



Security Guide for Cisco Unity (With Microsoft Exchange)

Release 5.x
Revised October 23, 2008

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

Text Part Number: OL-13850-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R)

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

Security Guide for Cisco Unity Release 5.x (With Microsoft Exchange)
© 2008 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface vii

- Audience and Use vii
- Cisco Unity Documentation vii
- Obtaining Documentation, Obtaining Support, and Security Guidelines vii
- Cisco Product Security Overview vii

CHAPTER 1

Securing the Cisco Unity Server(s) and the Operating System 1-1

- Securing the Physical Server 1-1
- Securing Windows 1-1
- Changing Windows 2000 Server Audit Policies and User Rights 1-2
- Changing Windows 2000 Server Event Log Settings 1-3
- Changing Permissions on Files in the CommServer Directory 1-3
- Changing Startup Type for Services on the Cisco Unity Server 1-3
- Securing TCP/UDP Ports 1-6

CHAPTER 2

Securing Microsoft Software on the Cisco Unity Server(s) 2-1

- Securing SQL Server 2000 or MSDE 2000 2-2
 - Securing Additional Instances of MSDE 2000 2-2
- Securing Internet Explorer 2-3
- Securing IIS 2-3
 - Following IIS Configuration Guidelines 2-4
 - Using the Internet Information Services Lockdown Wizard and URLScan Tool 2-4
- Securing Microsoft Message Queuing 2-5
- Securing Exchange 2-5
- Installing Service Packs and Security Updates 2-6

CHAPTER 3

IP Communications Required by Cisco Unity 3-1

- Overview 3-1
- Network Traffic from Cisco Unity to Various Servers and to Clients 3-1
 - Network Traffic from Cisco Unity to a Domain Controller 3-2
 - Network Traffic from Cisco Unity to a Global Catalog Server 3-2
 - Network Traffic from Cisco Unity to a DNS Server 3-3
 - Network Traffic from Cisco Unity to the Partner Exchange Server 3-3

- Network Traffic Between Cisco Unity Failover Servers 3-4
- Network Traffic from Cisco Unity to Cisco Unified Communications Manager and Phones 3-5
- Network Traffic from Cisco Unity to SIP Endpoints, Including PIMG Devices and Phones 3-5
- Network Traffic from Cisco Unity to Subscriber Workstations (for the Cisco PCA or ViewMail for Outlook) 3-5
- Network Traffic from Clients to Cisco Unity 3-6
 - Network Traffic from Cisco Unified Communications Manager and Phones to Cisco Unity 3-6
 - Network Traffic from SIP Endpoints, Including PIMG Devices and Phones, to Cisco Unity 3-6
 - Network Traffic from VNC Client Workstations to Cisco Unity 3-6
 - Network Traffic from SNMP Management Stations to Cisco Unity 3-6
 - Network Traffic from Administrator Workstations to Cisco Unity 3-7
 - Network Traffic from Subscriber Workstations to Cisco Unity (for the Cisco PCA or ViewMail for Outlook) 3-7
- Network Traffic to and from Exchange 3-8
 - Network Traffic from Exchange to Cisco Unity 3-8
 - Network Traffic from Exchange to DNS 3-8
 - Network Traffic from Exchange to a Domain Controller 3-8
 - Network Traffic from Exchange to a Global Catalog Server 3-9
 - Network Traffic Between Exchange Servers 3-10
 - Network Traffic Between Exchange and Other Voice-Messaging Systems 3-10
 - Network Traffic Between Other Voice-Messaging Systems and Exchange 3-10
- Network Traffic from Cisco Unity Subscriber Workstations to Various Servers 3-10
 - Network Traffic from Cisco Unity Subscriber Workstations to a DNS Server 3-11
 - Network Traffic from Cisco Unity Subscriber Workstations to the Exchange Server on Which the Subscriber Mailbox Is Homed 3-11
- Restricting DCOM Dynamic Port Allocation 3-11

CHAPTER 4

Using Security Software 4-1

- Using Cisco Security Agent 4-1
- Using Antivirus Software 4-2

CHAPTER 5

Preventing Toll Fraud 5-1

- Using Restriction Tables to Help Prevent Toll Fraud 5-1

CHAPTER 6

Securing the Connection Between Cisco Unity, Cisco Unified Communications Manager, and IP Phones 6-1

- Security Issues for Connections Between Cisco Unity, Cisco Unified Communications Manager, and IP Phones 6-1
- Cisco Unified Communications Manager Security Features for Cisco Unity Voice Messaging Ports 6-2

Security Mode Settings for Cisco Unified Communications Manager and Cisco Unity	6-4
Best Practices	6-4

CHAPTER 7**Securing Accounts 7-1**

Understanding Accounts	7-1
Best Practices for Accounts That Are Used to Access the Cisco Unity Administrator	7-2
Best Practices for Accounts That Are Used to Access the Cisco Unity Server	7-3
Best Practices When Deleting Cisco Unity Subscriber Accounts	7-4
Securing the Account That Was Used to Install Cisco Unity	7-4
Securing the Directory Services and Message Store Services Accounts	7-4
Best Practices for Securing Default Accounts	7-5

CHAPTER 8**Authentication for Cisco Unity Applications 8-1**

Determining Which Authentication Method to Use for the Cisco Unity Administrator and Status Monitor	8-2
How Integrated Windows Authentication Works with the Cisco Unity Administrator and Status Monitor	8-2
Advantages and Disadvantages of Using Integrated Windows Authentication with the Cisco Unity Administrator and the Status Monitor	8-3
How Anonymous Authentication Works with the Cisco Unity Administrator and Status Monitor	8-4
Advantages and Disadvantages of Using Anonymous Authentication with the Cisco Unity Administrator and Status Monitor	8-5
Configuring IIS so That the Cisco Unity Administrator and Status Monitor Use Integrated Windows Authentication	8-5
Configuring IIS so That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication	8-7
Best Practices for Securing Access to the Cisco Unity Administrator and Status Monitor	8-8
Understanding How Cisco Personal Communications Assistant (PCA) Authentication Works	8-10
Best Practices for Securing Access to the Cisco PCA	8-11
Determining Whether to Offer Enhanced Phone Security	8-12
Configuring the Cisco Unity Conversation to Use Enhanced Phone Security	8-12

CHAPTER 9**Password and Account Policy Management 9-1**

About the Passwords That Subscribers Use to Access Cisco Unity Applications	9-2
Securing Passwords On Default Accounts That Are Created by Cisco Unity	9-2
Ensuring That Subscribers Are Initially Assigned Unique and Secure Windows Passwords	9-4
Ensuring That Subscribers Are Initially Assigned Unique and Secure Phone Passwords	9-5
Changing Passwords That Are Used to Access the Cisco Unity Administrator	9-5

- Changing Cisco PCA Passwords 9-6
- Changing Cisco Unity Phone Passwords 9-6
- Defining Account Policies for Accessing the Cisco Unity Administrator 9-7
- Defining Account Policies for Accessing the Cisco PCA 9-7
- Defining Account Policies for Phone Access to Cisco Unity 9-8
 - Setting Phone Password Restrictions 9-8
 - Setting Account Lockout Restrictions 9-9

CHAPTER 10

- Using SSL to Secure Client/Server Connections 10-1**
 - Determining Whether to Set Up Cisco Unity Applications to Use SSL 10-1
 - Manually Setting Up the System to Use SSL 10-2
 - Installing the Microsoft Certificate Services Component 10-3
 - Creating and Submitting a Certificate Request 10-3
 - Issuing and Installing the Certificate 10-4
 - Setting Up Cisco Unity Web Applications to Use SSL 10-6
 - Distributing the Root Certificate to the Trusted Root Store 10-7
 - Setting Up SSL Redirection 10-10
 - Managing Security Alerts When Using SSL Connections with BlackBerry Servers 10-10

CHAPTER 11

- Securing Subscriber Messages 11-1**
 - How Cisco Unity Handles Messages That Are Marked Private 11-1
 - Secure Messaging 11-2
 - Understanding How Cisco Unity Handles Secure Messages 11-2
 - Limitations of Secure Messaging 11-4
 - Installing and Configuring Secure Messaging 11-6
 - Maintenance Considerations When Secure Messaging Is in Use 11-15
 - Secure Messaging and Legal Discoverability 11-16
 - Technical Details of Secure Messaging 11-17
 - Best Practices for Using Text to Speech (Unified Messaging) 11-18
 - Disabling the Copy to File Option in the Media Master for the Cisco Unity Inbox 11-18

INDEX



Preface

Audience and Use

The *Security Guide for Cisco Unity* provides information related to all aspects of the security of your Cisco Unity system. Within each chapter, you will find descriptions of potential security issues; information on any actions you need to take; recommendations that will help you make decisions; discussion of the ramifications of the decisions you make; and in many cases, best practices.

Cisco Unity Documentation

For descriptions and the URLs of Cisco Unity documentation on Cisco.com, see the *Documentation Guide for Cisco Unity*. The document is shipped with Cisco Unity and is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_documentation_roadmaps_list.html.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>. If you require further assistance, contact us by sending e-mail to export@cisco.com.



CHAPTER 1

Securing the Cisco Unity Server(s) and the Operating System

In this chapter, you will find descriptions of potential security issues related to securing the physical server and securing Windows; information on any actions that you need to take; recommendations that will help you make decisions; and some best practices.

Use the recommendations in this chapter to secure the physical Cisco Unity server and the operating system.

See the following sections for details:

- [Securing the Physical Server, page 1-1](#)
- [Securing Windows, page 1-1](#)
- [Changing Windows 2000 Server Audit Policies and User Rights, page 1-2](#)
- [Changing Windows 2000 Server Event Log Settings, page 1-3](#)
- [Changing Permissions on Files in the CommServer Directory, page 1-3](#)
- [Changing Startup Type for Services on the Cisco Unity Server, page 1-3](#)
- [Securing TCP/UDP Ports, page 1-6](#)

Securing the Physical Server

You can find best practices for securing a physical unit from unwanted access on the CERT Coordination Center (CERT/CC) website. On the CERT site, in the “CERT Security Improvement Modules,” see the “Practices About Hardening and Securing Systems” section.

Securing Windows

Microsoft provides a variety of recommendations for installing and securing a Windows Server 2003 or Windows 2000 Server system:

- For Windows Server 2003, see the article “Checklists; Windows Server 2003, Standard Edition,” and for Windows 2000 Server, see the article “Installing and Securing a New Windows 2000 System,” both available on the Microsoft website.
- See the Microsoft Security Home page for the most current hardening and security guide for Windows 2000 Server and Windows Server 2003, and for the *IIS 5.0 Baseline Security Checklist*.

To check an existing Windows 2000 Server or Windows Server 2003 installation for vulnerabilities:

- Confirm that the latest supported service pack and all recommended Microsoft updates are installed on the server. (Supported service packs and recommended updates are listed in *Recommended and Supported Service Packs and Updates for Use with Cisco Unity and the Cisco Unity Bridge*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_device_support_tables_list.html.)
- Query the Microsoft TechNetWeb site for the latest information on securing an existing Windows 2000 Server or Windows Server 2003 system.

A security policy can be applied to the Cisco Unity server, but it should not be applied until after the Cisco Unity installation is complete. For more information about security policies and how to apply them, refer to the Microsoft website, or to Windows Help.

Applying certain security templates can render Cisco Unity inoperable. If you apply security templates, first verify that they use the suggested security settings outlined in the following “[Changing Windows 2000 Server Audit Policies and User Rights](#)” section. These settings enable the Cisco Unity server to maintain full functionality.

Changing Windows 2000 Server Audit Policies and User Rights

Use the recommended Windows 2000 Server settings shown in [Table 1-1](#) to track when and how the Cisco Unity server is being accessed, and to restrict access to the Cisco Unity server. To change these settings, use the Local Security Policy MMC (on the Windows Start menu, click Programs > Administrative Tools > Local Security Policy).

Best Practice

If your site already has a security policy in place, review the following policy settings to determine whether the additional settings are necessary for securing the Cisco Unity server.

Table 1-1 *Recommended Windows 2000 Server Local Security Policies: Audit Policies and User Rights*

Setting	Recommended Value
Audit account login events	Failure
Audit account management	Success, Failure
Audit directory service access	Failure
Audit login events	Failure*
Audit object access	No auditing*
Audit policy change	Success, Failure
Audit privilege use	Failure*
Audit system events	No auditing*
Act as part of the operating system	Account used to install Cisco Unity*
Access this computer from the network	Backup Operators, Power Users, Users, Administrators, servername\IWAM, domainname\ISUR_servername
Shut down the system	Backup Operators, Administrators

* The recommended value is the same as the default value.

Changing Windows 2000 Server Event Log Settings

Use the recommended settings shown in [Table 1-2](#) to ensure that event log entries are not overwritten and to restrict access to the event log. To change these settings, use the Local Security Policy MMC (on the Windows Start menu, click Programs > Administrative Tools > Local Security Policy).

Table 1-2 Recommended Windows 2000 Server Event Log Settings

Setting	Recommended Value
Maximum application log size	8192 KB or greater
Maximum security log size	8192 KB
Maximum system log size	8192 KB
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled
Retain system log	14 days
Retention method for application log	As needed*
Retention method for security log	As needed

* The recommended value is the same as the default value.

Changing Permissions on Files in the CommServer Directory

Cisco Unity Setup grants Full Control permissions to Everyone for all of the files in the directory where Cisco Unity is installed (CommServer by default). Changing these permissions is not supported.



Caution

If you change permissions on files in this directory, Cisco Unity may not function properly.

Changing Startup Type for Services on the Cisco Unity Server

Revised October 12, 2007

The services shown in [Table 1-3](#) should be set to the recommended startup type. You can change the setting in the Services MMC (on the Windows Start menu, click Programs > Administrative Tools > Services). Note that for Windows 2000 Server, the recommended values marked with an asterisk (*) are the same as the default values.

Table 1-3 Services Settings

Setting	Recommended Startup Type
Alerter	Disabled

Table 1-3 Services Settings (continued)

Setting	Recommended Startup Type
Application Management	Manual*
Automatic Updates	Automatic*
Background Intelligent Transfer Service	Manual*
Clipboard	Disabled
COM+ Event System	Manual*
Computer Browser	Automatic*
CsBridgeConnector	Manual*
DHCP Client	Disabled
Distributed File System	Disabled
Distributed Link Tracking Client	Disabled
Distributed Link Tracking Server	Disabled
Distributed Transaction Coordinator	Automatic*
DNS Client	Automatic*
DNS Server	Automatic* if in use, disabled otherwise
Event Log	Automatic*
Fax Service	Disabled
File Replication Service	Automatic*
IIS Admin Service	Automatic*
Indexing Service	Manual*
Internet Connection Sharing	Disabled
Intersite Messaging	Automatic*
IPSEC Policy Agent	Automatic*
Kerberos Key Distribution Center	Automatic*
License Logging Service	Disabled
Logical Disk Manager	Automatic*
Logical Disk Manager Administrative Service	Manual*
Message Queuing	Automatic*
Messenger	Disabled
Microsoft Exchange Event	Manual*
Microsoft Exchange IMAP4	Disabled
Microsoft Exchange Information Store	Automatic*
Microsoft Exchange Management	Automatic*
Microsoft Exchange MTA Stacks	Automatic*
Microsoft Exchange POP3	Disabled
Microsoft Exchange Routing Engine	Automatic*
Microsoft Exchange Site Replication Service	Disabled*

Table 1-3 Services Settings (continued)


Setting	Recommended Startup Type
Microsoft Exchange System Attendant	Automatic*
Microsoft Search	Automatic*
MSSQLSERVER	Automatic*
MSSQLServerADHelper	Manual*
Net Logon	Automatic*
NetMeeting Remote Desktop Sharing	Disabled
Network Connections	Manual*
Network DDE	Manual*
Network DDE DSDM	Manual*
Network News Transport Protocol (NNTP)	Disabled
NT LM Security Support Provider	Manual*
Performance Logs and Alerts	Manual*
Plug and Play	Automatic*
Print Spooler	Disabled
Protected Storage	Automatic*
QoS RSVP	Manual*
Remote Access Auto Connection Manager	Disabled
Remote Access Connection Manager	Disabled
Remote Procedure Call (RPC)	Automatic*
Remote Procedure Call (RPC) Locator	Automatic*
Remote Registry Service	Disabled
 Caution The Remote Registry Service must be enabled to install Cisco Unity and to configure failover. As soon as Cisco Unity is installed or failover is configured, the service should be disabled again.	
Removable Storage	Automatic*
Routing and Remote Access	Disabled*
RunAs Service	Automatic*
Security Accounts Manager	Automatic*
Server	Automatic*
Simple Mail Transport Protocol (SMTP)	Automatic* if Exchange is installed on the Cisco Unity server. Disabled if Exchange is not installed on the Cisco Unity server.
Smart Card	Manual*
Smart Card Helper	Manual*

Table 1-3 Services Settings (continued)

Setting	Recommended Startup Type
SQLSERVERAGENT	Automatic*
System Event Notification	Automatic*
Task Scheduler	Automatic*
TCP/IP NetBIOS Helper Service	Automatic*
Telephony	Manual*
Telnet	Disabled*
Terminal Services	Automatic*
Uninterruptible Power Supply	Manual*
Utility Manager	Manual*
Windows Installer	Manual*
Windows Management Instrumentation	Automatic*
Windows Management Instrumentation Driver Extensions	Manual*
Windows Time	Automatic*
Workstation	Automatic*
World Wide Web Publishing Service	Automatic*

* For Windows 2000 Server, the recommended value is the same as the default value.

Securing TCP/UDP Ports

Revised April 17, 2008

The “[IP Communications Required by Cisco Unity](#)” chapter lists the TCP and UDP ports that are used by Cisco Unity and by associated servers. The information is useful for configuring a firewall and for configuring Quality of Service (QoS) by using destination ports and protocols as queuing criteria. (Cisco Unity does not assign DSCP values for traffic other than voice traffic.)

Do not separate the Cisco Unity server (or the primary server, in a failover or standby-redundancy configuration) by a firewall from the following servers:

- The partner Exchange server.
- The domain controller that Cisco Unity monitors for directory updates.
- The global catalog server that Cisco Unity monitors for directory updates.
- The global catalog server with which the Cisco Unity MAPI client communicates.

Cisco Unity failover and standby redundancy were designed with the expectation that the primary server would generally be the active server. In a failover or standby-redundancy configuration, when the secondary server is separated from any of the listed servers by a firewall, the secondary server must be used as the active server only for brief periods. The problem with the primary server must be resolved promptly, and the primary server must be made the active server again at the earliest opportunity.

**Note**

Additional ports may need to be opened for supported third-party hardware-related software components and supported third-party applications (such as virus protection and backup software) that are installed on the Cisco Unity server. For information, refer to the manufacturer or software publisher documentation.

All the protocols and services use static ports except DCOM, MAPI notifications, and RTP. For information on restricting DCOM to a known port range, see the [“Restricting DCOM Dynamic Port Allocation”](#) section on page 3-11.



CHAPTER 2

Securing Microsoft Software on the Cisco Unity Server(s)

In this chapter, you will find descriptions of potential security issues related to the software that is installed on the Cisco Unity server; information on any actions you need to take; recommendations that will help you make decisions; discussion of the ramifications of the decisions you make; and in many cases, best practices.

The Cisco Unity operating environment includes all of the third-party components needed to service subscribers. These components consist mainly of Microsoft products, although other third-party products such as Intel Dialogic software may also be installed. At the time this document was written, the following Microsoft products were required components of the Cisco Unity operating environment:

- Windows Server 2003 or Windows 2000 Server with the latest recommended service pack and updates
- Internet Information Server (IIS) 5.0 (for Windows 2000 Server) and IIS 6.0 (for Windows Server 2003)
- Internet Explorer (IE) 6.0 with Service Pack 1 and the latest recommended updates
- Microsoft Message Queuing 2.0
- MSXML 3.0 with Service Pack 1
- Microsoft .NET Framework 1.1
- SQL Server 2000 or MSDE 2000 with Service Pack 3a and the latest recommended updates
- Exchange 2003 or Exchange 2000 with the latest recommended service pack and updates

Each component in the Cisco Unity operating environment presents a security risk, because if a component is compromised, it may prevent Cisco Unity from running reliably and effectively. By default, most of these components are installed with minimum security. As applicable, use the guidelines presented in the following sections in conjunction with the applicable Cisco Unity installation guide (available at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html) to harden the Cisco Unity operating environment during or after a new Cisco Unity installation.

For detailed current information, see the following:

- For Cisco Unity operating environment components, see *System Requirements for Cisco Unity*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

- For recommended service packs and updates, see *Recommended and Supported Service Packs and Updates for Use with Cisco Unity and the Cisco Unity Bridge*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_device_support_tables_list.html.

See the following sections for details:

- [Securing SQL Server 2000 or MSDE 2000, page 2-2](#)
- [Securing Internet Explorer, page 2-3](#)
- [Securing IIS, page 2-3](#)
- [Securing Microsoft Message Queuing, page 2-5](#)
- [Securing Exchange, page 2-5](#)
- [Installing Service Packs and Security Updates, page 2-6](#)

Securing SQL Server 2000 or MSDE 2000

SQL Server 2000 or MSDE 2000 is installed on the Cisco Unity server for use as a back-end database; neither should be used for any other purpose.

Best Practices

When you install SQL Server 2000 or MSDE 2000 on the Cisco Unity server, use the following security guidelines:

- When you install SQL Server 2000, choose Windows Authentication Mode, as documented in the Cisco Unity installation guide.

Although you can use either a domain user account or the Local System account to run the SQL Server services, it is best to use the Local System account, which is the default. (If you are configuring Cisco Unity failover, you must change the account that SQL Server services log on as to a domain account that has the right to log on as a service and is a member of the local Administrators group. The Cisco Unity installation guide tells you when and how to make this change.)

- Assign a password to the SQL administrator (SA) account.
- Note the password and keep it in a secure location.
- Restrict client access to SQL Server 2000.

Grant access to SQL Server 2000 directories, folders, and files only to the Cisco Unity service accounts and to a highly privileged account designated for use by a system administrator. The Cisco Unity installation process gains access to SQL Server 2000 by its membership in the local Administrators group.

- Detach the default Northwind and Pubs databases.

Securing Additional Instances of MSDE 2000

When installed according to the instructions in the Cisco Unity installation guide, the installation of SQL Server 2000 or MSDE 2000 on the Cisco Unity server is protected from viruses like the W32.Slammer worm. However, any MSDE 2000 database installed by third-party applications (for example, Dell OpenManage IT Assistant, Hewlett-Packard Insight Manager, Hewlett-Packard OpenView, VERITAS Backup Exec, VERITAS NetBackup) may still be vulnerable. For more information, see the section

“Detecting and Patching Additional Instances of MSDE on the Cisco Unity Server” in the tech note *Cisco Unity 3.x and 4.0 Are Vulnerable to W32.Slammer Worm*, available at http://www.cisco.com/en/US/customer/products/sw/voicesw/ps2237/products_tech_note09186a008013435f.shtml.

Securing Internet Explorer

At a minimum, Internet Explorer (IE) 6.0 with Service Pack 1 must be installed on the Cisco Unity server.

Best Practices

- Use IE on the Cisco Unity server for Cisco Unity administration only, and not for any other purpose.
- Do the following “[To Reduce Exposure to Malicious Scripts](#)” procedure to reduce the chance of being exposed to a worm like the Blaster and Nachi viruses. For additional information on preventing exposure to and recovering from the Blaster virus, refer to Microsoft Knowledge Base article 826955.

