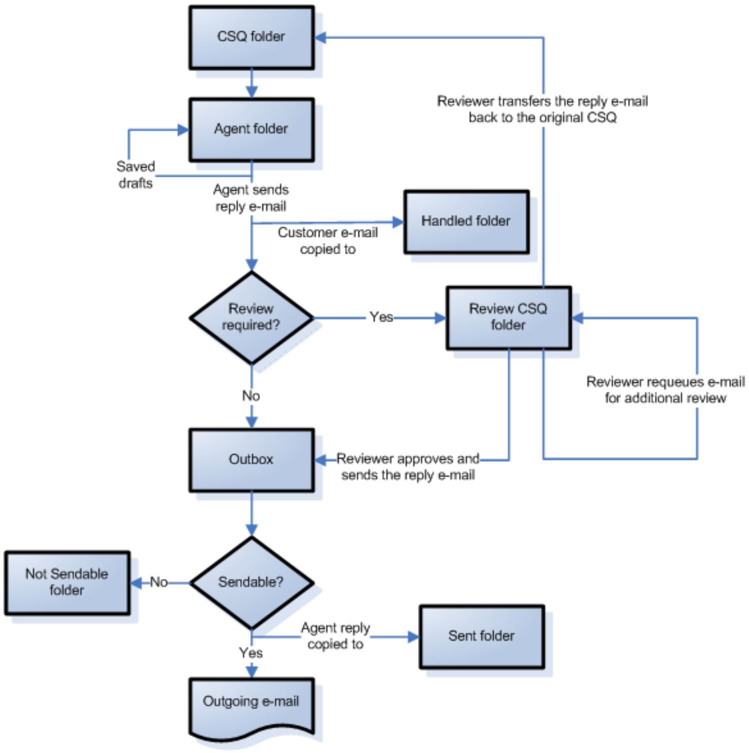


Figure 3. Agent reply e-mail flowchart (outgoing e-mail)



Agent E-Mail Microsoft Exchange Mailbox Folders

The following folders, with the exception of the Inbox folder, are created by the Agent E-Mail service in Exchange 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 e-mails and moves them to the appropriate subfolder based on the routing rules (configured in Desktop Administrator). 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.

E-mails in Agent E-Mail should never be manually manipulated with a third party IMAP client. Doing so could cause inaccuracies in the related Recording & Statistics service Agent E-Mail reports. A possible exception to this is if the Agent E-Mail service is unable to process an e-mail in the Inbox folder and an error occurs. If this happens, you can use any IMAP client to move the e-mail 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 ID>

This e-mail subfolder contains the customer e-mail and any saved draft response to that e-mail. They are periodically cleaned up after an agent finishes processing the e-mail related to them.

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-mail and agent drafts are moved to this folder.

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

> **NOTE:** Exchange performance can suffer if a large number of messages (more than 10,000) accumulate in this folder. If your contact center handles large volumes of e-mail, be sure to set the cleanup interval short enough to avoid this issue.

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 address set up in Desktop Administrator. (Refer to “Agent E-Mail Problems” in *Cisco CAD Troubleshooting Guide* for information on how to configure Send As permissions.) Once this issue is resolved, you can use a third party IMAP client to move the unsent e-mails back into the Outbox folder for processing.

Outbox Folder

The Outbox folder contains reply e-mails waiting to be sent to customers. Agent Desktop moves e-mails 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 e-mail it finds using SMTP. If the e-mail is not sendable for some reason, it is moved to the Not Sendable folder.

Pending Error Folder

The Pending Error folder is a subfolder of the Outbox folder and is used for holding e-mails which encountered errors during sending due to SMTP timeout. Such errors are usually due to transient network issues (such as congestion) and as a result, sending the same e-mail later may be successful.

Specifically, if the Exchange server cannot send an e-mail and responds to the Agent E-Mail service with “421 4.4.1 Connection timed out”, the Agent E-Mail service will attempt to re-send. If the same error is received three times, Agent E-Mail service will move the e-mail to the Pending Error folder. The Agent E-Mail Service will scan the Pending Error folder once an hour and attempt to re-send all contained e-mails. If e-mails still cannot be sent, they will remain in the Pending Error folder for up to 24 hours before finally being 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 e-mail was determined to be non-routable when it arrived in the Inbox. E-mails deleted by agents are in CSQ subfolders, and those deleted by the Agent E-Mail service (due to routing failures) are in the Not Routable folder.

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

Not Routable Folder

Inbound e-mails are sent to the Not Routable folder when the receiving e-mail address does not have a CSQ folder assigned to it.

In the case of e-mails 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 Desktop

Administrator when they arrived. After configuring the e-mail address, you can use a third-party IMAP client to move the e-mails from the Not Routable folder back into the Inbox so that they can be processed.

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, but e-mails will be copied to the Sent folder before sendability is determined.

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

> **NOTE:** Exchange performance can suffer if a large number of messages (more than 10,000) accumulate in this folder. If your contact center handles large volumes of e-mail, be sure to set the cleanup interval short enough to avoid this issue.

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 Desktop Administrator.

Transfer Folder

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

Agent E-mail Routing Expectations

Agent E-Mail manages the distribution of e-mails to agents based first on the time an agent entered queue, and then on the time an e-mail entered queue. The agent in queue the longest is distributed the oldest e-mail from that agent's assigned queues, using a first-in-first-out (FIFO) distribution method.

The agent in the queue the longest is routed the oldest e-mail found in all of the agent's assigned queues. In the event no e-mail is found, the agent is moved to the end of the queue. The agent is not eligible to receive an e-mail again until the agent reaches the front of the queue.

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.

E-mail routing is not instantaneous. The Unified CCX e-mail routing service interacts with MS Exchange to move e-mails to the appropriate folders, and as a result, some delays are to be expected. Table 5 identifies the routing steps and potential delays that can be experienced.

> **NOTE:** The delay times shown in Table 5 are calculated under the assumption that an IMAP operation takes about 1/16 second to complete. Results for different systems might vary.

The success maximum delay is based on the assumption that the system is running on a 7845 server at full capacity and without any severe Exchange/Unified CCX communication failures.

Table 5. E-mail routing process and possible delays

	Success		**Failure/Multiple Attempts**[1]	
Step	**Minimum Delay**	**Maximum Delay**	**Minimum Delay**	**Maximum Delay**
1. Assign e-mail from Exchange inbox to CSQ folder				
	1 second	10 seconds	5 seconds	15 seconds
2. Scan CSQ folders for new e-mails.				
	1 second (no rescan all messages)	26 seconds (rescan all messages)	1 second (no rescan all messages)	26 seconds (rescan all messages)
3. Scan waiting agents, determine if messages are available				
	1 second (no waiting agents ahead in queue)	18 seconds (119 waiting agents ahead in queue)	1 second (no waiting agents ahead in queue)	18 seconds (119 waiting agents ahead in queue)
4. Create Agent Assignment folder in Exchange and move messages to that folder				

Table 5. E-mail routing process and possible delays

Step	Success		Failure/Multiple Attempts[1]	
	Minimum Delay	Maximum Delay	Minimum Delay	Maximum Delay
	1 second (go to Step 5)	12 seconds (go to Step 5)	1 second (assignment succeeds: go to Step 5)	12 seconds (multiple attempts succeed: go to Step 5) 144 seconds (multiple attempts fail: go to Step 4a)
4a. Abort assignment attempt, delete Agent Assignment folder, and requeue agent				
	not observed	not observed	1 second (go back to Step 2)	144 seconds (go back to Step 2)
5. Agent E-Mail service notifies agent of e-mail assignment				
	1 second	1 second	1 second	144 seconds (multiple attempts succeed: go to Step 6) 144 seconds (multiple attempts fail: go to Step 5a)
5a. Move e-mail back to CSQ, delete Agent Assignment folder, and requeue agent				
	not observed	not observed	1 second (go back to Step 2)	144 seconds (go back to Step 2)
6. Agent initiates e-mail download from Agent Assignment folder				
	1 second	depends on e-mail size and bandwidth	1 second	depends on e-mail size and bandwidth
TOTALS				
	6 seconds	85 seconds		

[1] "Failure/Multiple Attempts" means that Exchange and the Agent E-Mail service experience a communication failure that results in a programmatic recovery side step.

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 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

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

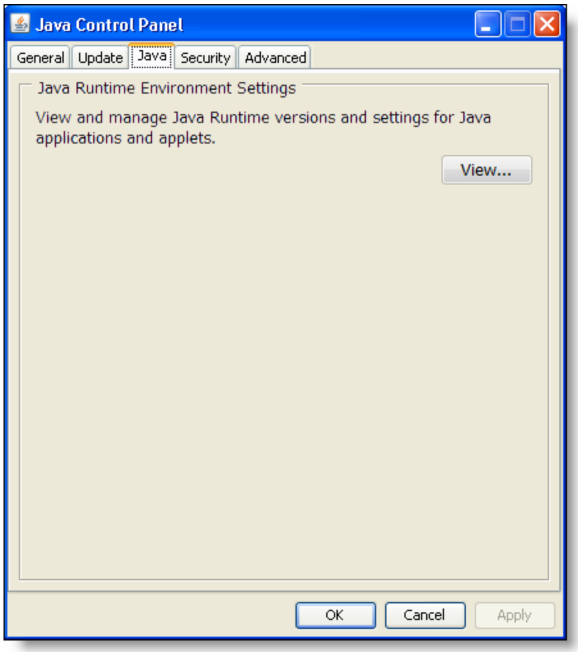
It is possible that some e-mails will be too large to be readily displayed in Agent Desktop. In general, e-mails over 1 MB in size can take a long time to download and display or might not display at all. The reason for this is that the default maximum heap size for the Java applet used for Agent E-Mail 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 4).

Figure 4. Java Control Panel



Java Runtime Environment Settings

View and manage Java Runtime versions and settings for Java applications and applets.

5. Click View. The Java Runtime Environment Settings dialog box appears.
6. On the System tab, on the row for the most recent JRE version supported by CAD (JRE 1.7.0_51), 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 Exchange so that it supports Agent E-Mail.

CAD supports the following versions of Exchange:

- Exchange 2007
- Exchange 2010
- Exchange 2013 (supports up to 30 users only)

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 Desktop Administrator (see the *Cisco Desktop Administrator User Guide* for more information).

> **NOTE:** It is recommended that you apply the latest updates and patches released by Microsoft to Exchange. However, doing so might result in the need to reconfigure the settings described in the following sections.

CAD uses the following protocols:

- IMAP4 for retrieving messages. IMAP4 is used to communicate to the Exchange server from the Unified CCX servers and all e-mail agent desktops.
- SMTP for sending messages. SMTP is used to communicate with the Exchange server from the Unified CCX servers only. SMTP is not used from agent desktops for Agent E-mail.

These protocols must be enabled in Exchange. Note that the IMAP4 protocol is 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.

Configuration requirements differ depending of which version of Exchange you support. Refer to the following sections for more detailed configuration procedures:

- "Configuring Exchange 2007" on page 43
- "Configuring Exchange 2010" on page 62
- "Configuring Exchange 2013" on page 77

NOTE: Exchange 2003 is not supported with CAD 10.5. You can migrate Exchange 2003 accounts to Exchange 2007 or newer. See "Creating a User" on page 50 for information on Exchange 2003 account migration.

General Process for Configuring Microsoft Exchange for Agent E-Mail

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

To configure Exchange:

1. Configure a single e-mail account for 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 using Desktop Administrator.
7. Configure the following global and mailbox settings in Exchange:
   - Message size restrictions
   - Exchange connection limits
   - Mailbox size limits
   - Message format settings
   - Message throttling policies

Configuring Exchange 2007

The following procedures are a guideline for configuring Exchange 2007.

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

Configuring Security Settings

Exchange enables you to set up virtual IMAP and SMTP servers. Agent E-Mail 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 Exchange administrator set up IMAP and SMTP virtual servers.

Configuring IMAP Security Settings

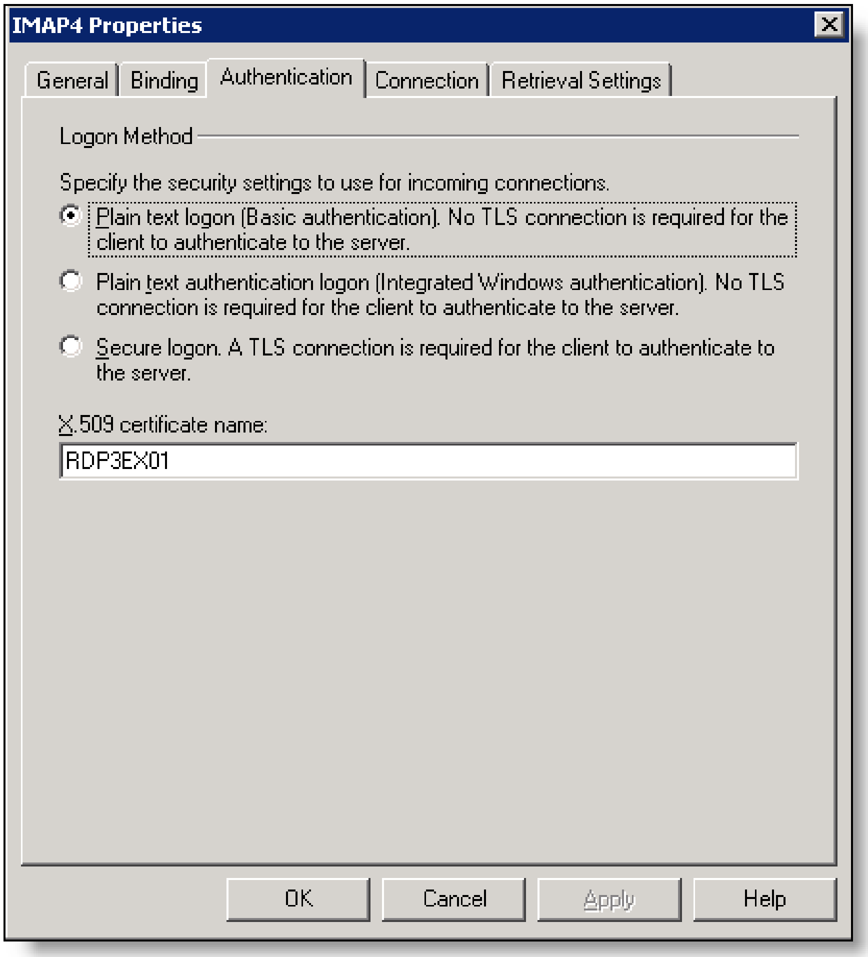
The following section contains information on how to configure IMAP4 security settings for use with Agent E-Mail.

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 select Properties from the popup menu. The Properties window appears (Figure 5).

Figure 5. IMAP4 Properties window



Logon Method

Specify the security settings to use for incoming connections.

● Plain text logon (Basic authentication). No TLS connection is required for the client to authenticate to the server.

○ Plain text authentication logon (Integrated Windows authentication). No TLS connection is required for the client to authenticate to the server.

○ Secure logon. A TLS connection is required for the client to authenticate to the server.

X.509 certificate name: RDP3EX01

5. Select the Authentication tab, and configure the tab as shown in Figure 5. You can select either of the following options:
   - Plain text logon (Basic or Integrated Windows authentication)
   - Secure logon

     If you choose Secure logon, you must configure a valid security certificate. See your MS Exchange 2007 documentation for further details.
6. Click Apply and then OK to save your changes and dismiss the window.
7. Restart the Microsoft Exchange IMAP4 service from Windows Services Control after you have made your changes.

Configuring SMTP Security Settings

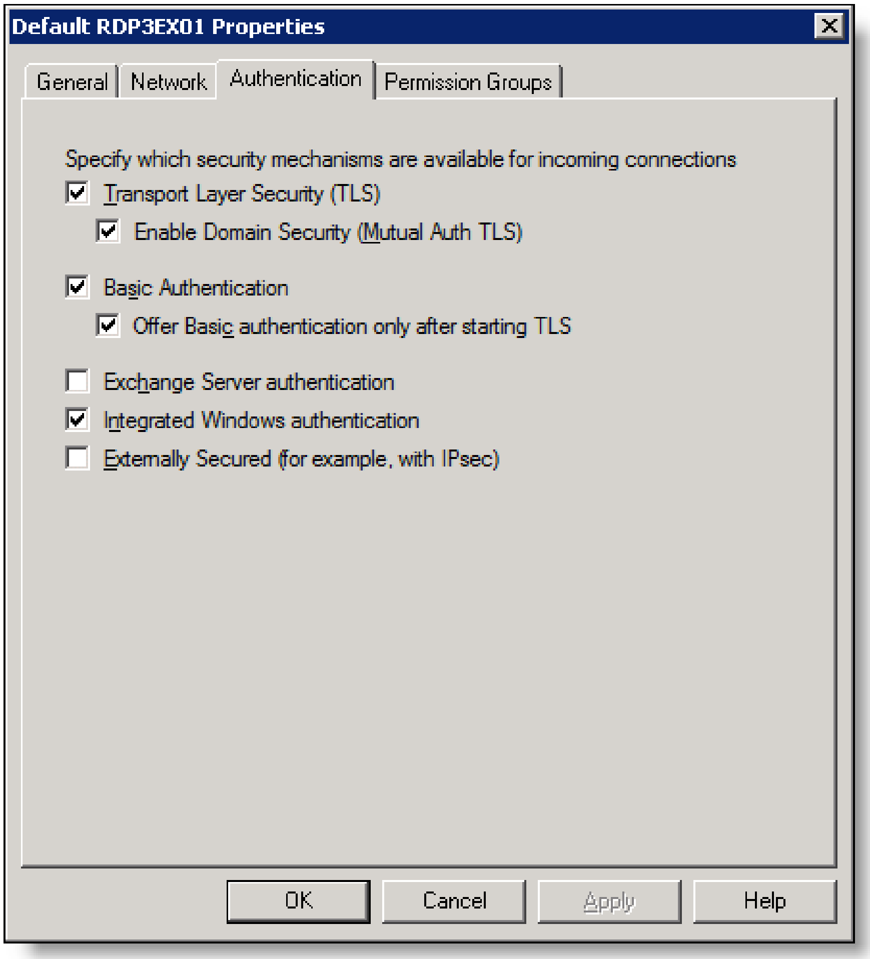
There are two types of connectors that can be used with Agent E-Mail: Authenticated and Open Relay.

Authenticated Connectors

To configure SMTP security settings using Authenticated connectors:

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 on the Receive Connectors tab, and choose Properties from the popup menu. The Properties window appears (Figure 6).

Figure 6. Properties window (Authentication tab)



Specify which security mechanisms are available for incoming connections

☑ Transport Layer Security (TLS)

☑ Enable Domain Security (Mutual Auth TLS)

☑ Basic Authentication

☑ Offer Basic authentication only after starting TLS

□ Exchange Server authentication

☑ Integrated Windows authentication

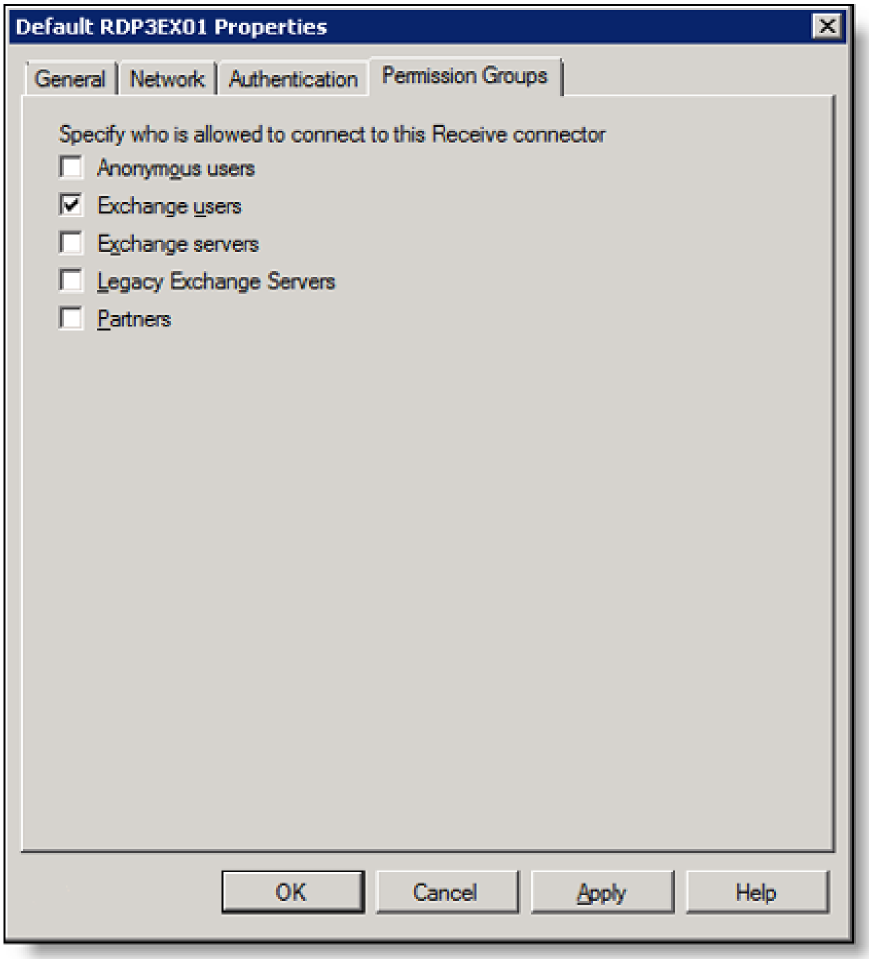
□ Externally Secured (for example, with IPsec)

4. Select the Authentication tab. You can select any combination of the check boxes selected in Figure 6. You must at least select either the Basic Authentication or the Integrated Windows authentication for Agent E-Mail to function properly.

   NOTE: Do not select Exchange Server authentication; it is not supported with Agent E-Mail. Do not select Externally Secured; it is not a valid option with Authenticated connectors.

5. Select the Permissions Groups tab (Figure 7). At a minimum, you must at least select Exchange users. You can also select additional groups, but Agent E-Mail requires the Exchange users permission group with an Authenticated connector.

Figure 7. Properties window (Permission Groups tab)



Specify who is allowed to connect to this Receive connector

☐ Anonymous users
☑ Exchange users
☐ Exchange servers
☐ Legacy Exchange Servers
☐ Partners

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

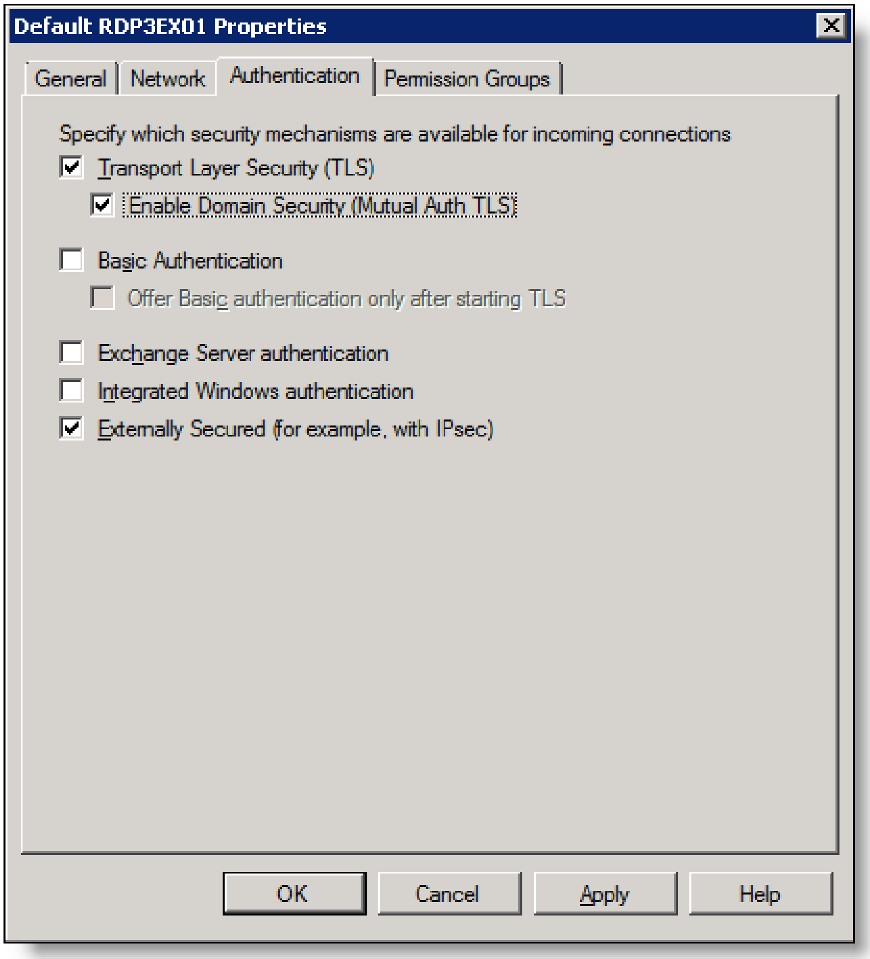
7. Restart the Microsoft Exchange Transport service from Windows Services Control after you have made your changes.

