



Upgrading Cisco Unity 4.x Software to the Shipping Version

The task lists and procedures in this chapter apply only to upgrading the Cisco Unity software from version 4.x to the currently shipping version. Note that the lists contain some tasks that reference instructions in other Cisco Unity documentation.

For information on adding Cisco Unity features, see the “[Adding Features to the Cisco Unity System](#)” chapter after you have finished upgrading the software.

This chapter contains the following sections:

- [Task List for Upgrading Cisco Unity 4.x Software to the Shipping Version Without Failover](#), page 1-2
- [Task List for Upgrading Cisco Unity 4.x Software to the Shipping Version with Failover Configured](#), page 1-6
- [Downloading Software for the Upgrade](#), page 1-10
- [Checking the Consistency of the Cisco Unity Database, and Backing Up Cisco Unity Data](#), page 1-12
- [Determining Whether to Set Up Cisco Unity to Use SSL](#), page 1-13
- [Installing the Microsoft Certificate Services Component](#), page 1-14
- [Extending the Active Directory Schema for Cisco Unity](#), page 1-15
- [Creating New Active Directory Accounts for Cisco Unity Installation and Services](#), page 1-16
- [Setting Permissions on an Active Directory Location by Using the Permissions Wizard](#), page 1-17
- [Disabling Virus-Scanning and Cisco Security Agent Services](#), page 1-17
- [Running the Cisco Unity System Preparation Assistant](#), page 1-18
- [Installing Exchange 2000 Service Pack 3 and the Post-Service Pack 3 Rollup](#), page 1-20
- [Installing Exchange 2003 Service Pack 2](#), page 1-21
- [Installing the Latest Microsoft Service Packs and Updates Recommended for Use with Cisco Unity](#), page 1-21
- [Upgrading and Configuring Cisco Unity Software](#), page 1-22
- [Designating the Phone System as Cisco CallManager Express](#), page 1-30
- [Re-enabling Virus-Scanning and Cisco Security Agent Services](#), page 1-31
- [Installing Additional Dialogic Software for D/120JCT-Euro Rev 2 Voice Cards](#), page 1-31

- [Setting Up the Cisco Unity Administrator and Status Monitor to Use SSL](#), page 1-32
- [Configuring Internet Explorer to Display the Cisco Unity Administrator When You Use the Cisco Unity Administration Account \(Windows Server 2003 Only\)](#), page 1-33
- [Securing the Example Administrator and Example Subscriber Accounts Against Toll Fraud](#), page 1-34
- [Disabling or Deleting Old Installation and Service Accounts](#), page 1-35
- [Hardening the Cisco Unity Server](#), page 1-35

Task List for Upgrading Cisco Unity 4.x Software to the Shipping Version Without Failover



Note

If the system is using Cisco Unity Bridge version 2.x, refer instead to the “Upgrading from Bridge 2.x to Bridge 3.x” chapter of the *Cisco Unity Bridge Networking Guide, Release 3.0* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/ex/index.htm. The order and timing of upgrade tasks are different.



Caution

Windows Server 2003 is supported only with Cisco Unity version 4.0(4) and later. Upgrading from Windows 2000 to Windows Server 2003 is not supported when any additional software has been installed on the server (for example, SQL Server 2000 or MSDE 2000, Exchange or Exchange administration software, or Cisco Unity). Upgrading to Windows Server 2003 on an existing Cisco Unity server is supported only when you back up Cisco Unity data by using the Cisco Unity Disaster Recovery Backup tool, reinstall all software on the Cisco Unity server, and restore Cisco Unity data by using the Cisco Unity Disaster Recovery Restore tool.

The Cisco Unity server will be out of service while the Cisco Unity software is upgraded.

1. Download software for the upgrade. See the “[Downloading Software for the Upgrade](#)” section on [page 1-10](#).
2. *If the partner Exchange server is running Exchange 5.5:* Upgrade Exchange. Do the procedures in the applicable section in the “[Upgrading Exchange on the Cisco Unity System](#)” chapter.



Caution

For Cisco Unity 4.2(1) and later, Exchange 5.5 is not supported as the message store.

3. Refer to *Release Notes for Cisco Unity Release <Version>* for additional information on upgrading to the shipping version of Cisco Unity. In particular, note the items in the sections “Installation and Upgrade Notes” and “Limitations and Restrictions.” Release notes are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.
4. Check the consistency of the Cisco Unity database by using the Cisco Unity Directory Walker (DbWalker) utility, and back up Cisco Unity data by using the Cisco Unity Disaster Recovery Backup tool. See the “[Checking the Consistency of the Cisco Unity Database, and Backing Up Cisco Unity Data](#)” section on [page 1-12](#).
5. *If Cisco Unity is not already using SSL:* Determine whether to set up Cisco Unity to use SSL. See the “[Determining Whether to Set Up Cisco Unity to Use SSL](#)” section on [page 1-13](#).

6. *If you plan to set up Cisco Unity to use SSL and want to use the Microsoft Certificate Services available with Windows to issue your own certificate:* Install the Microsoft Certificate Services component. See the “[Installing the Microsoft Certificate Services Component](#)” section on page 1-14.
7. Update the Active Directory schema. See the “[Extending the Active Directory Schema for Cisco Unity](#)” section on page 1-15.
8. *Optional:* Create new Active Directory accounts for Cisco Unity installation and services.
Beginning with Cisco Unity 4.2(1), the Permissions wizard sets only the permissions that Cisco Unity requires to function rather than setting permissions at a higher level. If you want to take advantage of the reduced permissions, you must create new Active Directory accounts for Cisco Unity installation and services. Later in the task list, you will be alerted when to run the Permissions wizard to set permissions on the new accounts, and when to change the accounts that Cisco Unity services log on as and disable or delete the old accounts. See the “[Creating New Active Directory Accounts for Cisco Unity Installation and Services](#)” section on page 1-16.
9. If you downloaded the latest version of the Permissions wizard from CiscoUnityTools.com, install and run that version. Otherwise, run the version that appears in the Utilities\PermissionsWizard directory on the shipping Cisco Unity CD or DVD. For more information, refer to the Permissions wizard Help file, PWHelp_<language>.htm.

**Caution**

You must run the Permissions wizard even if you did not create new installation and service accounts in Task 8.

We recommend that you run the Cisco Unity Permissions wizard during off-peak hours unless you are installing a new Cisco Unity system in a Voice Messaging configuration and you are not creating subscriber accounts in the corporate directory. The new version of Permissions wizard sets permissions at a more granular level that requires more changes to the Active Directory database than previous versions.

The Permissions wizard sets permissions for installation and services accounts in Active Directory, and also sets permissions on the local server. When there is more than one Cisco Unity server in the forest (with or without failover configured), and when you are using the same three Active Directory accounts for installation, directory services, and message store services on multiple servers, the Permissions wizard only needs to set Active Directory permissions once for those accounts. When you run the Permissions wizard on the second and subsequent servers, the Permissions wizard displays a message asking whether you want to reapply permissions to those accounts. Click No, and the Permissions wizard will apply only the permissions required by the local server.

**Note**

When you run the Permissions wizard on a Cisco Unity server that is in a different domain than the installation and services accounts, the Permissions wizard cannot read or write the attribute that it uses to detect that permissions have already been set on those accounts. If you will be running the Permissions wizard on any Cisco Unity servers that are in a different domain than the installation and services accounts, we recommend that you give the account that you are using to run Permissions wizard read and write rights on the ciscoEcsbuUnityInformation property set for the installation and service accounts.

When the Permissions wizard completes, the Lsass.exe process updates the Active Directory database with the new permissions. While Lsass.exe is processing the updates, it uses 100 percent of available processor time on one of the domain controllers in the domain where the Permissions wizard was run. (Other domain controllers in the domain are also affected, but the impact is less significant.) The updates take a few minutes to several hours, depending on the size of the database.

Except when the Cisco Unity server is the domain controller and the Lsass.exe process slows the screen refresh, you may continue with the Cisco Unity installation while Lsass.exe is processing changes.

10. *If Cisco Unity is configured to automatically create Bridge or VPIM subscribers in a different AD location than regular subscribers:* Re-run the Permissions wizard, and specify the domain and location on the Set Active Directory Containers for New Objects page. See the [“Setting Permissions on an Active Directory Location by Using the Permissions Wizard”](#) section on page 1-17.
11. *If virus-scanning software or Cisco Security Agent for Cisco Unity is installed on the Cisco Unity server:* Disable virus-scanning services and the Cisco Security Agent service. See the [“Disabling Virus-Scanning and Cisco Security Agent Services”](#) section on page 1-17.
12. Run the Cisco Unity System Preparation Assistant to update the required Windows components, browser, database, and service packs. See the [“Running the Cisco Unity System Preparation Assistant”](#) section on page 1-18.
13. *If the partner Exchange server is running Exchange 2000 or Cisco Unity subscribers are homed in Exchange 2000:* Install the latest recommended service pack and the latest post-service pack rollup, if any. You must install at least Exchange 2000 Service Pack 3 and the Post-Service Pack 3 Rollup because they resolve an intermittent problem with message notification.

**Note**

When Service Pack 3 and the rollup are not installed, Exchange 2000 Server sends extra UDP packets to ports on the Cisco Unity server that are not listening for packets. Such activity is seen by intrusion-detection systems as port scans or attacks.

Install the software on all of the following servers on which either Exchange 2000 or Exchange 2000 administration software is installed:

- The Cisco Unity server.
- The partner Exchange server.
- The Exchange 2000 servers on which Cisco Unity subscribers are homed.

If you are installing Exchange 2000 Service Pack 3 and the Post-Service Pack 3 Rollup, see the [“Installing Exchange 2000 Service Pack 3 and the Post-Service Pack 3 Rollup”](#) section on page 1-20. If you are installing a later service pack and/or rollup, see the Microsoft documentation that you printed when you downloaded the software.

14. *If the partner Exchange server is running Exchange 2003 or Cisco Unity subscribers are homed in Exchange 2003:* Install the latest recommended service pack and the latest post-service pack rollup, if any. You must install at least Service Pack 2 or Cisco Unity Setup will fail.