To Reduce Exposure to Malicious Scripts

- Step 1** On the Cisco Unity server, start Internet Explorer.
- Step 2** Click **Tools > Internet Options**.
- Step 3** Click the **Security** tab.
- Step 4** Change script settings for all web content zones (Internet, Local Intranet, Trusted Sites, and Restricted Sites) as follows:
- a. Click the applicable web content zone icon.
 - b. Click **Custom Level**.
 - c. In the Security Settings dialog box, in the Scripting section, under Allow Paste Operations Via Script, click **Prompt**.
 - d. Also in the Scripting section, under Scripting of Java Applets, click **Prompt**.
 - e. Click **OK**.
 - f. For the remaining web content zones, repeat Step [Step 4a.](#) through Step [Step 4e.](#)
- Step 5** Click **OK**.
- Step 6** Exit Internet Explorer.
-

Securing IIS

Use the guidelines in the “[Following IIS Configuration Guidelines](#)” section that follows for securing the IIS 5.0 installation on the Cisco Unity server, before the Cisco Unity application is installed. Also note the additional reference information contained in the “[Using the Internet Information Services Lockdown Wizard and URLScan Tool](#)” section on page 2-4, which can be used after the installation is complete.

Following IIS Configuration Guidelines

Confirm that the most current cumulative update patch for IIS 5.0 is installed. If the operating system is installed or updated by using the method described in the [“Securing Windows” section on page 1-1](#), secure IIS 5.0 by removing the default settings. In addition, use the following guidelines (from *Secure Internet Information Services 5 Checklist*, available on the Microsoft TechNet website) to configure IIS on the Cisco Unity server.

**Caution**

Failure to follow the guidelines in this section may render the Cisco Unity Web server components inoperable.

- Remove sample files, folders, and Web applications.
Follow Microsoft recommendations regarding the removal of sample files, folders, and Web applications.
- Secure Cisco Unity Web components.
Follow Microsoft recommendations with one exception: grant Full Control access to Cisco Unity directories, folders, and files only to Cisco Unity service accounts and the local server administrators group.
- Disable all default IIS COM objects.
Follow Microsoft recommendations regarding unneeded COM components with one exception: do not disable the File System Object (FSO).
- Remove unused script mappings.
Cisco Unity uses only the ASA and ASP script mappings. Follow Microsoft recommendations by removing all remaining unused script mappings.
- Do not disable the Parent Paths option.
Do not follow Microsoft recommendations regarding parent paths. By default, the Parent Paths option is enabled, and should remain so on the Cisco Unity server.

Using the Internet Information Services Lockdown Wizard and URLScan Tool

You can use the Microsoft Internet Information Services Lockdown wizard and URLScan tool to harden the IIS server.

**Caution**

If you change the IIS configuration in ways other than those documented in the following procedure and in the [“Following IIS Configuration Guidelines” section on page 2-4](#), Cisco Unity may not function properly.

To Harden the IIS Server by Using the Microsoft Internet Information Services Lockdown Wizard

- Step 1** Download the Internet Information Services Lockdown wizard from the Microsoft Technet website, and install it on the IIS server. (You can find the wizard by searching for “Internet Information Services Lockdown Tool” on the Microsoft website.)
- Step 2** Run the Internet Information Services Lockdown wizard.
- Step 3** Follow the on-screen prompts until the Select Server Template page appears.

- Step 4** On the Select Server Template page, click **Exchange Server 2000 (OWA, PF Management, IM, SMTP, NNTP)**.
- Step 5** Check the **View Template Settings** check box, and click **Next**.
- Step 6** On the Internet Services page, check the following check boxes:
- **Web Service (HTTP)**
 - **E-Mail Service (SMTP)**
 - **News Service (NNTP)**
- Step 7** Click **Next**.
- Step 8** On the Script Maps page, do the following sub-steps:
- a. Uncheck the **Active Server Pages (.asp)** check box.
 - b. Check all of the other check boxes.
 - c. Click **Next**.
- Step 9** On the Additional Security page, do not change any settings.
- Step 10** Click **Next**.
- Step 11** On the URL Scan page, check **Install URLScan Filter on the Server**, and click **Next**.
- Step 12** On the Ready to Apply Settings page, click **Next**.
- Step 13** When the Internet Information Services Lockdown wizard has finished applying security settings, click **Next**, and then click **Finish**.
-

Securing Microsoft Message Queuing

Microsoft Message Queuing (MSMQ) 2.0 acts as an intermediary between the Cisco Unity service that detects changes to Active Directory and the service that writes those changes to the SQL Server database.

Best Practice

Do not change the default MSMQ setting of Local Use Only.

Securing Exchange

Depending on the Cisco Unity configuration, you can either install Exchange on the Cisco Unity server or configure the Cisco Unity server to access Exchange on another server. For details on the requirements for using Exchange, see *System Requirements for Cisco Unity*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Best Practice

Regardless of where Exchange is installed, use the recommendations provided by Microsoft for securing Exchange.

Installing Service Packs and Security Updates

Best Practices

- Regularly update the Cisco Unity server with the Microsoft service packs and updates listed in *Recommended and Supported Service Packs and Updates for Use with Cisco Unity and the Cisco Unity Bridge*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_device_support_tables_list.html.
- Subscribe to the Microsoft Security Notification Service, which provides links to security-related software updates. For more information, go to the Microsoft Website and search for “Microsoft technical security notifications.”



CHAPTER 3

IP Communications Required by Cisco Unity

See the following sections:

- [Overview, page 3-1](#)
- [Network Traffic from Cisco Unity to Various Servers and to Clients, page 3-1](#)
- [Network Traffic from Clients to Cisco Unity, page 3-6](#)
- [Network Traffic to and from Exchange, page 3-8](#)
- [Network Traffic from Cisco Unity Subscriber Workstations to Various Servers, page 3-10](#)
- [Restricting DCOM Dynamic Port Allocation, page 3-11](#)

Overview

Companies have long used firewalls to protect their networks from external threats, but they are now starting to protect mission-critical infrastructure from other internal networks. This chapter details the minimum protocol dependencies for Cisco Unity to function. Note the following:

- This document describes both the client and server communication vectors for each of the roles in the environment. If a server performs multiple roles, consider the protocol dependencies for all of the roles of that server. For example, if an Exchange server is also a domain controller and global catalog server, consider the needs described for each of those three roles as applying to that one server.
- The information in this document cites Microsoft-recommended procedures to make Windows RPC negotiations more predictable, as well as manual procedures to configure some Exchange services to static port numbers. The information presented in this document assumes that the mentioned procedures are followed.

For more information, see the [“Securing TCP/UDP Ports”](#) section on page 1-6.

Network Traffic from Cisco Unity to Various Servers and to Clients

See the following sections:

- [Network Traffic from Cisco Unity to a Domain Controller, page 3-2](#)
- [Network Traffic from Cisco Unity to a Global Catalog Server, page 3-2](#)

- [Network Traffic from Cisco Unity to a DNS Server](#), page 3-3
- [Network Traffic from Cisco Unity to the Partner Exchange Server](#), page 3-3
- [Network Traffic Between Cisco Unity Failover Servers](#), page 3-4
- [Network Traffic from Cisco Unity to Cisco Unified Communications Manager and Phones](#), page 3-5
- [Network Traffic from Cisco Unity to SIP Endpoints, Including PIMG Devices and Phones](#), page 3-5
- [Network Traffic from Cisco Unity to Subscriber Workstations \(for the Cisco PCA or ViewMail for Outlook\)](#), page 3-5

Network Traffic from Cisco Unity to a Domain Controller

Revised April 17, 2008



Caution

Do not separate the Cisco Unity server (or the primary server in a failover or standby-redundancy configuration) by a firewall from the domain controller that Cisco Unity monitors for directory updates.

In a failover or standby-redundancy configuration in which the secondary server is separated by a firewall from the domain controller that Cisco Unity monitors for directory updates, the secondary server must be able to establish TCP and UDP client connections to the following ports on the domain controller:

Port on the Domain Controller	Protocol or Service
TCP and UDP 88	Kerberos
TCP and UDP 464	Kerberos Password v5
TCP and UDP 389	LDAP
TCP 636	LDAP over SSL
UDP 137	NetBIOS
UDP 138	
TCP 139	
TCP 445	
UDP 123	NTP
TCP 135	WinRPC endpoint locator
TCP and UDP 5000–5020	DCOM RPC range after restriction. See the “Restricting DCOM Dynamic Port Allocation” section on page 3-11.

Network Traffic from Cisco Unity to a Global Catalog Server

Revised April 17, 2008



Caution

Do not separate the Cisco Unity server (or the primary server in a failover or standby-redundancy configuration) by a firewall from the global catalog server that Cisco Unity monitors for directory updates or from the global catalog server with which the Cisco Unity MAPI client communicates.

In a failover or standby-redundancy configuration in which the secondary server is separated by a firewall from either:

- the global catalog server that Cisco Unity monitors for directory updates, or
- the global catalog server with which the Cisco Unity MAPI client communicates,

the Cisco Unity secondary server must be able to establish TCP and UDP client connections to the following ports on the GCs.

Port on the Global Catalog Server	Protocol or Service
TCP and UDP 88	Kerberos
TCP and UDP 464	Kerberos Password v5
TCP and UDP 389 (only the GC that Cisco Unity monitors for directory updates)	LDAP
TCP 636 (only the GC that Cisco Unity monitors for directory updates)	LDAP over SSL
TCP and UDP 3268 (only the GC that Cisco Unity monitors for directory updates)	LDAP
TCP 3269 (only the GC that Cisco Unity monitors for directory updates)	LDAP over SSL
UDP 137 UDP 138 TCP 139 TCP 445	NetBIOS
TCP 135 (only the GC with which the Cisco Unity MAPI client communicates)	WinRPC endpoint locator
TCP and UDP 5000–5020 (only the GC with which the Cisco Unity MAPI client communicates)	DCOM RPC range after restriction. See the “Restricting DCOM Dynamic Port Allocation” section on page 3-11.

Network Traffic from Cisco Unity to a DNS Server

Cisco Unity must be able to establish TCP and UDP connections to its DNS server at port 53.

Network Traffic from Cisco Unity to the Partner Exchange Server

Revised April 17, 2008



Caution

Do not separate the Cisco Unity server (or the primary server in a failover or standby-redundancy configuration) by a firewall from the partner Exchange server.

In a failover or standby-redundancy configuration in which the secondary server is separated by a firewall from the partner Exchange server, the secondary server must be able to establish TCP and UDP connections to the partner server on the following ports:

Port on the Partner Exchange Server	Protocol or Service
TCP 135	WinRPC endpoint locator
TCP and UDP 5000–5020	DCOM RPC range after restriction. See the “Restricting DCOM Dynamic Port Allocation” section on page 3-11.
UDP 137	NetBIOS
UDP 138	
TCP 139	
TCP 445	
Static TCP and UDP Exchange ports configured according to Microsoft Knowledge Base article 270836, <i>Exchange Server Static Port Mappings</i>	See Microsoft Knowledge Base article 270836, <i>Exchange Server Static Port Mappings</i> .

Network Traffic Between Cisco Unity Failover Servers

Revised April 17, 2008

When failover is configured and the Cisco Unity servers are separated by a firewall, the servers in the failover pair must be able to establish the following connections to each other:

Port on Each Cisco Unity Server	Protocol or Service
UDP 137	NetBIOS
UDP 138	
TCP 139	
TCP 445	
TCP 1433 and UDP 1434	Microsoft SQL Server
TCP 3372	Microsoft Distributed Transaction Coordinator
TCP 3653	Failover node manager

Network Traffic from Cisco Unity to Cisco Unified Communications Manager and Phones

Cisco Unity has the same communications requirements as a SCCP phone. Cisco Unity must be able to establish the following connections:

Port on the Cisco Unified Communications Manager Server or on Each Phone	Protocol or Service
TCP 2000 or 2443	Port 2000 is the default SCCP port. If SCCP is secured with TLS, Cisco Unity must be able to connect to port 2443, the TLS port configured on the Cisco Unified Communications Manager server.
TCP 8443	Web server port on Cisco Unified Communications Manager 5.0 and later.
UDP 22800-32767	RTP (voice media traffic). This traffic must also be allowed to VoIP phones and gateways that Cisco Unity will communicate directly with.

Network Traffic from Cisco Unity to SIP Endpoints, Including PIMG Devices and Phones

If SIP is used, Cisco Unity must be able to establish the following connections with the SIP endpoints (including PIMG devices) that Cisco Unity directly connects to:

Port on SIP Endpoints	Protocol or Service
TCP 5060	Default SIP control port of the SIP device.
UDP 22800–32767	RTP (voice media traffic). This traffic must also be allowed to SIP phones and gateways that Cisco Unity will communicate directly with.

Network Traffic from Cisco Unity to Subscriber Workstations (for the Cisco PCA or ViewMail for Outlook)

If Cisco Unity subscribers are using the Cisco Personal Communications Assistant (PCA) or ViewMail for Outlook, subscriber workstations must be able to serve the following TCP and UDP connections from Cisco Unity servers:

Port on Subscriber Workstations	Protocol or Service
TCP 135	WinRPC endpoint locator
TCP and UDP 5000–5020	DCOM RPC range after restriction. See the “Restricting DCOM Dynamic Port Allocation” section on page 3-11.

Network Traffic from Clients to Cisco Unity

See the following sections:

- [Network Traffic from Cisco Unified Communications Manager and Phones to Cisco Unity, page 3-6](#)
- [Network Traffic from SIP Endpoints, Including PIMG Devices and Phones, to Cisco Unity, page 3-6](#)
- [Network Traffic from VNC Client Workstations to Cisco Unity, page 3-6](#)
- [Network Traffic from SNMP Management Stations to Cisco Unity, page 3-6](#)
- [Network Traffic from Administrator Workstations to Cisco Unity, page 3-7](#)
- [Network Traffic from Subscriber Workstations to Cisco Unity \(for the Cisco PCA or ViewMail for Outlook\), page 3-7](#)

Network Traffic from Cisco Unified Communications Manager and Phones to Cisco Unity

If you are using Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager) (using SCCP), Cisco Unified CM and IP phones need to be able to deliver UDP RTP traffic to Cisco Unity UDP ports 22800–32767.

Network Traffic from SIP Endpoints, Including PIMG Devices and Phones, to Cisco Unity

(If SIP is used) Those SIP endpoints that will directly communicate with Cisco Unity will need to be able to establish the following connections to Cisco Unity:

Port on the Cisco Unity Server	Protocol or Service
TCP 5060	Default SIP control port of the SIP device.
UDP 22800–32767	RTP (voice media traffic).

Network Traffic from VNC Client Workstations to Cisco Unity

If Cisco Unity will be managed over VNC, VNC client workstations used for remote management must be able to connect to the selected VNC desktop on the Cisco Unity server(s). The default VNC remote desktop port is TCP port 5900.

Network Traffic from SNMP Management Stations to Cisco Unity

If Cisco Unity will be monitored over SNMP, SNMP management stations must be able to deliver data to UDP port 161 on the Cisco Unity server.

Network Traffic from Administrator Workstations to Cisco Unity

If Cisco Unity will be administered over HTTP or HTTPS, workstations performing web administration must be able to establish connections to the following ports on Cisco Unity servers:

Port on the Cisco Unity Server	Protocol or Service
If HTTPS is disabled, TCP 80	IIS web server
If HTTPS is enabled, TCP 443	IIS web server
TCP 135	WinRPC endpoint locator
TCP and UDP 5000–5020	DCOM RPC range after restriction. See the “Restricting DCOM Dynamic Port Allocation” section on page 3-11.
UDP 137	NetBIOS. Required if the Windows file share for Cisco Unity reports will be directly accessed by administrators.
UDP 138	
TCP 139	
TCP 445	
TCP 3389	If Cisco Unity is managed over WTS or RDP.

Network Traffic from Subscriber Workstations to Cisco Unity (for the Cisco PCA or ViewMail for Outlook)

If subscribers will use ViewMail for Outlook, subscriber workstations must be able to establish connections to the following ports on Cisco Unity servers:

Port on the Cisco Unity Server	Protocol or Service
TCP 135	WinRPC endpoint locator
TCP and UDP 5000–5020	DCOM RPC range after restriction. See the “Restricting DCOM Dynamic Port Allocation” section on page 3-11.

If subscribers will access the Cisco PCA, subscriber workstations must be able to establish connections to the following ports on Cisco Unity servers:

Port on the Cisco Unity Server	Protocol or Service
If HTTPS is disabled, TCP 80	IIS web server
If HTTPS is enabled, TCP 443	IIS web server
TCP 135	WinRPC endpoint locator
TCP and UDP 5000–5020	DCOM RPC range after restriction. See the “Restricting DCOM Dynamic Port Allocation” section on page 3-11.

Network Traffic to and from Exchange

See the following sections:

- [Network Traffic from Exchange to Cisco Unity, page 3-8](#)
- [Network Traffic from Exchange to DNS, page 3-8](#)
- [Network Traffic from Exchange to a Domain Controller, page 3-8](#)
- [Network Traffic from Exchange to a Global Catalog Server, page 3-9](#)
- [Network Traffic Between Exchange Servers, page 3-10](#)
- [Network Traffic Between Exchange and Other Voice-Messaging Systems, page 3-10](#)
- [Network Traffic Between Other Voice-Messaging Systems and Exchange, page 3-10](#)

Network Traffic from Exchange to Cisco Unity

Revised April 17, 2008

**Caution**

Do not separate the Cisco Unity server (or the primary server in a failover or standby-redundancy configuration) by a firewall from the partner Exchange server.

The Exchange message store must be able to deliver UDP traffic to dynamic ports on the Cisco Unity server; ports are negotiated by MAPI. These notifications tell Cisco Unity when a message for a subscriber has been read, when a new message has been delivered, and similar information. If a firewall is between Cisco Unity and the Exchange message store, and the firewall is not Exchange-client aware, Exchange must be able to deliver UDP traffic to Cisco Unity ports 1024-65535. For more information, see Microsoft Knowledge Base article 264035, *No Way to Configure Port for UDP New Mail Notification Packets*.

The executables on Cisco Unity servers that need to receive these UDP packets are AvMsgStoreMonitorSvr.exe and AvCsMgr.exe.

Network Traffic from Exchange to DNS

Each Exchange server must be able to establish TCP and UDP connections to its DNS Server at port 53.

Network Traffic from Exchange to a Domain Controller

Revised April 17, 2008

**Caution**

Do not separate the partner Exchange server by a firewall from the domain controllers that the partner server communicates with.

The Exchange message store must be able to establish the following connections to all domain controllers in the Active Directory forest:

Port on the Domain Controller	Protocol or Service
TCP and UDP 88	Kerberos
TCP and UDP 464	Kerberos Password v5
TCP and UDP 389	LDAP
TCP 636	LDAP over SSL
UDP 137	NetBIOS
UDP 138	
TCP 139	
TCP 445	
UDP 123	NTP
TCP 135	WinRPC endpoint locator
TCP and UDP 5000–5020	DCOM RPC range after restriction. See the “Restricting DCOM Dynamic Port Allocation” section on page 3-11.

Network Traffic from Exchange to a Global Catalog Server

Revised April 17, 2008



Caution

Do not separate the partner Exchange server by a firewall from the global catalog server that the partner server communicates with.

The Exchange message store must be able to establish the following connections to all global catalog servers in the Active Directory forest:

Port on the Global Catalog Server	Protocol or Service
TCP and UDP 88	Kerberos
TCP and UDP 464	Kerberos Password v5
TCP and UDP 389	LDAP
TCP 636	LDAP over SSL
TCP and UDP 3268	LDAP
TCP 3269	LDAP over SSL
UDP 137	NetBIOS
UDP 138	
TCP 139	
TCP 445	

Port on the Global Catalog Server	Protocol or Service
TCP 135	WinRPC endpoint locator
TCP and UDP 5000–5020	DCOM RPC range after restriction. See the “Restricting DCOM Dynamic Port Allocation” section on page 3-11.

Network Traffic Between Exchange Servers

If Cisco Unity subscriber mailboxes are homed on an Exchange server other than the partner Exchange server, the partner server and all Exchange message store servers on which Cisco Unity subscriber mailboxes are homed must be able to establish connections with one another on the following ports:

Port on Exchange Servers	Protocol or Service
TCP 25	SMTP
TCP 135	WinRPC endpoint locator
TCP 691	Message routing
TCP and UDP 5000–5020	DCOM RPC range after restriction. See the “Restricting DCOM Dynamic Port Allocation” section on page 3-11.
Static TCP and UDP Exchange ports configured according to Microsoft Knowledge Base article 270836, <i>Exchange Server Static Port Mappings</i>	See Microsoft Knowledge Base article 270836, <i>Exchange Server Static Port Mappings</i> .

Network Traffic Between Exchange and Other Voice-Messaging Systems

If Cisco Unity is using Cisco Unity Bridge networking or VPIM networking to communicate with other voice-messaging systems, the Exchange server on which the Cisco Unity Voice Connector for Microsoft Exchange is installed must be able to establish SMTP connections to TCP port 25 on the Bridge server(s), on the other voice-messaging systems, and on SMTP relay server(s).

Network Traffic Between Other Voice-Messaging Systems and Exchange

If Cisco Unity is using VPIM or Cisco Unity Bridge networking to communicate with other voice-messaging systems, the Bridge server(s), the other voice-messaging systems, and SMTP relay server(s) must be able to establish SMTP connections to TCP port 25 on the Exchange server on which the Cisco Unity Voice Connector for Microsoft Exchange is installed.

Network Traffic from Cisco Unity Subscriber Workstations to Various Servers

See the following sections:

- [Network Traffic from Cisco Unity Subscriber Workstations to a DNS Server, page 3-11](#)

- [Network Traffic from Cisco Unity Subscriber Workstations to the Exchange Server on Which the Subscriber Mailbox Is Homed, page 3-11](#)

Network Traffic from Cisco Unity Subscriber Workstations to a DNS Server

Each Cisco Unity subscriber workstation must be able to establish TCP and UDP connections to its DNS Server at port 53.

Network Traffic from Cisco Unity Subscriber Workstations to the Exchange Server on Which the Subscriber Mailbox Is Homed

Subscriber workstations must be able to make TCP and UDP connections to its Exchange mail server on the following ports:

Port on the Exchange Servers on Which Subscriber Mailboxes Are Homed	Protocol or Service
TCP 135	WinRPC endpoint locator
TCP and UDP 5000–5020	DCOM RPC range after restriction. See the “Restricting DCOM Dynamic Port Allocation” section on page 3-11.
UDP 137	NetBIOS
UDP 138	
TCP 139	
TCP 445	
Static TCP and UDP Exchange ports configured according to Microsoft Knowledge Base article 270836, <i>Exchange Server Static Port Mappings</i>	

Restricting DCOM Dynamic Port Allocation

By default, DCOM dynamically allocates TCP and UDP ports in the range 1024–65535. To restrict dynamic port allocation to a narrower range, do the following procedure.

To Restrict DCOM Dynamic Port Allocation

- Step 1** On the Windows Start menu, click **Programs > Administrative Tools > Component Services**.
- Step 2** Expand the Component Services and Computers nodes. Right-click **My Computer**, and then click **Properties**.
- Step 3** On the Default Protocols tab, in the DCOM Protocols list, click **Connection-Oriented TCP/IP**, and then click **Properties**.
- Step 4** In the Properties for COM Internet Services dialog box, click **Add**.
- Step 5** In the Port range text box, add a port range (for example, enter 5000–5020), and then click **OK**.



Note Entering a port range smaller than 20 ports will cause some services not to start.

- Step 6** Leave the Port Range Assignment and the Default Dynamic Port Allocation options set to **Internet Range**.
- Step 7** Click **OK** three times.
- Step 8** Restart the Cisco Unity server.
-

For more information on restricting dynamic port ranges, refer to Microsoft Knowledge Base article 300083, *How To Restrict TCP/IP Ports on Windows 2000 and Windows XP*, available on the Microsoft support website.