Open Relay Connectors

To configure SMTP security settings using Open Relay connectors:

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 on the Receive Connectors tab, and choose Properties from the popup menu. The Properties window appears (Figure 8).

Figure 8. Properties window (Authentication tab)



Default RDP3EX01 Properties

Specify which security mechanisms are available for incoming connections

☑ Transport Layer Security (TLS)

☑ Enable Domain Security (Mutual Auth TLS)

□ Basic Authentication

□ Offer Basic authentication only after starting TLS

□ Exchange Server authentication

□ Integrated Windows authentication

☑ Externally Secured (for example, with IPsec)

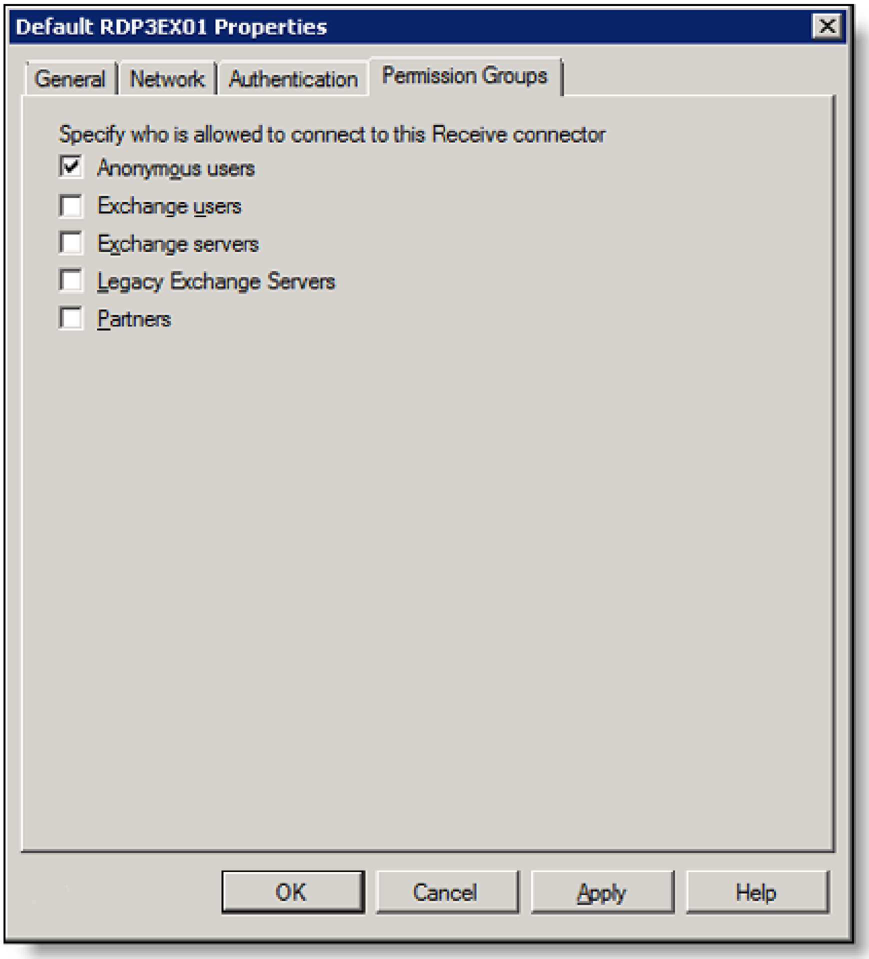
4. Select the Authentication tab. You can select any combination of the check boxes selected in Figure 8, or you can select nothing.

   NOTE: You cannot select both Enable Domain Security and Externally Secured. If you do, you will receive an error message.

5. Select the Permissions Groups tab (Figure 9). At a minimum, you must at least select Anonymous users. You can also select additional groups, but Agent E-Mail requires the Anonymous users permission group with an Open Relay connector.

   If you selected Externally Secured and Transport Layer Security (TLS) on the Authentication tab, you must also select Exchange servers.

Figure 9. Properties window (Permission Groups tab)



Default RDP3EX01 Properties

Specify who is allowed to connect to this Receive connector

☑ Anonymous users

□ Exchange users

□ Exchange servers

□ Legacy Exchange Servers

□ Partners

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

7. Restart the Exchange Transport service from the Windows Services Control after you have made your changes.

If you are using Open Relay connectors, there are additional configuration considerations:

- If you are not using the Externally Secured option, then special permissions must be granted to the connector in order to use it as an open relay. In Exchange Management Shell, execute the following command:

  ```
  Get-ReceiveConnector "<Receive Connector Name>" | Add-ADPermission -User
  "NT AUTHORITY\ANONYMOUS LOGON" -ExtendedRights
  "ms-Exch-SMTP-Accept-Any-Recipient"
  ```

  where <Receive Connector Name> is the name of the Open Relay connector being used with Agent E-Mail.

  For more information on properly configuring Open Relay with Exchange, refer to the following Exchange article:

  http://blogs.technet.com/b/exchange/archive/2006/12/28/3397620.aspx

- If you are using the Enable Domain Security (Mutual Auth TLS) option with Open Relay connectors, you must perform additional configuration. Refer to the following Exchange article:

  http://technet.microsoft.com/en-us/library/bb123543.aspx

Creating a User

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

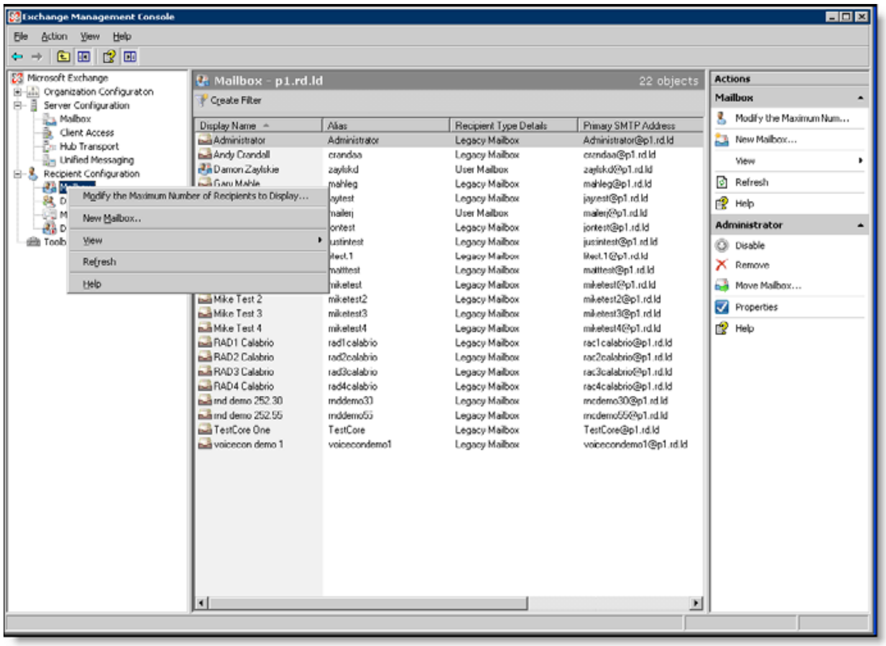
http://blogs.technet.com/b/exchange/archive/2006/09/05/3394830.aspx

To create a user:

1. Launch the Exchange Management Console.

2. In the left navigation tree pane, select the Recipient Configuration > Mailbox node (Figure 10).

Figure 10. Exchange Management Console



Display Name	Alias	Recipient Type Details	Primary SMTP Address
Administrator	Administrator	Legacy Mailbox	Administrator@p1.rd.ld
Andy Crandall	crandaa	Legacy Mailbox	crandaa@p1.rd.ld
Damon Zaylskie	zaylskd	User Mailbox	zaylskd@p1.rd.ld
Gary Mahle	mahleg	Legacy Mailbox	mahleg@p1.rd.ld
	jaytest	Legacy Mailbox	jaytest@p1.rd.ld
	mailerj	User Mailbox	mailerj@p1.rd.ld
	jontest	Legacy Mailbox	jontest@p1.rd.ld
	justintest	Legacy Mailbox	jusintest@p1.rd.ld
	ltest.1	Legacy Mailbox	ltest.1@p1.rd.ld
	matttest	Legacy Mailbox	matttest@p1.rd.ld
	miketest	Legacy Mailbox	miketest@p1.rd.ld
Mike Test 2	miketest2	Legacy Mailbox	miketest2@p1.rd.ld
Mike Test 3	miketest3	Legacy Mailbox	miketest3@p1.rd.ld
Mike Test 4	miketest4	Legacy Mailbox	miketest4@p1.rd.ld
RAD1 Calabrio	rad1calabrio	Legacy Mailbox	rac1calabrio@p1.rd.ld
RAD2 Calabrio	rad2calabrio	Legacy Mailbox	rac2calabrio@p1.rd.ld
RAD3 Calabrio	rad3calabrio	Legacy Mailbox	rac3calabrio@p1.rd.ld
RAD4 Calabrio	rad4calabrio	Legacy Mailbox	rac4calabrio@p1.rd.ld
rnd demo 252.30	rnddemo30	Legacy Mailbox	rncdemo30@p1.rd.ld
rnd demo 252.55	rnddemo55	Legacy Mailbox	rncdemo55@p1.rd.ld
TestCore One	TestCore	Legacy Mailbox	TestCore@p1.rd.ld
voicecon demo 1	voicecondemo1	Legacy Mailbox	voicecondemo1@p1.rd.ld

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

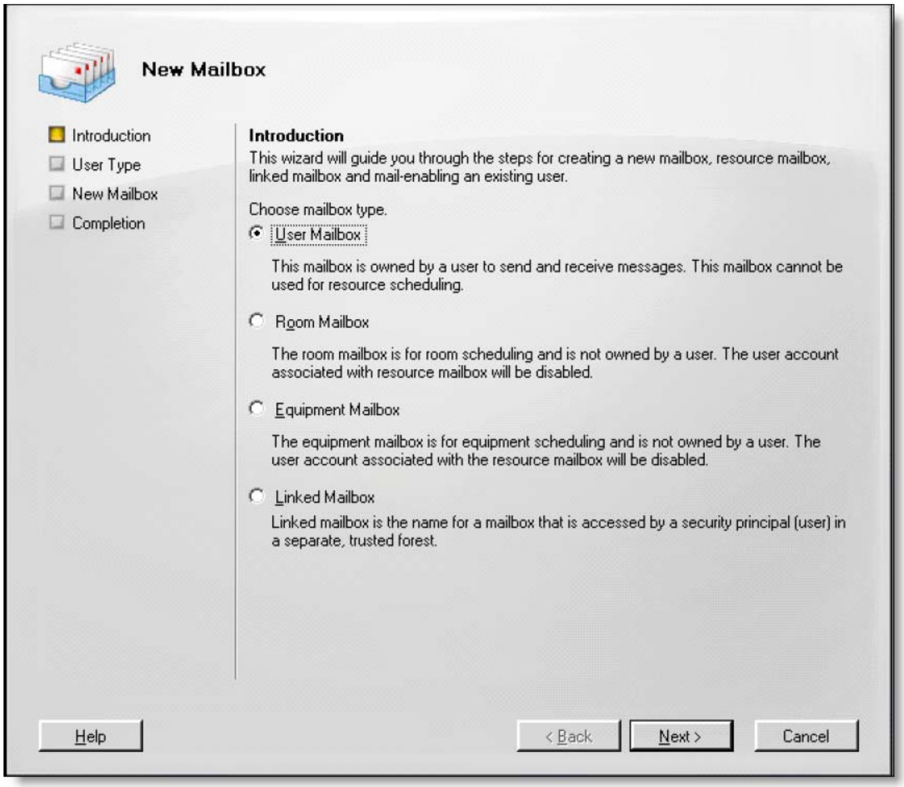
- User = Exchange 2007

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.

4. The New Mailbox wizard appears (Figure 11).

Figure 11. New Mailbox wizard window 1



New Mailbox

Introduction

This wizard will guide you through the steps for creating a new mailbox, resource mailbox, linked mailbox and mail-enabling an existing user.

Choose mailbox type.

● User Mailbox

This mailbox is owned by a user to send and receive messages. This mailbox cannot be used for resource scheduling.

○ Room Mailbox

The room mailbox is for room scheduling and is not owned by a user. The user account associated with resource mailbox will be disabled.

○ Equipment Mailbox

The equipment mailbox is for equipment scheduling and is not owned by a user. The user account associated with the resource mailbox will be disabled.

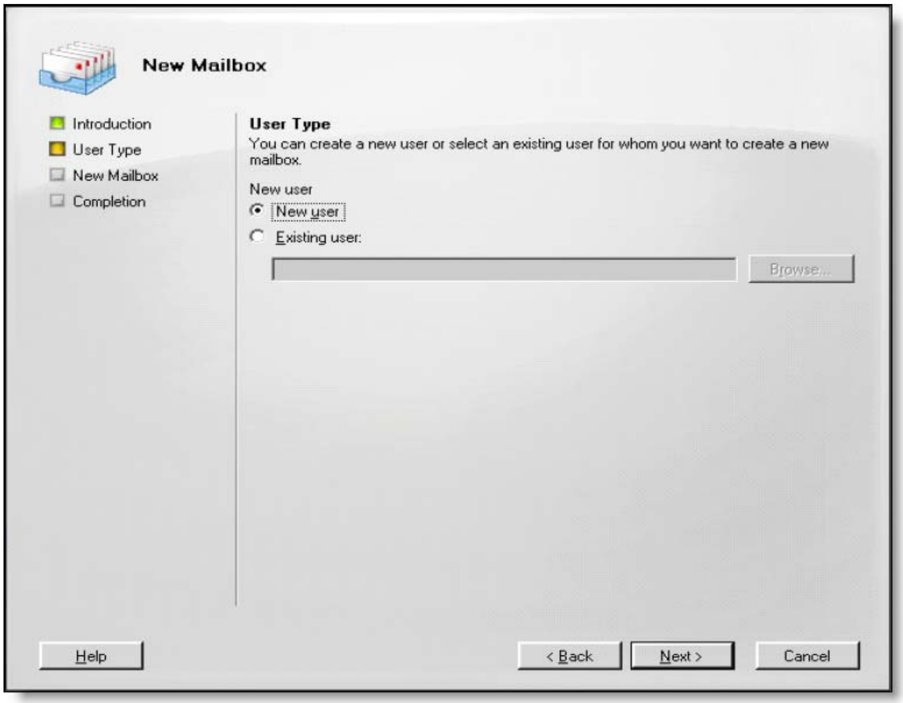
○ Linked Mailbox

Linked mailbox is the name for a mailbox that is accessed by a security principal (user) in a separate, trusted forest.

5. Select User Mailbox and click Next.

6. The User Type window of the wizard appears (Figure 12).

Figure 12. New Mailbox wizard window 2



User Type

You can create a new user or select an existing user for whom you want to create a new mailbox.

New user

● New user

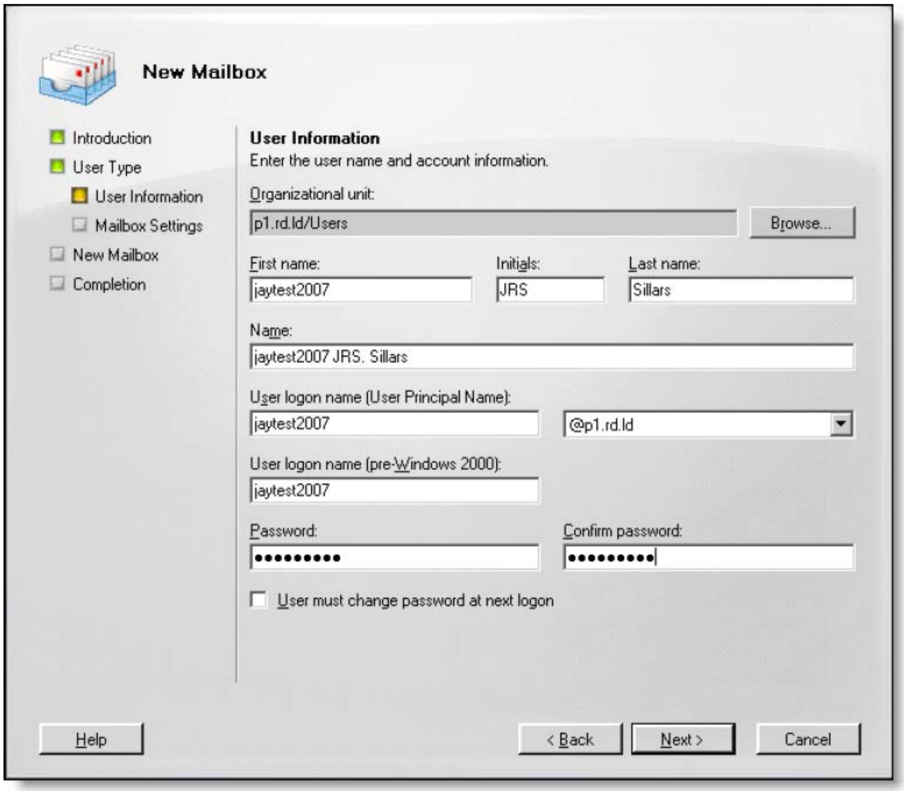
○ Existing user:

7. Select New User and click Next.

NOTE: Exchange 2003 is not supported with CAD 10.5. You can migrate MS Exchange 2003 accounts to Exchange 2007 or newer. If you want to migrate an account from Exchange 2003, select Existing User and then browse to the account name. Keep in mind that if you do this, the account will no longer be available in MS Exchange 2003.

8. The User Information window of the wizard appears (Figure 13).

Figure 13. New Mailbox wizard window 3



New Mailbox

User Information

Enter the user name and account information.

Organizational unit: p1.rd.ld/Users

First name: jaytest2007

Initials: JRS

Last name: Sillars

Name: jaytest2007 JRS. Sillars

User logon name (User Principal Name): jaytest2007 @p1.rd.ld

User logon name (pre-Windows 2000): jaytest2007

Password: ●●●●●●●●●●

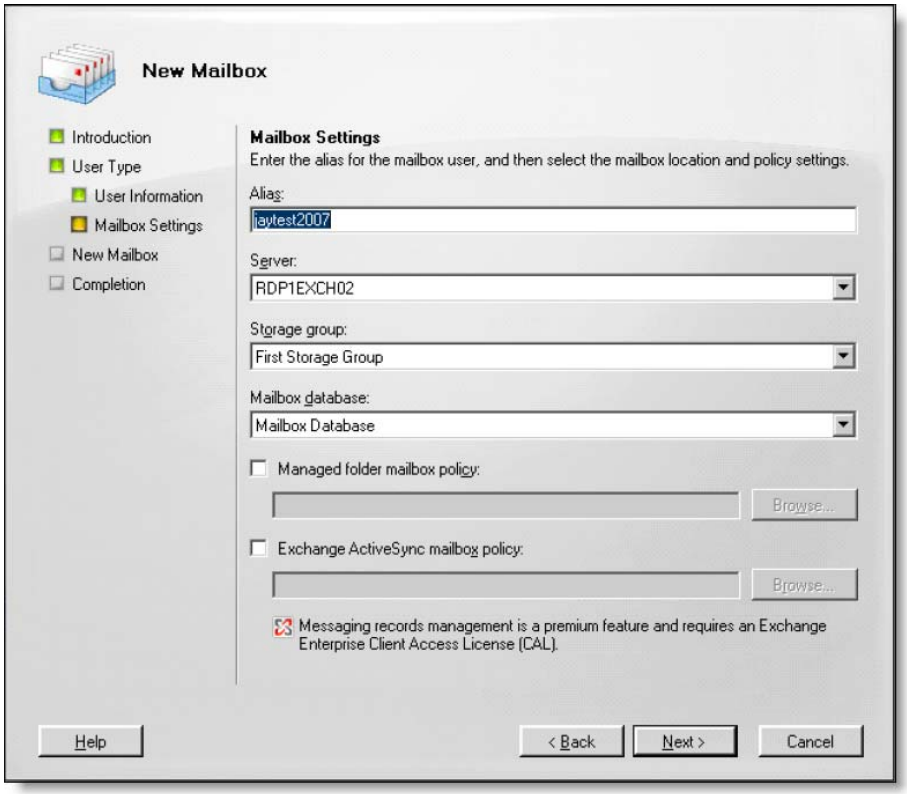
Confirm password: ●●●●●●●●●●

□ User must change password at next logon

9. Enter the user information for the new account and click Next.

10. The Mailbox Settings window of the wizard appears (Figure 14).

Figure 14. New Mailbox wizard window 4



Mailbox Settings

Enter the alias for the mailbox user, and then select the mailbox location and policy settings.

Alias: jaytest2007

Server: RDP1EXCH02

Storage group: First Storage Group

Mailbox database: Mailbox Database

☐ Managed folder mailbox policy:

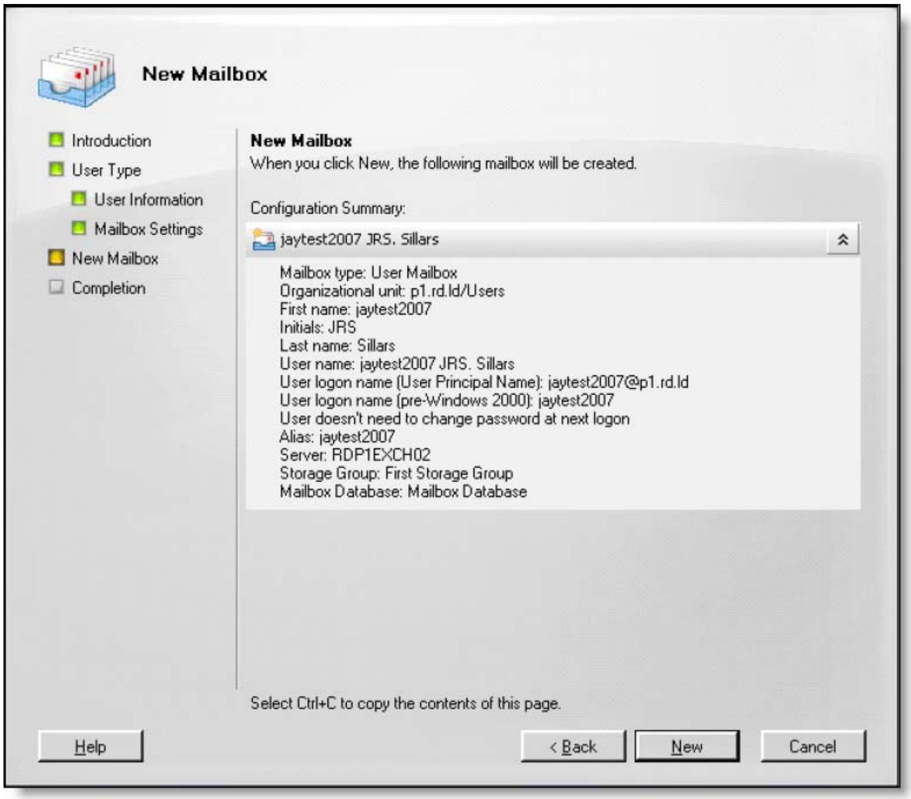
☐ Exchange ActiveSync mailbox policy:

Messaging records management is a premium feature and requires an Exchange Enterprise Client Access License (CAL).

11. Accept the defaults or configure the mailbox settings as desired, and then click Next.

12. A window containing the summary of the new mailbox settings appears (Figure 15).

Figure 15. New Mailbox wizard window 5



New Mailbox
When you click New, the following mailbox will be created.