Install the software on all of the following servers on which either Exchange 2003 or Exchange 2003 administration software is installed:

- The Cisco Unity server.
- The partner Exchange server.
- The Exchange 2003 servers on which Cisco Unity subscribers are homed.

If you are installing Exchange 2003 Service Pack 2, see the “[Installing Exchange 2003 Service Pack 2](#)” section on page 1-21. If you are installing a later service pack and/or rollup, see the Microsoft documentation that you printed when you downloaded the software.

15. Install the Microsoft updates recommended for use with Cisco Unity. In addition, if we recommend any Windows or SQL Server/MSDE service packs later than those that are installed by the Cisco Unity System Preparation Assistant, install the latest recommended service packs. See the “[Installing the Latest Microsoft Service Packs and Updates Recommended for Use with Cisco Unity](#)” section on page 1-21.
16. Run the Cisco Unity Installation and Configuration Assistant to upgrade and configure the Cisco Unity software, and to set up the Cisco Personal Communications Assistant to use SSL. See the “[Upgrading and Configuring Cisco Unity Software](#)” section on page 1-22.
17. Install the service release for the shipping version of Cisco Unity, if available. For installation instructions, refer to *Release Notes for Cisco Unity <Version> Service Release 1* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.
18. *If you are upgrading from Cisco Unity 4.0(1) through 4.0(4) and Cisco Unity is integrated with Cisco CallManager Express or with a Cisco CallManager cluster that includes a Cisco CallManager Express server:* Designate the phone system as Cisco CallManager Express. See the “[Designating the Phone System as Cisco CallManager Express](#)” section on page 1-30.
19. *If virus-scanning software or Cisco Security Agent for Cisco Unity is installed on the Cisco Unity server:* Re-enable virus-scanning services and the Cisco Security Agent service. See the “[Re-enabling Virus-Scanning and Cisco Security Agent Services](#)” section on page 1-31.
20. *If you are upgrading from Cisco Unity 4.0(1) through 4.0(4), and if Cisco Unity uses Intel Dialogic D/120JCT-Euro Rev 2 voice cards to integrate with a circuit-switched phone system:* Install additional Dialogic .prm files. See the “[Installing Additional Dialogic Software for D/120JCT-Euro Rev 2 Voice Cards](#)” section on page 1-31.
21. *If you are setting up Cisco Unity to use SSL:* Set up the Cisco Unity Administrator and Status Monitor to use SSL. See the “[Setting Up the Cisco Unity Administrator and Status Monitor to Use SSL](#)” section on page 1-32.
22. Review the substitute objects on the System > Configuration > Settings page of the Cisco Unity Administrator. The objects are Substitute Recipient, Substitute Owner, Substitute After Message Call Handler, and Substitute Exit Call Handler. Cisco Unity uses the objects to substitute references to any subscriber that is deleted by using the Cisco Unity Administrator without first reassigning such references (for example, ownership of a call handler or distribution list). For new installations, the Example Administrator is configured as the Substitute Recipient and Substitute Owner, and the Goodbye call handler is configured as the Substitute After Message Call Handler and Substitute Exit Call Handler. For upgrades, any changes made to the defaults will not be overwritten. However, we recommend that you review these settings now and update them if you wish to use different substitute objects. Refer to Cisco Unity Administrator Help for a description of each object and where it applies.
23. *If Windows Server 2003 is installed on the Cisco Unity Server:* Update Internet Explorer security settings. See the “[Configuring Internet Explorer to Display the Cisco Unity Administrator When You Use the Cisco Unity Administration Account \(Windows Server 2003 Only\)](#)” section on page 1-33.
24. Secure the Example Administrator and Example Subscriber accounts against toll fraud. See the “[Securing the Example Administrator and Example Subscriber Accounts Against Toll Fraud](#)” section on page 1-34.

25. *Optional:* If Cisco Security Agent for Cisco Unity is not installed on the Cisco Unity server, install it. Refer to *Release Notes for Cisco Security Agent for Cisco Unity* for installation and configuration instructions. Release notes for all version are available at http://www.cisco.com/en/US/products/sw/voicew/ps2237/prod_release_notes_list.html.
26. *If the Cisco Unity server is connected to the corporate network:* Harden the Cisco Unity server. See the “[Hardening the Cisco Unity Server](#)” section on page 1-35.
27. *If the system is using the AMIS, SMTP, or VPIM networking options:* Refer to the applicable “Upgrading with <Networking Option>” section in the “Upgrading and Uninstalling Networking Options” chapter of the *Networking in Cisco Unity Guide, Release 4.0(5)* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/net/net405/ex/index.htm.
28. *If the system is using Cisco Unity Bridge version 3.x:* Refer to the “Upgrading from Cisco Unity 4.0(3) or Later with Bridge 3.x” chapter of the *Cisco Unity Bridge Networking Guide, Release 3.0* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/ex/index.htm.

Task List for Upgrading Cisco Unity 4.x Software to the Shipping Version with Failover Configured



Note

If the system is using Cisco Unity Bridge version 2.x, refer instead to the “Upgrading from Bridge 2.x to Bridge 3.x” chapter of the *Cisco Unity Bridge Networking Guide, Release 3.0* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/ex/index.htm. The order and timing of upgrade tasks are different.



Caution

Windows Server 2003 is supported only with Cisco Unity version 4.0(4) and later. Upgrading from Windows 2000 to Windows Server 2003 is not supported when any additional software has been installed on the server (for example, SQL Server 2000, Exchange or Exchange administration software, or Cisco Unity). Upgrading to Windows Server 2003 on an existing Cisco Unity server is supported only when you back up Cisco Unity data by using the Cisco Unity Disaster Recovery Backup tool, reinstall all software on the Cisco Unity server, and restore Cisco Unity data by using the Cisco Unity Disaster Recovery Restore tool.

Start the upgrade on the primary Cisco Unity server. The task list alerts you when to begin upgrading the secondary Cisco Unity server. Some failover tasks reference detailed instructions in the *Cisco Unity Failover Configuration and Administration Guide, Release 4.x* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/fail/fail401/ex/index.htm.

The failover feature cannot be used for continuing Cisco Unity service on one server while upgrading the Cisco Unity software on the other server. Both the primary and secondary servers must be out of service while the Cisco Unity software is upgraded. The secondary server cannot handle voice messaging while the primary server is being upgraded. While you do the upgrade, callers and subscribers will not be able to record or listen to voice messages. We recommend that you upgrade when phone traffic is light, for example, after business hours.

1. Download software for the upgrade. See the “[Downloading Software for the Upgrade](#)” section on page 1-10.
2. *If the partner Exchange server is running Exchange 5.5:* Upgrade Exchange. Do the procedures in the applicable section in the “[Upgrading Exchange on the Cisco Unity System](#)” chapter.



Caution For Cisco Unity 4.2(1) and later, Exchange 5.5 is not supported as the message store.

3. Refer to *Release Notes for Cisco Unity Release <Version>* for additional information on upgrading to the shipping version of Cisco Unity. In particular, note the items in the sections “Installation and Upgrade Notes” and “Limitations and Restrictions.” Release notes are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.
4. Check the consistency of the Cisco Unity database by using the Cisco Unity Directory Walker (DbWalker) utility, and back up Cisco Unity data by using the Disaster Recovery Backup tool. See the “[Checking the Consistency of the Cisco Unity Database, and Backing Up Cisco Unity Data](#)” section on page 1-12.
5. *If Cisco Unity is not already using SSL:* Determine whether to set up Cisco Unity to use SSL. See the “[Determining Whether to Set Up Cisco Unity to Use SSL](#)” section on page 1-13.
6. *If you plan to set up Cisco Unity to use SSL and want to use the Microsoft Certificate Services available with Windows to issue your own certificate:* Install the Microsoft Certificate Services component. See the “[Installing the Microsoft Certificate Services Component](#)” section on page 1-14.
7. Update the Active Directory schema. See the “[Extending the Active Directory Schema for Cisco Unity](#)” section on page 1-15.
8. *Optional:* Create new Active Directory accounts for Cisco Unity installation and services.
Beginning with Cisco Unity 4.2(1), the Permissions wizard sets only the permissions that Cisco Unity requires to function rather than setting permissions at a higher level. If you want to take advantage of the reduced permissions, you must create new Active Directory accounts for Cisco Unity installation and services. Later in the task list, you will be alerted when to run the Permissions wizard to set permissions on the new accounts, and when to change the accounts that Cisco Unity services log on as and disable or delete the old accounts. See the “[Creating New Active Directory Accounts for Cisco Unity Installation and Services](#)” section on page 1-16.
9. If you downloaded the latest version of the Permissions wizard from CiscoUnityTools.com, install and run that version. Otherwise, run the version that appears in the Utilities\PermissionsWizard directory on the shipping Cisco Unity CD or DVD. For more information, refer to the Permissions wizard Help file, PWHelp_<language>.htm.



Caution You must run the Permissions wizard even if you did not create new installation and service accounts in Task 8.

We recommend that you run the Cisco Unity Permissions wizard during off-peak hours unless you are installing a new Cisco Unity system in a Voice Messaging configuration and you are not creating subscriber accounts in the corporate directory. The new version of Permissions wizard sets permissions at a more granular level that requires more changes to the Active Directory database than previous versions.

The Permissions wizard sets permissions for installation and services accounts in Active Directory, and also sets permissions on the local server. When there is more than one Cisco Unity server in the forest (with or without failover configured), and when you are using the same three Active Directory accounts for installation, directory services, and message store services on multiple servers, the Permissions wizard only needs to set Active Directory permissions once for those accounts. When you run the Permissions wizard on the second and subsequent servers, the Permissions wizard displays a message asking whether you want to reapply permissions to those accounts. Click No, and the Permissions wizard will apply only the permissions required by the local server.