CHAPTER 4

Using Security Software

In this chapter, you will find descriptions of potential security issues related to Cisco Security Agent for Cisco Unity and to antivirus software; information on any actions you need to take; recommendations that will help you make decisions; discussion of the ramifications of the decisions you make; and in many cases, best practices.

Administrators who are responsible for system security should consider using the following to protect their Cisco Unity systems from external threats:

- Cisco Security Agents for Cisco Unity and the Cisco Unity Bridge. These security agents protect the application and the operating system by blocking malicious attacks, such as buffer overflows, Trojan horses, malformed packets, and malicious HTML requests.
- Antivirus software. When updated regularly, antivirus software protects against internet worm attacks, removes viruses, and detects spyware.

We recommend that you install Cisco Security Agent for Cisco Unity and antivirus software as a part of your initial system installation. In addition, your system maintenance plan should include periodic reviews of system security measures.

See the following sections for more information:

- [Using Cisco Security Agent, page 4-1](#)
- [Using Antivirus Software, page 4-2](#)

Using Cisco Security Agent

Cisco Security Agents for Cisco Unity and the Cisco Unity Bridge provide:

- Intrusion detection and prevention.
- Defense against previously unknown attacks because Cisco Security Agents do not require signatures, as antivirus software does.
- Reduced downtime, propagation of attacks, and clean-up costs.

The agent is provided free of charge by Cisco Systems for use with Cisco Unity and the Cisco Unity Bridge software. The agent provides Windows platform security (host intrusion detection and prevention) that is based on a tested set of security rules, known as a policy. The agent controls system operations by using a policy that allows or denies specific system actions before system resources are accessed. A policy controls access to system resources based on:

- The resources being accessed
- The operation being invoked

- The process invoking the action

This occurs transparently and does not hinder overall system performance.

**Caution**

You should not view Cisco Security Agent software as providing complete security. Rather, view it as an additional line of defense that, when used correctly with other standard defenses such as antivirus software and firewalls, provides enhanced security. Each Cisco Security Agent provides enhanced defense for many different installations and configurations, and thus cannot enforce network access control rules, which block outbound or inbound network traffic, or act as a host-based firewall.

For system requirements and installation instructions for the Cisco Security Agents for Cisco Unity and the Cisco Unity Bridge, see the applicable release notes, at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Using Antivirus Software

To minimize the risk of viruses, install an antivirus software package on the Cisco Unity server.

Best Practices

- Selecting antivirus software—A list of supported antivirus software can be found in *Supported Hardware and Software, and Support Policies for Cisco Unity*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.
- Disabling antivirus software during Cisco Unity installation—If antivirus software is installed before you install Cisco Unity, disable it before proceeding. Note that in some cases, you may need to completely remove the antivirus software, and reinstall it after you have completed the Cisco Unity installation.
- Excluding from virus scanning the directory in which Cisco Unity is installed—If antivirus software is installed on the Cisco Unity server, exclude from scanning the directory in which Cisco Unity is installed (the default directory is CommServer), as well as all subdirectories, so that the Cisco Unity Administrator and the Cisco Unity Assistant will work properly. See the antivirus software Help for instructions on excluding directories from scanning.
- Blocking DCOM communications—Do not block DCOM communications on subscriber workstations, or the Media Master control bar will not function correctly.
- Blocking WAV attachments—Do not configure virus-scanning software to block WAV attachments, or recordings will be removed from voice messages.
- Updating antivirus definitions—Configure antivirus software to alert you every week or two to check the manufacturer website for new antivirus definitions. If you already have a policy for updating these definitions on the other computers on your network, follow the same policy for the Cisco Unity server. If you do not already have a policy, we recommend that you download and install the new definitions on the Cisco Unity server when the software prompts you to do so.
- Scheduling virus scanning—When scheduling virus scanning, select a time when the Cisco Unity server is processing a low volume of calls (for example, after the end of the regular business day), and when there are no other processes running (for example, do not schedule virus scanning concurrently with a backup or while generating reports).
- Using Microsoft recommendations to protect Exchange—If Exchange is installed on the Cisco Unity server, refer to the Microsoft website for the latest information on protecting an Exchange server from viruses.

- Using Microsoft recommendations to protect SQL Server and MSDE—See the Microsoft website for the latest information on protecting SQL Server and MSDE from viruses.



CHAPTER 5

Preventing Toll Fraud

In this chapter, you will find a description of toll fraud—a potential security issue in any organization. You will also find information that may help you to develop preventive measures, and best practices to avoid toll fraud.

Using Restriction Tables to Help Prevent Toll Fraud

Toll fraud is defined as any toll (long distance) call that is made at the expense of your organization and in violation of its policies. Cisco Unity provides restriction tables that you can use to help guard against toll fraud. Restriction tables control the phone numbers that can be used for transferring calls, for message notification, and for other Cisco Unity functions. Each class of service has several restriction tables associated with it, and you can add more as needed. By default, restriction tables prevent access to long distance phone numbers, but you can configure them to restrict additional numbers typically associated with toll fraud, such as international numbers.

Best Practices

To prevent toll fraud by subscribers, administrators, and even outside callers who have improperly gained access to a Cisco Unity mailbox, implement the following changes:

- Set up all restriction tables to block calls to the international operator (900). When this is done, a person cannot dial out to or configure call transfers from an extension to the international operator (900) for placing international calls.
- If Cisco Unity is integrated with two phone systems, add restriction table patterns to match applicable trunk access codes for both phone system integrations. For example, if the trunk access code for one of the phone system integrations is 99 and you want to restrict the call pattern 900, you would also restrict the pattern 99900. When patterns that include the trunk access codes are restricted, attempts to bypass the restriction table by first accessing either trunk and then dialing the international operator will be blocked.
- For those in your organization who do not need to access international numbers to do their work, set up restriction tables to block all calls to international numbers. This prevents a person who has access to a Cisco Unity mailbox that is associated with the restriction table from configuring call transfers or fax delivery from that extension to an international number.
- Set up restriction tables to permit calls only to specific domestic long distance area codes or to prohibit calls to long distance area codes. This prevents a person who has access to a Cisco Unity mailbox that is associated with the restriction table from configuring call transfers or fax delivery from that extension to a long distance number.

- Restrict the numbers that can be used for AMIS message delivery only to those numbers required for your system configuration.
- Restrict the numbers that can be used for system transfers—a feature that allows callers to dial a number and then transfer to another number that they specify. For example, set up the applicable restriction tables to allow callers to transfer to a lobby or conference room phone, but not to the international operator or to a long distance phone number.
- Set up the restriction tables that are associated with the class of service for the Example Administrator account to permit only a very limited set of phone numbers. Consider setting up the restriction tables to block calls to international numbers, and to permit calls only to specific domestic long distance area codes or to prohibit calls to long distance area codes.

To learn more about how restriction tables work and how to set them up, see the “Managing Restriction Tables” chapter of the *System Administration Guide for Cisco Unity*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.



CHAPTER 6

Securing the Connection Between Cisco Unity, Cisco Unified Communications Manager, and IP Phones

In this chapter, you will find descriptions of potential security issues related to connections between Cisco Unity, Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager), and IP phones; information on any actions you need to take; recommendations that will help you make decisions; discussion of the ramifications of the decisions you make; and best practices.

See the following sections:

- [Security Issues for Connections Between Cisco Unity, Cisco Unified Communications Manager, and IP Phones, page 6-1](#)
- [Cisco Unified Communications Manager Security Features for Cisco Unity Voice Messaging Ports, page 6-2](#)
- [Security Mode Settings for Cisco Unified Communications Manager and Cisco Unity, page 6-4](#)
- [Best Practices, page 6-4](#)

Security Issues for Connections Between Cisco Unity, Cisco Unified Communications Manager, and IP Phones

A potential point of vulnerability for a Cisco Unity system is the connection between Cisco Unity, Cisco Unified Communications Manager, and the IP phones. Possible threats include:

- Man-in-the-middle attacks (when the information flow between Cisco Unified CM and the Cisco Unity voice messaging ports is observed and modified)
- Network traffic sniffing (when software is used to capture phone conversations and signaling information that flow between Cisco Unified CM, the Cisco Unity voice messaging ports, and IP phones that are managed by Cisco Unified CM)
- Modification of call signaling between the Cisco Unity voice messaging ports and Cisco Unified CM
- Modification of the media stream between the Cisco Unity voice messaging ports and the endpoint (for example, an IP phone or a gateway)
- Identity theft of the Cisco Unity voice messaging port (when a non-Cisco Unity device presents itself to Cisco Unified CM as a Cisco Unity voice messaging port)

- Identity theft of the Cisco Unified CM server (when a non-Cisco Unified CM server presents itself to Cisco Unity voice messaging ports as a Cisco Unified CM server)

Cisco Unified Communications Manager Security Features for Cisco Unity Voice Messaging Ports

Cisco Unified Communications Manager can secure the connection with Cisco Unity against the threats listed in the “[Security Issues for Connections Between Cisco Unity, Cisco Unified Communications Manager, and IP Phones](#)” section on page 6-1. The Cisco Unified CM security features that Cisco Unity can take advantage of are described in [Table 6-1](#).

Table 6-1 *Cisco Unified Communications Manager Security Features That Are Used by Cisco Unity*

Security Feature	Description
Signaling authentication	<p>The process that uses the Transport Layer Security (TLS) protocol to validate that no tampering has occurred to signaling packets during transmission. Signaling authentication relies on the creation of the Cisco Certificate Trust List (CTL) file.</p> <p>This feature protects against:</p> <ul style="list-style-type: none"> • Man-in-the-middle attacks that modify the information flow between Cisco Unified CM and the Cisco Unity voice messaging ports. • Modification of the call signalling. • Identity theft of the Cisco Unity voice messaging port. • Identity theft of the Cisco Unified CM server.
Device authentication	<p>The process that validates the identity of the device and ensures that the entity is what it claims to be. This process occurs between Cisco Unified CM and Cisco Unity voice messaging ports when each device accepts the certificate of the other device. When the certificates are accepted, a secure connection between the devices is established. Device authentication relies on the creation of the Cisco Certificate Trust List (CTL) file.</p> <p>This feature protects against:</p> <ul style="list-style-type: none"> • Man-in-the-middle attacks that modify the information flow between Cisco Unified CM and the Cisco Unity voice messaging ports. • Modification of the media stream. • Identity theft of the Cisco Unity voice messaging port. • Identity theft of the Cisco Unified CM server.

Table 6-1 *Cisco Unified Communications Manager Security Features That Are Used by Cisco Unity (continued)*

Security Feature	Description
Signaling encryption	<p>The process that uses cryptographic methods to protect (through encryption) the confidentiality of all SCCP signaling messages that are sent between the Cisco Unity voice messaging ports and Cisco Unified CM. Signaling encryption ensures that the information that pertains to the parties, DTMF digits that are entered by the parties, call status, media encryption keys, and so on are protected against unintended or unauthorized access.</p> <p>This feature protects against:</p> <ul style="list-style-type: none"> • Man-in-the-middle attacks that observe the information flow between Cisco Unified CM and the Cisco Unity voice messaging ports. • Network traffic sniffing that observes the signaling information flow between Cisco Unified CM and the Cisco Unity voice messaging ports.
Media encryption	<p>The process whereby the confidentiality of the media occurs through the use of cryptographic procedures. This process uses Secure Real Time Protocol (SRTP) as defined in IETF RFC 3711, and ensures that only the intended recipient can interpret the media streams between Cisco Unity voice messaging ports and the endpoint (for example, a phone or gateway). Support includes audio streams only. Media encryption includes creating a media master key pair for the devices, delivering the keys to Cisco Unity and the endpoint, and securing the delivery of the keys while the keys are in transport. Cisco Unity and the endpoint use the keys to encrypt and decrypt the media stream.</p> <p>This feature protects against:</p> <ul style="list-style-type: none"> • Man-in-the-middle attacks that listen to the media stream between Cisco Unified CM and the Cisco Unity voice messaging ports. • Network traffic sniffing that eavesdrops on phone conversations that flow between Cisco Unified CM, the Cisco Unity voice messaging ports, and IP phones that are managed by Cisco Unified CM.

Authentication and signaling encryption serve as the minimum requirements for media encryption; that is, if the devices do not support signaling encryption and authentication, media encryption cannot occur.



Note

Cisco Unified Communications Manager security (authentication and encryption) only protects calls to Cisco Unity. Messages recorded on the message store are not protected by the Cisco Unified CM authentication and encryption features but can be protected by the Cisco Unity private secure messaging feature. For details on the Cisco Unity private secure messaging feature, see the [“Secure Messaging” section on page 11-2](#).

Security Mode Settings for Cisco Unified Communications Manager and Cisco Unity


Cisco Unified Communications Manager and Cisco Unity have the security mode options shown in [Table 6-2](#) for voice messaging ports.



Caution

The Cluster Security Mode setting for Cisco Unity voice messaging ports must match the security mode setting for the Cisco Unified Communications Manager ports. Otherwise, Cisco Unified CM authentication and encryption will fail.

Table 6-2 Security Mode Options for Voice Messaging Ports

Setting	Effect
Non-secure	<p>The integrity and privacy of call-signaling messages will not be ensured because call-signaling messages will be sent as clear (unencrypted) text and will be connected to Cisco Unified CM through a non-authenticated port rather than an authenticated TLS port.</p> <p>In addition, the media stream cannot be encrypted.</p>
Authenticated	<p>The integrity of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an authenticated TLS port. However, the privacy of call-signaling messages will not be ensured because they will be sent as clear (unencrypted) text.</p> <p>In addition, the media stream will not be encrypted.</p>
Encrypted	<p>The integrity and privacy of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an authenticated TLS port, and the call-signaling messages will be encrypted.</p> <p>In addition, the media stream can be encrypted.</p> <p> Caution Both end points must be registered in encrypted mode for the media stream to be encrypted. However, when one end point is set for non-secure or authenticated mode and the other end point is set for encrypted mode, the media stream will not be encrypted. Also, if an intervening device (such as a transcoder or gateway) is not enabled for encryption, the media stream will not be encrypted.</p>

Best Practices

We recommend that you enable authentication and encryption for the voice messaging ports on both Cisco Unity and Cisco Unified Communications Manager.

For information on enabling authentication and encryption, see the applicable Cisco Unified Communications Manager integration guide, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.



CHAPTER 7

Securing Accounts

In this chapter, you will find descriptions of potential security issues related to securing accounts; information on any actions you need to take; recommendations that will help you make decisions; ramifications of the decisions you make; and in many cases, best practices.

See the following sections:

- [Understanding Accounts, page 7-1](#)
- [Best Practices for Accounts That Are Used to Access the Cisco Unity Administrator, page 7-2](#)
- [Best Practices for Accounts That Are Used to Access the Cisco Unity Server, page 7-3](#)
- [Best Practices When Deleting Cisco Unity Subscriber Accounts, page 7-4](#)
- [Securing the Account That Was Used to Install Cisco Unity, page 7-4](#)
- [Securing the Directory Services and Message Store Services Accounts, page 7-4](#)
- [Best Practices for Securing Default Accounts, page 7-5](#)

For the latest requirements for Cisco Unity service accounts and permissions, see the applicable Cisco Unity installation guide, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Understanding Accounts

Each Cisco Unity subscriber account has a corresponding Active Directory domain account. Depending on the method you use to create Cisco Unity subscriber accounts, the Active Directory account may be created automatically.

If the Active Directory account for a subscriber has been disabled, the subscriber:

- Cannot access the Cisco Personal Communications Assistant (PCA).
- Cannot access the Cisco Unity Administrator.
- Cannot use the phone as a recording and playback device for the Media Master.

Best Practices

- On Cisco Unity systems that are configured for Voice Messaging, if you do not want subscribers to have access to the Cisco PCA, the Cisco Unity Administrator, or the Media Master, we recommend that you disable Active Directory accounts for the subscribers.

**Note**

If you have Cisco Unity create Active Directory accounts at the same time that you create Cisco Unity subscribers, you can configure Cisco Unity so the Active Directory accounts are created disabled. For more information, in Cisco Unity Tools Depot, run the Advanced Settings Tool, and review the help for the setting “Administration - Disable AD accounts created by Unity.”

- Depending on how subscriber accounts are created, all of the corresponding Active Directory domain accounts may be created with the same default password. We recommend that you change these passwords immediately—before subscribers start to use Cisco Unity—to prevent subscribers from accessing accounts other than their own.

For information on Active Directory passwords, see the “[Ensuring That Subscribers Are Initially Assigned Unique and Secure Windows Passwords](#)” section on page 9-4.

Best Practices for Accounts That Are Used to Access the Cisco Unity Administrator

The Cisco Unity Administrator is a website that you use to do most administrative tasks. Depending on the associated class of service rights, accounts that can be used to access the Cisco Unity Administrator can offer access to settings used to define how Cisco Unity works for individual subscribers (or for a group of subscribers), system schedules, call management options, and other important data. If your site is comprised of multiple Cisco Unity servers, an account used to access one Cisco Unity Administrator may be able to gain access to the other Cisco Unity Administrators as well. To secure access to the Cisco Unity Administrator, consider the following best practices.

Best Practice: Limit the Use of the Administration Account

Until you create a Cisco Unity subscriber account specifically for the purpose of administering Cisco Unity, you log on to the Cisco Unity Administrator by using the Active Directory credentials that are associated with the administration account that was selected when Cisco Unity was installed. The administration account is automatically associated with a class of service that offers full system access rights to the Cisco Unity Administrator. This means that not only can the administration account access all pages in the Cisco Unity Administrator, but it also has read, edit, add, and delete privileges for all Cisco Unity Administrator pages. For this reason, you should limit the use of this highly privileged account to only one or to very few individuals.

As an alternative to the administration account, you can create additional accounts that have class of service rights to access the Cisco Unity Administrator, but offer fewer privileges. If your organization depends on more than person to administer Cisco Unity, you can modify the class of service rights for each account so that access to the Cisco Unity Administrator is appropriate to the administrative tasks that each person performs. By creating additional accounts, you also ensure that additional accounts are available to access the Cisco Unity Administrator in the event that the administration account is deleted or corrupted.

To learn about the ways in which you create additional accounts or grant administrative rights to existing accounts so that they can be used to access the Cisco Unity Administrator, see the “About the Accounts That Can Be Used to Administer Cisco Unity” section in the “Managing Cisco Unity Administrator Accounts” chapter of the *System Administration Guide for Cisco Unity*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Best Practices: Use Class of Service to Restrict Access to the Cisco Unity Administrator

When modifying class of service settings and assignments to secure access to the Cisco Unity Administrator, consider the following best practices:

- Do not modify the system access settings for the Default Administrator class of service. Instead, reassign subscriber accounts to a new class of service that offers an appropriate level of access to the Cisco Unity Administrator. For example, you may want to associate an account with a class of service that offers read-only access to the Cisco Unity Administrator, or only offers access of specific pages in the Cisco Unity Administrator for the purpose of unlocking accounts or changing passwords.
- Verify that at least one subscriber account is assigned to the Default Administrator class of service. If you do not have at least one Active Directory account with class of service rights to access the Cisco Unity Administrator, you may lose the ability to administer Cisco Unity, and be required to reinstall.
- By default, the Default Subscriber class of service prohibits access to the Cisco Unity Administrator, and should not be changed to allow it. Instead, use it to offer access to Cisco Unity features and applications that are more appropriate to end users.

To learn how to create and modify classes of service, see the “Managing Classes of Service” chapter of the *System Administration Guide for Cisco Unity*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Best Practice: Do Not Use Other Accounts to Access the Cisco Unity Administrator

Cisco Unity administrators should not use the same account to access the Cisco Unity Administrator that they use to log on to the Cisco Personal Communications Assistant (PCA). In addition, administrators should not use Cisco Unity service accounts to access the Cisco Unity Administrator.

Best Practices for Accounts That Are Used to Access the Cisco Unity Server

When you install Cisco Unity, you can choose the drive and directory where it is installed. By default, it is installed in the CommServer directory.

By default, the Active Directory accounts that Cisco Unity services log on as have Full Control access to the CommServer directory because they belong either to the local Administrators group (when the Cisco Unity server is a member server) or the Domain Admins group (when the Cisco Unity server is a domain controller). However, we recommend that you not use these accounts as administration accounts. Instead, we recommend that you designate a highly privileged account for use by a system administrator, and grant Full Control permissions to the Cisco Unity directories and files so that the account can be used for administration and troubleshooting.

Best Practice

Verify that other domain accounts used by Cisco Unity system administrators are restricted to read-only access, and verify that all Cisco Unity subscribers and any other domain accounts and groups have no access rights to the directories or files on the Cisco Unity server. To restrict access, exclude the System Group Everyone from the default user permissions for C:\ or the root of any other drive on the Cisco Unity server. Instead, as applicable, assign authenticated users. Finally, verify that no explicitly privileged assignments have been made to individual groups or accounts.

Best Practices When Deleting Cisco Unity Subscriber Accounts

Deleting the Cisco Unity subscriber account does not delete the Active Directory account (if there is one) or the Exchange mailbox for that subscriber. You can delete the Active Directory account and Exchange mailbox separately after you delete the subscriber account in the Cisco Unity Administrator.

Securing the Account That Was Used to Install Cisco Unity

Cisco Unity Setup creates a variety of objects in Active Directory and also creates mailboxes in Exchange. As a result, the account that is used to install Cisco Unity requires a broad range of user rights, group memberships, and Active Directory permissions. If you are concerned that an account with so many permissions will be available after the Cisco Unity installation is complete, you can disable the account in Active Directory Users and Computers.

We recommend that you not delete the account because when you upgrade to a later version of Cisco Unity you will again need an installation account with the same permissions. If you delete the current account, you will have to create another, re-run the Cisco Unity Permissions wizard to set the required permissions, and manually delegate Exchange administrative control to the account.

For more information on the permissions set by the Permissions wizard, see the *Permissions Granted by the Cisco Unity 5.0(1)+ Permissions Wizard Help*. The Help file is available at http://www.ciscounitytools.com/App_PW_501.htm.

Securing the Directory Services and Message Store Services Accounts

Added October 23, 2008

The Permissions wizard adds the directory services and message store services accounts to the local Administrators group. Cisco Unity requires most of the permissions that are associated with being a member of the local Administrators group, and denying these permissions will prevent Cisco Unity from functioning properly. However, if you want, you can deny the accounts the right to log on locally. Do the following procedure.

To Deny the Directory Services and Message Store Services Accounts the Right to Log On Locally

-
- Step 1** On the Windows Start menu, click **Programs > Administrative Tools > Local Security Policy**.
 - Step 2** In the left pane of the Local Security Policy MMC, expand **Local Policies**, and click **User Rights Assignment**.
 - Step 3** In the right pane, right-click **Deny Log on Locally**, and click **Properties**.
 - Step 4** In the Deny Logon Locally Properties dialog box, on the Local Security Settings tab, click **Add User or Group**, select the directory services and message store services accounts, and click **OK**.
 - Step 5** In the Deny Logon Locally Properties dialog box, click the names of the two accounts that you selected in **Step 4**, and click **OK**.

In the right pane of the Local Security Policy MMC, the Deny Log on Locally policy now lists the two accounts in the Security Setting column.

Best Practices for Securing Default Accounts

Table 7-1 lists the Active Directory accounts and Exchange mailboxes that are created by Cisco Unity, when they are created, and best practices for securing them.