Configuration Summary:

jaytest2007 JRS. Sillars

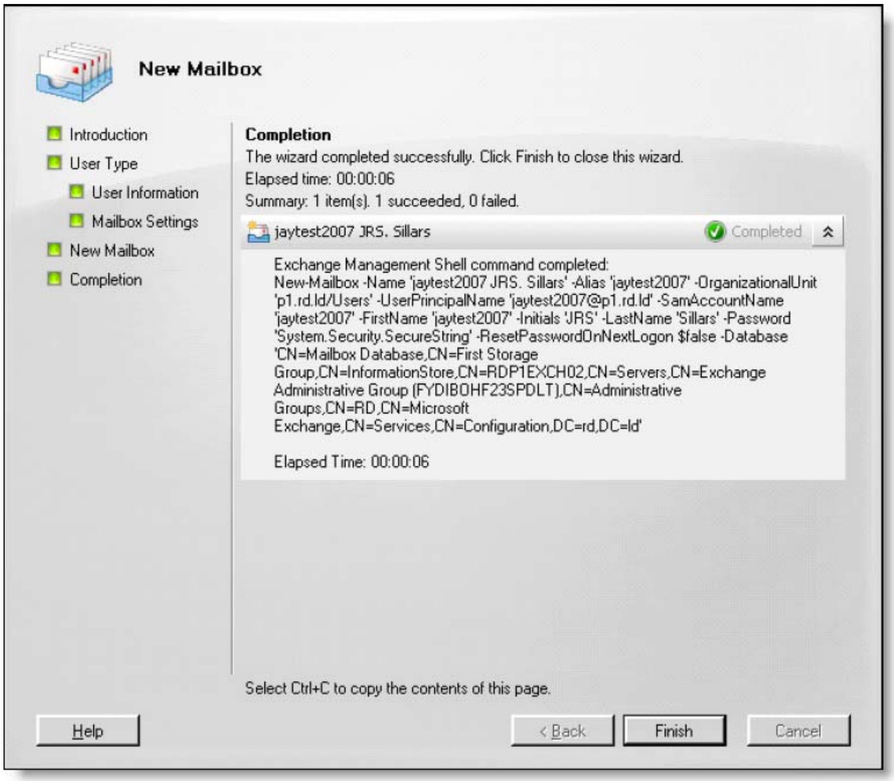
Mailbox type: User Mailbox
Organizational unit: p1.rd.ld/Users
First name: jaytest2007
Initials: JRS
Last name: Sillars
User name: jaytest2007 JRS. Sillars
User logon name (User Principal Name): jaytest2007@p1.rd.ld
User logon name (pre-Windows 2000): jaytest2007
User doesn't need to change password at next logon
Alias: jaytest2007
Server: RDP1EXCH02
Storage Group: First Storage Group
Mailbox Database: Mailbox Database

Select Ctrl+C to copy the contents of this page.

13. If the settings are not correct, click Back and correct the errors. If the settings are as you desire, click New.

14. The final window of the wizard appears (Figure 16).

Figure 16. New Mailbox wizard window 6



Completion

The wizard completed successfully. Click Finish to close this wizard.

Elapsed time: 00:00:06

Summary: 1 item(s). 1 succeeded, 0 failed.

jaytest2007 JRS. Sillars

```
Exchange Management Shell command completed:
New-Mailbox -Name 'jaytest2007 JRS. Sillars' -Alias 'jaytest2007' -OrganizationalUnit
'p1.rd.ld/Users' -UserPrincipalName 'jaytest2007@p1.rd.ld' -SamAccountName
'jaytest2007' -FirstName 'jaytest2007' -Initials 'JRS' -LastName 'Sillars' -Password
'System.Security.SecureString' -ResetPasswordOnNextLogon $false -Database
'CN=Mailbox Database,CN=First Storage
Group,CN=InformationStore,CN=RDP1EXCH02,CN=Servers,CN=Exchange
Administrative Group (FYDIBOHF23SPDLT),CN=Administrative
Groups,CN=RD,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=rd,DC=ld'

Elapsed Time: 00:00:06
```

Select Ctrl+C to copy the contents of this page.

15. Click Finish to close the wizard and create the new mailbox.

Creating Distribution Groups

By default, 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.

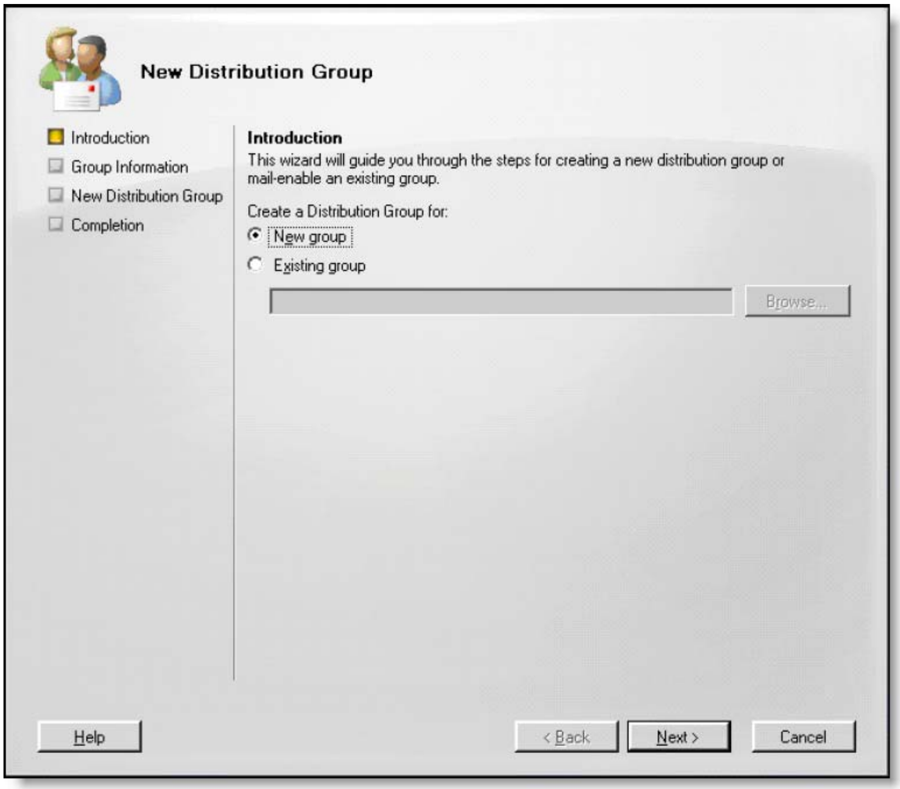
In Desktop Administrator, use the distribution group address to associate e-mails with an e-mail CSQ.

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 17).

Figure 17. New Distribution Group wizard window 1



New Distribution Group

Introduction

This wizard will guide you through the steps for creating a new distribution group or mail-enable an existing group.

Create a Distribution Group for:

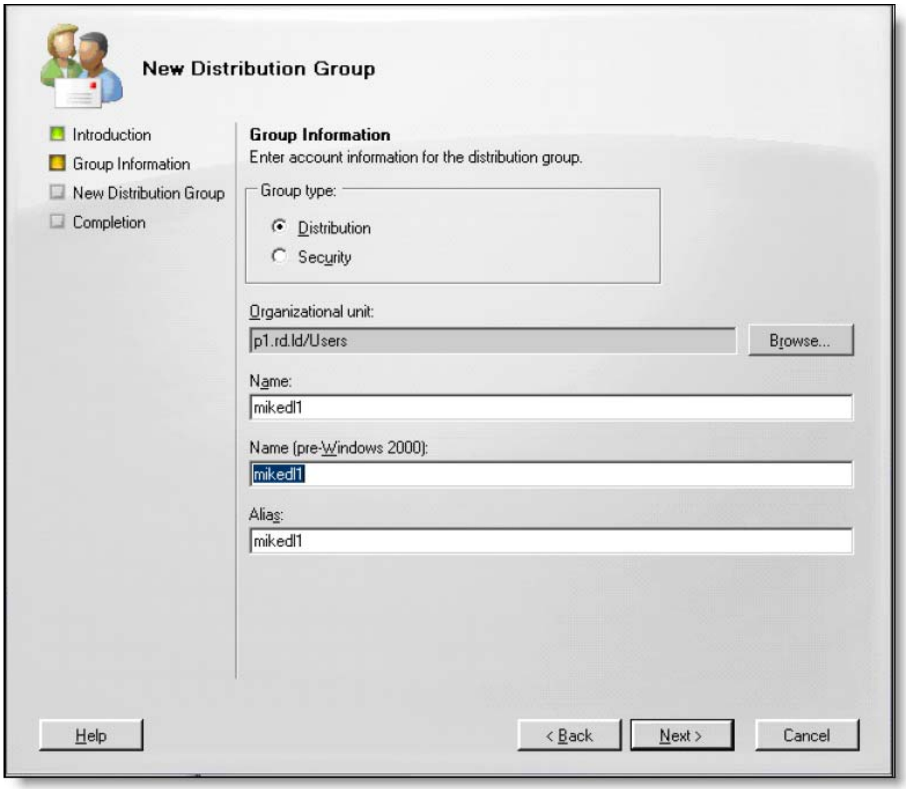
● New group

○ Existing group

4. Select New Group and then click Next.

5. The Group Information window appears (Figure 18).

Figure 18. New Distribution Group wizard window 2



Group Information

Enter account information for the distribution group.

Group type:

● Distribution

○ Security

Organizational unit: p1.rd.ld/Users

Name: mikedl1

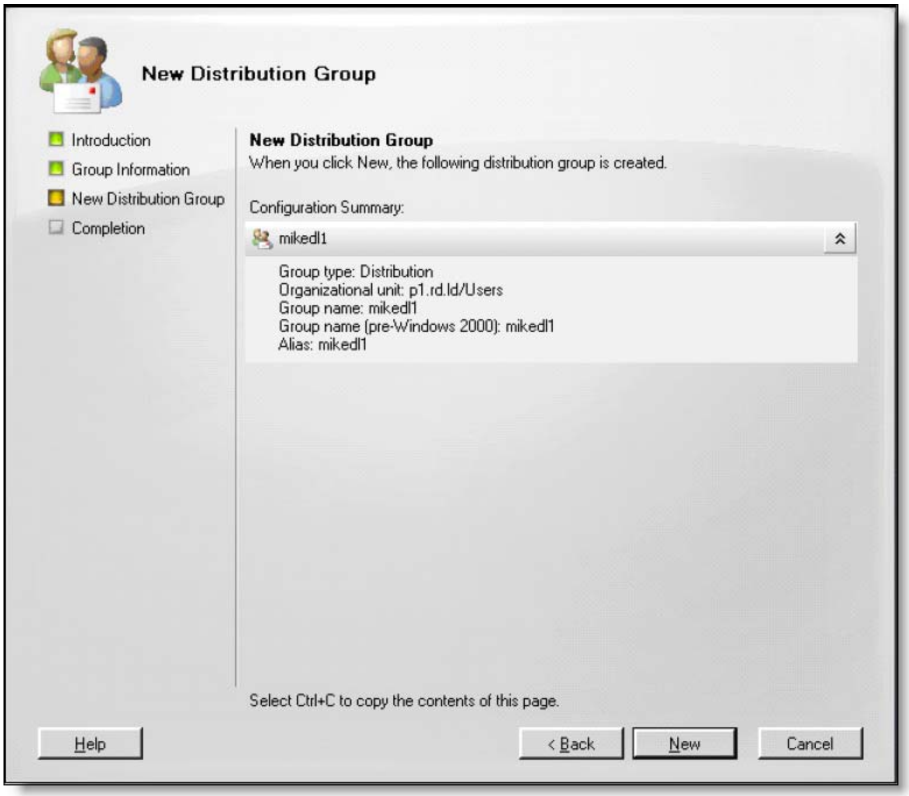
Name (pre-Windows 2000): mikedl1

Alias: mikedl1

6. Select Distribution as the group type, complete the required information for the new group, and then click Next.

7. The final window in the wizard appears (Figure 19).

Figure 19. New Distribution Group wizard window 3



New Distribution Group

When you click New, the following distribution group is created.

Configuration Summary:

mikedl1

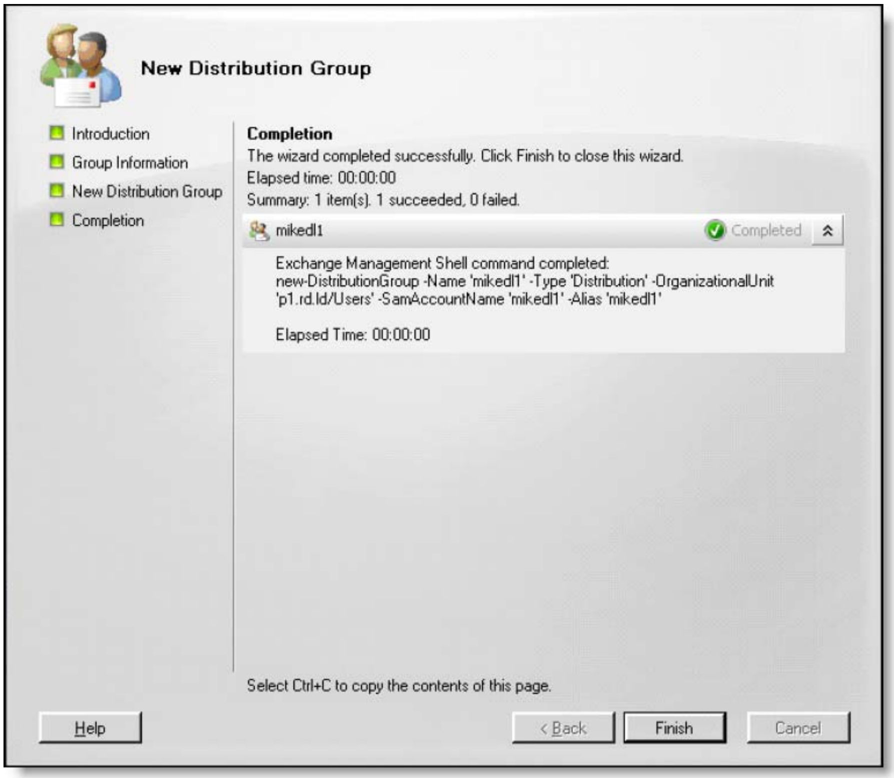
Group type: Distribution
Organizational unit: p1.rd.ld/Users
Group name: mikedl1
Group name (pre-Windows 2000): mikedl1
Alias: mikedl1

Select Ctrl+C to copy the contents of this page.

8. If the settings are not correct, click Back and correct the errors. If the settings are as you desire, click New.

9. The final window of the wizard appears (Figure 20).

Figure 20. New Distribution Group wizard window 4



New Distribution Group

Completion

The wizard completed successfully. Click Finish to close this wizard.

Elapsed time: 00:00:00

Summary: 1 item(s). 1 succeeded, 0 failed.

mikedl1 ✓ Completed

```
Exchange Management Shell command completed:
new-DistributionGroup -Name 'mikedl1' -Type 'Distribution' -OrganizationalUnit
'p1.rd.ld/Users' -SamAccountName 'mikedl1' -Alias 'mikedl1'

Elapsed Time: 00:00:00
```

Select Ctrl+C to copy the contents of this page.

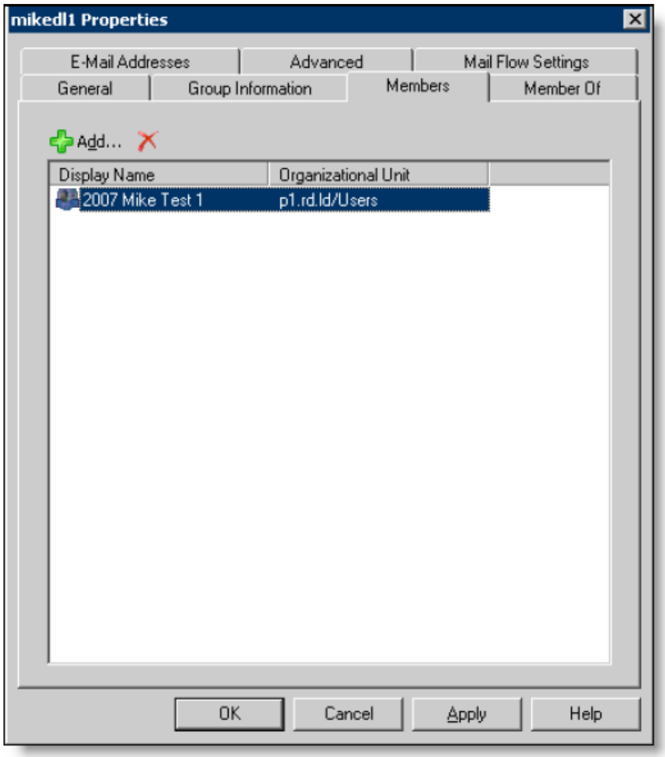
10. Click Finish to create the new distribution group and close the wizard. The new distribution group is now listed under the Distribution Group node.

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 21).

Figure 21. Distribution Group Properties window



Display Name	Organizational Unit
2007 Mike Test 1	p1.rd.ld/Users

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

Configuring Miscellaneous Settings

Use the procedures in "Configuring Miscellaneous Settings" on page 75 for other Exchange settings that must be configured. Since installations of Exchange 2007 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 Exchange 2007 documentation for more complete instructions.

Configuring Exchange 2010

Use the following procedures to configure Exchange 2010.

> **NOTE:** Since installations of Exchange 2010 can be configured differently, it is recommended that you consult your Exchange 2010 documentation for more complete and up-to-date instructions.

Configuring IMAP and SMTP

Exchange 2010 uses the same interface and options for configuring IMAP and SMTP settings as Exchange 2007. For information on configuring IMAP and SMTP security settings, see "Configuring Security Settings" on page 44.

Creating a User

The following procedure is an example of how to create a user in Exchange 2010. For more in-depth information, see Creating a Mailbox for an Existing User, at:

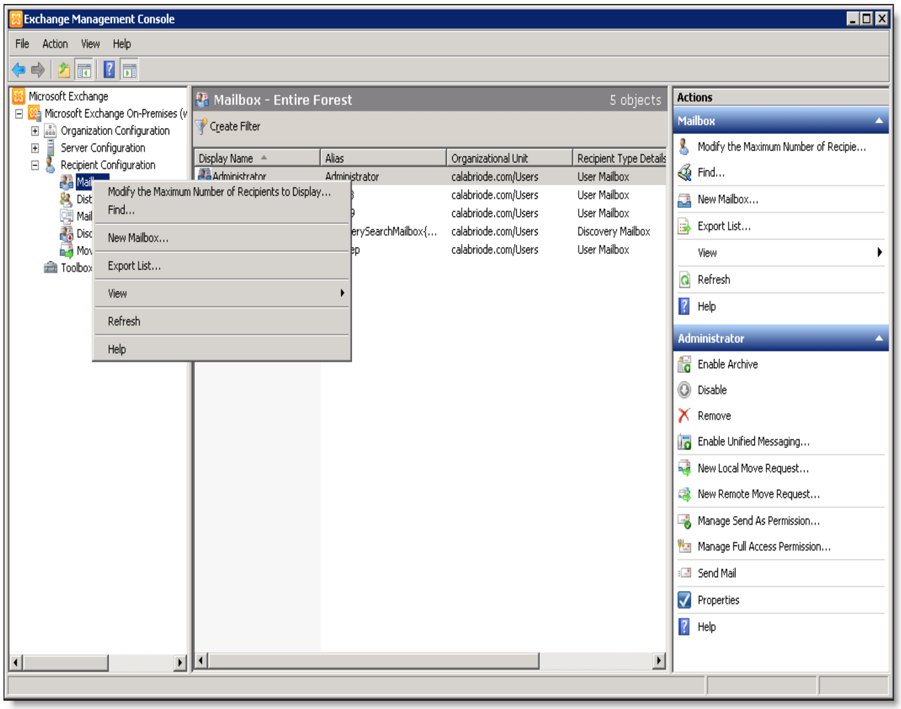
http://technet.microsoft.com/en-us/library/aa998319.aspx

To create a user:

1. Launch the Exchange Management Console.

2. In the left navigation pane, select the Recipient Configuration > Mailbox node (Figure 22).

Figure 22. Exchange Management Console



Display Name	Alias	Organizational Unit	Recipient Type Details
Administrator	Administrator	calabriode.com/Users	User Mailbox
	3	calabriode.com/Users	User Mailbox
	9	calabriode.com/Users	User Mailbox
	erySearchMailbox{...	calabriode.com/Users	Discovery Mailbox
	ep	calabriode.com/Users	User Mailbox

When you select the Mailbox node, three panes are displayed. The center pane lists all existing accounts for Exchange 2007 and 2010. The Recipient Type Details column indicates the type of account:

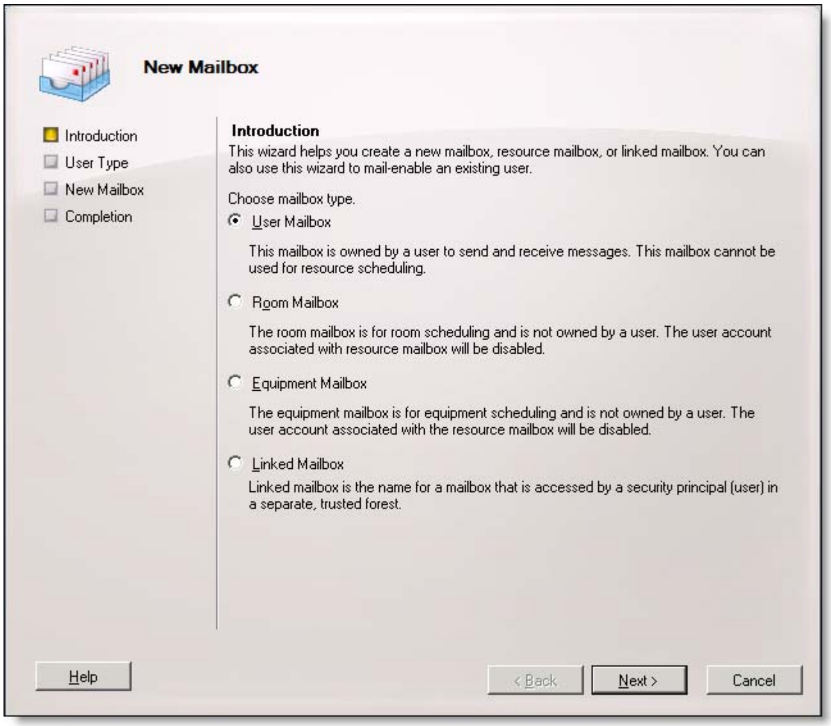
- Legacy = Exchange 2007

- User = Exchange 2010

You cannot share accounts among the Exchange 2007 and 2010 servers. You must set up 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.
4. The New Mailbox wizard appears (Figure 23).

Figure 23. New Mailbox wizard window 1



Introduction

This wizard helps you create a new mailbox, resource mailbox, or linked mailbox. You can also use this wizard to mail-enable an existing user.

Choose mailbox type.

● User Mailbox

This mailbox is owned by a user to send and receive messages. This mailbox cannot be used for resource scheduling.

○ Room Mailbox

The room mailbox is for room scheduling and is not owned by a user. The user account associated with resource mailbox will be disabled.

○ Equipment Mailbox

The equipment mailbox is for equipment scheduling and is not owned by a user. The user account associated with the resource mailbox will be disabled.