**Note**

When you run the Permissions wizard on a Cisco Unity server that is in a different domain than the installation and services accounts, the Permissions wizard cannot read or write the attribute that it uses to detect that permissions have already been set on those accounts. If you will be running the Permissions wizard on any Cisco Unity servers that are in a different domain than the installation and services accounts, we recommend that you give the account that you are using to run Permissions wizard read and write rights on the `ciscoEcsbuUnityInformation` property set for the installation and service accounts.

When the Permissions wizard completes, the `Lsass.exe` process updates the Active Directory database with the new permissions. While `Lsass.exe` is processing the updates, it uses 100 percent of available processor time on the root domain controller in the domain and on one of the global catalog servers in the site where the Permissions wizard was run. (Other domain controllers in the domain and other global catalog servers in the forest are also affected, but the impact is less significant.) The updates take a few minutes to several hours, depending on the size of the database. Except when the Cisco Unity server is the domain controller and the `Lsass.exe` process slows the screen refresh, you may continue with the Cisco Unity installation while `Lsass.exe` is processing changes.

10. *If Cisco Unity is configured to automatically create Bridge or VPIM subscribers in a different AD location than regular subscribers:* Re-run the Permissions wizard, and specify the domain and location on the Set Active Directory Containers for New Objects page. See the [“Setting Permissions on an Active Directory Location by Using the Permissions Wizard”](#) section on page 1-17.
11. *If virus-scanning software or Cisco Security Agent for Cisco Unity is installed on the Cisco Unity server:* Disable virus-scanning services and the Cisco Security Agent service. See the [“Disabling Virus-Scanning and Cisco Security Agent Services”](#) section on page 1-17.
12. Run the Cisco Unity System Preparation Assistant to update the required Windows components, browser, database, and service packs. See the [“Running the Cisco Unity System Preparation Assistant”](#) section on page 1-18.
13. *If the partner Exchange server is running Exchange 2000 or Cisco Unity subscribers are homed in Exchange 2000:* Install the latest recommended service pack and the latest post-service pack rollup, if any. You must install at least Exchange 2000 Service Pack 3 and the Post-Service Pack 3 Rollup because they resolve an intermittent problem with message notification.

**Note**

When Service Pack 3 and the rollup are not installed, Exchange 2000 Server sends extra UDP packets to ports on the Cisco Unity server that are not listening for packets. Such activity is seen by intrusion-detection systems as port scans or attacks.

Install the software on all of the following servers on which either Exchange 2000 or Exchange 2000 administration software is installed:

- Both Cisco Unity servers.
- The partner Exchange server.
- The Exchange 2000 servers on which Cisco Unity subscribers are homed.

If you are installing Exchange 2000 Service Pack 3 and the Post-Service Pack 3 Rollup, see the “[Installing Exchange 2000 Service Pack 3 and the Post-Service Pack 3 Rollup](#)” section on page 1-20. If you are installing a later service pack and/or rollup, see the Microsoft documentation that you printed when you downloaded the software.

14. *If the partner Exchange server is running Exchange 2003 or Cisco Unity subscribers are homed in Exchange 2003:* Install the latest recommended service pack and the latest post-service pack rollup, if any. You must install at least Service Pack 2 or Cisco Unity Setup will fail.

Install the software on all of the following servers on which either Exchange 2003 or Exchange 2003 administration software is installed:

- Both primary and secondary Cisco Unity servers.
- The partner Exchange server.
- The Exchange 2003 servers on which Cisco Unity subscribers are homed.

If you are installing Exchange 2003 Service Pack 2, see the “[Installing Exchange 2003 Service Pack 2](#)” section on page 1-21. If you are installing a later service pack and/or rollup, see the Microsoft documentation that you printed when you downloaded the software.

15. Install the Microsoft updates recommended for use with Cisco Unity. In addition, if we recommend any Windows or SQL Server service packs later than those that are installed by the Cisco Unity System Preparation Assistant, install the latest recommended service packs. See the “[Installing the Latest Microsoft Service Packs and Updates Recommended for Use with Cisco Unity](#)” section on page 1-21.
16. Run the Cisco Unity Installation and Configuration Assistant to upgrade and configure the Cisco Unity software, and to set up the Cisco Personal Communications Assistant to use SSL. See the “[Upgrading and Configuring Cisco Unity Software](#)” section on page 1-22.
17. Install the service release for the shipping version of Cisco Unity, if available. For installation instructions, refer to *Release Notes for Cisco Unity <Version> Service Release 1* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.
18. *If virus-scanning software or Cisco Security Agent for Cisco Unity is installed on the Cisco Unity server:* Re-enable virus-scanning services and the Cisco Security Agent service. See the “[Re-enabling Virus-Scanning and Cisco Security Agent Services](#)” section on page 1-31.
19. *If you are upgrading from Cisco Unity 4.0(1) through 4.0(4), and if Cisco Unity uses Intel Dialogic D/120JCT-Euro Rev 2 voice cards to integrate with a circuit-switched phone system:* Install additional Dialogic .prm files. See the “[Installing Additional Dialogic Software for D/120JCT-Euro Rev 2 Voice Cards](#)” section on page 1-31.
20. *If you are setting up Cisco Unity to use SSL:* Set up the Cisco Unity Administrator and Status Monitor to use SSL. See the “[Setting Up the Cisco Unity Administrator and Status Monitor to Use SSL](#)” section on page 1-32.
21. *If Windows Server 2003 is installed on the Cisco Unity Server:* Update Internet Explorer security settings. See the “[Configuring Internet Explorer to Display the Cisco Unity Administrator When You Use the Cisco Unity Administration Account \(Windows Server 2003 Only\)](#)” section on page 1-33.
22. Run the Configure Cisco Unity Failover wizard. Refer to the “[Configuring Failover on the Primary and Secondary Servers](#)” section in the “[Configuring Cisco Unity Failover](#)” chapter of the *Cisco Unity Failover Configuration and Administration Guide, Release 4.x* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/fail/fail401/ex/index.htm.
23. On the secondary server, run the Permissions wizard.

When you run the Permissions wizard on the secondary server, Lsass.exe does not affect performance on domain controllers.

24. On the secondary server, repeat Task 11. through Task 22. to upgrade the server.
25. Review the substitute objects on the System > Configuration > Settings page of the Cisco Unity Administrator. The objects are Substitute Recipient, Substitute Owner, Substitute After Message Call Handler, and Substitute Exit Call Handler. Cisco Unity uses the objects to substitute references to any subscriber that is deleted by using the Cisco Unity Administrator without first reassigning such references (for example, ownership of a call handler or distribution list). For new installations, the Example Administrator is configured as the Substitute Recipient and Substitute Owner, and the Goodbye call handler is configured as the Substitute After Message Call Handler and Substitute Exit Call Handler. For upgrades, any changes made to the defaults will not be overwritten. However, we recommend that you review these settings now and update them if you wish to use different substitute objects. Refer to Cisco Unity Administrator Help for a description of each object and where it applies.
26. Secure the Example Administrator and Example Subscriber accounts against toll fraud. See the “Securing the Example Administrator and Example Subscriber Accounts Against Toll Fraud” section on page 1-34.
27. *If the system is using the AMIS, SMTP, or VPIM networking options:* Refer to the applicable “Upgrading with <Networking Option>” section in the “Upgrading and Uninstalling Networking Options” chapter of the *Networking in Cisco Unity Guide, Release 4.0(5)* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/net/net405/ex/index.htm.
28. *If the system is using Cisco Unity Bridge version 3.x:* Refer to the “Upgrading from Cisco Unity 4.0(3) or Later with Bridge 3.x” chapter of the *Cisco Unity Bridge Networking Guide, Release 3.0* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/ex/index.htm.

Downloading Software for the Upgrade

This section lists the software needed to upgrade Cisco Unity. Note that if you do not have Cisco Unity DVDs or CDs for the currently shipping version, you must download additional software.

- [Software for All Upgrades, page 1-10](#)
- [Additional Software for Upgrades with No Cisco Unity DVDs or CDs for the Shipping Version, page 1-12](#)

Software for All Upgrades

Download the following software for all upgrades. Even if you have Cisco Unity DVDs or CDs for the currently shipping version, we recommend that you download the software, which may have been updated since the discs were produced or which is not included on the discs.

Cisco Unity Service Release

The Cisco Unity service release (a rollup of Cisco Unity engineering specials) for the shipping version, if available. Refer to the “Downloading Service Release 1” section of *Release Notes for Cisco Unity <Version> Service Release 1* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html. Note that if there are no release notes available, the service release for the shipping version has not been released yet.

Microsoft Service Packs

The latest service packs recommended for use with Cisco Unity, if any were qualified after the shipping version of Cisco Unity was released. Available on the Microsoft website. Also download or print the installation instructions.

To determine the service packs that are recommended, refer to *Recommended Service Packs and Updates for Use with Cisco Unity and the Cisco Unity Bridge* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/cmptblty/msupdate.htm. (Service packs that were recommended when the shipping version of Cisco Unity was released are available on the Cisco Unity 4.x Software Download page at <http://www.cisco.com/cgi-bin/tablebuild.pl/unity-40>.)

Microsoft Updates

The latest updates recommended for use with Cisco Unity. Available on the Microsoft Updates for Cisco Unity Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity_msft_updates. (Updates that were recommended when the shipping version of Cisco Unity was released are on the Cisco Unity<Version> Post-Install CD, but the download page is updated monthly, so you should check for new updates even if you have the CD.)



Caution

If the partner Exchange server is running Exchange 2000, you must install the Exchange 2000 Server Post-Service Pack 3 Update Rollup (KB 870540) on the Cisco Unity server, or you will not be able to install or upgrade to the shipping version of Cisco Unity.



Note

To access the software download page, you must be logged on to Cisco.com as a registered user.

Cisco Security Agent for Cisco Unity (Optional)

Cisco Security Agent for Cisco Unity is available on the Cisco Unity Crypto Software Download page at <http://www.cisco.com/cgi-bin/tablebuild.pl/unity3d>. Refer to *Release Notes for Cisco Security Agent for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html for information on supported configurations, and for download and installation instructions.