Table 7-1 Considerations for Securing Default Cisco Unity Accounts, Active Directory Accounts, or Exchange Mailboxes

Cisco Unity Subscriber Account	Active Directory Account and Exchange Mailbox	When Created	Best Practice
Example Administrator	EAdministrator	At installation	<p>The Cisco Unity Installation and Configuration Assistant prompts for a password for the Default Administrator template, which is used to create the Example Administrator account and the corresponding Active Directory account. If the system was upgraded from Cisco Unity version 4.0(3) or earlier, the Active Directory Example Administrator account may still have the default password. This account is created in a disabled state.</p> <p>For systems that were upgraded from Cisco Unity 4.0(3) or earlier:</p> <ul style="list-style-type: none"> • Change the Active Directory password. • Change the phone password. • Change the class of service to remove administration rights. <p>Optionally, you can disable (but not delete) this account.</p>
Example Subscriber	ESubscriber	At installation (for Cisco Unity version 4.0(2) and earlier only)	If present, delete this subscriber account and the associated Active Directory account and Exchange mailbox.
Unity Messaging System (not visible in the Cisco Unity Administrator)	Unity_<servername>	At installation	<p>For systems that were upgraded from a version prior to Cisco Unity 4.0(5), change the Active Directory password.</p> <p>Optionally, you can disable (but not delete) this account. This account is created in a disabled state when you install Cisco Unity.</p>

Table 7-1 Considerations for Securing Default Cisco Unity Accounts, Active Directory Accounts, or Exchange Mailboxes (continued)

Cisco Unity Subscriber Account	Active Directory Account and Exchange Mailbox	When Created	Best Practice
None	UAmis_<servername>	When configuring AMIS	<p>If the system was upgraded from Cisco Unity version 4.0(3) or earlier, the UAmis account may have a default password. This account is disabled by default.</p> <p>For systems that were upgraded from Cisco Unity 4.0(5) or earlier, change the Active Directory password.</p> <p>Optionally, you can disable this account. Do not hide this account from the Exchange address book if using the Voice Connector for Exchange 2000 or Exchange 2003 version 11.0(2) or earlier. Doing so may prevent AMIS networking from working properly. Do not delete this account, even if AMIS is no longer in use.</p>
None	UOmni_<servername>	When configuring the Cisco Unity Bridge	<p>The Cisco Unity Installation and Configuration Assistant prompts for a password for the Default Subscriber template, which is used to create the UOmni Active Directory account. If the system was upgraded from Cisco Unity version 4.0(3) or earlier, the UOmni account may still have a default password. By default, this account is disabled, hidden from the Exchange address book, and configured to appear in AD Advanced View only.</p> <p>For Cisco Unity systems that were upgraded from version 4.0(3) or earlier, change the Active Directory password.</p> <p>Optionally, you can disable this account. Do not hide this account from the Exchange address book if using the Cisco Unity Voice Connector for Microsoft Exchange 2000 or Exchange 2003 version 11.0(2) or earlier. Doing so may prevent Bridge networking from working properly. Do not delete this account, even if Bridge Networking is no longer in use.</p>

Table 7-1 *Considerations for Securing Default Cisco Unity Accounts, Active Directory Accounts, or Exchange Mailboxes (continued)*

Cisco Unity Subscriber Account	Active Directory Account and Exchange Mailbox	When Created	Best Practice
None	USbms_<servername>	At installation	The Cisco Unity Installation and Configuration Assistant prompts for a password for the Default Subscriber template, which is used to create the account. By default, this account is disabled, hidden from the Exchange address book, and configured to appear in AD Advanced View only. Do not delete this account, even if broadcast messaging is not in use.
None	UVpim_<servername>	When configuring VPIM	The Cisco Unity Installation and Configuration Assistant prompts for a password for the Default Subscriber template, which is used to create the account. By default, this account is disabled, hidden from the Exchange address book, and configured to appear in AD Advanced View only. Do not delete this account, even if VPIM is no longer in use.



CHAPTER 8

Authentication for Cisco Unity Applications

Each Cisco Unity application has its own way of authenticating user credentials. Understanding the methods that each application uses is an important step in securing Cisco Unity subscriber data and messages from unauthorized access. In this chapter, you will find descriptions of potential security issues related to the authentication methods used by the Cisco Unity Administrator, the Status Monitor, the Cisco Personal Communications Assistant (PCA) and the Cisco Unity conversation (the “TUI”). When you understand how authentication works for each application, you will be better prepared to decide:

- Whether to use Integrated Windows authentication or Anonymous authentication for the Cisco Unity Administrator and the Status Monitor.
- Whether to configure the Cisco PCA to use SSL to secure client/server connections.
- Whether to configure the Cisco Unity conversation for enhanced phone security, which uses a secure logon method known as two-factor user authentication.

For information that will help you make your decisions and guide you through any actions you need to take, see the following sections:

- [Determining Which Authentication Method to Use for the Cisco Unity Administrator and Status Monitor, page 8-2](#)
- [Configuring IIS so That the Cisco Unity Administrator and Status Monitor Use Integrated Windows Authentication, page 8-5](#)
- [Configuring IIS so That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication, page 8-7](#)
- [Best Practices for Securing Access to the Cisco Unity Administrator and Status Monitor, page 8-8](#)
- [Understanding How Cisco Personal Communications Assistant \(PCA\) Authentication Works, page 8-10](#)
- [Best Practices for Securing Access to the Cisco PCA, page 8-11](#)
- [Determining Whether to Offer Enhanced Phone Security, page 8-12](#)
- [Configuring the Cisco Unity Conversation to Use Enhanced Phone Security, page 8-12](#)

Determining Which Authentication Method to Use for the Cisco Unity Administrator and Status Monitor

Cisco Unity requires that the identity of the administrator be authenticated by a name and password prior to accessing the Cisco Unity Administrator and the Status Monitor. By default, IIS is configured so that the two applications use the Integrated Windows authentication method (formerly called NTLM or Windows NT Challenge/Response authentication) to authenticate the user name and password. During installation, the installer determines whether to configure IIS so that the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method instead.

You can change the authentication method that the Cisco Unity Administrator and the Status Monitor use at any time. Before you make a change, do the following tasks:

1. Make sure that you understand how each authentication method works. Review the following sections:
 - [How Integrated Windows Authentication Works with the Cisco Unity Administrator and Status Monitor, page 8-2](#)
 - [How Anonymous Authentication Works with the Cisco Unity Administrator and Status Monitor, page 8-4](#)
2. Evaluate the strengths and weaknesses of Integrated Windows and Anonymous authentication. Refer to the Microsoft website for information. In addition, review the following sections:
 - [Advantages and Disadvantages of Using Integrated Windows Authentication with the Cisco Unity Administrator and the Status Monitor, page 8-3](#)
 - [Advantages and Disadvantages of Using Anonymous Authentication with the Cisco Unity Administrator and Status Monitor, page 8-5](#)
3. Discuss the change with the network administrator to confirm that the method you choose aligns with the existing authentication scheme in your organization, and that it addresses security concerns for your site.

How Integrated Windows Authentication Works with the Cisco Unity Administrator and Status Monitor

When IIS is configured so that the Cisco Unity Administrator uses Integrated Windows authentication, Cisco Unity does not authenticate the subscriber. Instead, the identity of the subscriber is verified by Windows, as indicated in the steps below. (The same process is also used to authenticate users of the Status Monitor.)

1. A Cisco Unity subscriber starts Internet Explorer and attempts to browse to the Cisco Unity Administrator website.
2. Internet Explorer tries to get the home page for the Cisco Unity Administrator from IIS.
3. IIS indicates that it cannot authenticate the user.
4. When Internet Explorer is configured to prompt for a user name and password, it displays a dialog box and waits for the subscriber to enter the Active Directory account credentials. When the subscriber enters the credentials, Internet Explorer tries to get the Cisco Unity Administrator web page again, but this time, it also sends IIS an encrypted message regarding the Active Directory account (based on the credentials that the subscriber entered in the dialog box).

When Internet Explorer is not configured to prompt for a user name and password, Internet Explorer tries to get the Cisco Unity Administrator web page again, but this time, it also sends IIS an encrypted message regarding the Active Directory account (based on the credentials that the subscriber had previously entered to log on to Windows).

In neither scenario is the user password—or any representation of the password—sent across the network, because authentication relies on Windows challenge/response.

5. If Windows can confirm the identity of the Active Directory user, IIS sends the user and domain name to Cisco Unity, and the process continues with Step 6.

If Windows cannot validate the identity of the Active Directory user (as would be the case if the subscriber logged on to an untrusted domain), Internet Explorer prompts the subscriber for a user name and password. Once again, the credentials are not sent across the network; instead, Internet Explorer sends IIS an encrypted message regarding the Active Directory account based on the credentials that are entered in the dialog box.

If authentication occurs, the process continues with Step 6. However, if Windows still cannot authenticate the user, Internet Explorer displays a message indicating that access to the website is denied because the domain account is unknown.

6. Cisco Unity checks to see that there is a subscriber account associated with the Active Directory account used to authenticate the subscriber, and that the subscriber account has COS rights to access the Cisco Unity Administrator.

If the subscriber account exists and it has the proper COS rights, Cisco Unity presents the first page of the Cisco Unity Administrator website, which is displayed in the browser.

If the subscriber account does not exist or does not have the proper COS rights, Cisco Unity presents a web page indicating that the subscriber does not have permission to view the Cisco Unity Administrator website.

Advantages and Disadvantages of Using Integrated Windows Authentication with the Cisco Unity Administrator and the Status Monitor

For a list of advantages and disadvantages associated with using Integrated Windows authentication, see [Table 8-1](#).

Table 8-1 Advantages and Disadvantages of Using Integrated Windows Authentication with the Cisco Unity Administrator and the Status Monitor

Advantages	Disadvantages
<ul style="list-style-type: none"> We recommend that you use Integrated Windows authentication with the Cisco Unity Administrator and the Status Monitor. User credentials are not sent across the network. Instead, Internet Explorer and Windows use a challenge/response mechanism to authenticate the user. No additional setup is required; Integrated Windows authentication is the default in IIS. 	<ul style="list-style-type: none"> Windows cannot validate the identity of a user when the user is logged on to an untrusted domain, and therefore, denies the user access to the Cisco Unity Administrator. (To mitigate this problem, configure each subscriber browser to prompt for a user name and password, allowing subscribers to enter the applicable credentials for the domain that the Cisco Unity server is in. Alternatively, you can establish trusts across domains.) When subscribers log on to the Cisco Unity Administrator from another domain, they will be prompted to re-enter their credentials every time that they want to use the phone as a recording and playback device for the Media Master.

How Anonymous Authentication Works with the Cisco Unity Administrator and Status Monitor

When IIS is configured so that the Cisco Unity Administrator uses Anonymous authentication, Cisco Unity authenticates the credentials that subscribers enter on the Cisco Unity Log On page, as indicated in the steps below. (The same process is also used to authenticate users of the Status Monitor.)

1. A Cisco Unity subscriber starts Internet Explorer and attempts to browse to the Cisco Unity Administrator website.
2. Internet Explorer tries to get the home page for the Cisco Unity Administrator from IIS.
3. IIS allows access to Cisco Unity based on the privileges for the IUSR_<Computer name> account. (This is the anonymous account that IIS uses by default for Anonymous authentication.)
4. Cisco Unity presents the Cisco Unity Log On page, which is displayed in the browser.
5. The Log On page prompts subscribers to enter their Active Directory account credentials, as shown in [Table 8-2](#).

Table 8-2 Cisco Unity Log On Page for Windows Credentials

Field Name	Description
User Name	Subscribers enter the alias for the Active Directory account that is associated with their Cisco Unity subscriber account. (For example, a subscriber can enter tcampbell, or can enter the full path tcampbell@<Domain name>.) If subscribers enter the full path, they do not need to complete the Domain field.
Password	Subscribers enter the password for their Active Directory account.
Domain	Subscribers enter the name of the domain in which their Active Directory account resides, unless they entered a full path in the User Name field, in which case they leave this field blank.

6. Internet Explorer sends the credentials—in clear text—to Cisco Unity. (To mitigate this security risk, you can set up Cisco Unity to use SSL.)
7. Cisco Unity requests authentication of the credentials from Windows.
8. If Cisco Unity can authenticate the Windows credentials, Cisco Unity then confirms that there is a subscriber account associated with the Active Directory account used to authenticate the subscriber, and that the subscriber account has the proper COS rights. If the subscriber account exists and it has the proper COS rights, Cisco Unity presents the first page of the Cisco Unity Administrator website, which is displayed in the browser.

If the Windows credentials cannot be authenticated, or if the subscriber account does not exist or does not have the proper COS rights, Cisco Unity presents a web page indicating that the subscriber does not have permission to view the Cisco Unity Administrator website.

Advantages and Disadvantages of Using Anonymous Authentication with the Cisco Unity Administrator and Status Monitor

For a list of advantages and disadvantages associated with using Anonymous authentication, see [Table 8-3](#).

Table 8-3 *Advantages and Disadvantages of Using Anonymous Authentication with the Cisco Unity Administrator and the Status Monitor*

Advantages	Disadvantages
<ul style="list-style-type: none"> • You do not need to configure each subscriber browser to prompt for a user name and password, nor do you need to establish trusts across domains. When subscribers log on to the Cisco Unity Administrator from another domain, they can enter the applicable credentials on the Cisco Unity Log On page for the domain that the Cisco Unity server is in. • When subscribers log on to the Cisco Unity Administrator from another domain, they are not prompted to re-enter their credentials each time that they want to use the phone as a recording and playback device for the Media Master. 	<ul style="list-style-type: none"> • We recommend that you use Integrated Windows authentication with the Cisco Unity Administrator and the Status Monitor. • When a subscriber enters credentials on the Cisco Unity Log On page, the credentials are sent across the network in clear text. (To solve this problem, you can set up Cisco Unity to use SSL.) • You must configure the system to use Anonymous authentication; Integrated Windows authentication is the IIS default.

Configuring IIS so That the Cisco Unity Administrator and Status Monitor Use Integrated Windows Authentication

Do the applicable procedure to configure IIS so that the Cisco Unity Administrator and Status Monitor use the Integrated Windows authentication method (which is the default):

- [To Configure IIS so That the Cisco Unity Administrator and Status Monitor Use Integrated Windows Authentication \(Windows Server 2003\)](#), page 8-6
- [To Configure IIS so That the Cisco Unity Administrator and Status Monitor Use Integrated Windows Authentication \(Windows 2000 Server\)](#), page 8-6

To Configure IIS so That the Cisco Unity Administrator and Status Monitor Use Integrated Windows Authentication (Windows Server 2003)

-
- Step 1** On the Windows Start menu, click **Administrative Tools > Internet Information Services (IIS) Manager**.
- Step 2** In the left pane of Internet Information Services (IIS) Manager, expand **Web Sites > Default Web Site**.
- Step 3** Right-click **SAWeb**, and click **Properties**.
- Step 4** In the SaWeb Properties dialog box, click the **Directory Security** tab.
- Step 5** In the Authentication and Access Control section, click **Edit**.
- Step 6** In the Authentication Methods dialog box, uncheck the **Enable Anonymous Access** check box.
- Step 7** Check the **Integrated Windows Authentication** check box.
- Step 8** Click **OK** to close the Authentication Methods dialog box.
- Step 9** Click **OK** to close the SaWeb Properties dialog box.
- Step 10** Repeat [Step 3](#) through [Step 9](#) for the following virtual directories:
- Status
 - StatusXml
 - Web
-

To Configure IIS so That the Cisco Unity Administrator and Status Monitor Use Integrated Windows Authentication (Windows 2000 Server)

-
- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
- Step 2** In the Internet Information Services window, double-click **<System-name>** to expand it.
- Step 3** Under Default Web Site, right-click **Web**, and click **Properties**.
- Step 4** In the Web Properties dialog box, set the authentication method:
- a. Click the **Directory Security** tab.
 - b. Under Anonymous Access and Authentication Control, click **Edit**.
 - c. In the Authentication Methods dialog box, uncheck the **Anonymous Access** check box.
 - d. Check the **Integrated Windows Authentication** check box.
 - e. Click **OK** to close the Authentication Methods dialog box.
 - f. Click **OK** to close the Web Properties dialog box.
- Step 5** Under Default Web Site, right-click **SAWeb**, and click **Properties**.
- Step 6** Repeat [Step 4](#) to set the authentication method for SAWeb.
- Step 7** Under Default Web Site, right-click **Status**, and click **Properties**.
- Step 8** Repeat [Step 4](#) to set the authentication method for Status.
- Step 9** Under Default Web Site, click **AvXML**.
- Step 10** In the AvXML directory, right-click **AvXML.dll**, and click **Properties**.
- Step 11** Repeat [Step 4](#) to set the authentication method for AvXML.

Step 12 Close the **Internet Information Services** window.

Configuring IIS so That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication

Do the applicable procedure to configure IIS so that the Cisco Unity Administrator and Status Monitor use the Anonymous authentication method:

- [To Configure IIS so That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication \(Windows Server 2003\)](#), page 8-7
- [To Configure IIS so That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication \(Windows 2000 Server\)](#), page 8-8

To Configure IIS so That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication (Windows Server 2003)

- Step 1** On the Windows Start menu, click **Administrative Tools > Internet Information Services (IIS) Manager**.
- Step 2** In the left pane, right-click **Application Pools**, and click **Properties**.
- Step 3** In the Application Pools Properties dialog box, click the **Identity** tab.
- Step 4** In the Predefined list, click **Local System**.
- Step 5** Click **OK** to close the Application Pools Properties dialog box.
- Step 6** In the IIS Manager message box, click **Yes** to confirm that you want to run this application pool as Local System.
- Step 7** In the left pane of Internet Information Services (IIS) Manager, expand **Web Sites > Default Web Site**.
- Step 8** Right-click **SAWeb**, and click **Properties**.
- Step 9** In the SaWeb Properties dialog box, click the **Directory Security** tab.
- Step 10** In the Authentication and Access Control section, click **Edit**.
- Step 11** In the Authentication Methods dialog box, check the **Enable Anonymous Access** check box.
- Step 12** Uncheck the **Integrated Windows Authentication** check box.
- Step 13** Click **OK** to close the Authentication Methods dialog box.
- Step 14** Click **OK** to close the SaWeb Properties dialog box.
- Step 15** Repeat [Step 8](#) through [Step 14](#) for the following virtual directories:
- Status
 - StatusXml
 - Web
-

To Configure IIS so That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication (Windows 2000 Server)

-
- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
- Step 2** In the Internet Information Services window, double-click <System-name> to expand it.
- Step 3** Under Default Web Site, right-click **Web**, and click **Properties**.
- Step 4** In the Properties dialog box, set the authentication method for the Web directory:
- Click the **Directory Security** tab.
 - Under Anonymous Access and Authentication Control, click **Edit**.
 - In the Authentication Methods dialog box, check the **Anonymous Access** check box.
 - Uncheck the **Integrated Windows Authentication** check box.
 - Click **OK** to close the Authentication Methods dialog box.
 - Click **OK** to close the Properties dialog box.
- Step 5** Under Default Web Site, right-click **SAWeb**, and click **Properties**.
- Step 6** Repeat [Step 4](#) to set the authentication method for the SAWeb directory.
- Step 7** Under Default Web Site, right-click **Status**, and click **Properties**.
- Step 8** Repeat [Step 4](#) to set the authentication method for the Status directory.
- Step 9** Under Default Web Site, click **AvXML**.
- Step 10** In the AvXML directory, right-click **AvXML.dll**, and click **Properties**.
- Step 11** Repeat [Step 4](#) to set the authentication method for AvXML.dll.
- Step 12** Close the Internet Information Services window.
-

Best Practices for Securing Access to the Cisco Unity Administrator and Status Monitor

Once you have determined which authentication method you want to use with the Cisco Unity Administrator and the Status Monitor, consider implementing the following best practices to further prevent unauthorized access to subscriber and system data.

Best Practice: Always Prompt for a Name and Password (Integrated Windows Authentication)

When the Cisco Unity Administrator uses the Integrated Windows authentication method, it is possible to configure your system so that you are not prompted for a name and password when you access the Cisco Unity Administrator. This is the case when Internet Explorer is not configured to prompt for a user name and password, and administrators log on to Windows in a trusted domain by using either the administration account or an applicable Active Directory account. As a best practice, configure the browser to prompt for a user name and password, or lock the workstation when it is unattended.

Best Practice: Do Not Send User Credentials in Clear Text (Anonymous Authentication Only)

By default, when subscribers log on to the Cisco Unity Administrator and the Status Monitor, their user credentials are sent across the network to Cisco Unity in clear text. The information that a subscriber enters on the Cisco Unity Administrator pages is also not encrypted. For increased security, set up Cisco Unity to use SSL. See the [“Using SSL to Secure Client/Server Connections”](#) chapter.

Best Practice: Require Administrators to Enter User Credentials (Anonymous Authentication Only)

When the Cisco Unity Administrator is set up to use Anonymous authentication, you can use the settings on the Authentication page in the Cisco Unity Administrator to specify whether the Log On page offers the following options:

- Remember User Name
- Remember Password
- Remember Domain

When you specify that Cisco Unity remember the user name, password, or domain, subscribers will not have to enter them the next time that they log on to the Cisco Unity Administrator. Instead, the fields are automatically populated in the Log On page and the credentials are stored as encrypted cookies on the subscriber workstation.

For security reasons, the Log On page by default does not offer subscribers the above options; your organization may want to keep it that way.

Best Practice: Review the Account Policy

Review the account policy that applies when subscribers use the Cisco Unity Administrator and the Status Monitor to verify that the following items are defined appropriately:

- What happens when users attempt to log on and repeatedly enter incorrect passwords
- How many failed logon attempts are allowed before the user account cannot be used to access the Cisco Unity Administrator and Status Monitor
- The length of time that a user remains locked out

Depending on your authentication method, the account policy may be set in Windows or in the Cisco Unity Administrator. See the [“Defining Account Policies for Accessing the Cisco Unity Administrator”](#) section on page 9-7 for more information and recommended settings.

Best Practice: Limit How Long the Browser Can Be Left Unattended

The length of time that the browser can be left unattended before Cisco Unity automatically logs you off is governed by the Session Timeout limit, as specified in Internet Information Services (IIS). When the browser session times out, you must refresh the browser and log on to the Cisco Unity Administrator again.

Depending on the authentication method used by the Cisco Unity Administrator, you set the timeout value for IIS as follows:

- When the Cisco Unity Administrator uses the Anonymous authentication method, you can set the session timeout value for IIS in the Cisco Unity Administrator.
- When the Cisco Unity Administrator uses the Integrated Windows authentication method, you must set session limits directly in IIS.

Understanding How Cisco Personal Communications Assistant (PCA) Authentication Works

Cisco Unity offers application-level authentication to allow subscribers to access the Cisco Personal Communications Assistant (PCA). This means that IIS is configured so that the Cisco PCA uses Anonymous authentication, and therefore Cisco Unity authenticates the credentials that subscribers enter when they log on to the Cisco PCA. Note that unlike the Cisco Unity Administrator, you cannot change the authentication method used by the Cisco PCA.

Cisco Unity authenticates the credentials that subscribers enter on the Cisco Unity Log On page, as follows:

1. A Cisco Unity subscriber starts Internet Explorer and attempts to browse to the Cisco PCA website.
2. Internet Explorer tries to get the home page for the Cisco PCA from IIS.
3. IIS allows access to Cisco Unity based on the privileges for the IUSR_<Computer name> account. (This is the anonymous account that by default IIS uses for Anonymous authentication.)
4. Cisco Unity presents the Cisco Unity Log On page, which is displayed in the browser.
5. The Log On page prompts subscribers to enter their Active Directory account credentials, as shown in [Table 8-4](#).

Table 8-4 Cisco Unity Log On Page for Windows Credentials

Field Name	Description
User Name	Subscribers enter the alias for the Active Directory account that is associated with their Cisco Unity subscriber account. (For example, a subscriber can enter tcampbell, or can enter the full path tcampbell@<domain name>.) If subscribers enter the full path, they do not need to complete the Domain field.
Password	Subscribers enter the password for their Active Directory account.
Domain	Subscribers enter the name of the domain in which their Active Directory account resides, unless they entered a full path in the User Name field, in which case they leave this field blank.