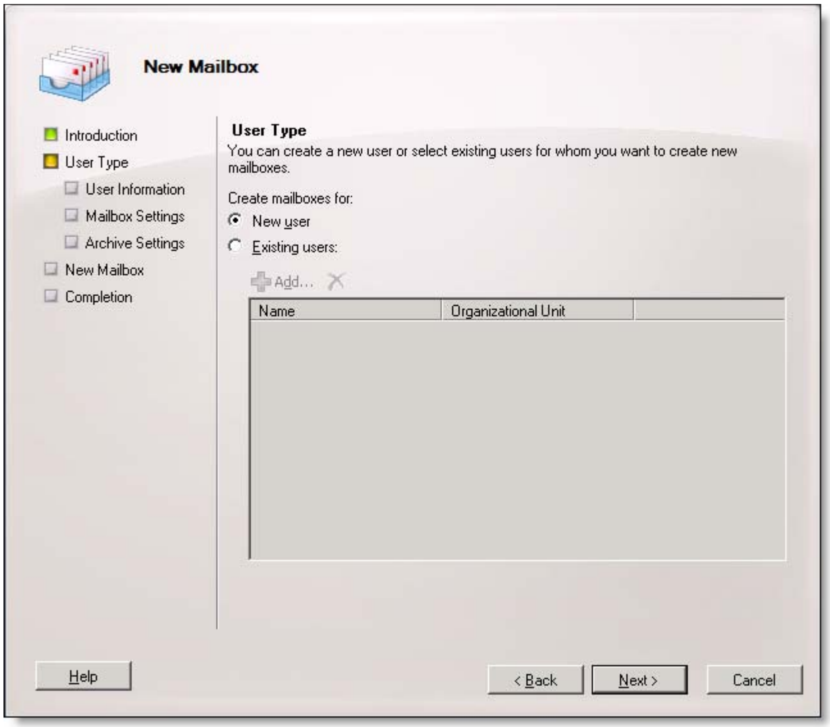
○ Linked Mailbox

Linked mailbox is the name for a mailbox that is accessed by a security principal (user) in a separate, trusted forest.

5. Select User Mailbox and click Next.

6. The User Type window of the wizard appears (Figure 24).

Figure 24. New Mailbox wizard window 2



User Type

You can create a new user or select existing users for whom you want to create new mailboxes.

Create mailboxes for:

● New user

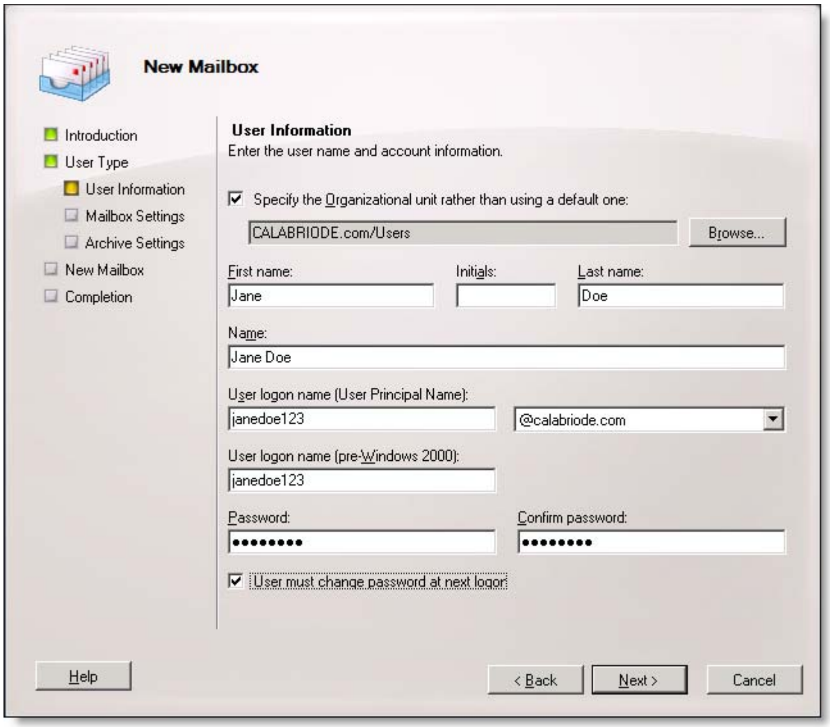
○ Existing users:

Name	Organizational Unit

7. Select New User and click Next. If you want to migrate an account from MS Exchange 2007, select Existing User and then browse to the account name. Keep in mind that if you do this, the account will no longer be available in the corresponding earlier version of Exchange.

8. The User Information window of the wizard appears (Figure 25).

Figure 25. New Mailbox wizard window 3



New Mailbox

User Information

Enter the user name and account information.

☑ Specify the Organizational unit rather than using a default one: CALABRIODE.com/Users

First name: Jane

Initials:

Last name: Doe

Name: Jane Doe

User logon name (User Principal Name): janedoe123 @calabriode.com

User logon name (pre-Windows 2000): janedoe123

Password: ••••••••

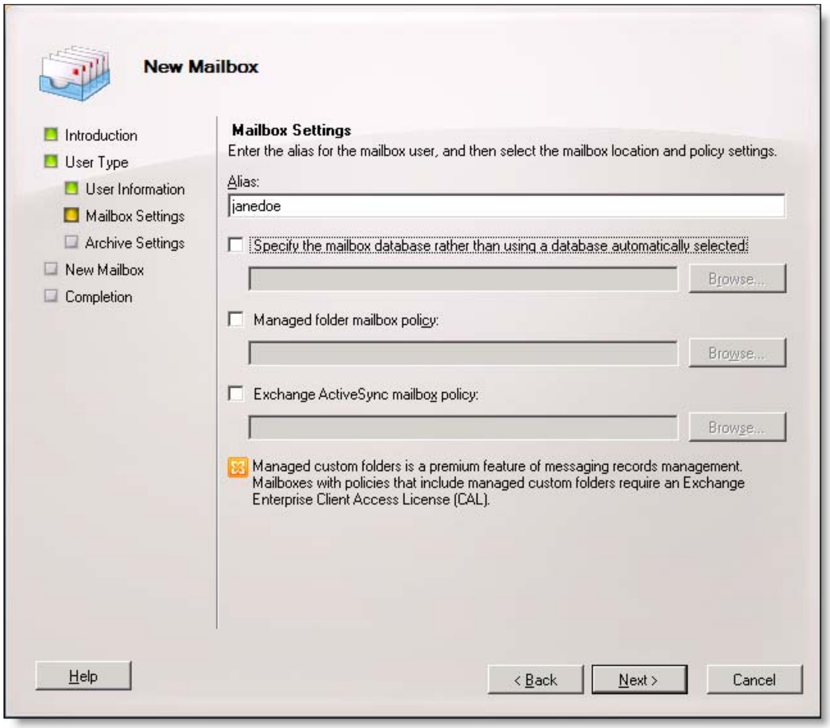
Confirm password: ••••••••

☑ User must change password at next logon

9. Enter the user information for the new account and click Next.

10. The Mailbox Settings window of the wizard appears (Figure 26).

Figure 26. New Mailbox wizard window 4



Mailbox Settings

Enter the alias for the mailbox user, and then select the mailbox location and policy settings.

Alias:

janedoe

□ Specify the mailbox database rather than using a database automatically selected:

□ Managed folder mailbox policy:

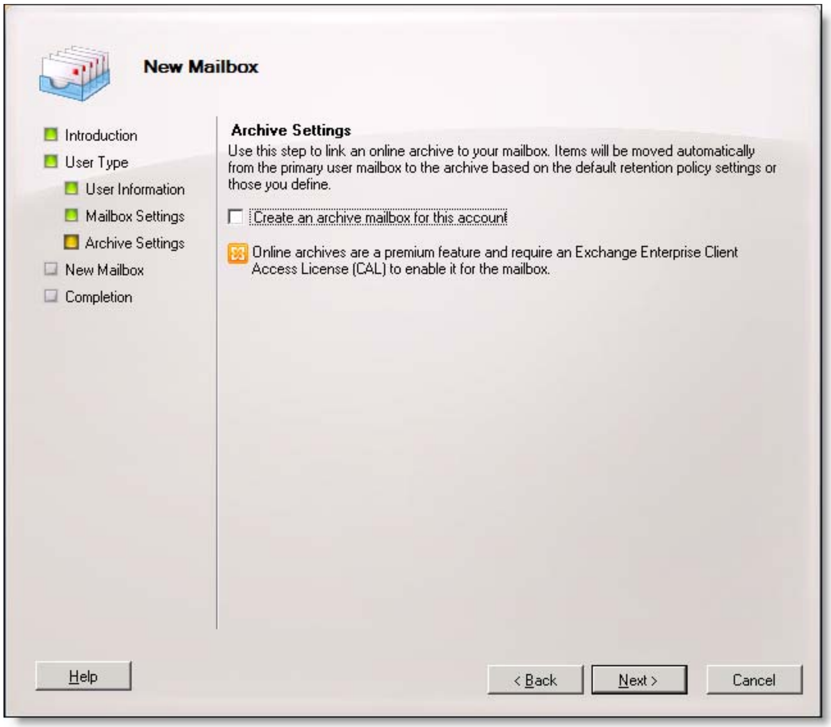
□ Exchange ActiveSync mailbox policy:

Managed custom folders is a premium feature of messaging records management. Mailboxes with policies that include managed custom folders require an Exchange Enterprise Client Access License (CAL).

11. Accept the defaults, or configure the mailbox settings as desired, and then click Next.

12. The Archive Settings window of the wizard appears (Figure 27).

Figure 27. New Mailbox wizard window 5



Archive Settings

Use this step to link an online archive to your mailbox. Items will be moved automatically from the primary user mailbox to the archive based on the default retention policy settings or those you define.

□ Create an archive mailbox for this account

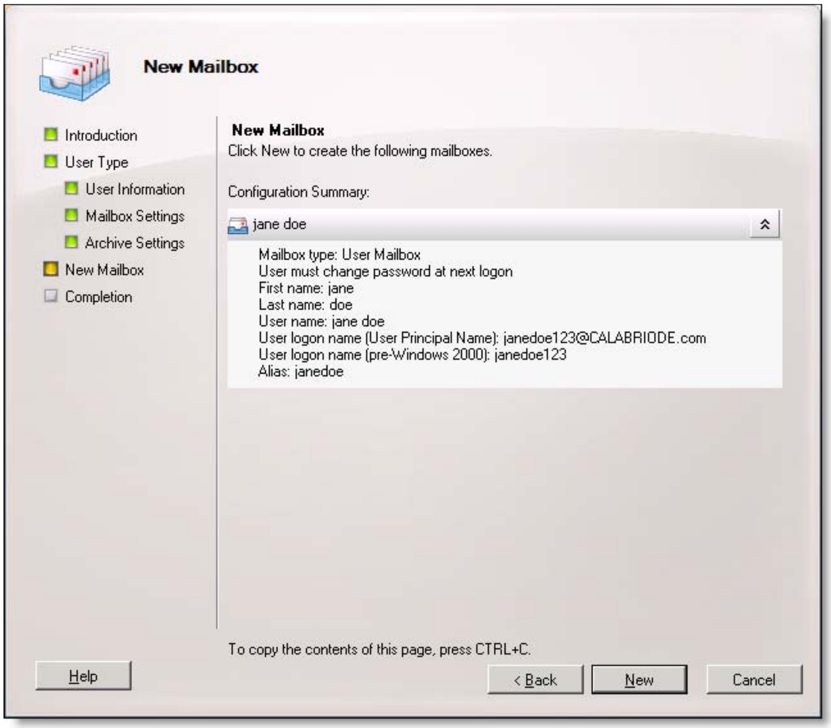
Online archives are a premium feature and require an Exchange Enterprise Client Access License (CAL) to enable it for the mailbox.

13. Leave the Create an archive mailbox for this account box unselected, and then click Next.

NOTE: It is possible to associate the mailbox with an available online archive to archive mailbox items. However, it is recommended that an archive mailbox for this account is not created because it might interfere with Agent E-Mail's functionality.

14. A window containing the summary of the new mailbox settings appears (Figure 28).

Figure 28. New Mailbox wizard window 6



New Mailbox

Click New to create the following mailboxes.

Configuration Summary:

jane doe

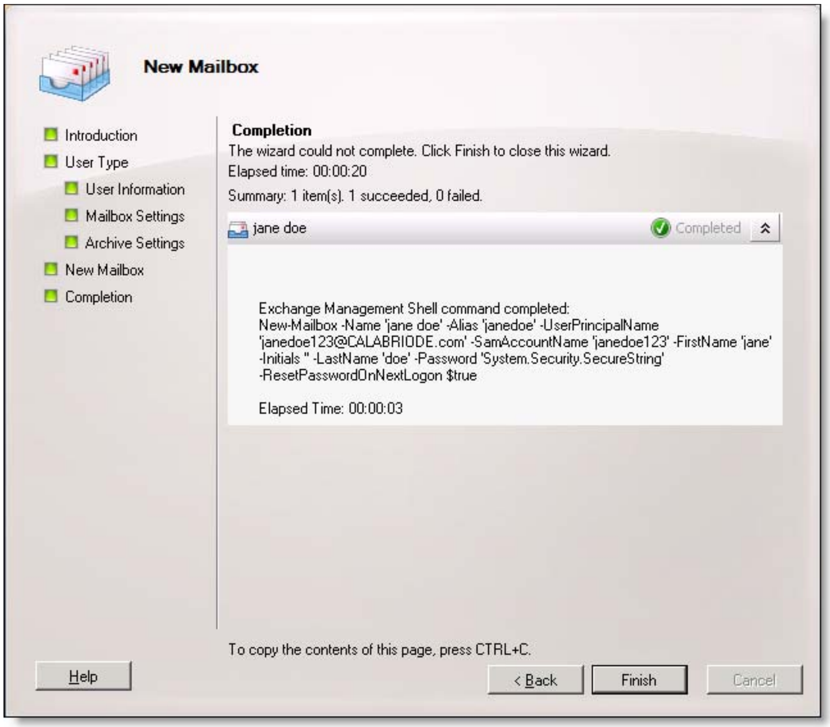
Mailbox type: User Mailbox
User must change password at next logon
First name: jane
Last name: doe
User name: jane doe
User logon name (User Principal Name): janedoe123@CALABRIODE.com
User logon name (pre-Windows 2000): janedoe123
Alias: janedoe

To copy the contents of this page, press CTRL+C.

15. If the settings are not correct, click Back and correct the errors. If the settings are as you desire, click New.

16. The final window of the wizard appears (Figure 29).

Figure 29. New Mailbox wizard window 7



Completion

The wizard could not complete. Click Finish to close this wizard.

Elapsed time: 00:00:20

Summary: 1 item(s). 1 succeeded, 0 failed.

```
Exchange Management Shell command completed:
New-Mailbox -Name 'jane doe' -Alias 'janedoe' -UserPrincipalName
'janedoe123@CALABRIODE.com' -SamAccountName 'janedoe123' -FirstName 'jane'
-Initials '' -LastName 'doe' -Password 'System.Security.SecureString'
-ResetPasswordOnNextLogon $true

Elapsed Time: 00:00:03
```

To copy the contents of this page, press CTRL+C.

17. Click Finish to close the wizard and create the new mailbox.

Creating Distribution Groups

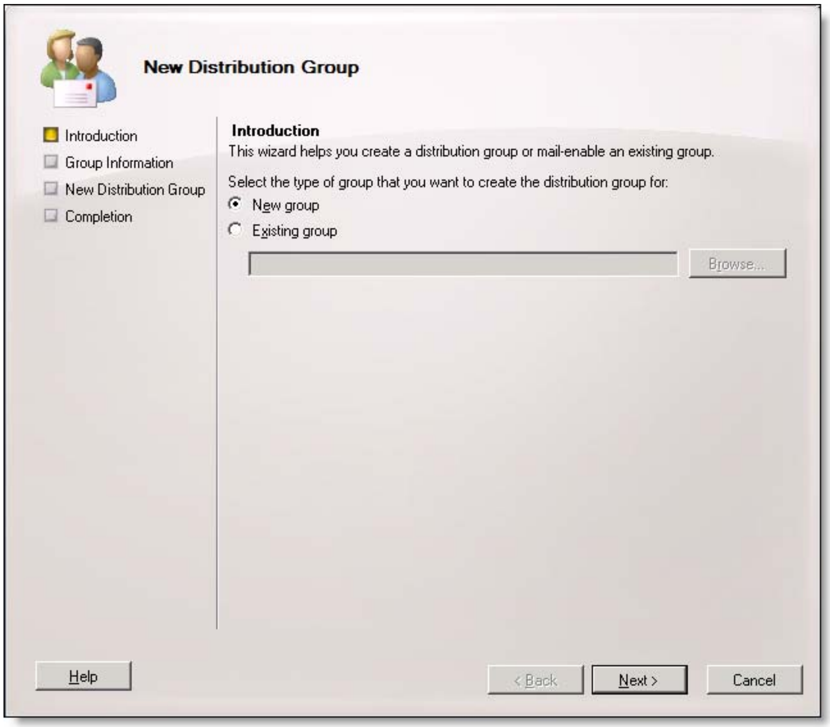
In Desktop Administrator, use the distribution group address to associate e-mails with an e-mail CSQ.

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 30).

Figure 30. New Distribution Group wizard window 1



New Distribution Group

Introduction

This wizard helps you create a distribution group or mail-enable an existing group.

Select the type of group that you want to create the distribution group for:

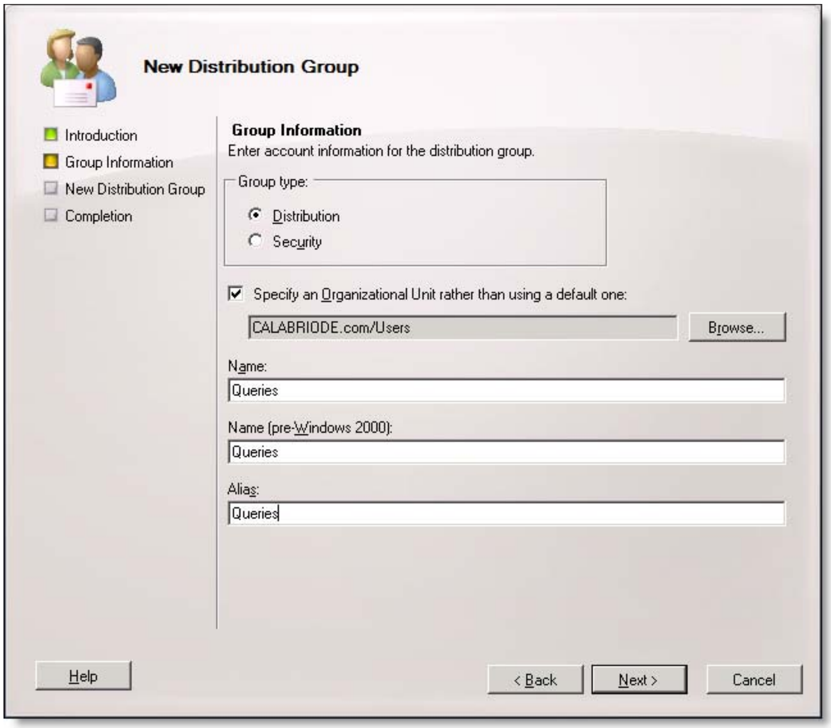
● New group

○ Existing group

4. Select New Group and then click Next.

5. The Group Information window appears (Figure 31).

Figure 31. New Distribution Group wizard window 2



Group Information

Enter account information for the distribution group.

Group type:

● Distribution
○ Security

☑ Specify an Organizational Unit rather than using a default one:

CALABRIODE.com/Users

Name:
Queries

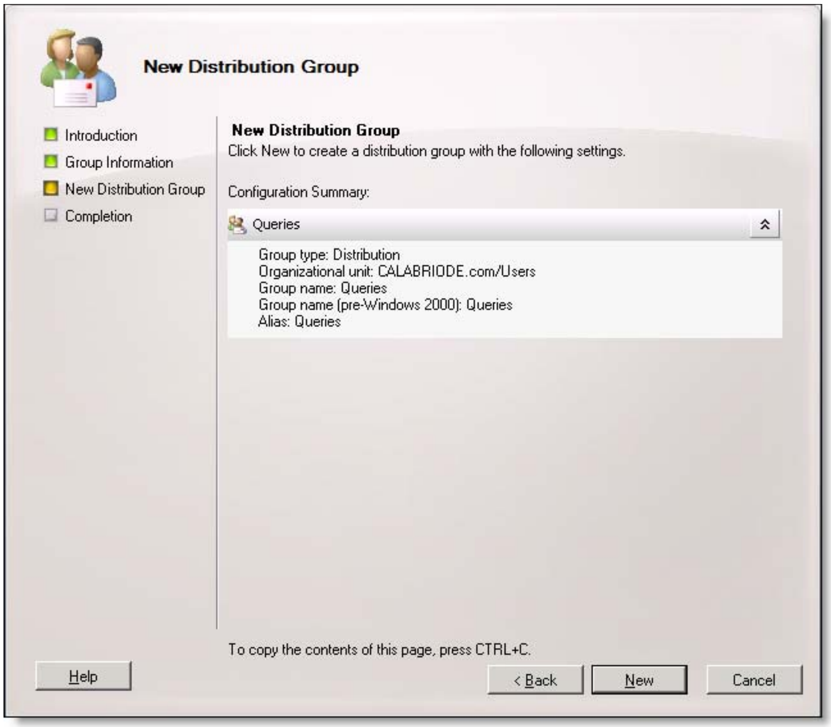
Name (pre-Windows 2000):
Queries

Alias:
Queries

6. Select Distribution as the group type, complete the required information for the new group, and then click Next.

7. The final window in the wizard appears (Figure 32).

Figure 32. New Distribution Group wizard window 3



New Distribution Group

Click New to create a distribution group with the following settings.

Configuration Summary:

Queries

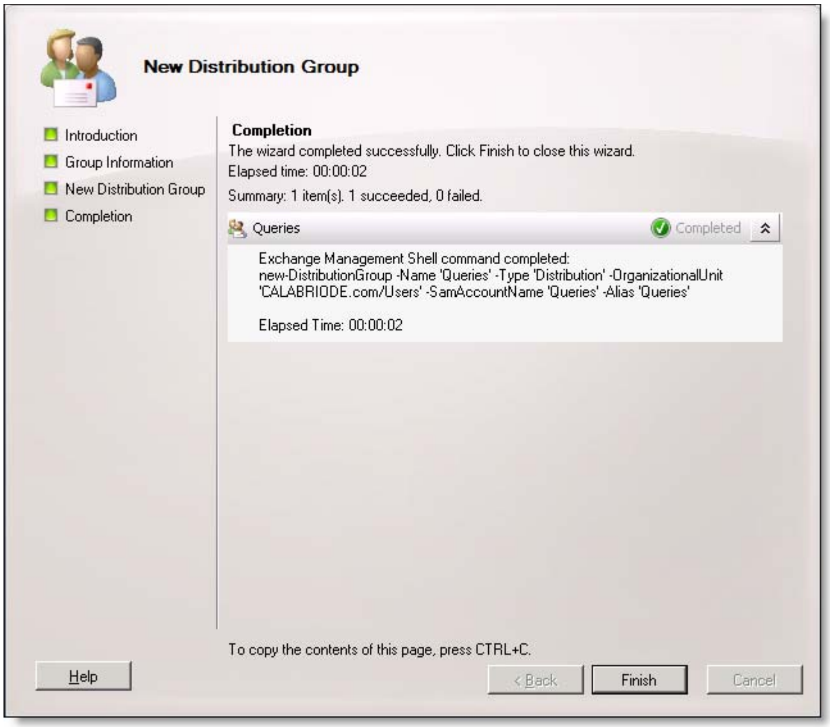
Group type: Distribution
Organizational unit: CALABRIODE.com/Users
Group name: Queries
Group name (pre-Windows 2000): Queries
Alias: Queries

To copy the contents of this page, press CTRL+C.

8. If the settings are not correct, click Back and correct the errors. If the settings are as you desire, click New.

9. The final window of the wizard appears (Figure 33).

Figure 33. New Distribution Group wizard window 4



Completion

The wizard completed successfully. Click Finish to close this wizard.

Elapsed time: 00:00:02

Summary: 1 item(s). 1 succeeded, 0 failed.

Queries — Completed

```
Exchange Management Shell command completed:
new-DistributionGroup -Name 'Queries' -Type 'Distribution' -OrganizationalUnit
'CALABRIODE.com/Users' -SamAccountName 'Queries' -Alias 'Queries'

Elapsed Time: 00:00:02
```

To copy the contents of this page, press CTRL+C.