Because of export controls on strong encryption, the first time you download Cisco Security Agent for Cisco Unity, you need to fill out a brief questionnaire. Follow the on-screen prompts.

Cisco Unity Directory Walker Utility and Cisco Unity Disaster Recovery Tools

The latest versions of the Cisco Unity Directory Walker (DbWalker) utility and the Cisco Unity Disaster Recovery tools (DiRT). DbWalker is used to check the consistency of and correct errors in the Cisco Unity database before the upgrade. DiRT is used to back up Cisco Unity data before the upgrade and to restore Cisco Unity data, if necessary. (All are included on the Cisco Unity discs, but updates are posted regularly to the Cisco Unity Tools website.)

DbWalker for Cisco Unity 4.x is available at http://ciscounitytools.com/App_DirectoryWalker4.htm. DiRT is available at http://ciscounitytools.com/App_DisasterRecoveryTools.htm.

Cisco Unity Permissions Wizard

The latest version of the Cisco Unity Permissions wizard. The Permissions wizard for Cisco Unity 4.2(1) and later is available at http://ciscounitytools.com/App_PW_421.htm.

Additional Software for Upgrades with No Cisco Unity DVDs or CDs for the Shipping Version

If you do not have Cisco Unity DVDs or CDs for the shipping version, you also need to download the following software.

Cisco Unity CDs

Cisco Unity CDs for the shipping version. Refer to the “Downloading Software for Cisco Unity <Version>” section of *Release Notes for Cisco Unity Release <Version>* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Cisco Unity Service Pack CDs

Cisco Unity Service Pack CD 1, which includes the Cisco Unity System Preparation Assistant.

Cisco Unity Service Pack CD 2, if you are using Exchange 2000 and if Exchange 2000 Service Pack 3 is not already installed.

Cisco Unity Service Pack CD 3, if you are using Exchange 2003 and if Exchange 2003 Service Pack 1 is not already installed.

Refer to the “Downloading Software for Cisco Unity <Version>” section of *Release Notes for Cisco Unity Release <Version>* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Microsoft Updates for Cisco Unity

Microsoft updates recommended for use with Cisco Unity. Refer to the “Downloading Software for Cisco Unity <Version>” section of *Release Notes for Cisco Unity Release <Version>* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.



Caution

If the partner Exchange server is running Exchange 2000, you must install the Exchange 2000 Server Post-Service Pack 3 Update Rollup (KB 870540) on the Cisco Unity server, or you will not be able to install or upgrade to the shipping version of Cisco Unity.

Checking the Consistency of the Cisco Unity Database, and Backing Up Cisco Unity Data

Before you upgrade Cisco Unity, we recommend that you run the DbWalker utility to check the consistency of the Cisco Unity database. Running DbWalker fixes most minor errors automatically and flags any major errors.

On a system with a few hundred subscribers, running DbWalker takes only a few minutes. However, on a large system, running DbWalker may take several hours. The duration depends on the speed of the processor, the amount of RAM in the server, the number of calls that Cisco Unity is taking, and other variables.

We also recommend that you back up Cisco Unity data by using the Disaster Recovery Backup tool. Running the tool takes only a few minutes, and having a DiRT backup allows you to restore Cisco Unity data easily, if necessary.

To Check the Consistency of the Cisco Unity Database

- Step 1** On the Cisco Unity server, install the latest version of DbWalker, if it is not already installed. If Cisco Unity failover is configured, do this procedure on the primary server.
- Step 2** Run DbWalker, and correct all errors that the utility finds. Refer to DbWalker Help for detailed instructions on running the utility and on correcting errors in the database. (The Help file, DbWalker.htm, is in the same directory as DbWalker.exe.)
-

If you choose to back up messages as well as Cisco Unity data in the next procedure, backing up takes longer, the size of the backup is significantly larger, and the account with which you log on to Windows requires additional permissions. Refer to DiRT Help for detailed information.

To Back Up Cisco Unity Data

- Step 1** On the Cisco Unity server, install the latest versions of DiRT, if the tools are not already installed. If Cisco Unity failover is configured, do this procedure on the secondary server.
- Step 2** Back up Cisco Unity data by using the Disaster Recovery Backup tool. Refer to DiRT Help for detailed instructions. (The Help file, UnityDisasterRecovery.htm, is in the same directory as UnityDisasterRecoveryBackup.exe.)



Caution Follow Help carefully. DiRT includes a variety of options that you must understand to use the tools successfully. In addition, the account you are logged on as when you back up Cisco Unity data must have sufficient permissions or the backup will fail.

Determining Whether to Set Up Cisco Unity to Use SSL



Note If Cisco Unity is already using SSL, skip this section.

When subscribers log on to the Cisco Personal Communications Assistant (PCA), their credentials are sent across the network to Cisco Unity in clear text. The same is true in the following situations:

- When the Cisco Unity Administrator and the Status Monitor are configured to use the Anonymous authentication method.
- With the Mobile Message Access for BlackBerry feature, when data is sent between the Cisco Unity server and the BlackBerry server.

In addition, the information that subscribers enter on the pages of the Cisco PCA and of the Cisco Unity Administrator (regardless of which authentication method it uses) is not encrypted.

For increased security, we recommend that you set up Cisco Unity to use the Secure Sockets Layer (SSL) protocol. SSL uses public/private key encryption to provide a secure connection between servers and clients, and uses digital certificates to authenticate servers or servers and clients. (A digital certificate is a file that contains encrypted data that attests to the identity of an organization or entity, such as a computer.)

Using the SSL protocol ensures that all Cisco Unity subscriber credentials—as well as the information that a subscriber enters on any page of the Cisco Unity Administrator and the Cisco PCA—are encrypted as the data is sent across the network. In addition, when you set up Cisco Unity to use SSL, each time that a subscriber tries to access any Cisco Unity web application, the browser will confirm that it is connected with the real Cisco Unity server—and not an entity falsely posing as such—before allowing the subscriber to log on.

To set up a web server such as Cisco Unity to use SSL, you can either obtain a digital certificate from a certificate authority (CA) or use Microsoft Certificate Services available with Windows to issue your own certificate. (A CA is a trusted organization or entity that issues and manages certificates at the request of another organization or entity.) Cost, certificate features, ease of setup and maintenance, and the security policies practiced by the organization are some of the issues to consider when determining whether you should purchase a certificate from a CA or issue your own.

Information on third-party CAs, Microsoft Certificate Services, and SSL is widely available on the Internet, as well as in the Windows and IIS online documentation. Such sources can help you determine whether to use SSL and how to set up a web server to use it.

Installing the Microsoft Certificate Services Component



Note

If you do not plan to set up Cisco Unity to use SSL or if you want to use a digital certificate from a Certificate Authority to set up Cisco Unity to use SSL, skip this section.

Do the procedure in this section if you plan to set up Cisco Unity to use SSL and you want to use the Microsoft Certificate Services available with Windows to issue your own certificate. You may install the component on the Cisco Unity server or on another server.

To Install the Microsoft Certificate Services Component

- Step 1** On the server that will act as your certificate authority (CA) and issue certificates, on the Windows Start menu, click **Settings > Control Panel > Add/Remove Programs**.
- Step 2** Click **Add/Remove Windows Components**.
- Step 3** In the Windows Components dialog box, check the **Certificate Services** check box. Do not change any other items. When the warning appears about not being able to rename the computer, or to join or be removed from a domain, click **Yes**.
- Step 4** Click **Next**.
- Step 5** Click **Stand-alone Root CA**, and click **Next**. (A stand-alone CA is a CA that does not require Active Directory.)

- Step 6** Follow the on-screen prompts to complete the installation. For information, refer to the Windows documentation.
- If a message appears that Internet Information Services is running on the computer and must be stopped before proceeding, click **OK** to stop the services.
- Step 7** In the Completing the Windows Components Wizard dialog box, click **Finish**.
- Step 8** Close the Add Remove Programs dialog box and Control Panel.
-

Extending the Active Directory Schema for Cisco Unity

Several changes to the Active Directory schema are required for Cisco Unity to work properly. To see the changes that the schema update program makes, browse to the directory SchemaLdifScripts on Cisco Unity CD 1, and view the file Avdirmonex2k.ldf.

Changes to the Active Directory schema may take 15 minutes or more to replicate throughout the forest. These changes must finish replicating before you can install Cisco Unity.

To Extend the Active Directory Schema

- Step 1** Confirm that all domain controllers are on line. (The Active Directory schema extensions replicate only when all domain controllers are on line.)
- Step 2** On the computer that has the schema master role (typically the first DC/GC in the forest), log on to Windows as a user who is a member of the Schema Admins group.
- Step 3** On Cisco Unity DVD 1 or CD 1, or from the location to which you saved the downloaded Cisco Unity CD 1 image files, browse to the directory **ADSchemaSetup**, and double-click **ADSchemaSetup.exe**.
- Step 4** In the Active Directory Schema Setup dialog box, check the **Exchange 2000 or Exchange 2003 Directory Monitor** check box.
- Step 5** If you have ever used, are currently using, or plan to use VPIM Networking or Bridge Networking, check the applicable boxes.



Caution

If the schema has ever been updated with Bridge Connector and/or VPIM Connector extensions (for Bridge Networking and VPIM Networking, respectively) from an earlier version of Cisco Unity, you must update those extensions and the Directory Monitor extensions even if you are no longer using the Bridge or VPIM.

- Step 6** Click **OK**.
- Step 7** When the schema extension has finished, Ldif.log and Ldif.err files are saved to the desktop. View the contents of these files to confirm that the extension completed successfully.
-

Creating New Active Directory Accounts for Cisco Unity Installation and Services

Beginning with Cisco Unity 4.2(1), the Permissions wizard sets only the permissions that Cisco Unity requires to function rather than setting permissions at a higher level. If you want to take advantage of the reduced permissions, create new Active Directory domain accounts for Cisco Unity installation and services.



Caution

The Permissions wizard does not take permissions away, it only grants permissions. If you run the Permissions wizard on existing accounts, permissions will not be reduced.