6. Internet Explorer sends the credentials—in clear text—to Cisco Unity. (To mitigate this security risk, you can set up Cisco Unity to use SSL.)
7. Cisco Unity requests authentication of the credentials from Active Directory.
8. If Cisco Unity can authenticate the Active Directory credentials, Cisco Unity then confirms that there is a subscriber account associated with the Active Directory account used to authenticate the subscriber and that the subscriber account has the proper COS rights. If the subscriber account exists and it has the proper COS rights, Cisco Unity presents the first page of the Cisco PCA website, which is displayed in the browser.

If the Active Directory credentials cannot be authenticated, or if the subscriber account does not exist or does not have the proper COS rights, Cisco Unity presents a web page that indicates that the subscriber does not have permission to view the Cisco PCA website.

Best Practices for Securing Access to the Cisco PCA

To help prevent unauthorized access to subscriber data and messages via the Cisco PCA, consider implementing the following best practices.

Best Practice: Do Not Send User Credentials in Clear Text

By default, when subscribers log on to the Cisco PCA, their user credentials are sent across the network to Cisco Unity in clear text. The information that a subscriber enters on the Cisco PCA pages is also not encrypted. For increased security, set up Cisco Unity to use SSL. See the [“Using SSL to Secure Client/Server Connections”](#) chapter.

Best Practice: Require Subscribers to Enter User Credentials

You can use the settings on the Authentication page in the Cisco Unity Administrator to specify whether the Cisco PCA Log On page offers the following options:

- Remember User Name
- Remember Password
- Remember Domain

When you specify that Cisco Unity remember the user name, password, or domain, subscribers will not have to enter them the next time that they log on to the Cisco PCA. Instead, the fields are automatically populated on the Log On page and the credentials are stored as encrypted cookies on the subscriber workstation. By default, the Log On page does not offer subscribers the above options, and for security reasons, your organization may want to keep it that way. However, note that by doing so, you also prevent the options from appearing on the Cisco PCA Log On page. By not allowing subscribers who use the Cisco PCA to specify whether Cisco Unity remembers their credentials, you may increase support desk requests for the information.

Best Practice: Review the Account Policy

Review the account policy that applies when subscribers use the Cisco PCA to verify that the following items are defined appropriately:

- Whether subscribers can use blank passwords
- What happens when subscribers attempt to log on and repeatedly enter incorrect passwords
- How many failed logon attempts are allowed before the subscriber account cannot be used to access the Cisco PCA
- The length of time that a subscriber remains locked out

See the [“Defining Account Policies for Accessing the Cisco PCA”](#) section on page 9-7 for more information and recommended settings.

Best Practice: Prevent the Browser From Displaying a Security Alert

If your organization set up Cisco Unity to use SSL, but did not add it to the Group Policy in order to distribute the certificate to the trusted root store for all users in the domain (or did not tell subscribers how to add the certificate to the trusted root store on their own computers), subscribers may be concerned about the security alert that will be displayed each time that they access the Cisco PCA. Tell subscribers that they can ignore the warning and proceed to use the Cisco PCA without doing any harm to their computers or the network.

To prevent the browser from displaying the security alert, see the [“Distributing the Root Certificate to the Trusted Root Store”](#) section on page 10-7.s

Determining Whether to Offer Enhanced Phone Security

You can set up Cisco Unity so that subscribers must use a secure logon method known as two-factor user authentication (which is the industry standard) to access the Cisco Unity conversation or “TUI.” Cisco Unity works with the RSA SecurID system to provide this method of enhanced phone security.

The RSA SecurID system is made up of three major components: RSA SecurID authenticators, the RSA ACE/Server, and the RSA ACE/Agent.

With the RSA SecurID system, each Cisco Unity subscriber is assigned an RSA SecurID authenticator. (RSA offers authenticators in the form of hardware, software, and smart cards.) Every 60 seconds, the authenticator generates and displays a new, unpredictable number—known as a secure ID or tokencode—that is unique to the subscriber. Each subscriber who has authenticator must have a user account on the ACE/Server. A user account contains the RSA alias and PIN, and information about the user authenticator. By using the information in a user account, the ACE/Server generates the same secure ID as the user authenticator.

When logging on to Cisco Unity over the phone, subscribers enter their Cisco Unity ID (often, their extension) as usual. Then, instead of a password, subscribers enter a passcode, which is a number that combines the subscriber PIN and the secure ID displayed on the subscriber authenticator. Cisco Unity uses the ID to look up the user RSA alias and sends the RSA alias and passcode to the ACE/Agent installed on the Cisco Unity server. The ACE/Agent encrypts the RSA alias and passcode and sends it to the ACE/Server. The ACE/Server looks up the user account, then validates the passcode by using the information stored in the account. The ACE/Server returns a code to the ACE/Agent, which in turn passes it along to Cisco Unity. Return code meanings are shown in [Table 8-5](#).

Table 8-5 ACE/Server Return Codes

Return Code	Meaning
Passcode accepted	Cisco Unity allows subscriber to log on.
Access denied	Cisco Unity prompts the subscriber to enter the passcode again. (This return code can also indicate that the ACE/Server is unavailable.)
Secure ID expired	Cisco Unity prompts the subscriber to enter the next secure ID displayed on the authenticator.
New PIN needed	Cisco Unity prompts the subscriber to enter a new PIN. Note that unless subscribers have pre-assigned PINs, the first time that they log on to Cisco Unity by phone, they will need to enter secure IDs instead of passcodes. (The same is true when subscribers log on to Cisco Unity after a PIN has been cleared in the RSA Database Administrator.) The conversation then guides subscribers through the process of creating new PIN.

Configuring the Cisco Unity Conversation to Use Enhanced Phone Security

Configuring the Cisco Unity conversation to use enhanced phone security essentially requires that you first install and configure an ACE/Server to communicate with the Cisco Unity servers at your site, and then assign the applicable subscribers to a class of service that offers enhanced phone security. You must restart the Cisco Unity server(s) during the configuration process.

Use the following procedure at any time. If you have an existing ACE/Server, skip the steps below that do not apply. See the RSA documentation for information on setting up the ACE/Server and ACE/Agent and for creating and maintaining user accounts.

**Note**

The RSA SecurID system is not available for subscribers who use the Cisco Unity Greetings Administrator.

To Configure Cisco Unity to Use Enhanced Phone Security

- Step 1** Install and configure the ACE/Server. Install only the Local Access Authentication (Client) and the Control Panel Applet components. Do not install the Web Access Authentication (Server) component.
- Step 2** On the ACE/Server, use the RSA Database Administrator program to create the applicable user accounts.
Note that when specifying settings for PIN assignments, indicate user-created PINs only. Cisco Unity does not support system-generated PINs.
- Step 3** Create a group that includes all the users who will use enhanced phone security on Cisco Unity.
- Step 4** Create an Agent Host for each Cisco Unity server that you want to use enhanced phone security (required on both the primary and secondary server when failover will be used).
- Step 5** Specify **Communications Server** as the Agent Host type.
- Step 6** Add the group you created in [Step 3](#) to the Group Activation section of the new client.
- Step 7** On the Cisco Unity server, install and configure the ACE/Agent to work with the Agent Host(s) you created on the ACE/Server.
- Step 8** Use the ACE/Agent Test Authentication utility to authenticate a user with the ACE/Server. If you cannot authenticate the user with the test program, troubleshoot the ACE client/server connection. If you are using failover, also test in a manual failover condition.
- Step 9** In the Cisco Unity Administrator, go to the **System > Configuration > Settings** page and check the **RSA Two Factor** check box.
- Step 10** Log off of the **Cisco Unity Administrator**.
- Step 11** Shut down and restart the Cisco Unity server.
- Step 12** In the Cisco Unity Administrator, create a new class of service (COS) or modify an existing COS for the subscribers who are using enhanced phone security.
- Step 13** On the **Subscribers > Class of Service > Profile** page of the applicable COS, in the Phone Security section, click **Enhanced Security**.
- Step 14** Assign subscribers to the enhanced phone security COS.
- Step 15** If the RSA alias for the subscriber is something other than the subscriber Exchange alias, go to the subscriber Profile page and enter the RSA alias in the Enhanced Security User Alias box.
- Step 16** As applicable, repeat [Step 7](#) through [Step 11](#) for each Cisco Unity server at your site.
- Step 17** Distribute the RSA authenticators to the applicable subscribers.



CHAPTER 9

Password and Account Policy Management

Your first steps in helping prevent unauthorized access to Cisco Unity applications are to secure the passwords that are associated with the default Cisco Unity accounts and to ensure that the passwords initially assigned to subscribers are unique. We also recommend that you define Cisco Unity account policies to require that subscribers change their passwords often and continue to use passwords that are unique and not easy to guess. A well-considered account policy can also thwart unauthorized access to Cisco Unity applications by locking out users who enter invalid passwords too many times.

In this chapter, you will find information on completing the above tasks and on other issues related to password security and account policy management. To help you understand the scope of Cisco Unity password management, the first section in this chapter describes the different passwords required to access the Cisco Unity Administrator, the Cisco Personal Communications Assistant (PCA), and the Cisco Unity conversation (the “TUI”). Each of the sections that follow offer information on actions you need to take; recommendations that will help you make decisions; discussion of the ramifications of the decisions you make; and in many cases, best practices.

For information that will guide you through the process of securing Cisco Unity passwords and defining account policies, see the following sections:

Understanding Which Passwords Subscribers Use

[About the Passwords That Subscribers Use to Access Cisco Unity Applications, page 9-2](#)

Securing Passwords for Default Cisco Unity Accounts

[Securing Passwords On Default Accounts That Are Created by Cisco Unity, page 9-2](#)

Understanding Which Passwords Are Required and How to Initially Secure Them

- [Ensuring That Subscribers Are Initially Assigned Unique and Secure Windows Passwords, page 9-4](#)
- [Ensuring That Subscribers Are Initially Assigned Unique and Secure Phone Passwords, page 9-5](#)

How to Change Subscriber Passwords

- [Changing Passwords That Are Used to Access the Cisco Unity Administrator, page 9-5](#)
- [Changing Cisco PCA Passwords, page 9-6](#)
- [Changing Cisco Unity Phone Passwords, page 9-6](#)

How to Define Account Policies

- [Defining Account Policies for Accessing the Cisco Unity Administrator, page 9-7](#)
- [Defining Account Policies for Accessing the Cisco PCA, page 9-7](#)
- [Defining Account Policies for Phone Access to Cisco Unity, page 9-8](#)

About the Passwords That Subscribers Use to Access Cisco Unity Applications

Cisco Unity subscribers use different passwords to access Cisco Unity applications. Knowing which passwords are required for each application is important in understanding the scope of Cisco Unity password management.

Cisco Unity Administrator

When IIS is configured so that the Cisco Unity Administrator uses Anonymous authentication, Cisco Unity prompts subscribers to enter the user name and password for their Active Directory account on the Cisco Unity Log On page.

When IIS is configured so that the Cisco Unity Administrator uses Integrated Windows authentication, subscribers enter the user name, password, and domain for the administration account that was selected when Cisco Unity was installed, or an applicable Active Directory account.

Cisco PCA

Subscribers are prompted to enter the user name and password for their Active Directory accounts on the Cisco PCA Log On page.

Cisco Unity Conversation

Subscribers use the phone keypad to enter a password, consisting entirely of digits.

Securing Passwords On Default Accounts That Are Created by Cisco Unity

During installation, Cisco Unity creates several default accounts. Some of the default accounts have phone and/or Windows passwords assigned to them that are not considered secure.

Best Practice: Secure Phone Passwords by Changing Them

You can change phone passwords on the Subscribers > Subscribers > Phone Password page in the Cisco Unity Administrator. Specify a long—20 or more digits—and non-trivial password for the following default accounts:

- Example Administrator—The Cisco Unity Installation and Configuration Assistant prompts for a phone password for the Default Administrator template, which is used for this account. If the system was upgraded from Cisco Unity version 4.0(3) or earlier, the Cisco Unity Example Administrator subscriber account may still have a phone password that needs to be changed.
- Example Subscriber—If you upgraded from a version of Cisco Unity prior to 4.0(3), you may have an automatically-created Example Subscriber account. If you have an Example Subscriber account and you do not use it, delete it. (Delete both the Cisco Unity subscriber account and the corresponding Active Directory account.) Otherwise, you should change the phone password.

Best Practice: Secure Active Directory Passwords by Changing Them

The default Cisco Unity accounts listed in [Table 9-1](#) are associated with Active Directory accounts whose passwords should be changed using Active Directory Users and Computers. Specify a password that meets the following specifications:

- Is at least eight characters long.

- Includes at least one character from at least three of the following categories:
 - Upper-case letters
 - Lower-case letters
 - Numbers 0 to 9
 - Special characters: ~ ! @ # \$ % ^ * “ ‘ , . : ; ? - _ () [] < > { } + = / \ |
- Does not consecutively repeat any character more than twice (for example, do not use “aaaB1*C9”).
- Does not match the current logon name, either forward or backward.

Table 9-1 Cisco Unity Default Accounts Whose Active Directory Account Passwords Should Be Changed

Cisco Unity Default Account	Considerations
Example Administrator	<p>The account name is EAdministrator.</p> <p>The Cisco Unity Installation and Configuration Assistant prompts for a password for the Default Administrator template, which is used to create the Example Administrator account and the corresponding Active Directory account. If the system was upgraded from Cisco Unity version 4.0(3) or earlier, the Active Directory Example Administrator account may still have the default password, which should be changed.</p>
Example Subscriber	<p>The account name is ESubscriber.</p> <p>If the system was upgraded from Cisco Unity version 4.0(2) or earlier, you may have an automatically-created Example Subscriber account, and the account may still have the default password.</p> <p>If you have an Example Subscriber account and you do not use it, delete it. (Delete both the Cisco Unity subscriber account and the corresponding Active Directory account.) Otherwise, change the password.</p>
Unity Messaging System	<p>The account name is Unity_<servername>.</p> <p>Note that the account is not visible in the Cisco Unity Administrator. If the system was upgraded from Cisco Unity version 4.0(4) or earlier, the Active Directory Example Administrator account may be enabled and may still have the default password, which should be changed.</p>
None	<p>The account name is UAmis_<servername>.</p> <p>The Cisco Unity Installation and Configuration Assistant prompts for a password for the Default Subscriber template, which is used to create the UAmis Active Directory account. If the system was upgraded from Cisco Unity version 4.0(3) or earlier, the UAmis account may still have the default password, which should be changed. This account is disabled by default.</p>
None	<p>The account name is UOmni_<servername>.</p> <p>The Cisco Unity Installation and Configuration Assistant prompts for a password for the Default Subscriber template, which is used to create the UOmni Active Directory account. If the system was upgraded from Cisco Unity version 4.0(3) or earlier, the UOmni account may still have the default password, which should be changed. This account is disabled by default.</p>

For additional information on managing default accounts, see the [“Best Practices for Securing Default Accounts” section on page 7-5](#).

Ensuring That Subscribers Are Initially Assigned Unique and Secure Windows Passwords

Subscribers use an Active Directory password to access the Cisco Unity Administrator (when it is configured to use Anonymous authentication) and the Cisco PCA. To protect Cisco Unity from unauthorized access, each subscriber should be assigned a unique Active Directory password. Additionally, each password should be eight or more characters long and non-trivial.

Simply changing the Active Directory password on the Subscribers > Subscriber Template > Passwords page in the Cisco Unity Administrator before you create subscriber accounts does not ensure that subscribers are assigned unique passwords. This is because the template might not be used to assign passwords, and when it is used, each subscriber account that you create will be assigned the same password.

Consider the following options to ensure that each subscriber is assigned a unique and secure password at the time that you create the account, or immediately thereafter.

Assigning Unique and Secure Active Directory Passwords When You Create Subscriber Accounts

Use one of the following methods to assign a unique and secure Active Directory password to each subscriber account that you create:

- Do not use the Cisco Unity Administrator or the Cisco Unity Bulk Import wizard to create new Active Directory accounts. Instead, first create an Active Directory account for each subscriber by using Active Directory Users and Computers, and assign each user a unique and secure password as you go. You can then use the Cisco Unity Administrator or the Cisco Unity Bulk Import wizard to create Cisco Unity subscriber accounts.
- Use the Cisco Unity Administrator to add subscribers one at a time. Use a different template for each subscriber that you create, specifying a unique and secure Active Directory password in each template. Alternatively, you can use one template for all subscribers, but specify a unique and secure password before each subscriber account that you add. If you use the same template for all subscribers, you will need to record the passwords that you assign to each subscriber in a secure place so that you can distribute them later. (Cisco Unity stores only the last value saved.)

Before you specify a template password, review the password policy for the Active Directory domain to make sure that the minimum length and complexity requirements do not conflict with the password that you specify in the template. Cisco Unity will not add a subscriber account when the length of the password on the subscriber template is less than the minimum length for passwords in the Active Directory domain.

Assigning Unique and Secure Active Directory Passwords After Subscriber Accounts Have Been Created

After you have created subscriber accounts, use one of the following methods to assign each account a unique and secure Active Directory password:

- Use Active Directory Users and Computers to change the existing password for each user.
- Ask subscribers to change their own passwords. Subscribers can change their Cisco PCA passwords in Windows by pressing Ctrl-Alt-Delete and then clicking Change Password. (If the Cisco Unity server is on a different domain than the one that subscribers typically access, subscribers will also need to specify the domain name for the Cisco Unity server.)

Note that subscribers may assume that their phone and Cisco PCA passwords are the same. As a result, they may think that they are changing both passwords when Cisco Unity prompts them to change their phone password during first-time enrollment. For this reason, you may find that many subscribers do not change their Cisco PCA passwords in Windows, even though you request that they do so.

Ensuring That Subscribers Are Initially Assigned Unique and Secure Phone Passwords

To help protect Cisco Unity from unauthorized access and toll fraud, every subscriber should be assigned a unique phone password. Additionally, each password should be eight or more characters long and non-trivial.

Simply changing the phone password on the Subscribers > Subscriber Template > Passwords page in the Cisco Unity Administrator before you create subscriber accounts does not ensure that subscribers are assigned unique passwords. This is because the template might not be used to assign passwords, and when it is used, each subscriber account that you create is assigned the same password.

Consider the following options to ensure that each subscriber is assigned a unique and secure password at the time that you create the account, or immediately thereafter.

Assigning Unique and Secure Phone Passwords When You Create Subscriber Accounts

Use one of the following methods to assign a unique and secure phone password to each subscriber account that you create:

- Use the Cisco Unity Bulk Import wizard to import user data contained in a CSV file. Include the optional column header `DTMF_PASSWORD` in the CSV file to overwrite the template password for each subscriber.
- Use the Cisco Unity Administrator to add a subscriber one at a time. Use a different template for each subscriber that you create, specifying a unique and secure phone password in each template. Alternatively, you can use one template for all subscribers, but specify a unique and secure password before each subscriber account that you add. To avoid recording and distributing the passwords, tell subscribers to use the Cisco Unity Assistant to change their initial phone passwords. (The Cisco Unity Assistant does not require that subscribers enter the old phone password to change it.)

Assigning Unique and Secure Phone Passwords After Creating Subscriber Accounts

After you have created subscriber accounts by using either the Cisco Unity Administrator or the Cisco Unity Bulk Import wizard, use the Cisco Unity Bulk Import wizard to assign a unique phone password to each subscriber account that you created. To avoid recording and distributing the passwords, tell subscribers to use the Cisco Unity Assistant to change their initial phone passwords. (The Cisco Unity Assistant does not require that subscribers enter the old phone password to change it.)

Changing Passwords That Are Used to Access the Cisco Unity Administrator

Cisco Unity administrators can change their passwords in Windows by pressing Ctrl-Alt-Delete and then clicking Change Password. If the Cisco Unity server is in a different domain than the one that subscribers typically access with their Windows passwords, subscribers will also need to specify the domain name for the Cisco Unity server.

Best Practice

When you change a password used to access the Cisco Unity Administrator, specify a long—eight or more characters—and non-trivial password. Set up your account policy to require it. Passwords that are used to access the Cisco Unity Administrator should be changed every six months.

Changing Cisco PCA Passwords

You can change subscriber passwords by using Windows Active Directory for Users and Computers after you create subscriber accounts. Each subscriber should be assigned a unique Windows password. Subscribers cannot use the Cisco Unity phone conversation or the Cisco Unity Assistant to change their Cisco PCA passwords, nor can administrators change them in the Cisco Unity Administrator. Instead, subscribers change their Cisco PCA passwords only in Windows by pressing Ctrl-Alt-Delete and then clicking Change Password. (If the Cisco Unity server is in a different domain than the one that subscribers typically access with their Windows passwords, subscribers will also need to specify the domain name for the Cisco Unity server.)

Best Practice

Specify a long—eight or more characters—and non-trivial password. Encourage subscribers to follow the same practice whenever they change their Windows passwords, or set your domain account policy in Windows to require them to do so. Cisco PCA passwords should be changed every six months.

Changing Cisco Unity Phone Passwords

You can change the phone password for an individual subscriber on the Subscribers > Subscribers > Phone Password pages in the Cisco Unity Administrator at any time. Alternatively, you can use the Cisco Unity Bulk Import wizard to change the phone passwords for multiple subscribers at the same time. (See the Cisco Unity Bulk Import Help for details.)

As a best practice, each subscriber should be assigned a unique password that is eight or more digits long and non-trivial. If you allow subscribers to set their own passwords, encourage them to follow the same practice or use the settings on the Subscribers > Account Policy > Phone Password Restrictions page in the Cisco Unity Administrator to require them to do so.

When their accounts are configured to allow them, subscribers can use the Cisco Unity phone conversation or the Cisco Unity Assistant to set their phone passwords. Neither the Cisco Unity conversation nor the Cisco Unity Assistant require subscribers to enter their old phone passwords to reset them.

Note that AMIS, Bridge, Internet, and VPIM subscribers cannot log on to Cisco Unity by phone, use the Cisco Unity Assistant, or use the Cisco Unity Inbox.

Phone passwords should be changed every 30 days.

Best Practice: Train Subscribers to Protect Their Phone Passwords

Because subscribers can use the Cisco Unity Assistant to change their phone passwords, they should take appropriate measures to keep their Cisco PCA passwords secure. Subscribers need to understand that the phone and Cisco PCA passwords are not synchronized. While first-time enrollment prompts them to change their initial phone passwords, it does not let them change the password that they use to log on to the Cisco PCA website.

Best Practice: Check for Trivial Subscriber Passwords

After subscribers have set their passwords, confirm that the passwords are non-trivial. To create a report of subscribers who have trivial passwords, use the Subscriber Information Dump, which is in the Cisco Unity Tools Depot, and check the Trivial PW Check check box. The Subscriber Information Dump report will give one of six values for each subscriber account, as described in the Subscriber Information Dump Help. Subscribers with weak passwords can then be identified and trained to use stronger passwords for their Cisco Unity accounts.

Defining Account Policies for Accessing the Cisco Unity Administrator

How you set up an account policy depends on the authentication method used by the Cisco Unity Administrator. When the Cisco Unity Administrator uses the Integrated Windows authentication method (which is the default), the account policy that is specified for each Active Directory account determines the following:

- How Windows handles situations when users attempt to log on to Windows and repeatedly enter incorrect passwords
- The number of failed logon attempts that Windows allows before the user account cannot be used to access Windows
- The length of time that a user remains locked out

If the Cisco Unity Administrator uses Anonymous authentication, you can use the settings on the Authentication page in the Cisco Unity Administrator to customize the logon, password, and lockout policies that Cisco Unity applies when subscribers use the Cisco Unity Administrator to access Cisco Unity.