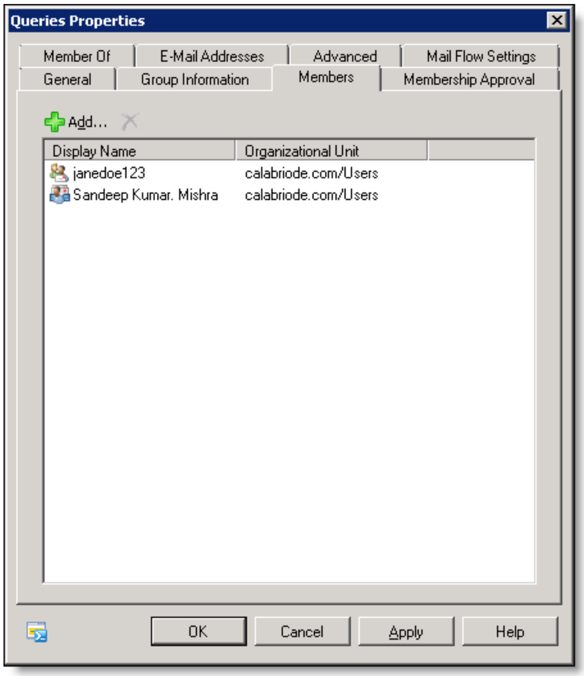
10. Click Finish to create the new distribution group and close the wizard. The new distribution group is now listed under the Distribution Group node.

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 34).

Figure 34. Distribution Group Properties window



Display Name	Organizational Unit
janedoe123	calabriode.com/Users
Sandeep Kumar. Mishra	calabriode.com/Users

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

Configuring Miscellaneous Settings

The following settings must be configured in Exchange 2007 and 2010 in order for Agent E-Mail to perform optimally.

Message Size Restrictions

Restrictions to message size might prevent messages from being sent or received. You must remove any restrictions to message size at the organizational level and the mailbox level.

> **NOTE:** These procedures are applicable to Exchange 2010. Message size restrictions must also be configured in Exchange 2007. Since installations of Exchange 2007 can be configured differently, it is recommended that you consult your Exchange documentation for more pertinent instructions.

To remove size restrictions of incoming and outgoing messages at the mailbox level:

1. In the Exchange Management Console left navigation pane, select Recipient Configuration > Mailbox.

2. In the middle pane, right-click the mailbox you want to configure and select Properties from the popup menu.
3. In the Properties window, select the Mail Flow Settings tab, and then select Message Size Restrictions.
4. In the Message Size Restrictions dialog, clear the Maximum message size (in KB) check boxes for both Sending message size and Receiving message size, and click OK.
5. Click Apply and then OK to save your changes and dismiss the window.

To configure size restrictions of messages at the organizational level:

1. In the Exchange Management Console left navigation pane, select Organization Configuration > Hub Transport.
2. In the middle pane, right-click Transport Settings, and select Properties from the popup menu.
3. In the Transport Settings Properties window, select the General tab, and configure the following fields:
   - Select the box and change the value for Maximum receive size (KB) to 10240.
   - Select the box and change the value for Maximum send size (KB) to 10240.
   - Select the box and change the value for Maximum number of recipients to 5000.
4. Click Apply and then OK to save your changes and dismiss the window.

Mailbox Size Limit

If the contents of a mailbox exceeds the specified limit, messages cannot be sent or received as long as the mailbox is full. Incoming messages are returned to the sender as non-deliverable until received messages are deleted.

You can set the mailbox size limit at the organizational level and the mailbox level. However, the mailbox level overwrites the organizational level. It is recommended that you verify the mailbox setting in addition to configuring at the organizational level.

> **NOTE:** It is recommended that you set the minimum mailbox size to at least 2.3 GB.

> **NOTE:** These procedures are applicable to Exchange 2010. Mailbox size limits must also be configured in Exchange 2007. Since installations of Exchange 2007 can be configured differently, it is recommended that you consult your Exchange documentation for more pertinent instructions.

To set the mailbox size limit at the organizational level:

1. In the Exchange Management Console left navigation pane, select Organization Configuration > Mailbox.

2. In the middle pane, select the Database Management tab.
3. Right-click the mailbox database you want to configure and select Properties from the popup menu.
4. In the Properties window, select the Limits tab and change the value for Prohibit Send and Receive at (KB) to 2411520.
5. Click Apply and then OK to save your changes and dismiss the window.

To set the mailbox size limit at the mailbox level:

1. In the Exchange Management Console left navigation pane, select Recipient Configuration > Mailbox.
2. In the middle pane, right-click the mailbox you wish to configure and select Properties from the popup menu.
3. In the Properties window, select the Mailbox settings tab and select Storage Quotas.
4. Select the Use mailbox database defaults check boxes under both Storage quotas and Deleted item retention and click OK to default to the organizational level setting. Or you can change the value for Prohibit Send and Receive at (KB) to 2411520 to overwrite the organizational setting.
5. Click Apply and then OK to save your changes and dismiss the window.

Configuring Exchange 2013

Use the following procedures to configure Exchange 2013 using the Exchange Admin Center web application.

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

Creating a User Mailbox

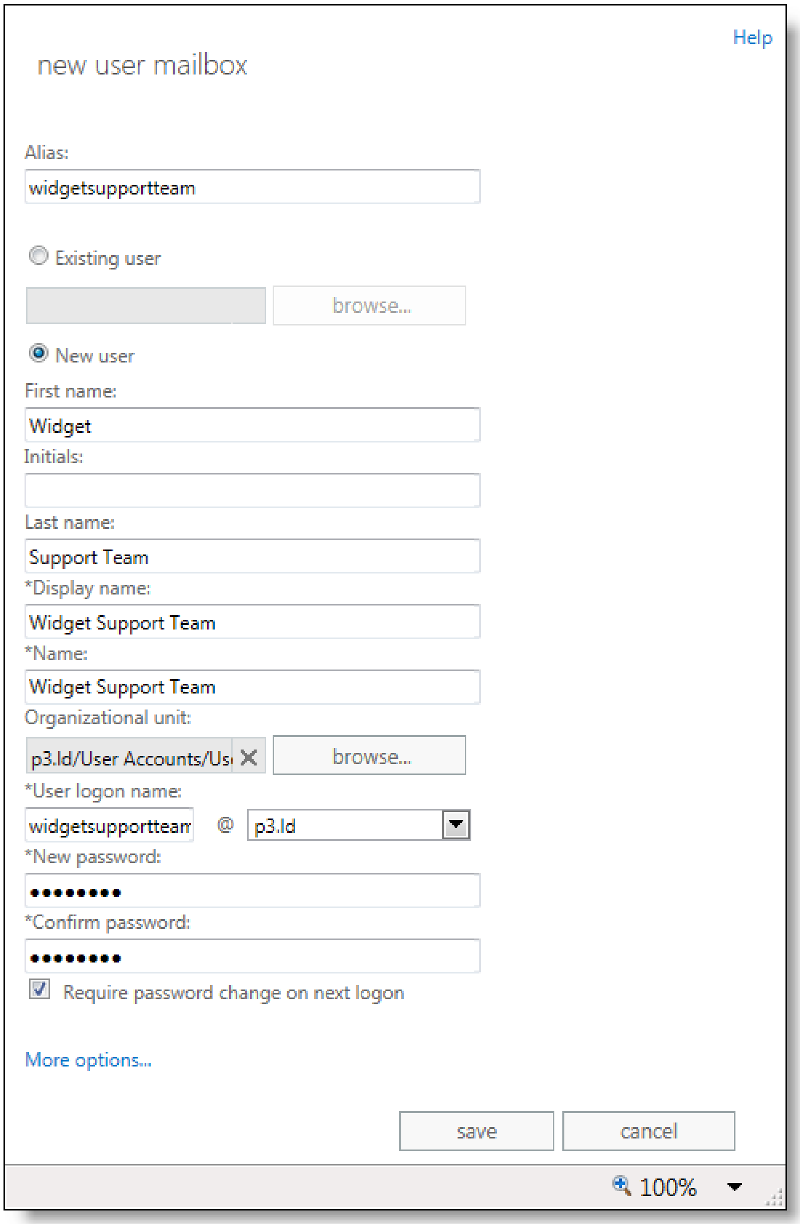
To create a new user mailbox:

1. Access the Exchange Admin Center web application by navigating to the following URL and logging in:

   https://<Exchange server host name or IP address>/ecp/
2. Select the recipients node from the left pane, and then choose the mailboxes tab.
3. Click the New icon (the plus sign) and select User mailbox.

4. Complete the new user mailbox window. An example is shown below.

Figure 35. New user mailbox window.



new user mailbox

Alias: widgetsupportteam

○ Existing user

● New user

First name: Widget

Initials:

Last name: Support Team

*Display name: Widget Support Team

*Name: Widget Support Team

Organizational unit: p3.ld/User Accounts/Us

*User logon name: widgetsupportteam @ p3.ld

*New password: ••••••••

*Confirm password: ••••••••

☑ Require password change on next logon

Select New user to set up a new user mailbox. If you want to migrate an account from an earlier version of Exchange, select Existing user and then browse to the account name. Keep in mind that if you do this, the account will no longer be available in the corresponding earlier version of Exchange.

It is not necessary to expand the window by clicking More options. The fields shown here are the only ones required.

5. When you have completed the fields in the window, click save. Your entries are validated, and if any are incorrect, you are prompted to correct them. If your entries are correct, the window closes after it is saved.

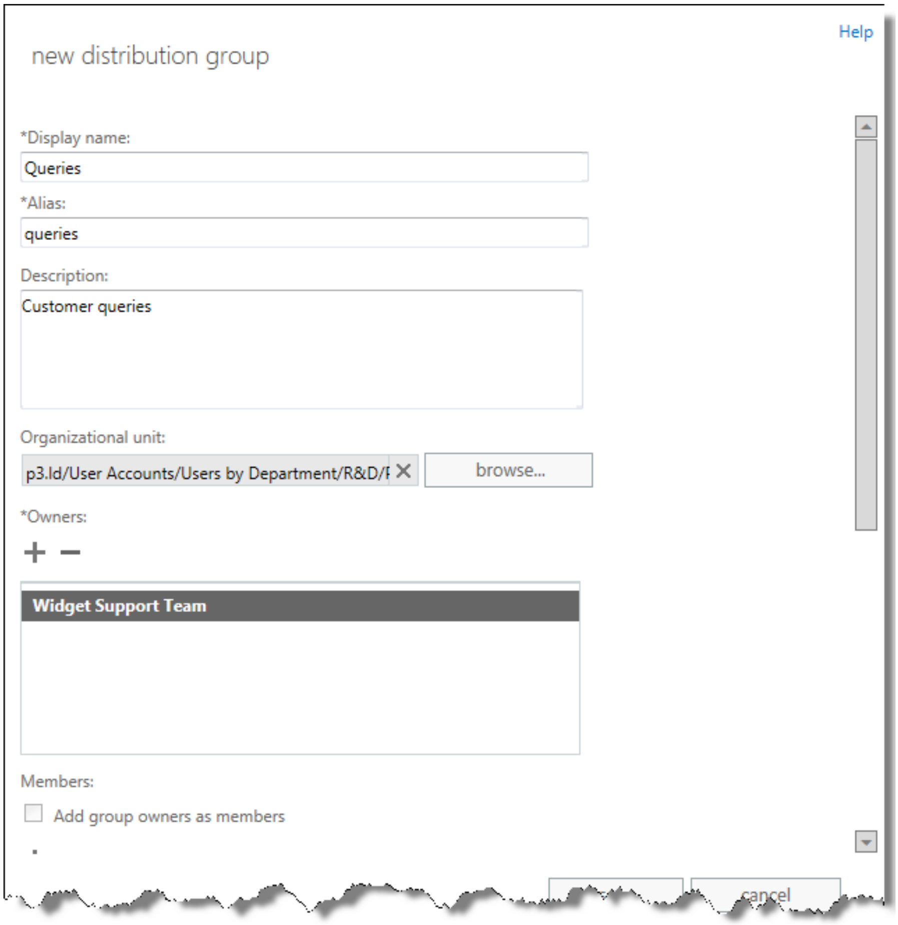
Creating a New Distribution Group

The distribution group is used in Desktop Administrator to associate e-mails with an e-mail CSQ.

To create a new distribution group:

1. In the Exchange Admin Center, select the recipients node from the left pane, and then choose the groups tab.
2. Click the New icon (the plus sign) and select Distribution group.
3. Complete the new distribution group window. An example is shown below.

Figure 36. New distribution group window, part 1



new distribution group

*Display name: Queries

*Alias: queries

Description: Customer queries

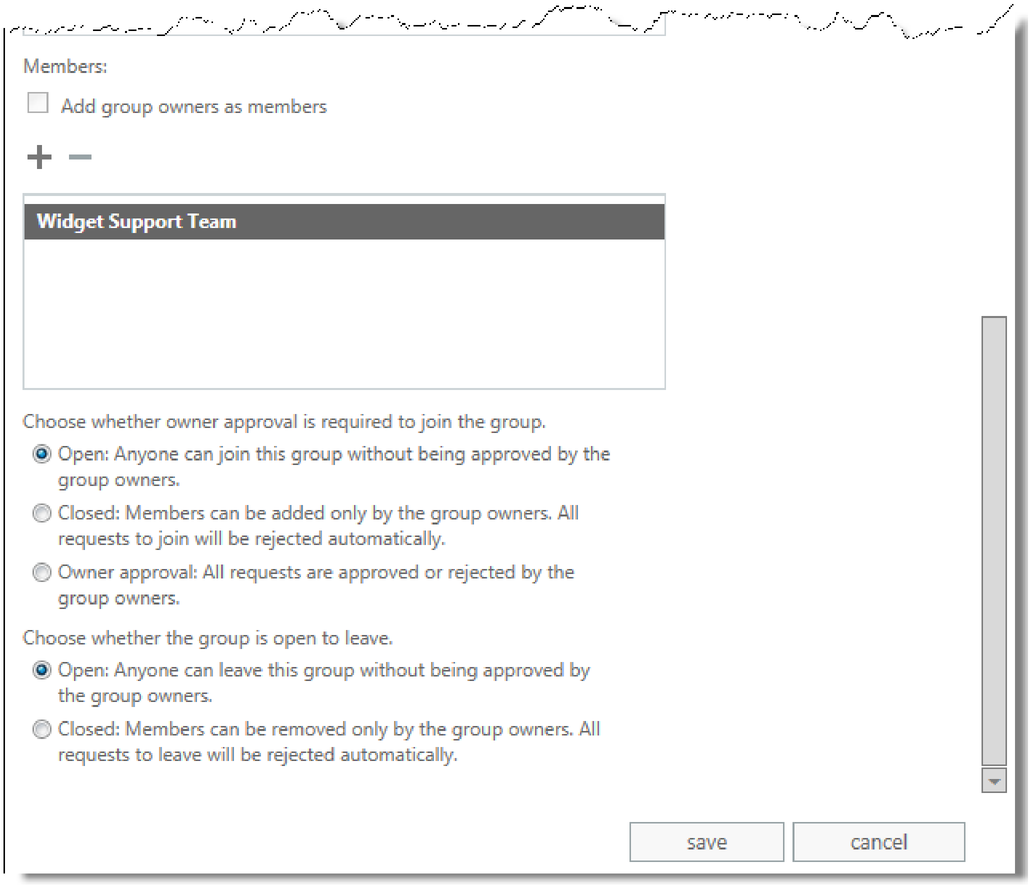
Organizational unit: p3.ld/User Accounts/Users by Department/R&D/F

*Owners: Widget Support Team

Members:

□ Add group owners as members

Figure 37. New distribution group window, part 2



Members:

□ Add group owners as members

Widget Support Team

Choose whether owner approval is required to join the group.

● Open: Anyone can join this group without being approved by the group owners.

○ Closed: Members can be added only by the group owners. All requests to join will be rejected automatically.

○ Owner approval: All requests are approved or rejected by the group owners.

Choose whether the group is open to leave.

● Open: Anyone can leave this group without being approved by the group owners.

○ Closed: Members can be removed only by the group owners. All requests to leave will be rejected automatically.

- The organizational unit should match the one configured for the new user mailbox.
- The owner of the distribution group does not have to be the user mailbox just created. Whoever creates the distribution group is the owner, and there can be others.
- The members of the distribution group should include the user mailbox just created, and anyone else who should get a copy of the messages sent to the distribution group.

4. When you have completed the fields in the window, click save. Your entries are validated, and if any are incorrect, you are prompted to correct them. If your entries are correct, the window closes after it is saved.

Configuring Miscellaneous Settings

Setting the Recipient Number Limit and Message Size Limit

Restrictions to message size might prevent messages from being sent or received. You can adjust any restrictions to message size and the number of recipients at the mailbox level and the organizational level. Note, however, that only default settings are supported with Agent E-Mail (10 MB maximum message size, 5,000 maximum recipients).

For more information on message size limits, see the Microsoft Technet article “Message Size Limits” at http://technet.microsoft.com/en-us/library/bb124345(v=exchg.150).aspx.

To set the recipient number limit at the mailbox level:

1. In the Exchange Admin Center, select the recipients node from the left pane, and then choose the mailboxes tab.
2. Select the user mailbox you created earlier, and then click the Edit icon (the pencil) to open the mailbox window.
3. Click mailbox features, scroll the window down to Delivery Options, and then click View Details.
4. In the delivery options window, the Recipient limit can be configured by selecting the Maximum recipients check box and filling in a value. By default this check box is cleared.
5. Click ok to dismiss the window.

To set the message size limit at the mailbox level:

1. In the Exchange Admin Center, select the recipients node from the left pane, and then choose the mailboxes tab.
2. Select the user mailbox you created earlier, and then click the Edit icon (the pencil) to open the mailbox window.
3. Click mailbox features, scroll the window down to Message Size Restrictions, and then click View details.
4. In the message size restrictions window, by default there are no restrictions on sent and received message size. To set a maximum size, select the check boxes for Sent message and Received messages and enter a value.
5. Click ok to dismiss the window.

To set the recipient number limit and message size limit for receive connectors at the organizational level:

1. In the Exchange Management Shell, type the following command:

   ```
   Set-ReceiveConnector -Identity "<Agent E-Mail Receive Connector>"
   -MaxMessageSize 10MB -MaxRecipientsPerMessage 5000
   ```

2. Repeat Step 1 for every receive connector to be used with Agent E-Mail.

To set the recipient number limit and message size limit for send connectors at the organizational level:

1. In the Exchange Admin Center, select the mail flow node from the left pane, and then choose the send connector tab.
2. Select the send connector that you will use with Agent E-Mail.

3. Click the ellipsis (...) for more options, and then choose Organization Transport Settings. In the window that pops up, configure these fields as shown:
   - Maximum number of recipients: 5000
   - Maximum receive message size (MB): 10
   - Maximum send message size (MB): 10
4. Click Save.

Setting the Mailbox Size Limit

If the contents of a mailbox exceeds the specified limit, messages cannot be sent or received as long as the mailbox is full. Incoming messages are returned to the sender as non-deliverable until received messages are deleted.

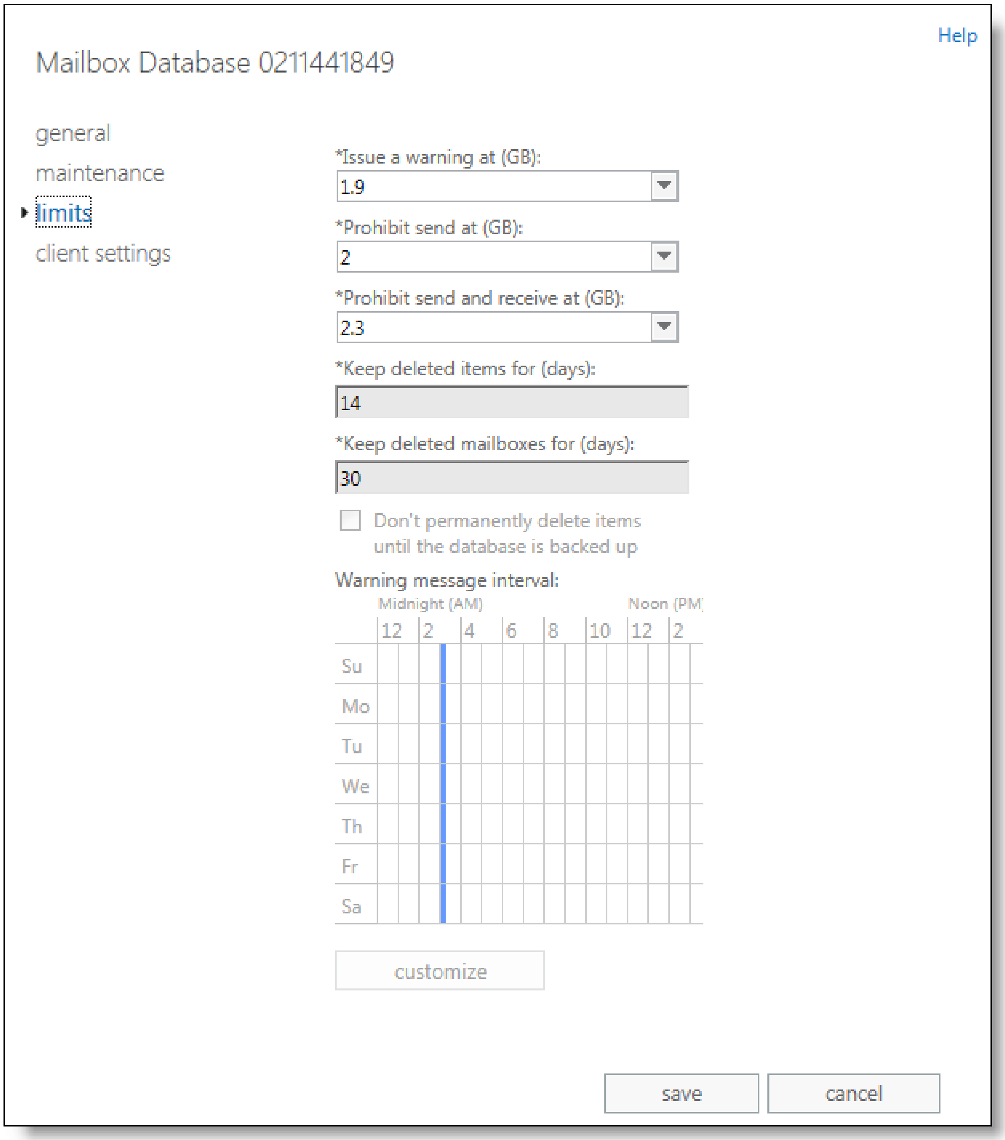
You can set the mailbox size limit at the organizational level and the mailbox level. However, the mailbox level overwrites the organizational level. It is recommended that you verify the mailbox setting in addition to configuring at the organizational level.

To set the mailbox size limit at the organizational level:

1. In the Exchange Admin Center, select the servers node from the left pane, and then choose the databases tab.
2. Select the appropriate mailbox database, and click Edit (the pencil).

3. Select limits, and set the default limits for the organization.

Figure 38. Database limits window.