To Create New Domain Accounts for Cisco Unity Installation and Services

- Step 1** On the Cisco Unity server or another server where Active Directory Users and Computers is installed, log on to Windows by using an account that is a member of the Domain Admins group.
- Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Active Directory Users and Computers**.
- Step 3** In the left pane, expand the domain, right-click **Users** or the organizational unit where you want to create the installation account, and click **New > User**.
- Step 4** Follow the on-screen prompts to create the installation account. Creating an Exchange mailbox is optional.

We suggest that you use the following names for the accounts.

Installation	UnityInstall
Account that Cisco Unity directory services log on as (directory services account)	UnityDirSvc
Account that Cisco Unity message store services log on as (message store services account)	UnityMsgStoreSvc

- Step 5** Repeat [Step 3](#) and [Step 4](#) to create the Cisco Unity directory services account and message store services account.
- Step 6** Ensure that for the accounts that Cisco Unity services log on as, the password will never expire. If the password expires, Cisco Unity will stop working the next time the server is restarted.
- Step 7** Close Active Directory Users and Computers.

Setting Permissions on an Active Directory Location by Using the Permissions Wizard

You re-run the Permissions Wizard to update the permissions on the Active Directory location where Cisco Unity automatically creates Bridge and/or VPIM subscribers, if it is different from the location where Cisco Unity creates regular subscribers. If Cisco Unity is configured to automatically create both Bridge and VPIM subscribers in different locations, do the following procedure for the Bridge subscriber location, and repeat the procedure for the VPIM subscriber location.

Run the Permissions wizard during off-peak hours. The Permissions wizard now sets permissions at a more granular level than previous versions did, which requires more changes to the Active Directory database.

**Caution**

When the Permissions wizard completes, the Lsass.exe process updates the Active Directory database with the new permissions. While Lsass.exe is processing the updates, it uses 100% of available processor time on the root domain controller in the domain and on one of the global catalog servers in the site where the Permissions wizard was run. (Other domain controllers in the domain and other global catalog servers in the forest are also affected, but the impact is less significant.) The updates take a few minutes to several hours, depending on the size of the database. Do not continue with the Cisco Unity upgrade until Lsass.exe has finished processing the changes, or Cisco Unity Setup may fail.

To Set Permissions on the AD Location by Using the Permissions Wizard

-
- Step 1** If you downloaded the latest version of Permissions wizard from CiscoUnityTools.com, install and run that version. Otherwise, run the version that appears in the Utilities\PermissionsWizard directory on the shipping Cisco Unity CD or DVD.
- Step 2** Click **Next** without changing any options until you arrive at the Set Active Directory Containers for New Objects page.
- Step 3** Select the domain and the applicable container or organizational unit in which Cisco Unity automatically creates Bridge or VPIM subscribers.
- Note** The Permissions wizard only has the ability to grant permissions—it does not remove any permissions. Following this procedure will add the necessary permissions on the container or OU that you select, but will not remove permissions that are already granted on other containers for Cisco Unity.
- Step 4** Click **Next** and follow the prompts to complete the Permissions wizard.
-

Disabling Virus-Scanning and Cisco Security Agent Services

**Note**

If the system is not using virus-scanning software or Cisco Security Agent for Cisco Unity, skip this section.

You disable virus-scanning and Cisco Security Agent services on the server so that they do not slow down the installation of software or cause the installations to fail. The *Cisco Unity Reconfiguration and Upgrade Guide* alerts you when to re-enable the services after all of the installation procedures that can be affected are complete.

To Disable and Stop Virus-Scanning and Cisco Security Agent Services

-
- Step 1** Refer to the virus-scanning software documentation to determine the names of the virus-scanning services.
- Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 3** Disable and stop each virus-scanning service and the Cisco Security Agent service:
- In the right pane, double-click the service.
 - On the General tab, in the Startup Type list, click **Disabled**. This prevents the service from starting when you restart the server.
 - Click **Stop** to stop the service immediately.
 - Click **OK** to close the Properties dialog box.
- Step 4** When the services have been disabled, close the Services MMC.
-

Running the Cisco Unity System Preparation Assistant

The Cisco Unity System Preparation Assistant is a program that helps customize the platform for Cisco Unity by checking for and installing Windows 2000 Server components, Microsoft service packs and updates, and other software required by Cisco Unity. (For a detailed list, refer to *Components and Software Installed by the Cisco Unity Platform Configuration Discs and the Cisco Unity System Preparation Assistant* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/pcd/pcd_inst.htm.)



Caution

Do not run the Cisco Unity System Preparation Assistant remotely by using Windows Terminal Services or other remote-access applications, or the installation of required software may fail.

If a Microsoft AutoMenu window appears while the Cisco Unity System Preparation Assistant is installing an application, close the window and allow the assistant to continue.

To Run the Cisco Unity System Preparation Assistant

-
- Step 1** Log on to Windows by using an account that is a member of the Local Administrators group.
- Step 2** On Cisco Unity Service Packs CD 1 or from the location to which you saved the downloaded Service Packs CD 1 image files, browse to the **Cuspa** directory, and double-click **Cuspa.vbs**.
- If you are accessing the Cisco Unity System Preparation Assistant files on another server, use Windows Explorer or the “net” command to map the network drive to a drive letter on the Cisco Unity server before you run Cuspa.vbs.

- Step 3** If prompted, double-click the language of your choice to continue the installation.
- Step 4** On the Welcome screen, click **Next**.
- Step 5** On the Cisco Unity Server Characteristics page, set the following fields:

Configuration	Click Unified Messaging or Voice Messaging Only , depending on the Cisco Unity configuration.
Failover	Check the This Is a Primary or Secondary Failover Server check box if the system is using failover.
Number of Ports	Enter the number of voice ports that you are connecting with the Cisco Unity server.

- Step 6** Click **Next**. The assistant lists the components and indicates whether or not they are installed.
- Step 7** Follow the on-screen prompts in the Cisco Unity System Preparation Assistant to install the additional software required by Cisco Unity.
- Step 8** If MSDE Service Pack 4 is being installed, skip to [Step 9](#).
If SQL Server Service Pack 4 is being installed, install it now:
- a. On the Welcome screen, click **Next**.
 - b. Follow the on-screen prompts until you are prompted to choose the authentication mode.
 - c. Choose Windows authentication, and click **Next**.
 - d. If the SA Password Warning dialog box appears, enter and confirm the password, and click **Next**.
 - e. On the Backward Compatibility Checklist page, do not check the Enable Cross-Database Ownership Chaining for All Databases [Not Recommended] check box.
 - f. Follow the on-screen prompts to continue.
 - g. If you are prompted about shutdown tasks before continuing with the installation, click **Next**.
 - h. Click **Finish** to begin installing components.
 - i. When the Setup message appears, click **OK**.
 - j. Click **Finish** to restart the server.
 - k. Skip to [Step 10](#).
- Step 9** If MSDE Service Pack 4 is being installed, install it now:
- a. Follow the on-screen prompts.
 - b. When the installation is complete, click **Yes** to restart the server.
- Step 10** Follow the on-screen prompts in the Cisco Unity System Preparation Assistant to install the additional software required by Cisco Unity.
- Step 11** When the Cisco Unity System Preparation Assistant has completed, click **Finish**.

Installing Exchange 2000 Service Pack 3 and the Post-Service Pack 3 Rollup


Note

If the partner Exchange server is not running Exchange 2000 and no Cisco Unity subscribers are homed in Exchange 2000, skip this section.

Exchange 2000 Service Pack 3 and the Exchange 2000 Server Post-Service Pack 3 Rollup that is described in Microsoft Knowledge Base article 824282 resolve an intermittent problem with message notification.


Note

If Service Pack 3 and the rollup are not installed, Exchange 2000 Server sends extra UDP packets to ports on the Cisco Unity server that are not listening for packets. Such activity is seen by intrusion-detection systems as port scans or attacks.

This section contains two procedures. Do both in the order listed on the following servers on which either Exchange 2000 or Exchange 2000 administration software is installed:

- The Cisco Unity server. If failover is configured, both the primary and secondary Cisco Unity servers.
- The partner Exchange server.
- The Exchange 2000 servers on which Cisco Unity subscribers are homed.

To Install Exchange 2000 Service Pack 3

-
- Step 1** On Cisco Unity Service Packs CD 2 or from the location to which you saved the downloaded Service Packs CD 2 image files, browse to the directory **Exchange_2000_SP3\Setup\I386**, and double-click **Update.exe**.
- Step 2** Follow the on-screen prompts to complete the installation.
- Step 3** Restart the server.
- Step 4** If you have not already done so, repeat this procedure on the partner Exchange server and on every Exchange 2000 server on which Cisco Unity subscriber mailboxes are homed.
-

To Install the Exchange 2000 Post-Service Pack 3 Rollup

-
- Step 1** From the location to which you extracted the latest Exchange 2000 updates recommended for use with Cisco Unity, browse to the directory **Post-SP3 Rollup**, and double-click **Exchange2000-KB824282-x86-<language>.exe**.
- or
- On the Cisco Unity Post-Install CD, browse to the directory **Exchange_2000_Post_SP3_Rollup\Setup\I386**, and double-click **Update.exe**.
- Step 2** Follow the on-screen prompts to complete the installation.

- Step 3** Restart the server.
- Step 4** If you have not already done so, repeat this procedure on the partner Exchange server and on every Exchange 2000 server on which Cisco Unity subscriber mailboxes are homed.
-

Installing Exchange 2003 Service Pack 2

**Note**

If the partner Exchange server is not running Exchange 2003 and no Cisco Unity subscribers are homed in Exchange 2003, skip this section.

Install Exchange 2003 Service Pack 2 on the following servers on which either Exchange 2003 or Exchange 2003 administration software is installed:

- The Cisco Unity server. If failover is configured, both the primary and secondary Cisco Unity servers.
- The partner Exchange server.
- The Exchange 2003 servers on which Cisco Unity subscribers are homed.