Best Practices

For increased security, prohibit the use of blank passwords, a restriction that Cisco Unity honors even when an Active Directory account allows them.

With either authentication method, the Active Directory account policies that you define should also require that subscribers change their Cisco Unity passwords at least once every six months and that when changed, the passwords are long—eight or more characters—and non-trivial.

Defining Account Policies for Accessing the Cisco PCA

The account policy that you specify on the Authentication page in the Cisco Unity Administrator determines how Cisco Unity handles situations when subscribers attempt to log on to the Cisco PCA and repeatedly enter incorrect passwords; whether subscribers can use blank passwords; the number of failed logon attempts that Cisco Unity allows before the subscriber account cannot be used to access the Cisco PCA; and the length of time that a user remains locked out.

In addition, you can use the settings on the Authentication page to specify whether the Log On page for the Cisco PCA offers subscribers the following options:

- Remember User Name
- Remember Password
- Remember Domain

When subscribers specify that Cisco Unity will remember their user name, password, or domain, subscribers will not have to enter them the next time that they log on to the Cisco PCA. Instead, the fields are automatically populated in the Log On page. Allowing subscribers to specify whether Cisco Unity will remember their credentials may reduce support desk requests for the information. However, you may not want the Log On page to offer subscribers the above options for security reasons. If this is the case, you can uncheck the Remember Logons for __ Days check box on the Authentication page to prevent the options from appearing on the Cisco PCA Log On page, and to require that subscribers enter their user name, password, and domain each time that they log on to the Cisco PCA.

Defining Account Policies for Phone Access to Cisco Unity

The account policy settings on the Phone Password Restrictions page and the Cisco Unity Account Lockout page in the Cisco Unity Administrator apply when subscribers access Cisco Unity by phone. Changes to settings in the account policy affect all existing subscribers.

See the following sections for more information:

- [Setting Phone Password Restrictions, page 9-8](#)
- [Setting Account Lockout Restrictions, page 9-9](#)

Setting Phone Password Restrictions

Phone password restriction settings allow you to define a system-wide password policy that applies when subscribers access Cisco Unity by phone. For greater security, establish rules that prevent passwords from being easy to guess and from being used for a long time. At the same time, it is also best to avoid requiring passwords that are so complicated or that must be changed so often that subscribers have to write them down to remember them.

Use the following guidelines as you specify a password policy on the Phone Password Restrictions page in the Cisco Unity Administrator:

Maximum Phone Password Age

As a best practice, do not enable the Password Never Expires option. Instead, confirm that the Days Until Password Expires field is selected so that subscribers are prompted to change their passwords every X days (X is the value specified in the adjacent box). We recommend that you set a maximum phone password age of 30 days.

Phone Password Length

As a best practice, do not enable the Permit Blank Password option. Instead, confirm that the Minimum Number of Characters in Password field is selected so that subscribers are required to create a password at least X characters long (X is the value specified in the adjacent box). When you change the minimum password length, subscribers will be required to use the new length the next time they change their passwords.

We recommend that you require subscribers to use a long—eight or more digits—password when you specify phone password length.

Phone Password Uniqueness

As a best practice, disable the Do Not Keep Password History option (it is enabled by default). Instead, specify a number in the Number of Passwords to Remember field. By doing so, you enable Cisco Unity to enforce password uniqueness by storing a specified number of previous passwords for each subscriber and then, comparing new passwords with those stored in the password history. Cisco Unity rejects any password that matches a password stored in the history.

As a best practice, specify that Cisco Unity store between 10 and 24 passwords in password history.

Check Against Trivial Passwords for Extra Security

As a best practice, do not enable the Permit Blank Password option. Instead, confirm that the Check Against Trivial Passwords for Extra Security field is enabled so that subscribers must use non-trivial passwords.

Cisco Unity applications reject phone passwords that contain the trivial characteristics shown in Table 9-2.

Table 9-2 Trivial Phone Password Characteristics Rejected by Application

Trivial Password Characteristic	Cisco Unity Conversation (TUI) ¹	Cisco Unity Assistant ¹	Cisco Unity Administrator ¹	Cisco Unity Bulk Import	Password Hardening Wizard
Consists entirely of repeated numbers, such as 44444	Yes	Yes	Yes	Yes	Yes
Contains at least one group of repeated numbers, such as 11579	No	No	Yes	No	Yes
Contains consecutive ascending numbers, such as 12345	Yes	Yes	Yes	Yes	Yes
Contains consecutive descending numbers, such as 87654	Yes	Yes	Yes	Yes	Yes
Matches the subscriber primary extension	Yes	Yes	Yes	No	Not applicable

1. Only when you enable the Check Against Trivial Passwords for Extra Security field.

Setting Account Lockout Restrictions

Cisco Unity account lockout settings allow you to specify whether you want Cisco Unity to use an account lockout policy that applies to all subscribers who access Cisco Unity by phone. You cannot change account policy settings for individual subscriber accounts, though you can lock individual subscriber accounts to prevent those subscribers from using the phone to access Cisco Unity (you lock out individual subscriber accounts on the applicable Subscribers > Subscribers > Account page in the Cisco Unity Administrator).

To specify an account lockout policy on the Account Lockout page, confirm that the Account Lockout field is selected. Then, use the following guidelines as you indicate how you want Cisco Unity to handle failed logon attempts, and if they occur, how long account lockouts last.

Lock Account After __ Invalid Attempts

Use this field to indicate how Cisco Unity handles situations when a caller attempts to log on to a subscriber account and repeatedly enters an incorrect password. We recommend that you change the default to specify that Cisco Unity blocks phone access to the subscriber account after three failed logon attempts.

Reset Count After __ Minutes

Use this field to specify the number of minutes after which Cisco Unity will clear the count of failed logon attempts (unless the failed logon limit is already reached and the account is locked).

Lockout Duration

Specify the length of time that a subscriber who is locked out must wait before attempting to access Cisco Unity by phone again. We recommend that you change the default value to 1440 minutes so that Cisco Unity will reset the count after one day. For even tighter security, you can select Forever, which prevents subscribers from accessing their accounts until a system administrator unlocks them on the

applicable Subscribers > Subscribers > Account page. Set the lockout duration to Forever only if a system administrator is readily available to assist subscribers or if the system is prone to unauthorized access and toll fraud.



CHAPTER 10

Using SSL to Secure Client/Server Connections

In this chapter, you will find descriptions of potential security issues related to the Secure Sockets Layer (SSL) protocol; information on any actions you need to take; recommendations that will help you make decisions; discussion of the ramifications of the decisions you make; and in many cases, best practices.

SSL can be used as a method of providing security for transmission of Cisco Unity data across the network through the use of public/private key encryption. SSL protects the security of Cisco Unity subscriber credentials when they are passed across the network. SSL also protects the security of all data entered in Cisco Unity web applications.

You can set up SSL during a new Cisco Unity installation or upgrade, or at any time after the Cisco Unity installation or upgrade is complete. (The Cisco Unity installation guide and the *Reconfiguration and Upgrade Guide for Cisco Unity* contain the procedures that an installer uses to set up Cisco Unity, the Cisco Personal Communications Assistant (PCA), and the Status Monitor to use SSL during a new installation or upgrade.)

This chapter describes the manual process that an administrator uses to set up Cisco Unity to use SSL at any time after the successful completion of a Cisco Unity installation or upgrade. This chapter also includes procedures that a network administrator or subscriber uses to set up subscriber workstations to access Cisco Unity web applications by using SSL.

See the following sections for more information:

- [Determining Whether to Set Up Cisco Unity Applications to Use SSL, page 10-1](#)
- [Manually Setting Up the System to Use SSL, page 10-2](#)

Determining Whether to Set Up Cisco Unity Applications to Use SSL

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 when the Cisco Unity Administrator and the Status Monitor are configured to use the Anonymous authentication method. 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.

In addition, if you plan to offer Mobile Message Access for BlackBerry to subscribers, we recommend that you set up Cisco Unity to use SSL for its communications with the BlackBerry server. By default, data—including subscriber phone passwords—is sent between the Cisco Unity server and the BlackBerry server in clear text.

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.

Manually Setting Up the System to Use SSL

The following task list guides you through the process of manually setting up Cisco Unity to use SSL with Microsoft Certificate Services. Do the procedures in each section, in the order listed. If a procedure does not apply to your situation, skip it.



Note

This section provides information on setting up Cisco Unity to use SSL with Microsoft Certificate Services. If you decide to set up SSL, but do not want to use Microsoft Certificate Services, refer to the third-party Certificate Authority documentation.

1. Designate a server to act as your certificate authority and install the Microsoft Certificate Services component. See the [“Installing the Microsoft Certificate Services Component”](#) section on page 10-3.
2. Create and submit a certificate request using Microsoft Certificate Services. See the [“Creating and Submitting a Certificate Request”](#) section on page 10-3.
3. Issue the certificate and install it on the Cisco Unity server. See the [“Issuing and Installing the Certificate”](#) section on page 10-4.
4. Set up the Cisco Unity Administrator, Status Monitor, and Cisco PCA to use SSL. Optionally, if you are planning to offer Mobile Message Access for BlackBerry to subscribers, set up Cisco Unity to use SSL when it communicates with the BlackBerry server. See the [“Setting Up Cisco Unity Web Applications to Use SSL”](#) section on page 10-6.
5. Set up subscriber workstations to use SSL when subscribers access the Cisco Unity Administrator, Status Monitor, and Cisco PCA. See the [“Distributing the Root Certificate to the Trusted Root Store”](#) section on page 10-7, and the [“Setting Up SSL Redirection”](#) section on page 10-10.
6. As applicable, prevent BlackBerry devices from displaying the resulting security alert. See the [“Managing Security Alerts When Using SSL Connections with BlackBerry Servers”](#) section on page 10-10.

Installing the Microsoft Certificate Services Component

Do the procedure in this section to install the Microsoft Certificate Services component (available with Windows) 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.
-

Creating and Submitting a Certificate Request

Do the two procedures in this section to create and submit a certificate request on the Cisco Unity server.

To Create a Certificate Request by Using Microsoft Certificate Services

-
- 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**.
Otherwise, skip to [Step 4](#).
 - Step 4** Right-click **Default Web Site**, and click **Properties**.
 - Step 5** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
 - Step 6** Under Secure Communications, click **Server Certificate**.
 - Step 7** On the Web Server Certificate wizard Welcome page, click **Next**.
 - Step 8** Click **Create a New Certificate**, and click **Next**.
 - Step 9** Click **Prepare the Request Now, But Send It Later**, and click **Next**.
 - Step 10** Enter a name and a bit length for the certificate.

We recommend that you choose a bit length of 512. Greater bit lengths may decrease performance.

Step 11 Click **Next**.

Step 12 Enter the organization information, and click **Next**.

Step 13 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 14 Click **Next**.

Step 15 Enter the geographical information, and click **Next**.

Step 16 Specify the certificate request file name and location, and write down the file name and location because you will need the information for the next procedure.

Save the file to a disk or to a directory that the certificate authority (CA) server can access.

Step 17 Click **Next**.

Step 18 Verify the request file information, and click **Next**.

Step 19 Click **Finish** to exit the Web Server Certificate wizard.

Step 20 Click **OK** to Close the Default Web Site Properties dialog box.

Step 21 Close the Internet Services Manager window.

To Submit the Certificate Request

Step 1 On the CA server, on the Windows Start menu, click **Run**, then run **certreq**.

Step 2 Browse to the directory where you saved the certificate request file in [Step 16](#) of the [“To Create a Certificate Request by Using Microsoft Certificate Services”](#) procedure on page 10-3, and double-click it.

Step 3 Click the CA to use, and click **OK**.

Issuing and Installing the Certificate

By default, when the CA processes the certificate request, it assigns a pending status for added security. This means that you must verify the authenticity of the request and manually issue the certificate on the virtual directories that will use it.

To Issue the Certificate

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, 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**.
Otherwise, skip to [Step 4](#).
 - Step 4** Right-click **Default Website**, and click **Properties**.
 - Step 5** In the Properties dialog box, click the **Directory Security** tab.
 - Step 6** Under Secure Communications, click **Server Certificate**.
 - Step 7** On the Web Server Certificate wizard welcome screen, click **Next**.
 - Step 8** Click **Process the Pending Request and Install the Certificate**, and click **Next**.
 - Step 9** Browse to the directory of the certificate (.cer) file, and double-click it.
 - Step 10** Verify the certificate information, and click **Next**.
 - Step 11** Click **Finish** to close the Web Server Certificate wizard window.
 - Step 12** Click **OK** to close the Default Website Properties dialog box.
 - Step 13** Close the **Internet Services Manager** window.
 - Step 14** Repeat [Step 1](#) through [Step 13](#) on each Cisco Unity server in your network, including if applicable both servers in a failover pair.
-

Setting Up Cisco Unity Web Applications to Use SSL

After the certificate has been installed, do the following procedure to set up the Cisco Unity Administrator, Status Monitor, and Cisco Personal Communications Assistant to use SSL. If you plan to offer Mobile Message Access for BlackBerry to subscribers, do the “[To Set Up the Cisco Unity Server and the BlackBerry Server to Use SSL](#)” procedure on page 10-7 to set up Cisco Unity to use SSL when communicating with the BlackBerry server.

To Set Up the Cisco Unity Administrator, the Status Monitor, and the Cisco PCA 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**. Otherwise, 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 Website, right-click **Jakarta**, and click **Properties**.
 - Step 12** Repeat [Step 6](#) to set the Cisco PCA to use SSL.
 - Step 13** Under Default Web Site, double-click **AvXml**.
 - Step 14** In the right pane, right-click **AvXml.dll**, and click **Properties**.
 - Step 15** In the Properties dialog box, click the **File Security** tab.
 - Step 16** Under Secure Communications, click **Edit**.
 - Step 17** Check the **Require Secure Channel (SSL)** check box.
 - Step 18** Click **OK** to close the Secure Communications dialog box.
 - Step 19** Click **OK** to close the AvXml.dll Properties dialog box.
 - Step 20** Close the Internet Services Manager window.
 - Step 21** If the Cisco Unity server is running Windows Server 2003, restart the Cisco Unity server.
-

To Set Up the Cisco Unity Server and the BlackBerry Server to Use SSL

When setting up Mobile Message Access for BlackBerry, it is necessary to set up Cisco Unity to use the SSL protocol before installing the Mobile Message Access for BlackBerry plug-in on the BlackBerry server. If you have already installed this plug-in on the BlackBerry server without first setting up SSL, you will need to re-install the plug-in after you complete this procedure.

See the “Task List for Setting Up Mobile Message Access for BlackBerry” section in the “Setting Up Subscriber Workstations” chapter of the *System Administration Guide for Cisco Unity* for a task list of steps for setting up Mobile Message Access for BlackBerry. The *System Administration Guide for Cisco Unity* is available at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

-
- 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**.
Otherwise, 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 **BAP**, and click **Properties**.
 - Step 8** Repeat [Step 6](#) to set the BAP directory to use SSL.
 - Step 9** Close the Internet Services Manager window.
 - Step 10** If the Cisco Unity server is running Windows Server 2003, restart the Cisco Unity server.
-

Distributing the Root Certificate to the Trusted Root Store

When Cisco Unity is set up to use SSL, it offers the digital certificate that you issued in the “[Manually Setting Up the System to Use SSL](#)” section on page 10-2 as proof of its identity each time a subscriber tries to access the Cisco Unity Administrator, the Status Monitor, or the Cisco PCA. If the certificate is not also added to the trusted root store on subscriber workstations, the browser will display a message to alert subscribers that the authenticity of the site cannot be verified and, therefore, its content cannot be trusted. Note that the appearance of the browser message does not prevent SSL from functioning correctly. However, the message may be a source of confusion for subscribers and could result in calls to the help desk.

To add the certificate to the trusted root store on subscriber workstations, do one or both of the following, as applicable:

- Distribute the certificate to all subscribers in the domain by adding it to the Group Policy. See the [“Distributing the Root Certificate to the Trusted Root Store for All Users in the Domain”](#) section on page 10-8.
- Add the certificate to the trusted root store on individual subscriber workstations. See the [“Adding the Cisco Unity Certificate to the Trusted Root Store on Subscriber Workstations”](#) section on page 10-9.

To manage security alerts that subscribers see when they use their BlackBerry devices to access Cisco Unity voice messages, see the [“Managing Security Alerts When Using SSL Connections with BlackBerry Servers”](#) section on page 10-10.

Distributing the Root Certificate to the Trusted Root Store for All Users in the Domain

To distribute the certificate to the trusted root store for all users in the domain, do the following two procedures.

To Export the CA Root Certificate

-
- Step 1** On the CA server, on the Windows Start menu, click **Programs > Administrative Tools > Certification Authority**.
 - Step 2** In the left pane of the Certification Authority window, right-click the <Root Certification Authority name>, and click **Properties**.
 - Step 3** Click **View Certificate**.
 - Step 4** Click the **Details** tab.
 - Step 5** In the Show list, choose **All**, and click **Copy to File**.
 - Step 6** On the Certificate Export wizard welcome screen, click **Next**.
 - Step 7** Accept the default export file format **DER Encoded Binary X.509 (.CER)**, and click **Next**.
 - Step 8** Specify a file name and a location, and click **Next**.
The location must be accessible to the Domain Admin account that will modify the group policy.
 - Step 9** Verify the settings, and click **Finish**.
 - Step 10** Click **OK** to close the Certificate Details dialog box.
 - Step 11** Click **OK** to close the Properties dialog box for the Root Certification Authority.
 - Step 12** Close the **Certification Authority** window.
-

To Add the Root Certificate to the Domain Group Policy for Trusted Root Certificate Authorities

-
- Step 1** On the CA server, 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 **Run**, then run **mmc**.
 - Step 3** On the top menu, click **Console**.
 - Step 4** Click **Add/Remove Snap-in**.
 - Step 5** On the Standalone tab, click **Add**.

- Step 6** In the Add Standalone Snap-in dialog box, click **Group Policy**, and click **Add**.
- Step 7** Click **Browse**.
- Step 8** In the Browse for a Group Policy Object dialog box, click the **Domains/OUs** tab.
- Step 9** In the Look In list, select the domain to which the Cisco Unity server belongs.
- Step 10** In the Domains, OUs, and Linked Group Policy Objects list, click **Default Domain Policy**, and click **OK**.
- Step 11** Click **Finish**.
- Step 12** Close the **Add Standalone Snap-in** dialog box.
- Step 13** Click **OK** to close the Add/Remove Snap-in dialog box.
- Step 14** In the left pane of the console window, expand **Default Domain Policy** for the Cisco Unity server domain.
- Step 15** Click **Computer Configuration > Windows Settings > Security Settings > Public Key Policies**.
- Step 16** Right-click **Trusted Root Certification Authorities**, and click **All Tasks > Import**.
- Step 17** On the Certificate Import wizard welcome screen, click **Next**.
- Step 18** Browse to the location of the saved Root Certification Authority certificate, and double-click it.
- Step 19** Click **Next**.
- Step 20** Accept the default for the certificate store, and click **Next**.
- Step 21** Verify the settings, and click **Finish**.
- Step 22** Save the console settings.
- Step 23** Close the console window.
-

Adding the Cisco Unity Certificate to the Trusted Root Store on Subscriber Workstations

The Cisco Unity certificate can be added to the trusted root store on subscriber workstations in the following circumstances:

- If you choose not to distribute the certificate to the trusted root store for all users in the domain.
- If subscribers can access Cisco Unity web applications from workstations that do not belong to a trusted domain, for example, from a computer at home. Tell subscribers how to add the certificate to the trusted root store on their own computers.

You can do the following procedure on all applicable workstations, or distribute the procedure to subscribers to do themselves, as needed. Keep in mind that you will need to do the procedure again each time a new subscriber workstation is installed after the initial setup of SSL.

To Add the Cisco Unity Certificate to the Trusted Root Store on Each Subscriber Workstation

- Step 1** On each subscriber workstation, start Internet Explorer.
- Step 2** Go to **http://<The Certificate Authority server>/Certsrv**.
- Step 3** On the Microsoft Certificate Services page, under Select a Task, click **Retrieve the CA Certificate or Certificate Revocation List**.
- Step 4** Click **Next**.

- Step 5** Click the **Install This CA Certification Path** link.
- Step 6** When prompted, click **Yes** to add the certificate to the Root Store.
-

Setting Up SSL Redirection

If the Cisco Unity server is running Windows Server 2003, SSL redirection from an http URL to an https URL may fail. If this happens, change the Windows shortcut that starts the Cisco Unity web application to point to the https URL instead of the http URL on each subscriber workstation, as applicable.

Managing Security Alerts When Using SSL Connections with BlackBerry Servers

When you configure Cisco Unity to use SSL in its communications with a BlackBerry server, the associated BlackBerry devices display a message to alert subscribers that the authenticity of the site cannot be verified and, therefore, its content cannot be trusted. Note that the appearance of the message does not prevent SSL from functioning correctly.

The message may be a source of confusion for subscribers and could result in calls to the help desk. To prevent the message from appearing, you can:

- Add the certificate to the trusted root store on the BlackBerry server. Refer to the BlackBerry Enterprise Server documentation for details.
- If applicable, tell subscribers to add Cisco Unity as a trusted server when prompted by their BlackBerry device. Depending on the device that subscribers use, the security alert may not offer subscribers the option of adding Cisco Unity as a trusted server.



CHAPTER 11

Securing Subscriber Messages

Cisco Unity offers the following message security options:

- All subscribers have the ability to mark messages private. Messages that are marked private cannot be forwarded by phone, from Cisco Unity ViewMail for Microsoft Outlook, or from the Cisco Unity Inbox.
- Secure Messaging is an optional feature that you can enable for subscribers. When enabled, messages sent by that subscriber will be encrypted. You can also enable message aging for secure messages, which after a specified period of time, force encrypted messages to expire.
- If you are using the Cisco Unity Inbox with Cisco Unity, you can disable the Copy to File option so that subscribers cannot save any message—regardless of its sensitivity—on their hard disks.

In addition, there are security issues you should consider before enabling the Text to Speech (TTS) feature for subscribers.

In this chapter, you will find descriptions of potential security issues related to securing messages; information on any actions you need to take; recommendations that will help you make decisions; discussion of the ramifications of the decisions you make; and in many cases, best practices.

See the following sections for details:

- [How Cisco Unity Handles Messages That Are Marked Private, page 11-1](#)
- [Secure Messaging, page 11-2](#)
- [Best Practices for Using Text to Speech \(Unified Messaging\), page 11-18](#)
- [Disabling the Copy to File Option in the Media Master for the Cisco Unity Inbox, page 11-18](#)

How Cisco Unity Handles Messages That Are Marked Private

Messages that are marked private cannot be forwarded by phone, from Cisco Unity ViewMail for Microsoft Outlook, or from the Cisco Unity Inbox. This includes any voice message that a Cisco Unity subscriber marked private, and as applicable, any e-mail message that a subscriber or another sender marked private in Outlook. In addition, when a message is marked private, the Copy and Copy To options are disabled on the Options menu on the Media Master control bar in ViewMail for Outlook and the Cisco Unity Inbox.

For subscribers who require more secure messaging, consider the following:

- You can set up secure messaging and enable subscribers to use it. Secure messaging provides security through the use of public/private key encryption for voice messages. Secure messages cannot be heard by anyone other than a Cisco Unity subscriber who is authenticated with their Cisco Unity server. For information on how to set up secure messaging, see the “[Secure Messaging](#)” section on page 11-2.
- You can prevent subscribers from saving any voice message—regardless of its sensitivity—to their hard disks by disabling the Copy to File option on the Options menu of the Media Master control bar in the Cisco Unity Inbox. To learn more, see the “[Disabling the Copy to File Option in the Media Master for the Cisco Unity Inbox](#)” section on page 11-18.