Mailbox Database 0211441849

*Issue a warning at (GB): 1.9

*Prohibit send at (GB): 2

*Prohibit send and receive at (GB): 2.3

*Keep deleted items for (days): 14

*Keep deleted mailboxes for (days): 30

□ Don't permanently delete items until the database is backed up

Warning message interval:

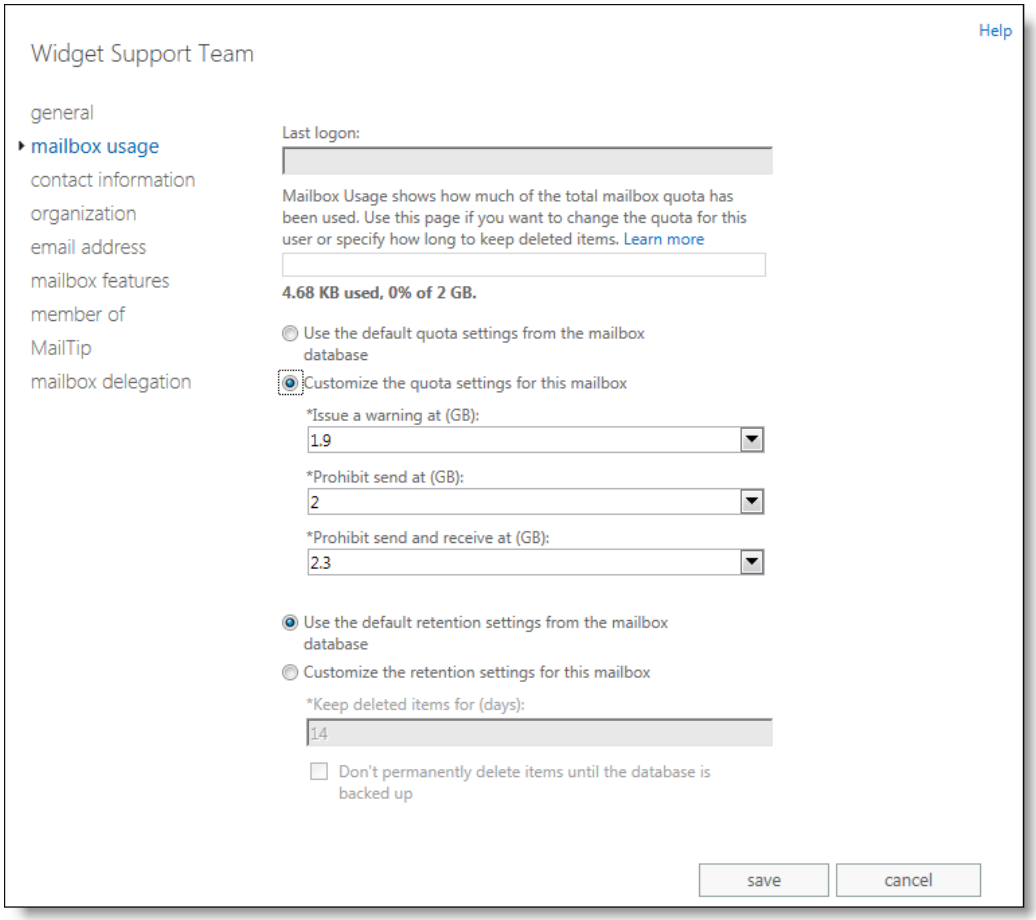
4. Click save.

To set the mailbox size limit at the mailbox level:

1. In the Exchange Admin Center, select the recipients node from the left pane, and then choose the mailboxes tab.
2. Select the user mailbox you set up previously, and click Edit (the pencil).

3. Click mailbox usage, and then click More options.

Figure 39. Mailbox usage window.



Widget Support Team

Last logon:

Mailbox Usage shows how much of the total mailbox quota has been used. Use this page if you want to change the quota for this user or specify how long to keep deleted items. Learn more

4.68 KB used, 0% of 2 GB.

○ Use the default quota settings from the mailbox database

● Customize the quota settings for this mailbox

*Issue a warning at (GB): 1.9

*Prohibit send at (GB): 2

*Prohibit send and receive at (GB): 2.3

● Use the default retention settings from the mailbox database

○ Customize the retention settings for this mailbox

*Keep deleted items for (days): 14

□ Don't permanently delete items until the database is backed up

4. Select the Customize the quota settings for this mailbox and set the limits as desired. It is recommended that you set the minimum Prohibit send and receive at (GB) limit to at least 2.3 GB.

5. Click save.

Message Formatting in Exchange

E-mail messages on the Internet can be sent and received in a variety of different message format types. In CAD, messages sent to and received from external e-mail clients must be converted so that both the sender and recipient can view the content regardless of what e-mail client they use. A message might be embedded with more than one format type.

When the message is delivered to Agent E-Mail, only the HTML version is displayed to the agent. If an HTML version is not present, then CAD will construct one if possible.

Messages sent from Agent E-Mail are embedded with both plain text and HTML formats. The format viewed by recipients depends on what their e-mail client supports.

For more information about the message formats supported by Exchange, see “Exchange 2010 and Outlook Message Formats”, at:

http://technet.microsoft.com/en-us/library/bb232174.aspx#Exchange

Table 6 describes the message formats supported by Agent E-Mail.

Table 6. Message Formats in Agent E-Mail

Incoming Message Format	Message Display Format	Outgoing Message Format
HTML	HTML	Plain text and HTML
Plain text	HTML	Plain text and HTML
Rich Text Format (RTF)	HTML	Plain text and HTML
Enriched text	Attachment	Plain text and HTML
MS-TNEF	HTML with a winmail.dat attachment	Plain text and HTML

Configuring the Message Retrieval Format

How you configure the message retrieval format determines how Exchange delivers messages to Agent E-Mail. By selecting Best body format in the procedures below, you configure MS Exchange to choose the most appropriate embedded format to display to the agent.

Configuration can be done at both the server and mailbox levels. However, the mailbox setting overwrites the server setting. It is recommended that you verify the mailbox setting in addition to configuring the server setting.

Message Retrieval Format for Exchange 2007 and 2010

To configure the message retrieval format at the server level:

1. In the Exchange Management Console left navigation pane, select Server Configuration > Client Access.
2. In the middle pane, select the POP3 and IMAP4 tab.
3. Right-click IMAP4 and select Properties from the popup menu.
4. In the IMAP4 Properties window, select the Retrieval Settings tab, and then select Best body format from the Message MIME format drop-down list.
5. Click Apply and then OK to save your changes and dismiss the window.

To configure the message retrieval format at the mailbox level:

1. In the Exchange Management Console left navigation pane, select Recipient Configuration > Mailbox.
2. In the middle pane, right-click the mailbox you want to configure and select Properties from the popup menu.
3. In the Properties window, select the Mailbox Features tab, and right-click IMAP4.
4. In the IMAP4 Properties window, select Best body format from the drop-down list.
5. Click OK to close the IMAP4 Properties window, and then click Apply and then OK to save your changes and close the window.

Message Retrieval Format for Exchange 2013

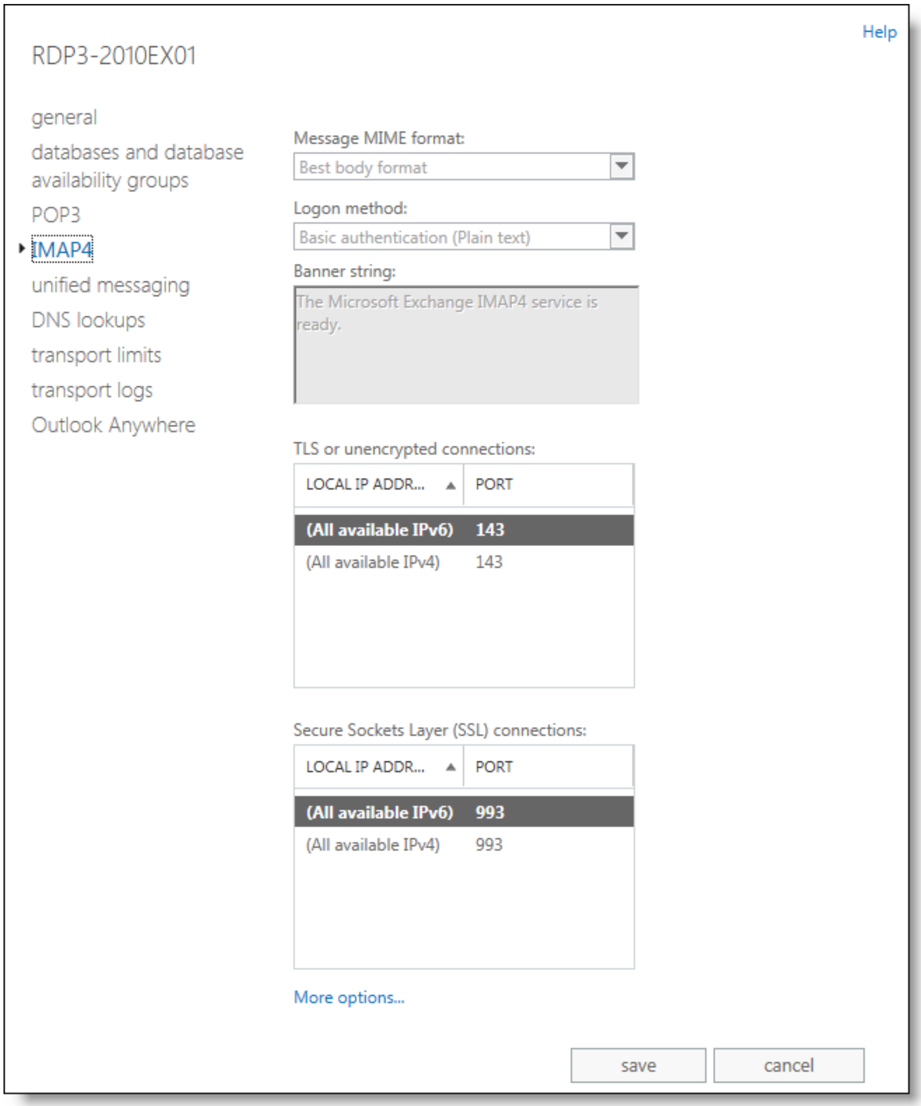
This can be done at the server and mailbox levels. See the Microsoft Technet article, “Configure POP3 and IMAP4 message retrieval format options” at http://technet.microsoft.com/en-us/library/aa997869(v=exchg.150).aspx.

To configure the message retrieval format at the server level:

1. In the Exchange Admin Center, select the servers node from the left pane, and then choose the servers tab.
2. Select the appropriate database server, and click Edit (the pencil).
3. Select IMAP4.

4. Verify that Best body format is selected in the Message MIME format field.

Figure 40. IMAP4 window.



RDP3-2010EX01

Message MIME format: Best body format

Logon method: Basic authentication (Plain text)

Banner string: The Microsoft Exchange IMAP4 service is ready.

TLS or unencrypted connections:

LOCAL IP ADDR...	PORT
(All available IPv6)	143
(All available IPv4)	143

Secure Sockets Layer (SSL) connections:

LOCAL IP ADDR...	PORT
(All available IPv6)	993
(All available IPv4)	993

5. Click save.

To configure the message retrieval format at the mailbox level:

- In the Exchange Management Shell, enter the following command:

```
Set-CASMailbox -Identity "<Agent E-Mail Mailbox>"
-ImapMessagesRetrievalMimeFormat BestBodyFormat
```

Configuring the Message Delivery Format

How you configure the message delivery format determines how Exchange delivers messages to external recipients. As described in Table 6 on page 85, messages in the MS-TNEF format contain a winmail.dat attachment. For Agent E-Mail to function properly, you must configure the message delivery format so that no winmail.dat attachment is included with outgoing messages.

This is done at the organizational level per remote domain.

> **NOTE:** The default remote domain is *.

To configure the message delivery format at the organizational level (Exchange 2007 and 2010):

1. In the Exchange Management Console left navigation pane, select Organization Configuration > Hub Transport.
2. In the middle pane, select the Remote Domains tab
3. Right-click the remote domain you want to configure and select Properties from the popup menu.
4. In the Properties window, select the Message Format tab, and then select Never use under the Exchange rich-text format heading.
5. Click Apply and then OK to save your changes and close the window.

To configure the message delivery format at the organizational level (Exchange 2013):

- In the Exchange Management Shell, enter the following command:

  ```
  Set-RemoteDomain * -TNEFEnabled $false
  ```

  This command disables MS-TNEF messages.

Testing Access to the Agent E-Mail Account

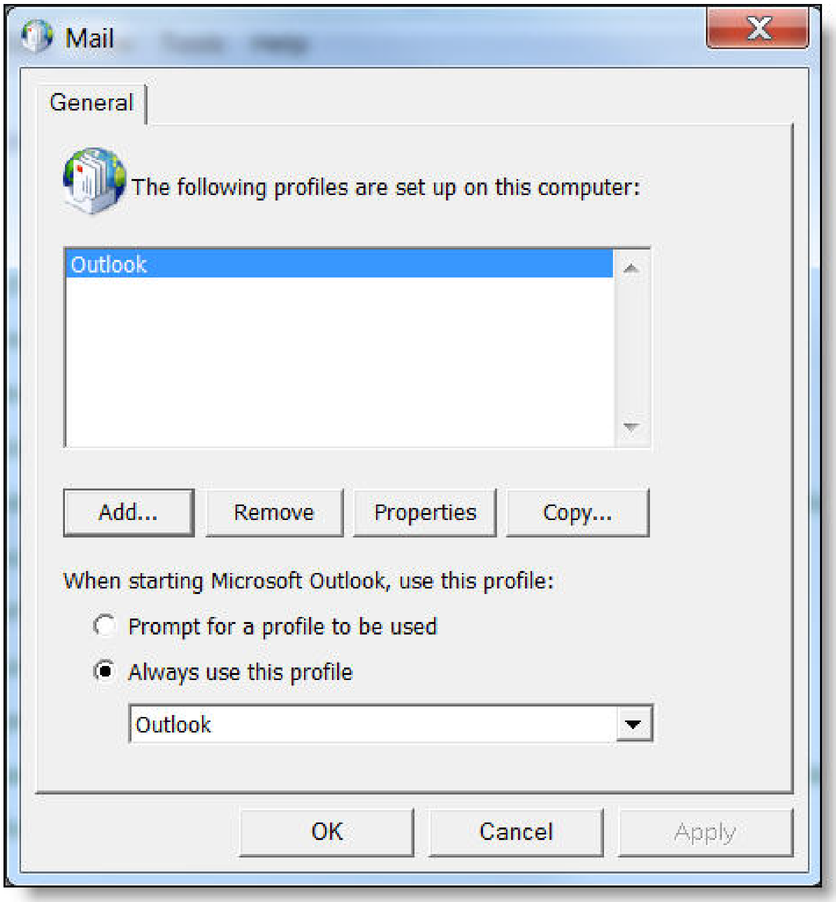
The new e-mail account can be accessed using an IMAP4-capable e-mail client, such as Microsoft Outlook 2010. Follow these steps to test access to the account.

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 41).

Figure 41. Mail Profiles window



The following profiles are set up on this computer:

Outlook

When starting Microsoft Outlook, use this profile:

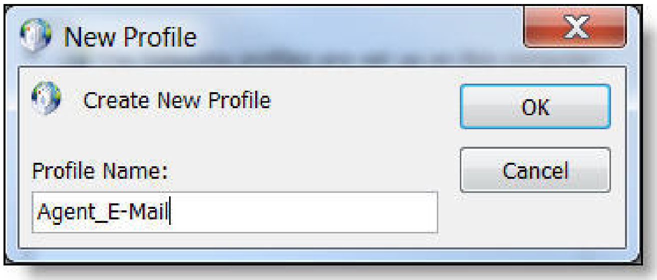
○ Prompt for a profile to be used

● Always use this profile

Outlook

3. Click Add.The New Profile dialog box appears (Figure 42).

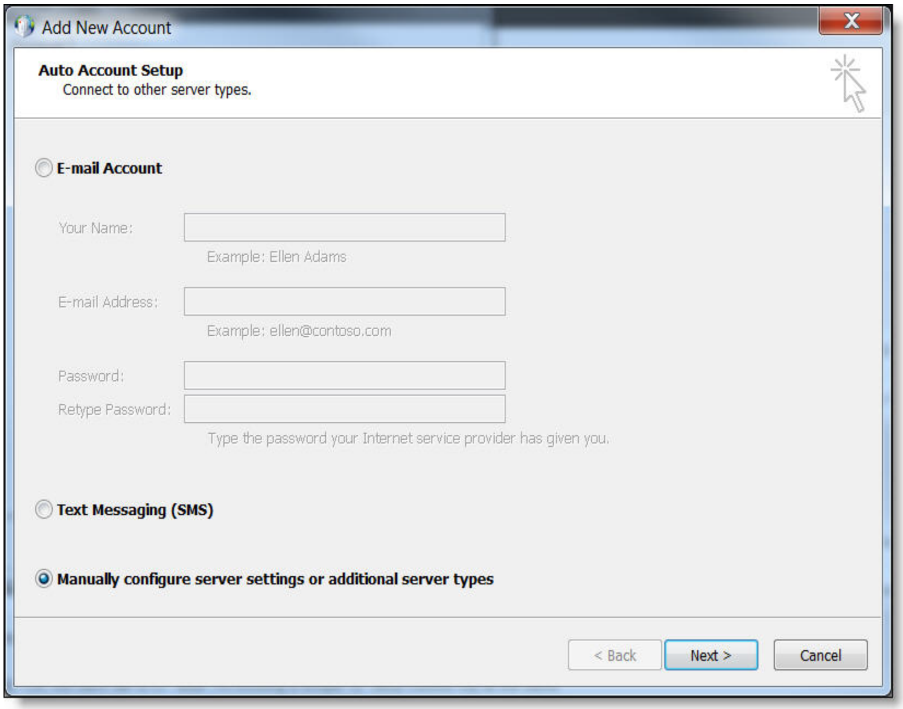
Figure 42. New Profile dialog box



Profile Name: Agent_E-Mail

4. Enter the name of the Agent E-Mail account and click OK. The Add New Account wizard appears (Figure 43).

Figure 43. Add New Account wizard window 1



Add New Account

Auto Account Setup
Connect to other server types.

○ **E-mail Account**

Your Name:
Example: Ellen Adams

E-mail Address:
Example: ellen@contoso.com

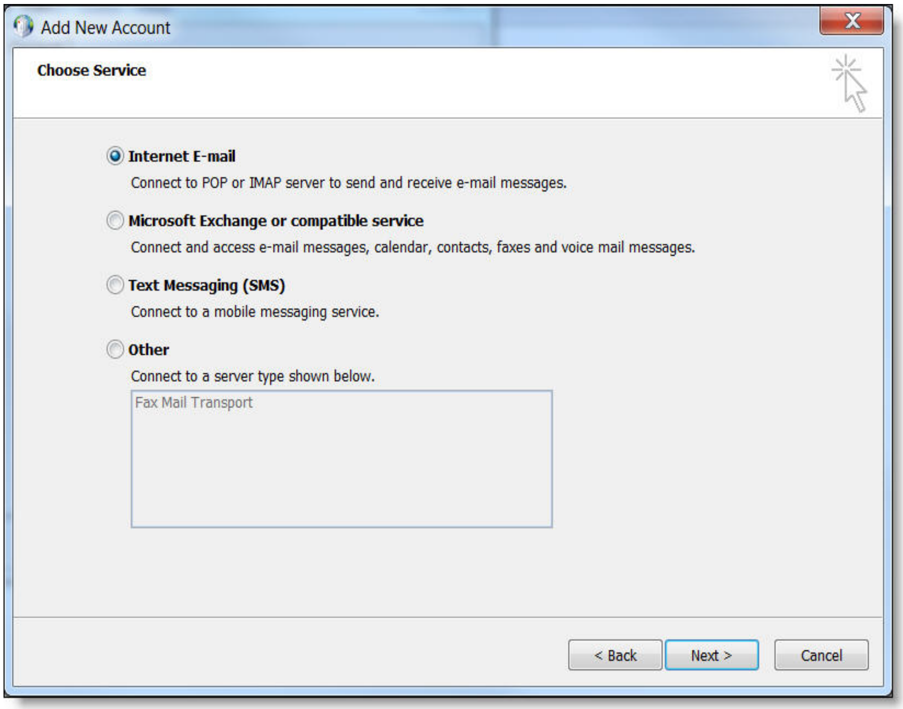
Password:
Retype Password:
Type the password your Internet service provider has given you.

○ **Text Messaging (SMS)**

● **Manually configure server settings or additional server types**

5. Select Manually configure server settings or additional server types and then click Next. The Choose Service window appears (Figure 44).

Figure 44. Add New Account wizard window 2



Add New Account

Choose Service

● Internet E-mail
Connect to POP or IMAP server to send and receive e-mail messages.

○ Microsoft Exchange or compatible service
Connect and access e-mail messages, calendar, contacts, faxes and voice mail messages.

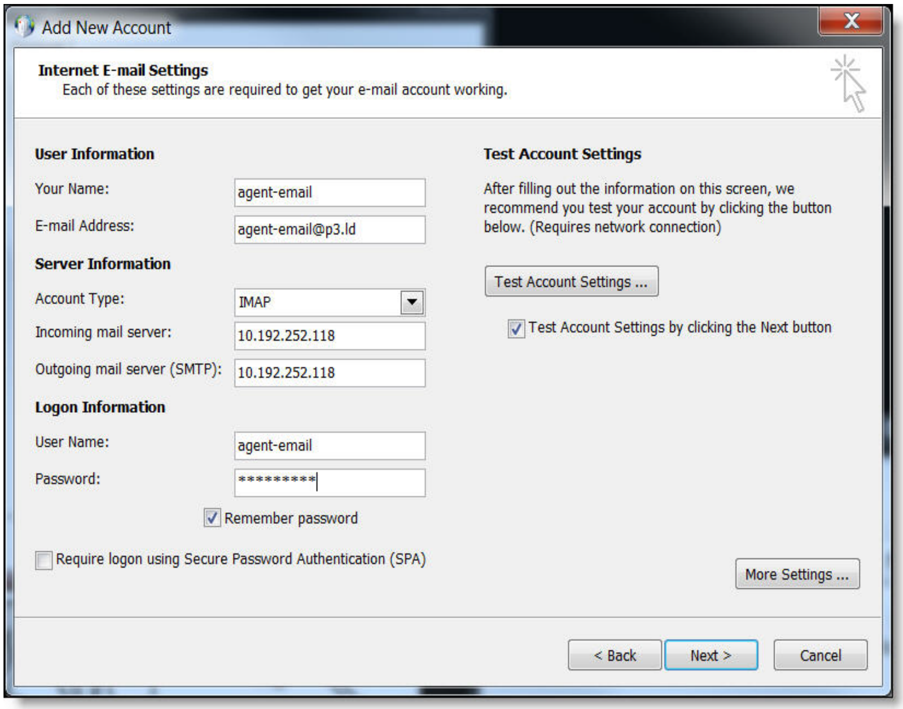
○ Text Messaging (SMS)
Connect to a mobile messaging service.

○ Other
Connect to a server type shown below.

Fax Mail Transport

6. Select Internet E-mail and then click Next. The Internet E-Mail Settings window appears (Figure 45).

Figure 45. Add New Account wizard window 3



Add New Account

Internet E-mail Settings

Each of these settings are required to get your e-mail account working.

User Information

Your Name: agent-email

E-mail Address: agent-email@p3.ld

Server Information

Account Type: IMAP

Incoming mail server: 10.192.252.118

Outgoing mail server (SMTP): 10.192.252.118

Logon Information

User Name: agent-email

Password: *********

☑ Remember password

□ Require logon using Secure Password Authentication (SPA)

Test Account Settings

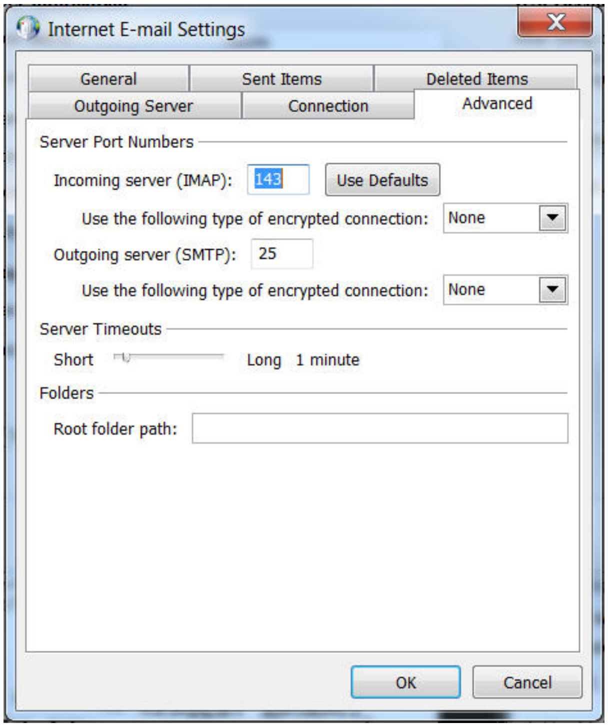
After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)

☑ Test Account Settings by clicking the Next button

7. Enter the required information for the Agent E-Mail account. In the Account Type field, select IMAP from the drop down list.

8. Click More Settings. If you have changed the SMTP and/or IMAP port numbers to something other than the defaults, configure the information on the Advanced tab (Figure 46).