To Install Exchange 2003 Service Pack 2

- Step 1** On Cisco Unity Service Packs CD 3 or from the location to which you saved the downloaded Service Packs CD 3 image files, browse to the directory **Exchange_2003_SP1\Setup\I386**, and double-click **Update.exe**.
- Step 2** Follow the on-screen prompts to complete the installation.
- Step 3** Restart the server.
- Step 4** If you have not already done so, repeat this procedure on the partner Exchange server and on every Exchange 2003 server on which Cisco Unity subscriber mailboxes are homed.
-

Installing the Latest Microsoft Service Packs and Updates Recommended for Use with Cisco Unity

While you were downloading software using the instructions in the [“Downloading Software for the Upgrade” section on page 1-10](#), if you identified any service packs

Some Microsoft updates can be installed only after a prerequisite service pack has been installed. Install all service packs, if any, before you install updates.

To Install the Latest Microsoft Service Packs Recommended for Use with Cisco Unity

Follow the instructions that you printed or downloaded from the Microsoft website when you downloaded the service packs.

To Install the Latest Microsoft Updates Recommended for Use with Cisco Unity

- Step 1** Insert the Cisco Unity Post-Install disc (either the disc shipped from Cisco or the disc that you created when you downloaded the latest Microsoft updates from Cisco.com) in the CD-ROM drive.
- Step 2** Browse to each of the applicable directories and install the correct language version of each update: English (ENU), French (FRA), German (DEU), or Japanese (JPN). (For example, if the French version of Windows 2000 Server is installed on the Cisco Unity server, install the French version of any Windows 2000 Server updates.)
- To speed the installation, you may want to:
- Install each update at a command prompt by using the /z option, so you do not have to restart the computer after installing each update.
 - Install each update at a command prompt by using the /m option, so the update installs without displaying any dialog boxes.
 - Create a batch file that installs all of the updates at once.
- Step 3** Restart the Cisco Unity server.
-

Upgrading and Configuring Cisco Unity Software

To upgrade and configure Cisco Unity software, you use the Cisco Unity Installation and Configuration Assistant to run four programs in a specific order. The programs:

- Check the system and upgrade the Cisco Unity software.
- Configure the Cisco Unity services.
- Configure Cisco Unity for the message store.
- Configure the Cisco Personal Communications Assistant to use SSL, if applicable.

Do the procedures in the following two subsections in the order listed.

Upgrading the Cisco Unity Software, and Configuring Services and Cisco Unity for the Message Store

To Upgrade and Configure the Cisco Unity Software

- Step 1** Log on to Windows by using the Cisco Unity installation account.



Caution If you have not already done so, disable virus-scanning and Cisco Security Agent services on the server, if applicable. Otherwise, the installation may fail.

- Step 2** On Cisco Unity DVD 1 or CD 1, or from the location to which you saved the downloaded Cisco Unity CD 1 image files, browse to the root directory and double-click **Setup.exe**.
- Step 3** If prompted, double-click the language of your choice to continue the upgrade.
- Step 4** On the Cisco Unity Installation and Configuration Assistant Welcome screen, click **Continue**.
- Step 5** If you already checked the consistency of the Cisco Unity database by using DbWalker, as recommended in the [“Checking the Consistency of the Cisco Unity Database, and Backing Up Cisco Unity Data” section on page 1-12](#), click **Skip DbWalker**, click **OK**, and skip to [Step 6](#).

If you have not checked the consistency of the Cisco Unity database recently, we recommend that you do so now. On a system with a few hundred subscribers, running DbWalker takes only a few minutes. However, on a large system, running DbWalker may take several hours. The duration depends on the speed of the processor, the amount of RAM in the server, the number of calls that Cisco Unity is taking, and other variables. Click **Run DbWalker from the Installation Media**, click **Continue**, and follow the on-screen prompts.

- Step 6** If you have already backed up Cisco Unity data by using the Disaster Recovery Backup tool, as recommended in the [“Checking the Consistency of the Cisco Unity Database, and Backing Up Cisco Unity Data” section on page 1-12](#), click **Skip DiRT**, click **OK**, and skip to [Step 7](#).
- If you have not backed up Cisco Unity data recently, we recommend that you do so now. Running the Disaster Recovery Backup tool takes only a few minutes, and having a DiRT backup allows you to restore Cisco Unity data easily, if necessary. Click **Run DiRT from the Installation Media**, click **Continue**, and follow the on-screen prompts.
- Step 7** In the main window of the assistant, click **Run the Cisco Unity Setup Program**.
- Step 8** If prompted, double-click the language of your choice to continue the upgrade.
- Step 9** If a message to stop services appears, click **OK**.
- Step 10** Click **Next** or **Continue** without changing values until the Select Features dialog box appears.
- Step 11** In the Select Features dialog box:
- Check the **Upgrade Cisco Unity** check box.
 - If the Cisco Unity license includes text to speech, check the **Enable TTS** check box.
If not, uncheck the **Enable TTS** check box.
 - Uncheck the **Install Voice Card Software** check box.



Caution If Cisco Unity is integrated with a circuit-switched phone system and you reinstall voice card software, the Dialogic quiet parameter and software settings for the D/120JCT-Euro and D/240PCI-T1 voice cards are reset to default values.

Step 12 Click **Next** or **Continue** without changing values until you are prompted to restart the Cisco Unity server.



Caution Do not cancel Cisco Unity Setup, or you may have to uninstall and reinstall Cisco Unity. In some cases, nothing may appear to be happening for long periods. To confirm that Cisco Unity Setup is still working, right-click the Windows taskbar and click **Task Manager**, then the **Processes** tab and **Image Name** (to sort by process name), and find **Setup.exe**. It should be using more than 0% of the CPU.

Step 13 Check the **Yes, I Want to Restart My Computer Now** check box, and click **Finish**.

Step 14 In the main window of the Cisco Unity Installation and Configuration Assistant, click **Run the Cisco Unity Services Configuration Wizard**. (You should be logged on to Windows with the Cisco Unity installation account.)

If you created a new installation account and service accounts in the “[Creating New Active Directory Accounts for Cisco Unity Installation and Services](#)” section on page 1-16, specify the new accounts when prompted.

Step 15 On the Welcome screen, click **Next**.

Step 16 Choose the message store type, and click **Next**.

Step 17 Follow the on-screen prompts to complete the configuration.

Step 18 In the main window of the assistant, click **Run the Cisco Unity Message Store Configuration Wizard**. (Note that you should be logged on to Windows with the Cisco Unity installation account.)

Step 19 Confirm that the message store server is running. If the message store server is not running, configuring the message store will fail.

Step 20 On the Welcome screen, click **Next**.

Step 21 Follow the on-screen prompts.

Step 22 When the message store configuration is complete, click **Next**.

Step 23 If you have not previously set up Cisco Unity to use SSL, the Set Up the Cisco Personal Communications Assistant to Use SSL page appears. Skip to the next subsection, “[Setting Up the Cisco Personal Communications Assistant to Use SSL](#).”

If Cisco Unity is already set up to use SSL, when the Summary screen appears, click **Close**.

Setting Up the Cisco Personal Communications Assistant to Use SSL

From the Cisco Unity Installation and Configuration Assistant, you can set up the Cisco PCA to use SSL. Using the SSL protocol ensures that all subscriber credentials—as well as the information that a subscriber enters on any page in the Cisco PCA—are encrypted as the data is sent across the network.

After the Cisco Unity Installation and Configuration Assistant is finished and the Cisco PCA is set up to use SSL, you manually set up the Cisco Unity Administrator and Status Monitor to use SSL. The *Cisco Unity Reconfiguration and Upgrade Guide* alerts you when to do the procedure.

If you do not want to set up the Cisco PCA to use SSL, see the “[Skipping Cisco PCA Setup for SSL](#)” section on page 1-25.

To set up the Cisco PCA to use SSL, do the procedures in the applicable section, depending on whether you are using a certificate authority:

- [Setting Up the Cisco PCA to Use SSL by Creating a Local Certificate Without a Certificate Authority, page 1-25](#)
- [Setting Up the Cisco PCA to Use SSL by Using a Certificate Authority, page 1-27](#)

If the Cisco Unity server is running Windows Server 2003, you can set up the Cisco Personal Communications Assistant to use SSL now. However, the option to do so by creating a local certificate without a certificate authority has not been automated for Windows Server 2003. If you want to set up the Cisco PCA to use SSL by using this method, you must do so manually. Refer to the “Using SSL to Secure Client/Server Connections” chapter of the *Cisco Unity Security Guide* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/usg/ex/index.htm.

Skipping Cisco PCA Setup for SSL

Do the procedure in this section if you do not want to set up the Cisco PCA to use SSL. (Note that without SSL when subscribers log on to the Cisco PCA, their credentials will be sent across the network to Cisco Unity in clear text. In addition, the information that subscribers enter on the pages of the Cisco PCA will not be encrypted.)

To Skip Cisco PCA Setup for SSL

- Step 1** On the Set Up the Cisco Personal Communications Assistant to Use SSL page, Click **Do Not Set Up Cisco Personal Communications Assistant to Use SSL**.
- Step 2** Click **Continue**.
- Step 3** Click **Close** to exit the Cisco Unity Installation and Configuration Assistant.
-

Setting Up the Cisco PCA to Use SSL by Creating a Local Certificate Without a Certificate Authority

To Set Up the Cisco PCA to Use SSL by Creating a Local Certificate Without a Certificate Authority

- Step 1** On the Set Up the Cisco Personal Communications Assistant to Use SSL page, click **Create a Local Certificate Without a Certificate Authority**.
- Step 2** Click **Internet Services Manager**.
- Step 3** Expand the name of the Cisco Unity server.
- Step 4** If the Cisco Unity server is running Windows Server 2003, expand **Web Sites**.
If not, skip to [Step 5](#).
- Step 5** Right-click **Default Web Site**, and click **Properties**.
- Step 6** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
- Step 7** Under Secure Communications, click **Server Certificate**.
- Step 8** On the Web Server Certificate wizard Welcome page, click **Next**.
- Step 9** Click **Create a New Certificate**, and click **Next**.