Secure Messaging

The secure messaging feature provides security through the use of public and private key encryption for voice messages. Secure messaging is available for systems running on Microsoft Exchange, including the partner Exchange server, if applicable.

A Cisco Unity service, the Secure Messaging Service, installs and maintains public and private key encryption certificates on each Cisco Unity server.

See the following sections for information on how secure messaging works, how to set it up, and how to maintain systems that have the feature enabled:

- [Understanding How Cisco Unity Handles Secure Messages, page 11-2](#)—Describes how and when secure messages can be sent and played.
- [Limitations of Secure Messaging, page 11-4](#)—Lists limitations of secure messaging that subscribers should understand before using the feature.
- [Installing and Configuring Secure Messaging, page 11-6](#)—Includes instructions for installing secure messaging, configuring the feature, and enabling subscribers to use it.
- [Maintenance Considerations When Secure Messaging Is in Use, page 11-15](#)—Discusses maintenance issues you should consider when using the secure messaging feature.
- [Secure Messaging and Legal Discoverability, page 11-16](#)—Discusses how you can respond to requests for legal discoverability of encrypted voice messages
- [Technical Details of Secure Messaging, page 11-17](#)—Provides in-depth detail of how secure messaging works.

For information on troubleshooting secure messaging, see the “[Troubleshooting Secure Voice Messages](#)” section in the “[Messages](#)” chapter of the *Troubleshooting Guide for Cisco Unity*. The guide is available at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_troubleshooting_guides_list.html.

Understanding How Cisco Unity Handles Secure Messages

When a secure message is recorded, Cisco Unity encrypts the WAV file before submitting the message to Exchange. When a recipient attempts to listen to the message, Cisco Unity attempts to decrypt it by using session keys that are stored in the message and encryption keys that are stored on the server. If the attempt fails, the recipient hears an error message explaining that the message cannot be decrypted. If the certificate has expired due to message aging, the recipient is informed that the message has expired.

Subscribers can play and send secure messages by using the phone interface, the Cisco Unity Inbox, or Cisco Unity ViewMail for Microsoft Outlook as long as the interfaces can authenticate the subscriber with the Cisco Unity server. When subscribers view a secure message by using Microsoft Outlook or any other SMTP e-mail client, the following text message is displayed along with the message:

“This message and any files transmitted with it are intended solely for the individual or entity to which they are addressed. If you received this message in error, delete it immediately and notify the sender.”

Cisco Unity plays the following decoy message when anyone attempts to play a secure message by using media player software other than the Cisco Unity Inbox or ViewMail:

“This voice message is secure and can be played only by using a Cisco Unity supported client. If you received this message in error, delete it immediately and notify the sender.”

When forwarding secure messages, the original message always remains encrypted. The introduction, if any, may be encrypted based on the security settings of the subscriber who forwarded the message. If message aging is enabled, the original secure message keeps its original expiration time and any introductions are aged, based on the date that the message was forwarded. Depending on your aging interval and when the message was forwarded, it is possible that the original message has expired and cannot be played, but the introduction can be. If this condition occurs and the subscriber is listening to messages by phone, the subscriber will hear a prompt saying that some portions of the message have expired. The subscriber can then listen to the unexpired portions. If this condition occurs and the subscriber is using the Cisco Unity Inbox or ViewMail for Outlook, an error message will explain that some parts of the message have expired and that only the portions of the message that have not expired can be played.

Automatic Message Aging for Secure Messaging

Message aging can be enabled for secure messages. After a specified period of time, the certificate used to encrypt a message will expire and Cisco Unity will no longer be able to decrypt the message. Message aging applies to all encrypted messages regardless of whether the message recipient has listened to the message.

When message aging is enabled, a new security certificate is created each day, and certificates that are older than the message expiration period are deleted. This prevents any messages that were encrypted by using the older certificates from being decrypted, and thus renders the messages inaccessible.

Expired secure messages remain in the recipient mailbox. If the recipient attempts to play an expired message, the recipient is informed that the message has expired and cannot be played.

Message aging of secure messages works in tandem with the Message Store Manager utility, by making secure messages that are older than the configured time period inaccessible until such time as the Message Store Manager and Exchange can delete them. For more information, see the “Message Store Manager Utility” section in the “Configuring Cisco Unity for Maintenance Tasks” chapter of the *Maintenance Guide for Cisco Unity*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

When messages expire, they expire at 12:00 a.m. coordinated universal time (UTC). We recommend that you set the time frame to 30 days or more. A short expiration period could result in undesired behavior. For example, if message aging is configured for a time frame of one day, and an encrypted message is recorded at 11:50 p.m. UTC, the recipient of that message has only ten minutes to listen to it before Cisco Unity will no longer be able to decrypt the message.

Secure Messaging with Networking Features in Cisco Unity

If you are using networking features in Cisco Unity, VPIM and Bridge locations can be configured to encrypt incoming messages before they are delivered to the recipients. The locations can be configured to encrypt:

- All incoming messages; or
- Only messages that are flagged as private

By default, VPIM and Bridge locations are configured not to encrypt incoming messages.

In addition, VPIM, Bridge, AMIS, and Trusted Internet locations can be configured to decrypt outgoing secure messages. The locations can be configured to decrypt:

- All outgoing secure messages; or
- Only secure messages that are flagged as private

By default, all locations are configured not to decrypt outgoing secure messages, in which case all secure messages that are sent to the location are undeliverable and will generate an NDR to the sender. Similarly, if a location is configured to decrypt only secure messages that are flagged as private, non-private secure messages that are sent to the location will generate an NDR to the sender.

Secure messages to Internet subscribers are sent directly by the Exchange server and cannot be decrypted and therefore cannot be played by the recipient. If you want to use secure messaging and also be able to send messages to Internet subscribers, configure trusted Internet subscribers instead. Trusted Internet subscribers are Internet subscribers that are trusted with decrypted secure messages. Trusted Internet subscribers must be associated with a Trusted Internet location. Based on the security settings of the Trusted Internet location, secure messages to Trusted Internet subscribers are decrypted by the Cisco Unity Voice Connector for Microsoft Exchange before they are sent by the Exchange server.

Backward Compatibility with Cisco Unity 4.x Servers

In Cisco Unity version 5.x, improvements were made to the encryption and decryption of secure messages. Messages encrypted by using the new format cannot be played on earlier versions of Cisco Unity. To address this issue, Cisco Unity version 5.x encrypts messages by using both the old and new formats, thus allowing secure messages to be played on both a Cisco Unity version 5.x or version 4.x server.

If a subscriber is using Cisco Unity version 4.x, secure messages can only be recorded and played by using the phone interface. If a subscriber is using Cisco Unity 5.x, secure messages that are sent from either a Cisco Unity version 4.x or Cisco Unity 5.x server can be played from within ViewMail for Outlook, the Cisco Unity Inbox, or by phone.

When all of the Cisco Unity servers in your Active Directory (AD) forest are installed with Cisco Unity version 5.x or later, you can disable the backward compatibility with Cisco Unity version 4.x servers. See the [“Disabling Backward Compatibility with Cisco Unity 4.x Servers”](#) section on page 11-13.

Limitations of Secure Messaging

Consider the following limitations of the secure messaging feature, and make sure that subscribers, administrators, and support desk personnel are aware of them.

- Broadcast messages are not encrypted.

- If your subscribers use Cisco Unity ViewMail for Microsoft Outlook and you are using Secure Messaging, you must use ViewMail for Outlook version 5.0(1) or later. Earlier versions of ViewMail will not encrypt messages and subscribers could unknowingly send unsecured messages. Before deploying ViewMail for Outlook version 5.0(1) or later, you must customize the ViewMail installation program to configure subscriber workstations for secure messaging.
- When a subscriber plays a secure message in the Cisco Unity Inbox or ViewMail for Outlook, the Copy and Copy To options on the Options menu on the Media Master control bar will not be available.
- If a subscriber attempts to play a secure message by using ViewMail for Outlook while using Outlook in an off-line mode—or if ViewMail for Outlook cannot communicate with the Cisco Unity sever for any other reason—the subscriber will be warned that the secure message cannot be decrypted or played at that time.
- If a subscriber attempts to send a secure message by using ViewMail for Outlook while using Outlook in an off-line mode—or if ViewMail for Outlook cannot communicate with the Cisco Unity sever for any other reason—the subscriber may not be able to send unencrypted messages (depending on how you have configured ViewMail for Outlook). See the [“Configuring Cisco Unity ViewMail for Microsoft Outlook for Secure Messaging”](#) section on page 11-10.
- Subscribers who use an IMAP4 compatible e-mail client to access their voice messages will not be able to play secure messages from the e-mail client unless they are using Microsoft Outlook and they have installed ViewMail for Outlook.
- Recipients who are associated with servers outside of the Active Directory forest cannot listen to a secure message, because the key required to decrypt the message is not available.
- The private keys that are required to decrypt secure messages are not specific to individual subscribers or workstations. Thus, if a secure message is sent to an unintended recipient—perhaps because of an addressing mistake made by the sender or due to a system problem—Cisco Unity will play the message for any recipient who receives the message as long as the recipient is authenticated with a Cisco Unity server or is a valid recipient on a networked voice mail system.
- If a subscriber is out of the office and not listening to messages for a period of time that is longer than the message aging period, then some messages will have expired before the subscriber has an opportunity to listen to them.
- If your deployment uses integrated messaging —where voice messages and e-mail are stored in separate mail stores, but subscribers use the IMAP protocol to view their voice messages in the same Outlook profile as their e-mail—encrypted voice messages that are sent or forwarded from Outlook must be sent to voice mail addresses. If encrypted voice messages are sent to e-mail addresses, they will become e-mails with WAV file attachments rather than native Cisco Unity voice messages, and the recipient will hear the decoy WAV file. To avoid this issue, you can add an LDAP address book with voice mail addresses to be used with the IMAP account for sending or forwarding voice messages.
- If subscribers configure the e-mail program to download voice messages off of the e-mail server by using POP3 or another protocol, they will not be able to listen to encrypted voice messages. They must configure their e-mail program to leave copies of the voice messages on the server so that they can play secure messages by using an alternative interface such as the phone interface or Cisco Unity Inbox.
- Secure messages that are sent to AMIS, Bridge, VPIM, or Trusted Internet subscribers are either decrypted by the Voice Connector before being sent, or are undeliverable and will generate an NDR to the sender. See the [“Configuring Cisco Unity Bridge, AMIS, VPIM, or Trusted Internet Delivery Locations for Secure Messaging”](#) section on page 11-8 for details.

- When Cisco Unity is configured for networking with other voice mail systems by using either the Cisco Unity Bridge or VPIM, messages that are sent from users on the other voice mail system to Cisco Unity subscribers can be encrypted, but only at the point at which they reach the Voice Connector, if the delivery location is configured for this functionality. See the [“Configuring Cisco Unity Bridge, AMIS, VPIM, or Trusted Internet Delivery Locations for Secure Messaging”](#) section on page 11-8 for details.
- When Cisco Unity is configured for networking with other voice mail systems by using the AMIS protocol, messages that are sent from users on the other voice mail system to Cisco Unity subscribers cannot be encrypted and therefore are not affected by the message aging functionality of Secure Messaging.
- Subscribers cannot use blind addressing to send messages to users at Trusted Internet locations.
- If Cisco Unity is unable to encrypt messages, the unencrypted message will be sent to the Unaddressed Messages distribution list with information about who the message is from and who it was addressed to.

Installing and Configuring Secure Messaging

During installation or upgrade, a secure messaging certificate is installed automatically on each Cisco Unity server and on any Exchange server on which the Voice Connector is installed, if applicable.

Secure Messaging is disabled by default. The following task list leads you through configuring and enabling the secure messaging feature. Do the procedures in the following sections, as applicable. If a section or procedure does not apply to your situation, skip it.

1. If you are configuring secure messaging on a Cisco Unity system that has been upgraded from Cisco Unity version 4.0(4)SR1 or earlier, enable MAPI Rich Text Format for all subscribers who are listed as contacts in Active Directory. See the [“Enabling MAPI Rich Text Format for All Contacts in the Active Directory”](#) section on page 11-7.
2. Enable secure messaging for messages from unidentified callers. See the [“Enabling Secure Messaging for Messages from Unidentified Callers”](#) section on page 11-7.
3. If you want secure messages to automatically expire after a specified period of time, enable message aging for secure messages. See the [“Enabling Message Aging for Secure Messages”](#) section on page 11-8.
4. If you are using networking features in Cisco Unity and want the secure messaging functionality available for messages to and from remote subscribers:
 - a. Set up outgoing and incoming secure message handling for each delivery location. See the [“Configuring Cisco Unity Bridge, AMIS, VPIM, or Trusted Internet Delivery Locations for Secure Messaging”](#) section on page 11-8.
 - b. If the Cisco Unity Voice Connector for Microsoft Exchange is not installed on the Cisco Unity server, you must install the Secure Messaging Service on the Voice Connector server. See the [“Installing the Cisco Unity Secure Messaging Service on the Voice Connector Server”](#) section on page 11-9.
 - c. If you have configured message aging on the Voice Connector server and want to either disable or change the time period for message aging, see the [“Disabling or Changing the Time Period for Message Aging on the Voice Connector Server”](#) section on page 11-10.
5. If your subscribers use ViewMail for Outlook, you must alter the installation files for ViewMail for Outlook before deploying it on client workstations. See the [“Configuring Cisco Unity ViewMail for Microsoft Outlook for Secure Messaging”](#) section on page 11-10.

6. Optionally, if your subscribers use ViewMail for Outlook, you can change the TCP port that ViewMail for Outlook uses to connect to the Cisco Unity server for encrypting and decrypting secure messages. See the [“Customizing the TCP Port That ViewMail for Outlook Uses For Encrypting and Decrypting Messages”](#) section on page 11-12.
7. Enable secure messaging for individual subscribers or all subscribers. See the [“Enabling Secure Messaging for Messages From Subscribers”](#) section on page 11-14.
8. If you do not have multiple Cisco Unity servers networked together or if all of your Cisco Unity servers have been upgraded to Cisco Unity 5.x, disable backward compatibility with Cisco Unity 4.x servers. See the [“Disabling Backward Compatibility with Cisco Unity 4.x Servers”](#) section on page 11-13.

Enabling MAPI Rich Text Format for All Contacts in the Active Directory

If you are installing secure messaging on an existing Cisco Unity system that has been upgraded from Cisco Unity version 4.0(4)SR1 or earlier to Cisco Unity version 5.x, do the following procedure to enable MAPI Rich Text Format for all subscribers who are listed as contacts in Active Directory. Otherwise, skip to the [“Enabling Secure Messaging for Messages from Unidentified Callers”](#) section on page 11-7.

Depending on the number of contact records to be updated, the Active Directory synchronization process can take several hours or more to complete. The synchronization process may also use a considerable percentage of available computer and network resources. Therefore, we recommend that you run the Enable Rich Text Format utility at a time when demand on Cisco Unity system resources is low, for example, on a weekend evening.

To Enable MAPI Rich Text Format

- Step 1** Log on to the Cisco Unity server by using an account that is a member of the Domain Admins group.
 - Step 2** On the Cisco Unity server, double-click the **Cisco Unity Tools Depot** icon.
 - Step 3** In the left pane, under Administration Tools, double-click **EnableRichTextFormat**. The Enable Rich Text Format window appears and displays all Contact records that do not have MAPI Rich Text Format enabled.
 - Step 4** Click **Process Contacts**. A status bar shows the progress of the Active Directory update.
 - Step 5** When the Active Directory update is complete, click **OK**.
 - Step 6** If desired, click **Save Report** to view and save a record of the updates that were made to the Active Directory.
 - Step 7** Click **Exit**.
-

Enabling Secure Messaging for Messages from Unidentified Callers

To Enable Secure Messaging for Messages from Unidentified Callers

- Step 1** In the Cisco Unity Administrator, go to the **System > Configuration > Message Security Settings** page.
- Step 2** Indicate whether messages from unidentified callers are encrypted:
 - **Do Not Encrypt Messages**—Messages are not encrypted.

- **Encrypt All Messages**—All messages are encrypted.
-

Enabling Message Aging for Secure Messages

To Enable Message Aging for Secure Messages

- Step 1** In the Cisco Unity Administrator, go to the **System > Configuration > Message Security Settings** page.
- Step 2** Check the **Enable** check box to enable message aging for secure messages.
- Step 3** In the Days Before Encrypted Messages Become Unavailable field, enter a time frame that is consistent with the message retention policy of your organization.
- Step 4** Repeat [Step 1](#) through [Step 3](#) on all Cisco Unity servers in your organization.



Note If you are using networking features in Cisco Unity, you must also configure message aging when installing the Secure Messaging Service on the Voice Connector server. See the [“Installing the Cisco Unity Secure Messaging Service on the Voice Connector Server”](#) section on page 11-9.

Configuring Cisco Unity Bridge, AMIS, VPIM, or Trusted Internet Delivery Locations for Secure Messaging

If you are using networking features in Cisco Unity and want secure messaging to be available for messages to and from remote subscribers, you need to configure how outgoing secure and incoming voice messages will be handled for each delivery location.

To Configure Bridge or VPIM Delivery Locations to Encrypt Incoming Messages

- Step 1** In the Cisco Unity Administrator, go to the **Delivery Locations** page for each VPIM or Bridge location in your system.
- Step 2** In the Incoming Messages From This Location field, select the applicable option:
- **Do Not Encrypt Messages**—The Voice Connector will not encrypt any messages.
 - **Encrypt Only Private Messages**—The Voice Connector will encrypt only messages that are flagged private.
 - **Encrypt All Messages**—The Voice Connector will encrypt all messages.
-

To Configure Bridge, VPIM, AMIS, or Trusted Internet Delivery Locations to Decrypt Outgoing Messages

- Step 1** In the Cisco Unity Administrator, go to the **Delivery Locations** page for each location in your system.
- Step 2** In the Outgoing Messages to This Location field, select the applicable option:
- **Do Not Decrypt Messages**—The Voice Connector will not decrypt or send secure messages, and will send an NDR back to the sender.

- **Decrypt Non-Private Messages**—The Voice Connector will not decrypt or send secure messages that are flagged private. An NDR will be sent back to the sender. All other messages will be decrypted before sending them to the remote location.
- **Decrypt All Messages**—The Voice Connector will decrypt all secure messages before sending them to the remote location. Depending on the configuration at the remote location, the message may or may not be re-encrypted before being delivered to the recipient.

Installing the Cisco Unity Secure Messaging Service on the Voice Connector Server

If the Cisco Unity Voice Connector for Microsoft Exchange is not installed on the Cisco Unity server, you must install the Cisco Unity Secure Messaging Service on the Exchange server on which the Voice Connector is installed. The Secure Messaging Service is included as an optional part of the Voice Connector setup program.



Note

The following procedure is for installing the Secure Messaging Service that is included with Voice Connector version 12.0(1), which shipped with Cisco Unity 5.0(1). We recommend that you first check for a later version of the Voice Connector, and that you install that version instead. Follow the installation instructions in the release notes for the applicable version. To check for a later version, go to the Cisco Unity Voice Connector for Microsoft Exchange Software Download page at <http://www.cisco.com/cgi-bin/tablebuild.pl/unity-voice-connector>.

To Install the Secure Messaging Service on the Voice Connector Server

- Step 1** Log on to the Exchange server on which you are installing the Voice Connector and Secure Messaging Service.
- Step 2** Disable any virus-scanning services on the Exchange server.
- Step 3** If you are installing the Voice Connector from a Cisco Unity DVD or CD, insert the disc in the computer, and browse to the **VoiceConnector-Ex2000** directory.
If you downloaded the Voice Connector files from the Software Center website, browse to the directory in which the files were extracted.
- Step 4** Double-click **Install.exe**, and click **Next**.
- Step 5** On the Voice Connector Setup Wizard Select Components dialog box, check the **Voice Connector for Exchange** check box. (If the Voice Connector is already installed, the check box will be checked and grayed out.)
- Step 6** Check the **Cisco Secure Messaging Service** check box. (If the Cisco Secure Messaging Service is already installed, the check box will be checked and grayed out and you can skip the rest of this procedure.)
- Step 7** Click **Next**.
- Step 8** On the Welcome screen, click **Next**.
- Step 9** On the Confirm SMTP Pickup Directory screen, click **Next**.
- Step 10** In the Address Types dialog, check the check boxes appropriate to your networking options.
- Step 11** If you are setting up Trusted Internet Subscribers, check the **Trusted Internet Location** check box.
- Step 12** Click **Next**.

- Step 13** On the Confirm Directory dialog box, click **Next** to launch the setup.
- Step 14** Do the following steps in the Cisco Unity Secure Messaging Service Setup wizard:
- a. On the Welcome screen, click **Next**.
 - b. On the Choose Destination Folder dialog, specify the destination, and click **Next**.
 - c. Optionally, on the Message Security Settings screen, check the **Enable Message Aging** check box, and enter the number of days that encrypted messages should be available. (If the check box is not checked, Cisco Unity will not limit the number of days for which encrypted messages will be available.)
- Step 15** Click **Next**.
- Step 16** On the Ready to Install Software screen, click **Install**.
- Step 17** When the setup is complete, click **Finish** to exit Setup and restart the server.
-

Disabling or Changing the Time Period for Message Aging on the Voice Connector Server

To Disable or Change the Time Period for Message Aging on the Voice Connector Server

- Step 1** Log on to the Exchange server on which the Voice Connector and Cisco Secure Messaging Service is installed.
- Step 2** Open **Control Panel > Add or Remove Programs**.
- Step 3** Click **Cisco Unity Voice Gateway Secure Message Setup Wizard**.
- Step 4** Click **Change**. The Cisco Unity Secure Messaging Service Setup wizard launches.
- Step 5** Click **Modify**, and then click **Next**.
- Step 6** On the Message Security Settings page, enable or disable message aging, and specify the number of days, as applicable.
- Step 7** Click **Next**, and then click **Finish**.
- Step 8** Close **Add or Remove Programs**.
-

Configuring Cisco Unity ViewMail for Microsoft Outlook for Secure Messaging

Because the encryption certificates and keys are stored on the Cisco Unity server, Cisco Unity ViewMail for Microsoft Outlook can play and send secure messages only when a connection can be made to the Cisco Unity server. ViewMail installs the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\Cisco Unity\VMO\Force Messages Secure on the subscriber workstations. If a subscriber attempts to send a secure message by using ViewMail while using Outlook in an off-line mode—or if ViewMail for Outlook cannot communicate with the Cisco Unity sever for any other reason, ViewMail will do one of the following, depending on the value of the registry key:

- 0—Send the message without encrypting it and without attempting to connect to the Cisco Unity server.
- 1—Warn the subscriber that a connection with Cisco Unity could not be made. (The subscriber will have to save the message and resend it at a later time.)

- 2—Warn the subscriber that the message will not be encrypted and offer the option to send it without encryption.

The registry key is set to zero by default—to send messages unencrypted without attempting to connect to the Cisco Unity server. If you want to send encrypted messages from ViewMail, administrators must customize the ViewMail.msi file to change the value of the registry key before installing ViewMail for Outlook on subscriber workstations.

Note that once ViewMail version 5.0(1) or later is installed on a subscriber workstation, the registry setting cannot be changed by running the ViewMail installation program again. Administrators must use a configuration management tool (for example, Microsoft Systems Management Server) to change the registry setting, or must uninstall ViewMail, customize the ViewMail.msi file to change the setting, and install ViewMail again.