Figure 46. More Settings - Advanced tab



Server Port Numbers

Incoming server (IMAP): 143

Use the following type of encrypted connection: None

Outgoing server (SMTP): 25

Use the following type of encrypted connection: None

Server Timeouts

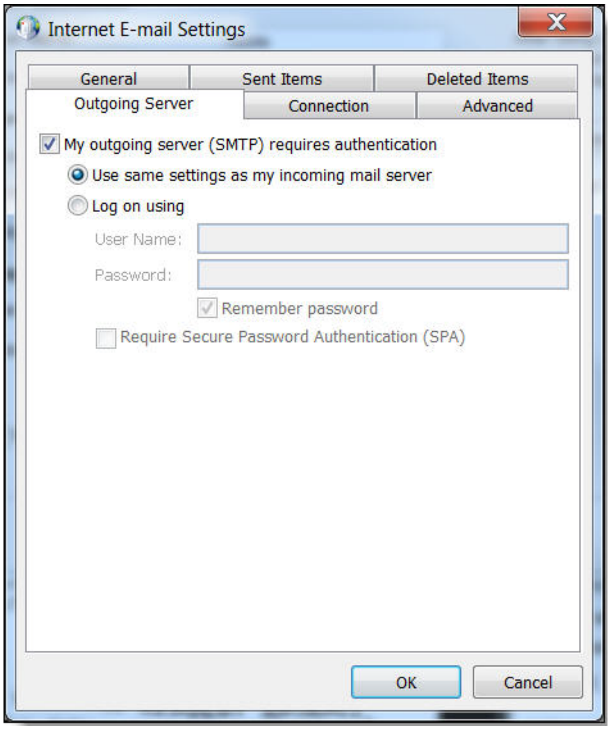
Short Long 1 minute

Folders

Root folder path:

9. On the Outgoing Server tab (Figure 47), select My outgoing server (SMTP) requires authentication and Use same settings as my incoming mail server. Click OK.

Figure 47. More Settings - Outgoing Server tab



☑ My outgoing server (SMTP) requires authentication

● Use same settings as my incoming mail server

○ Log on using

User Name:

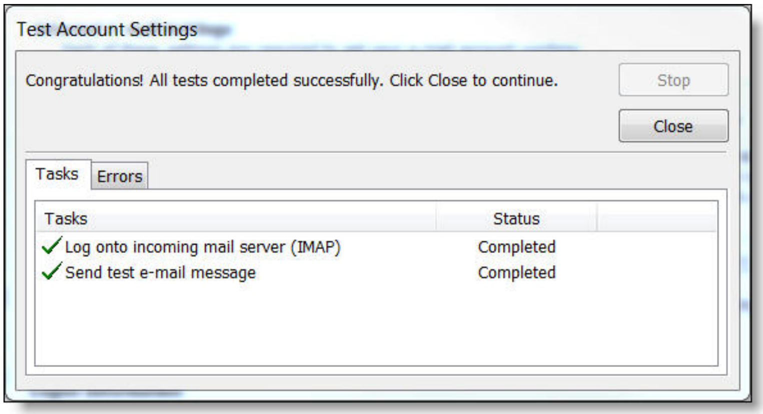
Password:

☑ Remember password

□ Require Secure Password Authentication (SPA)

10. On the Internet E-mail Settings window, click Next. The Test Account Settings window appears (Figure 48).

Figure 48. Test Account Settings window

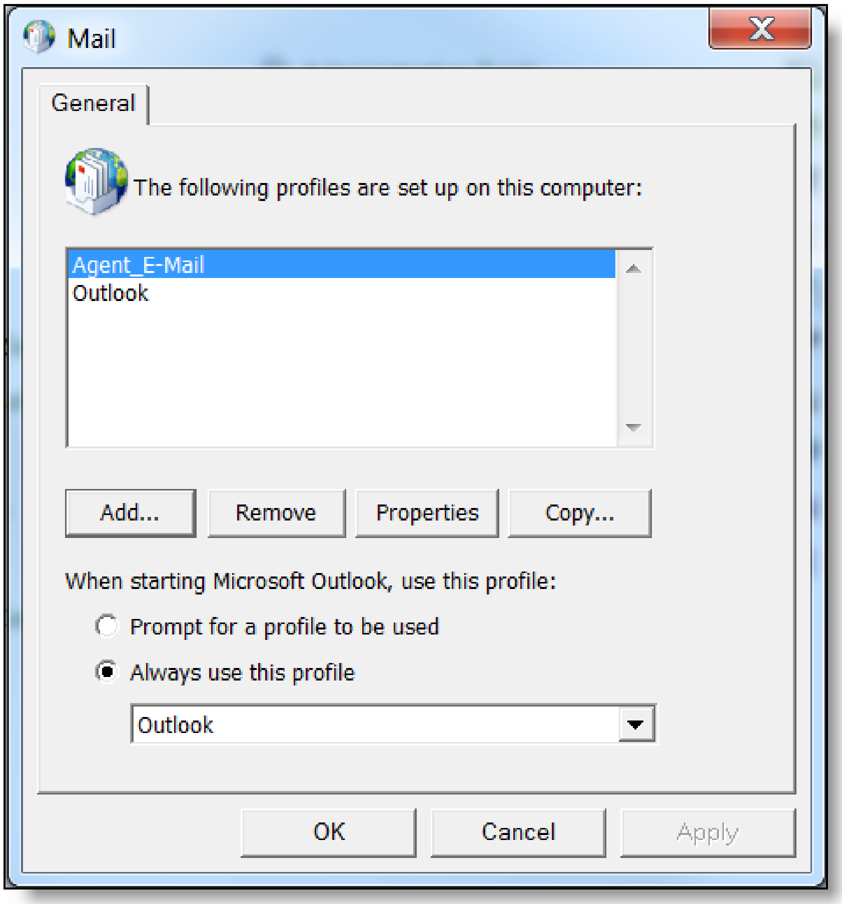


Congratulations! All tests completed successfully. Click Close to continue.

Tasks	Status
✓ Log onto incoming mail server (IMAP)	Completed
✓ Send test e-mail message	Completed

11. Click Close and then Finish to create the new e-mail account profile. The new profile is now listed on the Mail window (Figure 49).

Figure 49. Mail window displaying the new profile



The following profiles are set up on this computer:

Agent_E-Mail
Outlook

When starting Microsoft Outlook, use this profile:

○ Prompt for a profile to be used

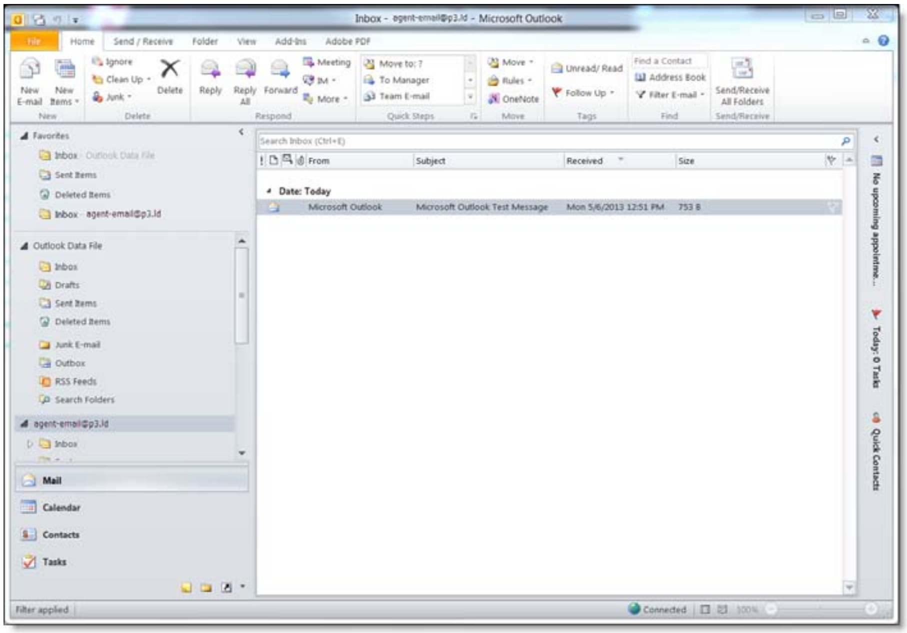
● Always use this profile

Outlook

12. 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.

13. MS Outlook is displayed. The Outlook profile is configured with multiple inboxes, because IMAP accounts use a separate inbox from that of the default Outlook inbox. The IMAP account for Agent E-Mail, which is highlighted in Figure 50, is listed below the default Outlook inbox. Note that by default Outlook subscribes to two Agent E-Mail folders, Inbox and Junk E-Mail.

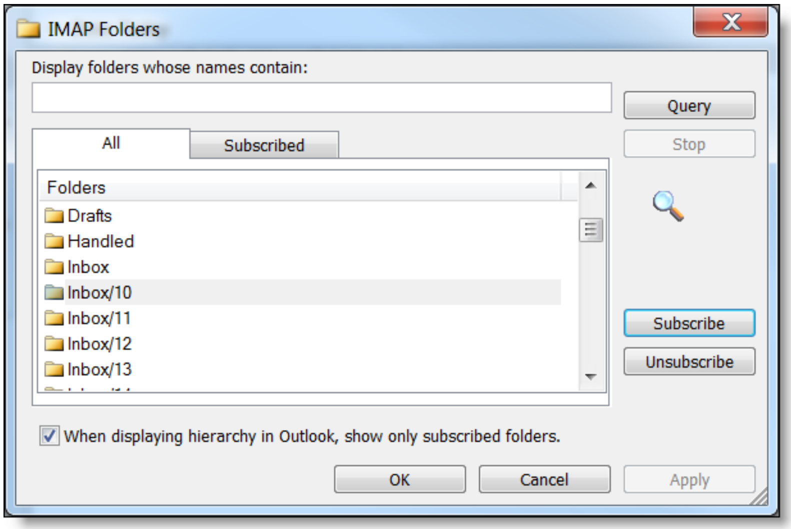
Figure 50. MS Outlook Inbox



Microsoft Outlook | Microsoft Outlook Test Message | Mon 5/6/2013 12:51 PM | 753 B

14. To subscribe to additional mailbox folders, right-click the account and choose IMAP folders from the popup menu. The IMAP folders dialog appears (Figure 51). For more information about mailbox folders, see "Agent E-Mail Microsoft Exchange Mailbox Folders" on page 33.

Figure 51. IMAP Folders dialog



☑ When displaying hierarchy in Outlook, show only subscribed folders.

15. Click the Query button to display all available folders. Select the folder to which you want to subscribe and then click the Subscribe button.

16. Click OK when you are finished subscribing to folders.

Message Throttling Policies in Exchange

Exchange employs message throttling to ensure optimal performance across all users of the system. The default throttling policies are too restrictive because Agent E-Mail uses a single MS Exchange user for all operations. The server and all agents log into Exchange under the same user account. In order for Agent E-Mail to function properly, you must reset the throttling policies. For more information about throttling policies, see *Understanding Message Throttling* at:

http://technet.microsoft.com/en-us/library/bb232205.aspx

IMAP Throttling Policies

By default, the maximum number of IMAP connections per user in Exchange is 10. Every agent and the Agent E-Mail service uses the same user ID so this number is far too low. It is recommended that you change the number of IMAP connections to 2,400.

IMAP throttling policies must be configured at the server level.

To configure the IMAP throttling policies at the server level:

- In the Exchange Management Shell, enter the following command:

  ```
  Set-ImapSettings -MaxCommandSize 10240 -MaxConnectionFromSingleIP 2000
  -MaxConnections 2400 -MaxConnectionsPerUser 2400
  ```

SMTP Throttling Policies

By default, some of the SMTP connection limits set by Exchange may be too restrictive for Agent E-Mail. It is recommended you adjust these limits using the procedures below on a per domain basis in order for Agent E-Mail to work optimally.

You must configure the SMTP throttling policies at the server level and the receive connector level.

To configure the SMTP throttling policies at the server level:

1. In the Exchange Management Shell, enter the following cmdlet to retrieve the transport server name that Unified CCX Agent E-Mail uses:

   ```
   Get-TransportServer
   ```

2. Enter the following command:

   ```
   Set-TransportServer -identity "<Transport Server Name>"
   -MaxConcurrentMailboxDeliveries 30 -MaxConcurrentMailboxSubmissions 30
   -MaxConnectionRatePerMinute 1200 -MaxOutboundConnections 1000
   -MaxPerDomainOutboundConnections 1000
   -PickupDirectoryMaxMessagesPerMinute 100
   ```

   where <Transport Server Name> is the transport server name retrieved in Step 1.

You must configure the transport throttling policies at the receive connector level for every applicable receive connector that Agent E-Mail uses.

To configure the SMTP throttling policies at the receive connector level in Exchange 2007 and 2010:

1. In the Exchange Management Shell, enter the following cmdlet to find the name for each receive connector that Unified CCX Agent E-Mail uses:

   ```
   Get-ReceiveConnector
   ```

2. Enter the following command:

   ```
   Set-ReceiveConnector -identity "<Receive Connector Name>"
   -MaxInboundConnection 5000 -MessageRateLimit 250
   -MaxInboundConnectionPercentagePerSource 5 -MaxInboundConnectionPerSource
   250
   ```

   where <Receive Connector Name> is a receive connector name retrieved in Step 1.

3. Repeat Step 2 for each applicable receive connector name.

Client Throttling Policies

Exchange 2010 and 2013 use a default client throttling policy that adversely affects the way that Agent E-Mail functions. In order for Agent E-Mail to function properly, you must create a new client throttling policy and apply it to each mailbox. For more information, see *Understanding Client Throttling Policies* at:

http://technet.microsoft.com/en-us/library/dd297964.aspx

NOTE: Client throttling policies are only used by Exchange 2010 and 2013. The following procedures do not apply to Exchange 2007.

Exchange 2010 Service Packs 1 and 2 have additional values that are not present in the base release. As a result, there are different throttling settings required for the base release and Service Packs 1 and 2.

To create a new throttling policy and apply it to a mailbox:

1. In Exchange Management Shell, enter the following command:

   ```
   New-ThrottlingPolicy -name "<Policy Name>"
   ```

   where <Policy Name> is the name of the new throttling policy.

2. Enter the following command:

   For Exchange 2010 base release:

   ```
   Set-ThrottlingPolicy -identity “<Policy Name>” -IMAPMaxConcurrency $null
   -IMAPPercentTimeInAD $null -IMAPPercentTimeInCAS $null
   -IMAPPercentTimeInMailboxRPC $null -RCAMaxConcurrency $null
   ```

```
-RCAPercentTimeInAD $null -RCAPercentTimeInCAS $null
-RCAPercentTimeInMailboxRPC $null -MessageRateLimit $null
-RecipientRateLimit $null -CPUStartPercent $null
```

For Exchange 2010 SP1, SP2, and SP3:

```
Set-ThrottlingPolicy -identity “<Policy Name>” -IMAPMaxConcurrency $null
-IMAPPercentTimeInAD $null -IMAPPercentTimeInCAS $null
-IMAPPercentTimeInMailboxRPC $null -RCAMaxConcurrency $null
-RCAPercentTimeInAD $null -RCAPercentTimeInCAS $null
-RCAPercentTimeInMailboxRPC $null -CPAMaxConcurrency $null
-CPAPercentTimeInCAS $null -CPAPercentTimeInMailboxRPC $null
-MessageRateLimit $null -RecipientRateLimit $null -CPUStartPercent $null
```

For Exchange 2013 SP1 and newer:

```
Set-ThrottlingPolicy -identity "<Policy Name>" -IMAPMaxConcurrency
Unlimited -ImapMaxBurst Unlimited -ImapRechargeRate Unlimited
-ImapCutoffBalance Unlimited -RCAMaxConcurrency Unlimited -RcaMaxBurst
Unlimited -RcaRechargeRate Unlimited -RcaCutoffBalance Unlimited
-CPAMaxConcurrency Unlimited -CpaMaxBurst Unlimited -CpaRechargeRate
Unlimited -CpaCutoffBalance Unlimited -MessageRateLimit Unlimited
-RecipientRateLimit Unlimited
```

3. Enter the following command:

   ```
   Set-Mailbox -Identity "<Mailbox Name>" -ThrottlingPolicy "<Policy Name>"
   ```

   where <Mailbox Name> is the name of the mailbox to which you want to apply the new throttling policy.

Other Message Throttling Policies

Agent E-Mail uses IMAP. Exchange also opens a MAPI session when an IMAP session is open, which can cause MAPI related throttling limits to impact Agent E-Mail performance. In order to avoid this, you must properly configure these limits. For more information, see *Exchange Store Limits* at:

http://technet.microsoft.com/en-us/library/ff477612.aspx

Granting the View Information Store Status Permission

First you must grant the View Information Store status permission to the account used for Agent E-Mail. For more background information, refer to the following article by Microsoft Support (Article ID: 842022) at:

http://support.microsoft.com/?kbid=842022

To grant View Information Store status permissions:

- In Exchange Management Shell, enter the following command:

  ```
  Get-OrganizationConfig | Add-ADPermission -user "<Mailbox Name>"
  -extendedrights "View Information Store status"
  ```

where, <Mailbox Name> is the name of the mailbox to which you want to apply the new throttling policy.

Modifying the Session Limits Registry

To ensure no MAPI limits affect Agent E-Mail you should also make the following registry modifications.

It is recommended that you back up your registry before you perform the following procedures. For more information, refer to the following article by Microsoft Support (Article ID: 322756) on backing up your registry, at:

http://support.microsoft.com/kb/322756

To perform the registry modification to speed up message routing:

1. Select the Start menu, then select Run.
2. In the Open field, enter regedit, and then click OK.
3. Select HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > MSExchangeIS > ParametersSystem.
4. If the Maximum Allowed Sessions Per User setting does not exist, do the following:
    a. Choose the Edit menu > New > DWORD Value.
    b. Enter Maximum Allowed Sessions Per User as the entry name.
5. Right-click Maximum Allowed Sessions Per User and then select Modify from the popup menu.
6. Click Decimal, enter 2,400 in the Value data box, and then click OK.
7. If the Maximum Allowed Service Sessions Per User setting does not exist, do the following:
    a. Choose the Edit menu > New > DWORD Value.
    b. Enter Maximum Allowed Service Sessions Per User as the entry name.
8. Right-click Maximum Allowed Service Sessions Per User and then select Modify from the popup menu.
9. Click Decimal, enter 2,400 in the Value data box, and then click OK.
10. If the Maximum Allowed Concurrent Exchange Sessions Per Service setting does not exist, do the following:
    a. Choose the Edit menu > New > DWORD Value.
    b. Enter Maximum Allowed Concurrent Exchange Sessions Per Service as the entry name.
11. Right-click Maximum Allowed Concurrent Exchange Sessions Per Service and then select Modify from the popup menu.
12. Click Decimal, enter 2,400 in the Value data box, and then click OK.

13. Exit the Registry Editor.
14. Select the Start menu, then select Run.
15. In the Open field, enter services.msc, and then click OK.
16. Select the Microsoft Exchange Information Store service, and then select Restart Service.

There are other settings within Exchange that define throttling limits that should not affect Agent E-Mail functionality at their default values. If you experience performance issues with Agent E-Mail, refer to the *Cisco CAD Troubleshooting Guide* for possible solutions to throttling related problems.

Installing CAD 10.5

4

Upgrade Notes

General

- It is recommended that after upgrading CAD, you check to ensure that all CAD services are started.
- Enterprise data fields and field layouts are created and customized in Cisco Desktop Administrator (Services Configuration > Enterprise Data > Fields). If you edited default Enterprise data fields or layouts, then your changes will be lost after an upgrade, except for the fields Call Variable 1–10. The default fields will revert back and must be re-configured after an upgrade. However, any custom fields that you created will remain after an upgrade.
- Team messages stored in the previous version of Supervisor Desktop are lost after upgrading to a new version of CAD.
- After an upgrade, it is recommended that you check any shortcut keys that might appear in your macros against the shortcut keys listed in the desktop client user guides, as they might have changed. Update your macros accordingly.
- After upgrading Cisco Unified Presence, you might need to add the CAD client type to Unified Presence Administration again. The CAD client type does not carry over. For more information, refer to the “Configuring the CAD Client Type” section of the *Cisco Desktop Administrator User Guide*.

Upgrading from CAD 8.0(2), 8.5(1), or 9.0(1) to CAD 10.5(1)

- After upgrading, you must reboot both high availability servers.
- If you upgrade and then roll back to the original software release, all e-mail historical data is lost.

- During an upgrade, do not run the Cisco Unified CCX Desktop Client Configuration tool until both nodes have been upgraded. If you run the Unified CCX Desktop Client Configuration tool before the standby node has been upgraded, CAD desktop applications will not be automatically updated. The CAD desktop applications will not be configured correctly until the standby node has been updated.

  If an error occurs and the standby node fails to upgrade, run the Unified CCX Desktop Client Configuration tool on the active node so that you have service. When the standby node has been successfully upgraded, run the Unified CCX Desktop Client Configuration tool again. This might require you to uninstall and reinstall CAD desktop applications to correct registry entries.

Standard Bundle Customers

It is important to remember that if you are upgrading to CAD 10.5, the 10.5 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.

CAD 10.5 Desktop Client Installation

Configuring CAD Desktop Client MSI Files

Because the CAD services are installed on a Linux platform, it is necessary to run one of two client MSI configuration tools in order to configure the Windows-based CAD client MSIs with the correct configuration information. The tool to use depends on when the MSIs are created:

- Run the Preconfiguration tool before the Unified CCX server is installed
- Run the CCX Desktop Client Configuration tool after the Unified CCX server is installed

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

The client MSI configuration tools configure the CAD client MSIs and, depending on which tool is run, either save them to the local machine or upload them to the Unified CCX server.

Run the Preconfiguration tool if you want to create client MSIs before the Unified CCX servers have been installed.

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
- After changing the IP address of one or more nodes of Unified CCX
- After changing the CAD Language that you want used in the agent and supervisor desktops
- 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 configures the CAD client MSIs, uploads them to the Unified CCX server, cleans up the created temporary files, and terminates. You must run the Unified CCX Desktop Client Configuration tool using an account with local administrator privileges in order for the process to complete properly.

> **NOTE:** The Windows PC on which you run the Unified CCX Desktop Client Configuration tool must have version 1.7.0 of the JRE plug-in. Only JRE 1.7 Update 51 is supported.

To run the Unified CCX Desktop Client Configuration tool:

1. In the web browser, access https://<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 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.

Running the Preconfiguration Tool

The Preconfiguration tool is located on the CAD 10.5 installation DVD. Run this tool if client MSIs are needed before the Unified CCX server is installed.

To run the Preconfiguration tool:

1. On the CAD 10.5 installation DVD, navigate to the Installer folder.
2. Copy the Installer folder and all its contents to any location on a Windows PC.

3. In the Installer folder, 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)
    - License type (Standard, Enhanced, or Premium)
5. The Preconfiguration tool runs and puts the configured MSI files in the Installer folder. The files created are:
    - Cisco Agent Desktop.msi
    - Cisco Supervisor Desktop.msi
    - Cisco Desktop Administrator.msi

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

Client MSI Configuration Tools and Automated Deployment Packages

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 tool, create the automated deployment packages in accordance with the requirements listed in the section, "Using Automated Package Distribution Tools" on page 112.

Before You Install CAD Desktop Client Applications

Before you install a CAD desktop client 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 Agent E-Mail in Agent Desktop, 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, Agent Desktop will function normally except for Agent E-Mail, which will be disabled until the correct version of JRE is installed. Agent Desktop will prompt the user to install the correct JRE version.

Upgrading From an Earlier Version

Over-the-top upgrades (installing the new version over the older version) from CAD 6.4(2), 6.6(1), 8.0(1), 8.5(1), 9.0(1), and 10.0(1) to CAD 10.5 are supported.

Upgrading from any other version of CAD requires that the older version of CAD is uninstalled before CAD 10.5 is installed.

Adding Desktop Client Applications After Initial Setup

You can install additional CAD desktop client applications on a workstation that already hosts a CAD desktop application (for example, adding Supervisor Desktop to a workstation that already has Desktop Administrator installed).

Note that the install for Supervisor Desktop installs both Supervisor Desktop and Agent Desktop. If the client desktop already hosts Agent Desktop and you want to install Supervisor Desktop, you must uninstall the existing instance of Agent Desktop first.

Methods for Installing CAD Desktop Applications

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

- The desktop client applications can be “pushed” to the Agent Desktops using an automated package distribution tool.
- The user can install the desktop client application from the Unified CCX Administration web application.