- Step 10** Click **Prepare the Request Now, But Send It Later**, and click **Next**.
- Step 11** Enter a name and a bit length for the certificate.
We strongly recommend that you choose a bit length of 512. Greater bit lengths may decrease performance.
- Step 12** Click **Next**.
- Step 13** Enter the organization information, and click **Next**.
- Step 14** For the common name of the site, enter either the system name of the Cisco Unity server or the fully qualified domain name.



Caution The name must exactly match the host portion of any URL that will access the system by using a secure connection.

- Step 15** Click **Next**.
- Step 16** Enter the geographical information, and click **Next**.
- Step 17** Specify the certificate request file name and location, and write down the file name and location because you will need the information later in this procedure.
- Step 18** Click **Next**.
- Step 19** Verify the request file information, and click **Next**.
- Step 20** Click **Finish** to exit the Web Server Certificate wizard.
- Step 21** Click **OK** to Close the Default Web Site Properties dialog box.
- Step 22** Close the Internet Services Manager window.
- Step 23** In the Cisco Unity Installation and Configuration Assistant, in the Enter Certificate Request File box, enter the full path and file name of the certificate request file that you specified in [Step 17](#).
- Step 24** Click **Create Certificate**.
- Step 25** Click **Internet Services Manager**.
- Step 26** Expand the name of the Cisco Unity server.
- Step 27** If the Cisco Unity server is running Windows Server 2003, expand **Web Sites**.
If not, skip to [Step 28](#).
- Step 28** Right-click **Default Web Site**, and click **Properties**.
- Step 29** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
- Step 30** Under Secure Communications, click **Server Certificate**.
- Step 31** On the Web Server Certificate wizard Welcome page, click **Next**.
- Step 32** Click **Process the Pending Request and Install the Certificate**.
- Step 33** Click **OK**.
- Step 34** In the Process a Pending Request dialog box, click **OK** to accept the default path and file name of the pending certificate request.
- Step 35** In the Certificate Summary dialog box, click **Next**.
- Step 36** Click **Finish** to exit the Web Server Certificate wizard.
- Step 37** Click **OK** to Close the Default Web Site Properties dialog box.
- Step 38** Close the Internet Services Manager window.

- Step 39** In the Cisco Unity Installation and Configuration Assistant, click **Enable Cisco PCA to Use SSL**.
 - Step 40** Click **Internet Services Manager**.
 - Step 41** Right-click the name of the Cisco Unity server, and click **Restart IIS**.
 - Step 42** In the Stop/Start/Restart dialog box, click **Restart Internet Services on <Servername>**.
 - Step 43** Click **OK**.
 - Step 44** Close the Internet Services Manager window.
 - Step 45** In the Cisco Unity Installation and Configuration Assistant, click **Continue**.
 - Step 46** Click **Close** to exit the Cisco Unity Installation and Configuration Assistant.
-

Setting Up the Cisco PCA to Use SSL by Using a Certificate Authority

This section contains four procedures.

If you are using Microsoft Certificate Services to issue your own certificate, do all four procedures in the order listed.

If you are using a certificate purchased from a Certificate Authority (for example, VeriSign), do only the fourth procedure, “[To Install the Certificate](#).”

To Create a Certificate Request by Using Microsoft Certificate Services

- Step 1** On the Set Up the Cisco Personal Communications Assistant to Use SSL page, click **Use a Certificate Authority**.
- Step 2** Click **Internet Services Manager**.
- Step 3** Expand the name of the Cisco Unity server.
- Step 4** If the Cisco Unity server is running Windows Server 2003, expand **Web Sites**.
If not, skip to [Step 5](#).
- Step 5** Right-click **Default Web Site**, and click **Properties**.
- Step 6** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
- Step 7** Under Secure Communications, click **Server Certificate**.
- Step 8** On the Web Server Certificate wizard Welcome page, click **Next**.
- Step 9** Click **Create a New Certificate**, and click **Next**.
- Step 10** Click **Prepare the Request Now, But Send It Later**, and click **Next**.
- Step 11** Enter a name and a bit length for the certificate.
We strongly recommend that you choose a bit length of 512. Greater bit lengths may decrease performance.
- Step 12** Click **Next**.
- Step 13** Enter the organization information, and click **Next**.

- Step 14** For the common name of the site, enter either the system name of the Cisco Unity server or the fully qualified domain name.



Caution The name must exactly match the host portion of any URL that will access the system by using a secure connection.

- Step 15** Click **Next**.
- Step 16** Enter the geographical information, and click **Next**.
- Step 17** Specify the certificate request file name and location, and write down the file name and location because you will need the information in the next procedure.
Save the file to a disk or to a directory that the certificate authority (CA) server can access.
- Step 18** Click **Next**.
- Step 19** Verify the request file information, and click **Next**.
- Step 20** Click **Finish** to exit the Web Server Certificate wizard.
- Step 21** Click **OK** to Close the Default Web Site Properties dialog box.
- Step 22** Close the Internet Services Manager window.
- Step 23** Click **Close** to exit the Cisco Unity Installation and Configuration Assistant.

To Submit the Certificate Request by Using Microsoft Certificate Services

- Step 1** On the server that is acting as the CA, on the Windows Start menu, click **Run**.
- Step 2** Run **Certreq**.
- Step 3** Browse to the directory where you saved the certificate request file, and double-click the file.
- Step 4** Click the CA to use, and click **OK**.

Once the CA submits the certificate request, it assigns a pending status by default for added security. This requires a person to verify the authenticity of the request and to manually issue the certificate.

To Issue the Certificate by Using Microsoft Certificate Services

- Step 1** On the server that is acting as the CA, on the Windows Start menu, click **Programs > Administrative Tools > Certification Authority**.
- Step 2** In the left pane of the Certification Authority window, expand **Certification Authority**.
- Step 3** Expand <Certification Authority name>.
- Step 4** Click **Pending Requests**.
- Step 5** In the right pane, right-click the request, and click **All Tasks > Issue**.
- Step 6** In the left pane, click **Issued Certificates**.

- Step 7** In the right pane, double-click the certificate to open it.
 - Step 8** Click the **Details** tab.
 - Step 9** In the Show list, choose **<All>**, and click **Copy to File**.
 - Step 10** On the Certificate Export wizard Welcome page, click **Next**.
 - Step 11** Accept the default export file format **DER encoded binary X.509 (.CER)**, and click **Next**.
 - Step 12** Specify a file name and a location that the Cisco Unity server can access, and click **Next**.
 - Step 13** Verify the settings, and click **Finish**.
 - Step 14** Click **OK** to close the Certificate Details dialog box.
 - Step 15** Close the Certification Authority window.
-

To Install the Certificate

- Step 1** On the Cisco Unity server, double-click the **CUICA** icon on the desktop.
- Step 2** In the Cisco Unity Installation and Configuration Assistant, click **Use a Certificate Authority**.
- Step 3** On the Set Up the Cisco Personal Communications Assistant to Use SSL page, at Step 3, click **Internet Services Manager**.
- Step 4** Expand the name of the Cisco Unity server.
- Step 5** If the Cisco Unity server is running Windows Server 2003, expand **Web Sites**.
If not, skip to [Step 6](#).
- Step 6** Right-click **Default Web Site**, and click **Properties**.
- Step 7** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
- Step 8** Under Secure Communications, click **Server Certificate**.
- Step 9** On the Web Server Certificate wizard Welcome page, click **Next**.
- Step 10** Click **Process the Pending Request and Install the Certificate**, and click **Next**.
- Step 11** Browse to the directory of the certificate (.cer) file, and double-click the file.
- Step 12** Verify the certificate information, and click **Next**.
- Step 13** Click **Finish** to exit the Web Server Certificate wizard.
- Step 14** Click **OK** to close the Default Web Site Properties dialog box.
- Step 15** Close the Internet Services Manager window.
- Step 16** In the Cisco Unity Installation and Configuration Assistant, click **Enable Cisco PCA to Use SSL**.
- Step 17** Restart IIS:
 - a. Click **Internet Services Manager**.
 - b. Right-click the name of the Cisco Unity server, and click **Restart IIS**.
 - c. In the Stop/Start/Restart dialog box, click **Restart Internet Services on <Servername>**.

- d. Click **OK**.
- e. Close the Internet Services Manager window.

Step 18 Click **Close** to exit the Cisco Unity Installation and Configuration Assistant.

Designating the Phone System as Cisco CallManager Express



Note

If the Cisco Unity system is configured for failover, skip this section. The Cisco CallManager Express integration is not supported with Cisco Unity failover.

You must do the procedure in this section when both of the following conditions apply:

- You are upgrading to the shipping version of Cisco Unity from Cisco Unity 4.0(1) through 4.0(4).
- Cisco Unity is integrated with Cisco CallManager Express or with a Cisco CallManager cluster that includes a Cisco CallManager Express server.

Doing the procedure enables all the Cisco CallManager Express integration features listed in the applicable Cisco CallManager Express integration guide.

To Designate the Phone System as Cisco CallManager Express

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Cisco Unity > Manage Integrations**. UTIM appears.
- Step 2** In the left pane of the UTIM window, click the Cisco CallManager Express integration or the Cisco CallManager integration that includes a Cisco CallManager Express server.
- Step 3** In the right pane, click the applicable cluster.
- Step 4** In the right pane, click the **Servers** tab.
- Step 5** In the list of servers, double-click the first Cisco CallManager Express server.
- Step 6** In the Modify Server dialog box, in the IP Address or Host Name field, enter the IP address of the Cisco CallManager Express server.
- Step 7** Check the **This Server Is Cisco CallManager Express** check box.
- Step 8** Click **OK**.
- Step 9** On the Servers tab, click **Save**.
- Step 10** At the prompt to restart the Cisco Unity services, click **Yes**. The Cisco Unity services restart.



Note

When restarting Cisco Unity, use the UTIM prompt instead of the Cisco Unity icon in the Windows taskbar. The taskbar icon does not restart all the Cisco Unity services.

- Step 11** Exit UTIM.
-

Re-enabling Virus-Scanning and Cisco Security Agent Services

You re-enable virus-scanning and Cisco Security Agent services now that all of the software installations that could have been affected if the services were running are complete.

To Re-enable and Start Virus-Scanning and Cisco Security Agent Services

- Step 1** Refer to the virus-scanning software documentation to determine the names of the virus-scanning services.
- Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 3** Re-enable and start each virus-scanning service and the Cisco Security Agent service:
- In the right pane, double-click the service.
 - On the General tab, in the Startup Type list, click **Automatic** to re-enable the service.
 - Click **Start** to start the service.
 - Click **OK** to close the Properties dialog box.
- Step 4** When the services have been re-enabled, close the Services MMC.
-

Installing Additional Dialogic Software for D/120JCT-Euro Rev 2 Voice Cards

The Intel Dialogic D/120JCT-Euro Rev 2 voice card requires some software that is installed automatically with Cisco Unity 4.0(5) and later but that was not installed for Cisco Unity versions 4.0(1) through 4.0(4). If you are upgrading to the shipping version from Cisco Unity 4.0(1) through 4.0(4) and you are using D/120JCT-Euro Rev 2 voice cards, do the following procedure.

To Install Additional Dialogic Software for the Dialogic D/120JCT-Euro Rev 2 Voice Card

- Step 1** On a secure server, go to the Other Cisco Unity Components Software Download page at <http://www.cisco.com/cgi-bin/tablebuild.pl/unity>, and download the file **DialogicD120JCTEuro.exe**.



Note To access the software download page, you must be logged on to Cisco.com as a registered user.

- Step 2** Click the file **DialogicD120JCTEuro.exe**.
- Step 3** When the download is complete, copy the file **DialogicD120JCTEuro.exe** to the Cisco Unity server.
- Step 4** On the Cisco Unity server, in Windows Explorer, double-click **DialogicD120JCTEuro.exe**.
- Step 5** Follow the on-screen prompts to extract the following three files to the directory **Commserver\Dialogic\Data**:
- nz_120jr2.prm
 - au_120jr2.prm

- eu_120jr2.prm
- Step 6** Right-click the **Cisco Unity** icon in the status area of the taskbar, and click **Stop Cisco Unity**.
- Step 7** On the Windows Start menu, click **Programs > Dialogic System Software > Dialogic Configuration Manager - DCM**.
- Step 8** On the Dialogic Configuration Manager Service menu, click **Stop Service**.
- Step 9** On the Dialogic Configuration Manager Service menu, click **Start Service**.
Stopping and restarting the service forces the Rev 2 card(s) to download the updated .prm files.
- Step 10** On the Windows Start menu, click **Programs > Startup > AvCsTrayStatus** to restart the Cisco Unity icon.
- Step 11** When the Cisco Unity icon appears in the status area of the taskbar, right-click it.
- Step 12** Click **Start Cisco Unity**.

Setting Up the Cisco Unity Administrator and Status Monitor to Use SSL



Note

If you are not setting up Cisco Unity to use SSL, skip this section.

Using the SSL protocol ensures that all subscriber credentials—as well as the information that a subscriber enters on any page in the Cisco Unity Administrator—are encrypted as the data is sent across the network.

To Set Up the Cisco Unity Administrator and Status Monitor to Use SSL

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
- Step 2** Expand the name of the Cisco Unity server.
- Step 3** If the Cisco Unity server is running Windows Server 2003, expand **Web Sites**.
If not, skip to [Step 4](#).
- Step 4** Expand **Default Web Site**.
- Step 5** Under Default Web Site, right-click **Web**, and click **Properties**.
- Step 6** In the Properties dialog box, set the Web directory to use SSL:
- a. Click the **Directory Security** tab.
 - b. Under Secure Communications, click **Edit**.
 - c. Check the **Require Secure Channel (SSL)** check box.
 - d. Click **OK** to close the Secure Communications dialog box.
 - e. Click **OK** to close the Properties dialog box.
- Step 7** Under Default Web Site, right-click **SAWeb**, and click **Properties**.

- Step 8** Repeat [Step 6](#) to set the SAWeb directory to use SSL.
- Step 9** Under Default Web Site, right-click **Status**, and click **Properties**.
- Step 10** Repeat [Step 6](#) to set the Status directory to use SSL.
- Step 11** Under Default Web Site, double-click **AvXml**.
- Step 12** In the right pane, right-click **AvXml.dll**, and click **Properties**.
- Step 13** In the Properties dialog box, click the **File Security** tab.
- Step 14** Under Secure Communications, click **Edit**.
- Step 15** Check the **Require Secure Channel (SSL)** check box.
- Step 16** Click **OK** to close the Secure Communications dialog box.
- Step 17** Click **OK** to close the AvXml.dll Properties dialog box.
- Step 18** Close the Internet Services Manager window.

Configuring Internet Explorer to Display the Cisco Unity Administrator When You Use the Cisco Unity Administration Account (Windows Server 2003 Only)

This section applies only when Windows Server 2003 is installed on the Cisco Unity server.

If you created a Cisco Unity administration account as recommended by the Cisco Unity installation guide, and if you log on to Windows using that account, the changes that Windows Server 2003 Service Pack 1 makes to default Internet Explorer security settings cause the Cisco Unity Administrator to display a blank page. Do the following procedure to configure Internet Explorer to display the Cisco Unity Administrator when you log on to Windows using the administration account.

To Configure Internet Explorer to Display the Cisco Unity Administrator

- Step 1** Log on to the Cisco Unity server using the Cisco Unity administration account.
- Step 2** Right click the Cisco Unity icon in the system tray, and click **Launch System Admin**.
- Step 3** If you are prompted to provide a user name and password, click **Cancel**.
- Step 4** On the Internet Explorer Tools menu, click **Internet Options**.
- Step 5** Click the **Security** tab.
- Step 6** Under Select a Web Content Zone to Specify Its Security Settings, click the **Trusted Sites** icon.
- Step 7** Click **Sites**.
- Step 8** In the Trusted Sites dialog box, in the Add This Website to the Zone field, enter the applicable value depending on whether the Cisco Unity Administrator is set up to use SSL:

If the Cisco Unity Administrator is set up to use SSL	Enter https:\\<CiscoUnityServerName>
If the Cisco Unity Administrator is not set up to use SSL	Enter http:\\<CiscoUnityServerName>

- Step 9** If the Cisco Unity Administrator is set up to use SSL, check the **Require Server Verification (https:)** for **All Sites in This Zone** check box. If not, uncheck the check box.
 - Step 10** Click **Add**.
 - Step 11** Click **Close** to close the Trusted Sites dialog box.
 - Step 12** On the Security tab, click **Custom Level**.
 - Step 13** In the Security Settings dialog box, change the value of the Reset To list to Low.
 - Step 14** Click **Reset**, and click **Yes** to confirm that you want to change the security settings for this zone.
 - Step 15** Click **OK** to close the Security Settings dialog box.
 - Step 16** If the Security Settings dialog box does not close:
 - a. Close the dialog box by clicking the **X** in the upper-right corner.
 - b. In the “not responding” message box, click **End Now**. (The “not responding” message box may take a few seconds to appear.)
 - Step 17** Restart the **Cisco Unity Administrator**.
-

Securing the Example Administrator and Example Subscriber Accounts Against Toll Fraud

It is possible for a malicious user to dial into Cisco Unity, log on as the Example Administrator or Example Subscriber by using the default extension and password, and configure Cisco Unity to forward calls to phone numbers for which there are charges or to reconfigure greetings so an operator believes the messaging system is personally accepting collect-call charges. To help secure Cisco Unity against toll fraud, we strongly recommend that you change the phone password for both accounts after Cisco Unity is installed.

Although the Example Subscriber account is no longer created during Cisco Unity installation in versions 4.0(3) and later, you may still have an Example Subscriber account from an earlier version, as the account is not removed during the upgrade process.

(For information on the accounts, refer to the “Default Accounts” section in the “Default Accounts and Message Handling” chapter of the *Cisco Unity System Administration Guide, Release 4.0(5)* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag405/ex/index.htm.)

To Change the Password on the Example Administrator and Example Subscriber Accounts

- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Subscribers** page.
- Step 2** Click the **Find** icon.
- Step 3** On the Find and Select Subscriber page, click **Find**.
- Step 4** Click **Example Administrator**.
- Step 5** In the left pane, click **Phone Password**.
- Step 6** In the right pane, check the **User Cannot Change Password** check box.
- Step 7** Check the **Password Never Expires** check box.

- Step 8** Under **Reset Phone Password**, enter and confirm a new password by using digits 0 through 9. We recommend that you enter a long and nontrivial password; 20 digits or more is desirable. (The minimum length of the password is set on the **Subscribers > Account Policy > Phone Password Restrictions** page.) In a nontrivial password:
- The digits are not all the same (for example, 9999).
 - The digits are not consecutive (for example, 1234).
 - The password is not the same as the extension assigned to the example account.
 - The password does not spell the name of the example account, the name of the company, the name of the IT manager, or any other obvious words.
- Step 9** Click the **Save** icon.
- Step 10** Click the **Find** icon.
- Step 11** On the Find and Select Subscriber page, click **Find**.
- Step 12** Click **Example Subscriber**.
- Step 13** Repeat [Step 5](#) through [Step 9](#) for Example Subscriber.
- Step 14** Close the Cisco Unity Administrator.
-

Disabling or Deleting Old Installation and Service Accounts

If you created new installation and service accounts to take advantage of the reduced Active Directory permissions that are set by the Permissions wizard beginning with Cisco Unity 4.2(1), use Active Directory Users and Computers (ADUC) to disable or delete the old accounts. Refer to ADUC Help for more information.

Hardening the Cisco Unity Server

**Note**

If the Cisco Unity server is not connected to the corporate network, skip this section.

We strongly recommend that you secure Cisco Unity and the Cisco Unity server. Refer to the *Cisco Unity Security Guide* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/usg/ex/index.htm.