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

Installing CAD Desktop Client Applications

The Unified CCX Administrator download page includes installation files for all CAD desktop client 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 https://<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 https://<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 https://<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, the application will not install.

4. Click Run.

5. Follow the instructions in the InstallShield Wizard to complete installing the selected application.
6. Just before the final InstallShield Wizard window is displayed, a command window opens, displaying the message, “This window is part of the <installer name> installation process. Do not close this window, it will self terminate when finished.” Ignore the command window. Click Finish on the InstallShield Wizard to complete the installation process.

   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.

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 107.

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 MSDN article, “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

Windows 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.

Automated Updates

If enabled, CAD automatically updates all instances of the CAD desktop client applications to a newer version if the services have been updated. By default, the automatic updates are enabled for the CAD desktop client applications.

Every time a desktop client 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 exist, and the automatic updates are enabled in Desktop Administrator, the application automatically runs the update process.

NOTE: Automatic software update requires either administrative or elevated (system) privileges.

The automated updates can be configured in Desktop Administrator. See the *Cisco Desktop Administrator User Guide* for more information on enabling/disabling automatic updates. An administrator must update the software to match the version on the server so that the application functions properly when the client logs in.

When an update is available, the user sees a dialog box notifying the user that the desktop application will be updated. The user 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 sees a final dialog box that the update is complete, and which applications were updated. If the user has more than one CAD desktop client application installed, they will all have been updated.

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

When the user clicks OK to close the dialog box, any CAD desktop client 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 webpage.

> **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 client applications will not automatically upgrade when the user logs into the new server. The user must shut down CAD desktop client applications and start them again for the automatic upgrade to take place.

Downgrading CAD Applications

CAD desktop client applications can be downgraded to the earlier version if required. If a service downgrade occurs, the CAD desktop applications are automatically downgraded to the older version. The existing CAD applications do not have to be manually uninstalled to install the older version.

> **NOTE:** Automatic software downgrade fails if the user does not have either administrative or elevated (system) privileges. In this case, an administrator must manually downgrade the existing application to the older version.

Java Runtime Environment

Every time the Premium edition of Agent Desktop that uses Agent E-Mail 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 Desktop Client Applications

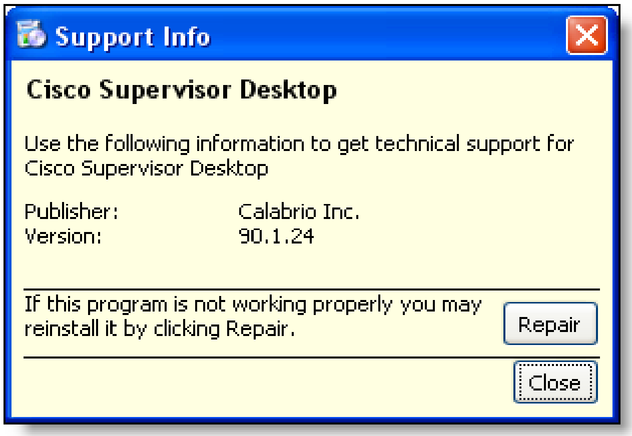
If one of the CAD desktop client applications is not functioning properly, you can use the Repair function to reinstall it. If you do repair a CAD desktop application, you must also repair any service release that has been installed.

The steps to repair a CAD desktop client application differ slightly between Windows XP systems and Windows 7 systems.

To repair a CAD client application:

1. On the client desktop, navigate to Windows Control Panel.
   - On a Windows XP system, start the Add or Remove Programs tool.
   - On a Windows 7 systems, start the Programs and Features 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 Supervisor Desktop”).
3. On a Windows XP System, click the Click here for support information link to display the Support Info dialog box (Figure 52). On a Windows 7 systems, this information is already displayed (Figure 53).

Figure 52. Windows XP Only: Support Info dialog box



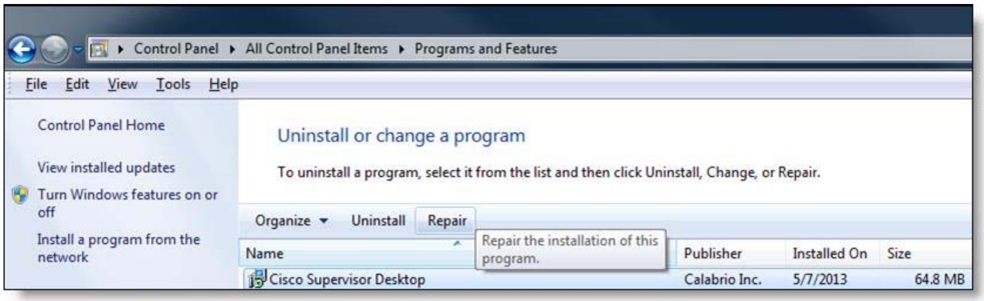
Cisco Supervisor Desktop

Use the following information to get technical support for Cisco Supervisor Desktop

Publisher: Calabrio Inc.
Version: 90.1.24

If this program is not working properly you may reinstall it by clicking Repair.

Figure 53. Windows 7 Only: Programs and Features



Control Panel ▸ All Control Panel Items ▸ Programs and Features
File Edit View Tools Help
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Organize ▾
Uninstall
Repair
Name
Publisher
Installed On
Size

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Repair the installation of this program.

Name	Publisher	Installed On	Size
Cisco Supervisor Desktop	Calabrio Inc.	5/7/2013	64.8 MB

4. Click Repair. The program reinstalls and displays the Location of Unified CCX server(s) dialog box (Figure 54 on page 119).
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 Work Flow 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 55 on page 120).
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 Server Configuration

CAD Configuration Setup

CAD Configuration Setup is used to configure the CAD base services. After initial installation, you can change your settings by launching CAD Configuration Setup. It can be launched from two different locations. However, the configuration options vary. You can change the configuration settings using the following methods:

- From the Desktop Work Flow Administrator menu bar (Setup > Configure Systems) or by running PostInstall.exe (located in the folder ...\Program Files\Cisco\Desktop\bin on any CAD desktop computer).

  The CAD Configuration Setup utility is launched as an application interface that enables you to do the following:

  - Change the location of the primary (and optional secondary) Cisco Unified CCX server
  - Change IP address of the network adaptor for network packet sniffing
  - Indicate if the client desktop application is running on a thin client environment

- Access CAD Configuration Setup window in Desktop Administrator. See “CAD Configuration Setup” in the *Cisco Desktop Administrator User Guide*.

  The CAD Configuration Setup window is launched as a browser page in Desktop Administrator that enables you to configure the following settings:

  - Enable/disable CAD automatic updates
  - Change the IP address of the CAD services
  - Change the login credentials for the BIPPA service

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 reinstalls the client desktop and makes 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

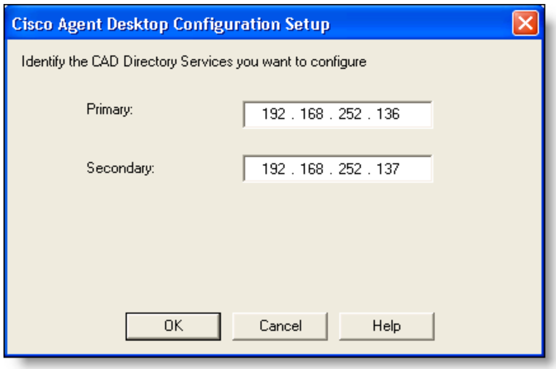
To modify configuration data in client:

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.

   CAD Configuration Setup starts and displays the Location of Unified CCX server dialog box (Figure 54).

   Figure 54. Cisco Agent Desktop Directory Services dialog box

   Cisco Agent Desktop Configuration Setup

   Identify the CAD Directory Services you want to configure

   Primary: 192 . 168 . 252 . 136

   Secondary: 192 . 168 . 252 . 137

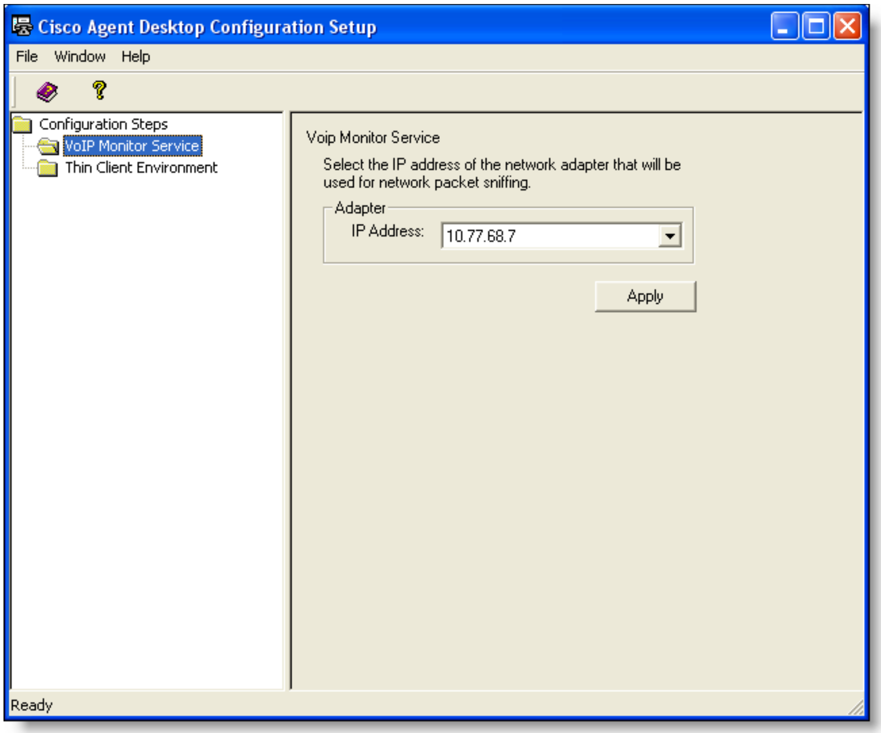
2. Ensure that the correct primary (and optional secondary) Unified CCX server IP address is entered, and then click OK.

   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 55).

Figure 55. CAD Configuration Setup



Voip Monitor Service

Select the IP address of the network adapter that will be used for network packet sniffing.

Adapter

IP Address: 10.77.68.7

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 and Shift+F6 to switch between the left and right pane.
4. When you are done making your changes, choose File > Exit from the menu or click X to close the window.
5. Stop and restart the desktop application for the change to go into effect.

Changing Settings with CAD Configuration Setup

Table 7 lists where you must access CAD Configuration Setup to change the desired setting.

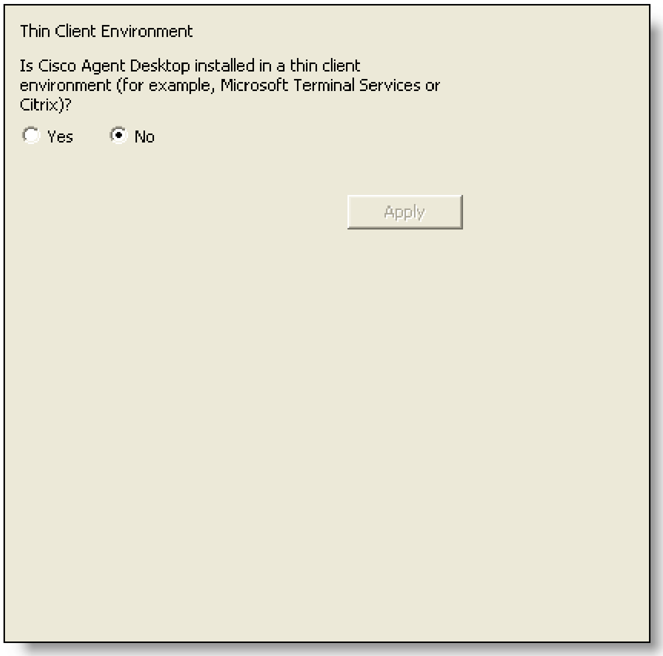
Table 7. CAD Configuration Setup configured as per host computer

Step Name	CAD and CSD[1]	CDA
Thin Client Environment (page 121)	×	
VoIP Monitor Service (page 122)	×	
Automatic Updates (page 122)		×
Services IP Address (page 123)		×
BIPPA User Login (page 123)		×
Reset Password (page 124)		×

[1] Header key: CAD—Cisco Agent Desktop, CSD—Cisco Supervisor Desktop; CDA—Cisco Desktop Administrator

Thin Client Environment

Figure 56. Thin Client Environment



Thin Client Environment

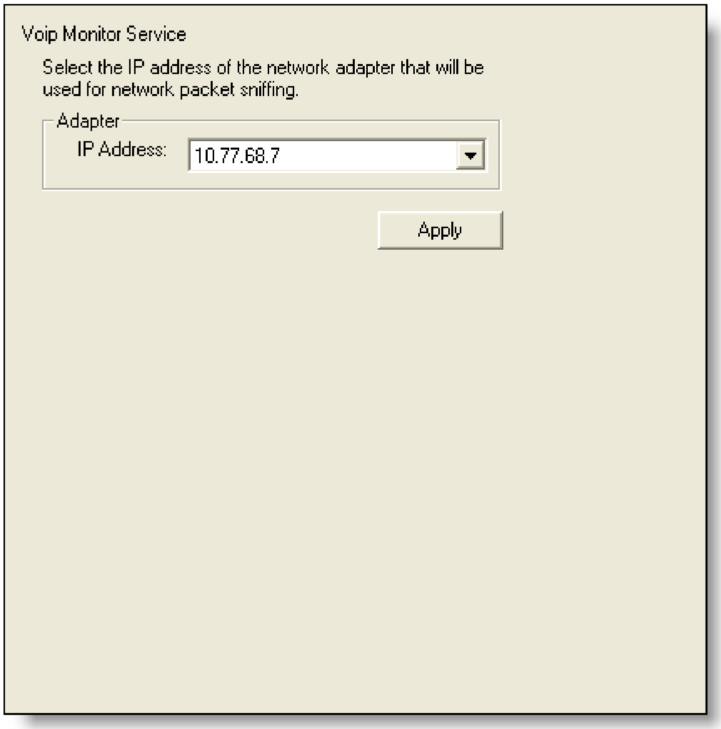
Is Cisco Agent Desktop installed in a thin client environment (for example, Microsoft Terminal Services or Citrix)?

○ Yes ● No

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

VoIP Monitor Service

Figure 57. VoIP Monitor Service



Voip Monitor Service

Select the IP address of the network adapter that will be used for network packet sniffing.

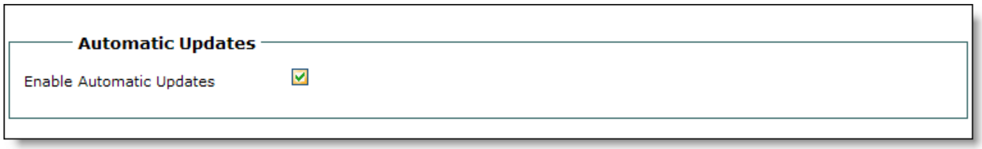
Adapter

IP Address: 10.77.68.7

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.

Automatic Updates

Figure 58. Automatic Updates



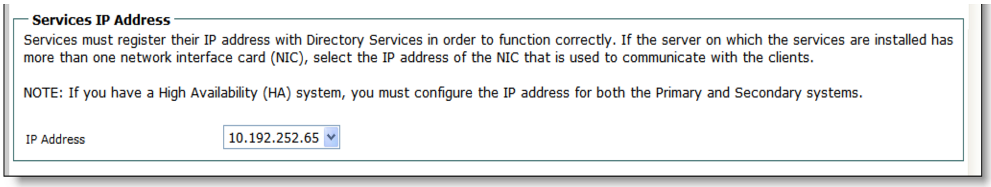
Automatic Updates

Enable Automatic Updates ☑

Select this check box to allow the CAD desktop applications to update automatically. By default, automatic update is enabled for all the CAD applications.

Services IP Address

Figure 59. Services IP Address



Services IP Address

Services must register their IP address with Directory Services in order to function correctly. If the server on which the services are installed has more than one network interface card (NIC), select the IP address of the NIC that is used to communicate with the clients.

NOTE: If you have a High Availability (HA) system, you must configure the IP address for both the Primary and Secondary systems.

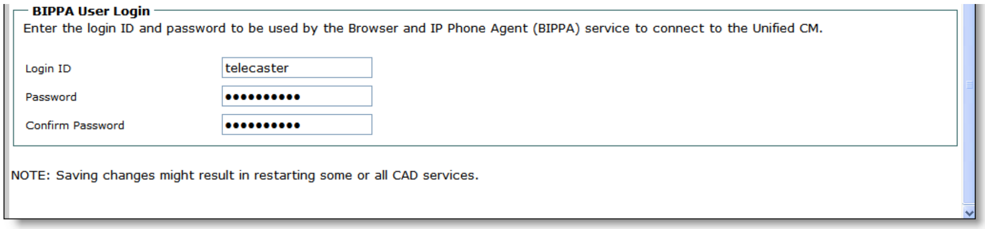
IP Address: 10.192.252.65

From Desktop Administrator, choose CAD Configuration Setup and scroll to the Services IP Address section (Figure 59):

- 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 60. BIPPA User Login



BIPPA User Login

Enter the login ID and password to be used by the Browser and IP Phone Agent (BIPPA) service to connect to the Unified CM.

Login ID: telecaster

Password: ••••••••••

Confirm Password: ••••••••••

NOTE: Saving changes might result in restarting some or all CAD services.

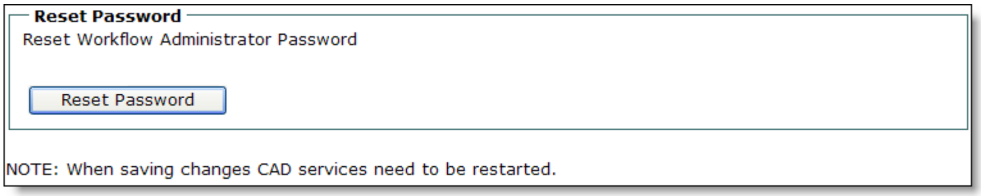
In order to connect to the Unified CM, the BIPPA service must have a login ID and password. This login ID and password are also set up in Unified CM (see "Configuring IP Phones" on page 126). You can complete these fields in the BIPPA User Login section (Figure 60) before setting up the user in Unified 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.

Reset Password

Figure 61. Reset Password



Reset Password

Reset Workflow Administrator Password

NOTE: When saving changes CAD services need to be restarted.

Click Reset Password to clear the password set for accessing Desktop Work Flow Administrator.

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 instructions, refer to 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

Configuring IP Phones for Cisco IP Phone Agent

After all IPPA 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 IPPA agent phone.
3. Create an application user named “telecaster” with “telecaster” as the password (or whatever BIPPA user ID and password was specified in CAD Configuration Setup).
4. Assign the telecaster application user to all the IPPA agent phones.

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 with 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 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 Services 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 123 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 List Application 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 Application User. The Find and List Application Users page appears.
2. Click Find to display a list of all application users.
3. From the list of search results, select the Unified CM user. The Application User Configuration page appears. (This page also appears when you click Save after creating the new Unified CM user with the previous procedure.)
4. In the Permissions Information section, click Add to Access Control Group. The Find and List Access Control Groups window appears.
5. Click Find to display a list of all access control groups. Select the Standard CTI Enabled check box, and then click Add Selected.
6. Click Save. 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).

Exporting Recordings From CAD

Recordings made by supervisors are archived using the RAW format as voice data packets, and can only be reviewed using the Supervisor Record Viewer. If you want to export recordings from CAD and convert them to WAV format so that they can be reviewed using other media players, you can use either of two methods:

- In Supervisor Record Viewer, use the Play and Save function (for more information, see the *Cisco Supervisor Desktop User Guide*).
- From a machine on which Desktop Work Flow Administrator is installed, download recordings from the Unified CCX server and convert them to WAV format using the procedure below.

To download and convert recordings from the RAW to WAV format, complete the following procedure.

To download and convert recordings:

1. Set the password for the uccxrecording user. For a detailed procedure, see "Setting the uccxrecording User Password" on page 132.
2. Create a folder on the machine on which Desktop Work Flow Administrator is installed. The folder must contain an SFTP client.

   NOTE: One SFTP client readily available on the internet is psftp.

3. In the same folder you created in step 2, create a text file named ftpcommands.txt that contains the following ftp commands.

   ```
   lcd "C:\Program Files\Cisco\Desktop_audio"
   mget *.Raw
   ```

   NOTE: You do not have to use the Desktop_audio folder; these steps use the Desktop_audio folder for purposes of illustration only. If you use a different folder, ensure you make the corresponding changes in step 4.

4. In the same folder you created in step 2, create a text file named convert.bat that contains the following commands:

   ```
   @echo off
   mkdir "C:\Program Files\Cisco\Desktop_audio"
   psftp <IP1> -l uccxrecording -pw <pw> -b ftpcommands.txt -batch
   psftp <IP2> -l uccxrecording -pw <pw> -b ftpcommands.txt -batch
   c:
   cd "C:\Program Files\Cisco\Desktop\bin"
   for %%c in (..\..\Desktop_audio\*.Raw) do raw2wav "%%~nc%%~xc"
   ```

   where:

- <IP1> is the IP address of the primary Unified CCX server
- <IP2> is the IP address of the secondary Unified CCX server
- <pw> is the uccxrecording user password you set in step 1

NOTE: When executed, these commands download all of the RAW recording files from the primary and secondary Unified CCX servers to the folder C:\Program Files\Cisco\Desktop_audio, convert the recordings to WAV format, and place the new WAV files in the folder C:\Program files\Cisco\Desktop_wav, leaving the original RAW files in the Desktop_audio folder. If desired, additional lines can be added to the batch file to copy the files to another folder or file server.

NOTE: The raw2wav 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.

5. Run the batch conversion file named convert.bat that you created in step 4.

Setting the uccxrecording User Password

To set the password for the uccxrecording user:

1. In the web browser, access https://<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 > Password Management. The Password Management page appears.
4. For Recording SFTP User, enter the new password and enter it again to confirm the password.
5. Click Save. The password is set for the uccxrecording user.

Running the Conversion Batch File Automatically

If you want the batch file to run automatically on specific days at a specific time, use the Windows “at” command.

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

NOTE: This assumes that convert.bat is in the C:\Program Files\Cisco\Desktop\bin folder.

About the RAW Format

Each RAW format recording is composed 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> is the date the file was recorded
- <HHMMSS> is the time the file was recorded
- <counter> is the recording number; it is reset to 00000 every time an agent logs in and is increased by one every time that agent is recorded
- <extension> is the extension of the agent recorded
- <agent ID> is the ID of the agent recorded

About the raw2wav Conversion Utility

The syntax to convert a RAW file to a WAV is:

```
raw2wav <filename> [<path>]
```

where:

- <filename> is either the <name>.to.raw or <name>.from.raw file.
- <path> is the location of the converted audio WAV files, if other than the default location; this parameter is optional

If the raw2wav utility finds a WAV file with a name that is identical to one that is about to be created, that file is not converted.

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

Removal

5

Removing CAD 10.5 Desktop Applications

To remove a CAD desktop application from a Windows XP system:

1. From the Start menu, select 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.

To remove a CAD desktop application from a Windows 7 system:

1. From the Start menu, select Control Panel.
2. Double-click Programs and Features.
3. From the list, select the application you want to remove and click Uninstall. The application is removed.

Upgrading and Downgrading CAD Desktop Applications

In CAD 8.0 and earlier, updates to CAD desktop applications were released in the form of service releases (SRs) that were installed on top of the base release. These SRs had to be uninstalled manually in order to remove the base CAD applications.

In CAD 8.5 and later, updates to CAD desktop applications are released as a complete software upgrade that is installed on top of an earlier version. You can roll later versions back to an earlier version by installing the earlier version on top of the current version.

> **NOTE:** Over-the-top rollbacks are possible within versions 8.5 and later. If you want to roll back to a version earlier than 10.5, you must manually uninstall and reinstall CAD.

In CAD 8.5 and later, if the CAD client desktop version does not match the CAD server version, CAD automatically updates the CAD desktop applications to the newer version. Similarly, if a service downgrade occurs, the CAD desktop applications are automatically downgraded to the older version. The existing CAD applications do not have to be manually uninstalled to install the older version. For more information on automatic upgrades and downgrades, see "Automated Updates" on page 114.