To Customize the ViewMail.msi File to Change the “Force Messages Secure” Registry Key

-
- Step 1** Browse to the ViewMail directory on the network drive to which you downloaded the ViewMail files. If you do not have permission to write to the directory, move the files to a directory on which you have write privileges.
- Step 2** In the ViewMail directory, browse to the **ENU** language directory (or to the language applicable to your installation).
- Step 3** Open **VMOInit.vbs** in a text editor.
- Step 4** Delete the **rem** text in front of the **Session.Property("ForceMessagesSecure") = "1"** line.

For example:

```
Function VMOInitFn()
rem Session.Property("EXTENSION") = ""
rem Session.Property("UNITYSERVER") = ""
rem To enable NoTextToVM, set property NOTEXTTOVM to 1
rem Session.Property("NOTEXTTOVM") = "1"
rem To enable g729a recording, set property DefaultWaveFormat to 5
rem Session.Property("DefaultWaveFormat") = "5"
rem To enable secure messaging, set property ForceMessagesSecure to 1 (Always Force
Messages Secure) or 2 (Allow User To Choose).
rem By default, it is set to 0 (Always Send Messages Unsecure).
Session.Property("ForceMessagesSecure") = "1"
rem To change RPC Port Number for Encryption and Decryption, set property
RpcPortNumberForEncryptionAndDecryption to a new port number.
rem By default, it is set to 5050.
rem Session.Property("RpcPortNumberForEncryptionAndDecryption") = "5050"
End Function
```

- Step 5** If you want subscribers to be able to choose to send unencrypted messages when ViewMail for Outlook is in an offline mode, change the “1” to “2”.
- Step 6** Save the script file and close the text editor.
- Step 7** Open a Command Prompt window. (On the Windows Start menu, click **Programs > Accessories > Command Prompt**.)
- Step 8** Change to the **ViewMail > ENU** directory (or to the language applicable to your installation).
- Step 9** Enter **vmaddbin ViewMail.msi VMOInit.vbs**, and press **Enter**. When the script completes, your cursor returns to the command line.
- Step 10** Run the file **ViewMail.msi** on a test machine to confirm that the installation completes successfully.

Step 11 Close the Command Prompt window.

Customizing the TCP Port That ViewMail for Outlook Uses For Encrypting and Decrypting Messages

By default, Cisco Unity uses TCP port number 5050 for incoming RPC connection requests from ViewMail for Outlook clients to encrypt and decrypt secure messages. In most cases, the default configuration is fine. However, you may want to change the port to configure for a firewall; any available TCP port can be used. If you need to change the port that is used, you must make the change on both the Cisco Unity server and on the ViewMail client workstations. Do the following procedures:

- [To Change the TCP Port for RPC Connections on the Cisco Unity Server](#)
- [To Customize the ViewMail.msi File to Change the TCP Port on the Subscriber Workstations](#)

ViewMail installs a registry key HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\Cisco Unity\VMO\RPC Port Number for Encryption and Decryption on the subscriber workstations.

Note that when ViewMail version 5.0(1) or later is installed on a subscriber workstation, the registry setting cannot be changed by running the ViewMail installation program again. Administrators must use a configuration management tool (for example, Microsoft Systems Management Server) to change the registry setting, or must uninstall ViewMail, customize the ViewMail.msi file to change the setting, and install ViewMail again.

To Change the TCP Port for RPC Connections on the Cisco Unity Server

- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.
- Step 3** In the Unity Settings pane, click **Security – Configure TCP Port Number for Incoming RPC Connections for Encryption/Decryption**.
- Step 4** In the New Value list, enter the TCP port number and click **Set**.
- Step 5** When prompted, click **OK**.
- Step 6** Click **Exit**.
- Step 7** Stop and restart the AvMMPoxySvr service.
-

To Customize the ViewMail.msi File to Change the TCP Port on the Subscriber Workstations

- Step 1** Browse to the ViewMail directory on the network drive on which you downloaded the ViewMail files. If you do not have permission to write to the directory, move the files to a directory on which you have write privileges.
- Step 2** In the ViewMail directory, browse to the **ENU** language directory (or to the language applicable to your installation).
- Step 3** Open the file **VMOInit.vbs** in a text editor.
- Step 4** Delete the **rem** text in front of the **Session.Property ("RpcPortNumberForEncryptionAndDecryption") = "5050"** line.

For example:

```

Function VMOInitFn()
rem Session.Property("EXTENSION") = ""
rem Session.Property("UNITYSERVER") = ""
rem To enable NoTextToVM, set property NOTEXTTOVM to 1
rem Session.Property("NOTEXTTOVM") = "1"
rem To enable g729a recording, set property DefaultWaveFormat to 5
rem Session.Property("DefaultWaveFormat") = "5"
rem To enable secure messaging, set property ForceMessagesSecure to 1 (Always Force
Messages Secure) or 2 (Allow User To Choose).
rem By default, it is set to 0 (Always Send Messages Unsecure).
rem Session.Property("ForceMessagesSecure") = "1"
rem To change RPC Port Number for Encryption and Decryption, set property
RpcPortNumberForEncryptionAndDecryption to a new port number.
rem By default, it is set to 5050.
Session.Property("RpcPortNumberForEncryptionAndDecryption") = "5050"
End Function

```

- Step 5** Change the “5050” part of the line to the TCP port number that you entered on your Cisco Unity server(s) in [Step 4](#) of the “[To Change the TCP Port for RPC Connections on the Cisco Unity Server](#)” procedure on page 11-12.
- Step 6** Save the script file and close the text editor.
- Step 7** Open a Command Prompt window. (On the Windows Start menu, click **Programs > Accessories > Command Prompt**.)
- Step 8** Change to the **ViewMail > ENU** directory (or to the language applicable to your installation).
- Step 9** Enter **vmaddbin ViewMail.msi VMOInit.vbs**, and press **Enter**. When the script completes, your cursor returns to the command line.
- Step 10** Run the file **ViewMail.msi** on a test machine to confirm that the installation completes successfully.
- Step 11** Close the Command Prompt window.

Disabling Backward Compatibility with Cisco Unity 4.x Servers

If all of the Cisco Unity servers in your Active Directory forest are installed with Cisco Unity version 5.0(1) or later, you can disable the backward compatibility with Cisco Unity version 4.x servers. There is a small CPU overhead when using secure messaging with backward compatibility enabled, so if you do not need it, you should disable it.

To Disable Backward Compatibility with Cisco Unity 4.x Servers

Note that you must change the setting on each Cisco Unity server in the AD forest. The change does not automatically replicate to other Cisco Unity servers.

- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.
- Step 3** In the Unity Settings pane, click **Security – Configure Recording Format for Backward Compatibility with Cisco Unity 4.x Servers**.
- Step 4** In the New Value list, click **1**, and then click **Set**.
- Step 5** When prompted, click **OK**.

You do not need to restart Cisco Unity to enable the registry changes.

Step 6 Click **Exit**.

If you are using networking features with Cisco Unity and the Cisco Unity Voice Connector for Microsoft Exchange is not installed on the Cisco Unity server, you must also disable backward compatibility with Cisco Unity 4.x on the Exchange server on which the Voice Connector is installed.

To Disable Cisco Unity 4.x Backward Compatibility on the Voice Connector Server

Step 1 On the Exchange server on which the Voice Connector is installed, on the Windows Start menu, click **Run**.

Step 2 In the Open field, enter **Regedit** and press **Enter**. The Registry Editor appears.



Caution Changing the wrong registry key or entering an incorrect value can cause the server to malfunction. Before you edit the registry, confirm that you know how to restore it if a problem occurs. (See the “Restoring” topics in Registry Editor Help.) If you have any questions about changing registry key settings, contact Cisco TAC.

Step 3 If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.

Step 4 Go to HKEY_LOCAL_MACHINE\SOFTWARE\Active Voice\AvIvc.

Step 5 Double-click the SecureMsgInterOpMode value. The Edit DWORD Value dialog box appears.

Step 6 In the Value Data field, enter **0** and click **OK**.

Step 7 Close **Regedit**.

Enabling Secure Messaging for Messages From Subscribers

In order to allow subscribers to send secure messages, you must enable it for them.



Note All subscribers are able to receive and listen to secure messages after you complete the installation and basic configuration, as instructed in the previous sections. You must enable secure messaging for subscribers in order for them to also be able to send secure messages.

You enable secure messaging for individual existing subscribers on the Subscribers > Subscribers > Features page. You can also enable secure messaging for future new subscribers by changing a setting on the Subscribers > Subscriber Templates > Features page. Do the following “[To Enable Secure Messaging for Subscribers](#)” procedure.

Enabling secure messaging only for certain subscribers may make system administration, troubleshooting, and training more labor-intensive than when the feature is enabled for all subscribers.

To enable secure messaging for multiple (or all) existing subscribers, use the Bulk Edit utility, available in Tools Depot.

To Enable Secure Messaging for Subscribers

- Step 1** In the Cisco Unity Administrator, go to the applicable page:
- **Subscribers > Subscribers > Features** for an individual subscriber.
 - **Subscribers > Subscriber Templates > Features** to make the change on a subscriber template (note that the change you make here will not be applied to currently existing subscriber accounts that were created by using this template; the setting applies only to subscriber accounts that are created by using this template after the change has been made).
- Step 2** Indicate whether messages will be encrypted when subscribers send messages to other subscribers:
- **Do Not Encrypt Messages**—Messages are not encrypted.
 - **Encrypt Only Private Messages**—Only messages that are flagged private are encrypted.
 - **Encrypt All Messages**—All messages are encrypted.
- Step 3** Click the **Save** icon.
- Step 4** Repeat [Step 1](#) through [Step 3](#) for additional subscribers or subscriber templates, as applicable.
-

Maintenance Considerations When Secure Messaging Is in Use

Incorporate the information from the following sections into your Cisco Unity system maintenance plan:

- [Monitoring the Unaddressed Messages Distribution List for Messages with Encryption Errors](#), page 11-15
- [Performance Monitoring When Using Secure Messaging](#), page 11-15
- [Limiting Access to the Cisco Unity Server](#), page 11-16
- [Backing Up and Restoring Public and Private Keys](#), page 11-16

Monitoring the Unaddressed Messages Distribution List for Messages with Encryption Errors

If Cisco Unity is unable to encrypt a message from subscribers, unidentified callers or an incoming message from Bridge or VPIM locations, the unencrypted message will be sent to the Unaddressed Messages distribution list with information—text in the body of the message—about who the message was from (if available) and who the message was addressed to. To route these messages properly, ensure that the Unaddressed Messages distribution list has at least one member who will monitor the mailbox and handle messages that could not be encrypted.

Performance Monitoring When Using Secure Messaging

Enabling secure messaging for all subscribers should not adversely affect Cisco Unity performance. However, if a Cisco Unity performance problem occurs when subscribers are using secure messaging, include the following performance counters in the performance testing and analysis:

- AvCSMgr Private MBytes
- AvCSMgr Virtual MBytes
- AvCSMgr % Processor Time
- Total % Processor Time

- Current Incoming Calls - Avg
- Current Incoming Calls - Max

For more information on collecting and analyzing Cisco Unity performance data, see the “Performance Monitoring” chapter of the *Maintenance Guide for Cisco Unity*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Limiting Access to the Cisco Unity Server

Sites need to protect their private keys from unauthorized internal or external access. Anyone who can log on to the Cisco Unity server as a user in the local administrator group can copy the private keys, and install them on any other server. Note that secure messaging public and private keys should be present only on the Cisco Unity servers and on the Exchange servers on which the Voice Connector is installed. The keys are never created on subscriber workstations, and should never be copied to another server or workstation.

Backing Up and Restoring Public and Private Keys

Exportable certificates are installed on a Cisco Unity server and the public and private keys that are created from these certificates can be backed up and restored by using the Cisco Unity Disaster Recovery tool (DiRT).

For more information on backing up Cisco Unity data, see the “About Backing Up a Cisco Unity System” chapter of the *Maintenance Guide for Cisco Unity*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Secure Messaging and Legal Discoverability

Companies and other entities involved in federal litigation may need to produce electronically stored information as part of the discovery process when evidence is shared by both sides before a trial. Your lawyers may request that you produce copies of the existing and all future voice messages for one or more subscribers. They may also request the date and timestamp of each message and its subject, which contains either the sender name or caller ID.

The following task list provides an overview for responding to requests for legal discoverability:

1. Run a report from within Exchange to identify the list of voice messages by subject, date, and time stamp.
2. Create a trusted Internet subscriber account that has the destination e-mail address of the mailbox that will be used to collect these messages. We recommend that you create a trusted Internet subscriber for each subscriber whose records are being requested. These trusted Internet subscriber accounts must be associated with a trusted Internet location that will decrypt outgoing secure messages.
3. Configure an Exchange forwarding rule to forward all of the applicable subscriber messages to the associated trusted Internet subscriber accounts.

**Note**

It is not possible to create a rule that will selectively forward only voice messages. However, when the Cisco Unity Voice Connector for Microsoft Exchange processes the messages to forward to the trusted Internet subscriber account, it will not forward e-mail messages, but will generate a non-delivery receipt (NDR) back to the Cisco Unity account of the subscriber. (This is a consideration only if your Cisco Unity is configured for Unified Messaging.)

4. Depending on the number of subscriber mailboxes and messages, you may want to consider installing and configuring a Voice Connector on a dedicated Exchange server just for processing these decryption requests.
5. Your lawyers can use the report created in task 1 to manually match up each decrypted message to determine the date and time stamp of the original voice message.
6. Turn off secure messaging for the subscriber so that future voice messages are no longer encrypted.
7. Modify the Exchange server forwarding rule to point to the mailbox that is collecting messages instead of the trusted Internet subscriber, thus bypassing the Voice Connector. Because the messages are no longer encrypted, they do not need to be decrypted.

Technical Details of Secure Messaging

Messages are secured by using public/private key encryption. When using digital networking, each Cisco Unity server in the organization generates its own public/private key pairs, and it publishes the public keys to the other Cisco Unity servers through Active Directory. When a secure message is recorded, a new session key is created for the message. The session key is used to encrypt the audio data, and this encrypted audio data is stored in the message. The public key from each Cisco Unity server is used to encrypt the session key, generating a list of encrypted session keys. This list of encrypted session keys is stored in the message.

When a secure message is played, the Cisco Unity server extracts the list of encrypted session keys and tries to decrypt one of the encrypted session keys by using its private key. If it is able to decrypt the session key by using its private key, the Cisco Unity server will then decrypt the audio data with that session key. If it is unable to decrypt the session key, the Cisco Unity server gives the subscriber the appropriate response, either that the message is expired or that it is not decryptable due to an error condition. The Cisco Unity server can differentiate between a message that has expired and a message that cannot be decrypted due to an error condition, and will give the appropriate response.

If message aging is enabled, each Cisco Unity server creates a new public/private key pair once a day at midnight UTC, and publishes the new public key to the other Cisco Unity servers via Active Directory. At the same time, Cisco Unity deletes the oldest private key from the operating system key store. This deletion of the private key is what causes a message to expire as soon as it is older than the configured message aging period. When the Cisco Unity server deletes the private key that corresponds to the public key that encrypted the session key, the session key cannot be decrypted, which thereby prevents decryption and play back of the audio data.

If subscribers are using ViewMail for Outlook or the Cisco Unity Inbox to record and play back secure messages, both the client PC and Cisco Unity server are involved in the operation. When a secure message is recorded on a client, the client PC generates the session key and encrypts the audio data. It then uses an encrypted channel to ask the Cisco Unity server to encrypt the session key. When that is complete, the client PC stores the list of encrypted session keys in the message and submits it to Microsoft Exchange. When a secure message is played back on a client, the client PC extracts the list of encrypted session keys from the message and uses an encrypted channel to ask the Cisco Unity server to

decrypt the session key. If that succeeds, the client PC uses it to decrypt the audio data and play it back. If it fails, the client PC will inform the subscriber that the message has expired or is not decryptable due to an error condition, as appropriate.

Best Practices for Using Text to Speech (Unified Messaging)

The Text to Speech (TTS) feature allows Unified Messaging subscribers to listen to their e-mail messages over the phone. Cisco Unity reads the text portion of e-mail messages and provides additional information such as the name of the sender (if the sender is a subscriber), and the time and date that the message was sent. No attachments are read over the phone.

TTS is a class of service offering. Before you enable subscribers to use TTS, consider the following best practices:

Best Practice: Use Enhanced Phone Security

Because a phone password is inherently less secure than a password that subscribers would typically use to log on to a workstation and/or their e-mail inboxes, offering TTS to subscribers can be considered a security risk. To provide a more secure way to authenticate subscribers when they access Cisco Unity by phone, and thereby increase the security of all subscriber messages, set up enhanced phone security. (See the [“Determining Whether to Offer Enhanced Phone Security”](#) section on page 8-12.)

Best Practice: Do Not Offer TTS If E-Mail Content Is Sensitive

Offering TTS can also be considered a security risk because subscribers can access Cisco Unity from any phone—inside or outside your organization. If the e-mail content in your organization contains classified information that you do not want played over unsecured connections, do not offer TTS to subscribers.

Disabling the Copy to File Option in the Media Master for the Cisco Unity Inbox

By default, subscribers can save their messages, except for secure messages and private messages, as WAV files on their hard disks by using the Copy to File option available on the Options menu on the Media Master control bar in the Cisco Unity Inbox. As an added security measure for Cisco Unity, you can disable the Copy to File option so that subscribers cannot save any message—regardless of its sensitivity—on their hard disks.

You can specify whether the Copy to File option is available in the Cisco Unity Inbox by using the Advanced Settings tool to change the registry. The registry change is applied system-wide to all subscribers who are associated with the Cisco Unity server. You cannot make the change for an individual subscriber or for a specific group of subscribers. Consider that when you prevent subscribers from archiving messages, they may choose to retain messages in their Inboxes and Deleted Items folders (if applicable) longer.



Note

For Cisco Unity failover, registry changes on one Cisco Unity server must be made manually on the other Cisco Unity server, because registry changes are not replicated.

Do the following procedure to disable the Copy to File option in the Media Master for the Cisco Unity Inbox.

To Disable the Copy to File Option in the Media Master for the Cisco Unity Inbox

- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.
- Step 3** In the Unity Settings pane, click **Unity Inbox—Disable Copy to File Option in Media Master**.
- Step 4** In the New Value list, click **1**, and click **Set**.
- Step 5** When prompted, click **OK**.
- Step 6** Click **Exit**.

You do not need to restart the Cisco Unity server for the change to take effect.



INDEX

A

account policy

- account lockout settings for phone access [9-9](#)
- phone password settings [9-8](#)

accounts, defining policy for logons, passwords, and lockouts [9-7](#)

ACE/Server return codes [8-12](#)

administration account

- limiting use of [7-2](#)
- using to log on to the Cisco Unity Administrator [7-2](#)

Anonymous authentication, how it works with the Cisco Unity Administrator [8-4](#)

audit policies, changing [1-2](#)

authentication

- Anonymous [8-4](#)
- best practice [6-4](#)
- Integrated Windows [8-2](#)
- overview [8-2](#)
- PCA passwords [8-10](#)
- settings in Cisco Unity [6-4](#)

C

call signaling, modification threat [6-1](#)

CA root certificate

- adding to Domain Group Policy [10-8](#)
- exporting [10-8](#)

changing

- Cisco PCA passwords [9-6](#)
- Cisco Unity Administrator passwords [9-5](#)
- permissions on files in the CommServer directory [1-3](#)
- phone passwords [9-6](#)

Cisco Certificate Trust List (CTL) file

used for device authentication [6-2](#)

used for signaling authentication [6-2](#)

Cisco PCA

authentication, how it works [8-10](#)

passwords [8-10](#)

passwords, changing [9-6](#)

preventing unauthorized access [8-11](#)

Cisco Security Agent

description [4-1](#)

policies [4-1](#)

Cisco Unified CM

call signaling modification [6-1](#)

device authentication as a security feature [6-2](#)

identity theft [6-2](#)

man-in-the-middle attacks on connection to Cisco Unity [6-1](#)

media (RTP) stream modification [6-1](#)

media encryption as a security feature [6-3](#)

network traffic sniffing (eavesdropping) [6-1](#)

security connection with Cisco Unity [6-1](#)

security issues [6-1](#)

signaling authentication as a security feature [6-2](#)

signaling encryption as a security feature [6-3](#)

Cisco Unity Administrator

accounts used to access [7-2](#)

limiting use of administration account [7-2](#)

passwords, changing [9-5](#)

preventing unauthorized access [8-8](#)

security concerns [7-2](#)

using appropriate accounts [7-3](#)

using class of service to restrict access [7-3](#)

Cisco Unity conversation, preventing unauthorized access [9-5](#)

Cisco Unity Inbox

disabling Copy to File option [11-18](#)

handling private messages [11-1](#)

Cisco Unity server, securing [1-1](#)

configuring

IIS for Integrated Windows authentication [8-5](#)

IIS so Cisco Unity Administrator and Status Monitor use Anonymous authentication [8-7](#)

IIS so Cisco Unity Administrator and Status Monitor use Integrated Windows authentication [8-5](#)

D

defining policies for logon, password, and lockout [9-7](#)

distributing root certificate [10-7](#)

E

eavesdropping Cisco Unified CM connections [6-1](#)

encryption

best practice [6-4](#)

settings in Cisco Unity [6-4](#)

used for media protection [6-3](#)

used for signaling protection [6-3](#)

enhanced phone security

ACE/Server return codes [8-12](#)

Cisco Unity Greetings Administrator, incompatibility [8-13](#)

class of service settings [8-12](#)

setting up [8-13](#)

event log settings, changing [1-3](#)

Exchange, securing [2-5](#)

exporting CA root certificate [10-8](#)

F

file permissions, changing on files in the CommServer directory [1-3](#)

firewall, configuring [3-1](#)

I

identity theft

Cisco Unified CM server [6-2](#)

Cisco Unity voice messaging port [6-1](#)

IIS

configuring for Integrated Windows authentication [8-5](#)

configuring so Cisco Unity Administrator and Status Monitor use Anonymous authentication [8-7](#)

configuring so Cisco Unity Administrator and Status Monitor use Integrated Windows authentication [8-5](#)

Lockdown wizard, hardening the Cisco Unity server with [2-4](#)

securing [2-3](#)

Integrated Windows authentication, how it works with the Cisco Unity Administrator [8-2](#)

Internet Explorer, securing [2-3](#)

IP phones

network traffic sniffing (eavesdropping) [6-1](#)

securing connection with Cisco Unity [6-1](#)

security issues [6-1](#)

L

local security policies, changing [1-2, 1-3](#)

lockouts

policy for accessing Cisco Unity by phone [9-9](#)

policy for Cisco Unity Administrator access [9-7](#)

logon policy [9-7](#)

M

man-in-the-middle attacks for Cisco Unified CM connections [6-1](#)

Media Master, disabling Copy to File [11-18](#)

media stream, modification threat [6-1](#)

Microsoft software, securing [2-1](#)

MSDE 2000, securing [2-2](#)

MSMQ, securing [2-5](#)

N

network traffic sniffing Cisco Unified CM connections [6-1](#)

NTLM authentication [8-2](#)

O

operating system, securing [1-1](#)

P

passwords

policy for accessing Cisco Unity by phone [9-8](#)

policy for Cisco Unity Administrator access [9-7](#)

TUI [9-2](#)

web applications [9-2](#)

permissions, changing on files in the CommServer directory [1-3](#)

phone access, account lockout policy [9-9](#)

phone passwords

changing [9-6](#)

default [9-5](#)

securing [9-1](#)

toll fraud [9-1](#)

policies

Cisco Security Agent [4-1](#)

logon, password, and lockout [9-7](#)

ports, voice messaging

best practice [6-4](#)

Cisco Unified CM security features [6-2](#)

identity theft [6-1](#)

security mode settings [6-4](#)

private messages, how Cisco Unity handles them [11-1](#)

R

restriction tables, best practices for use [5-1](#)

root certificate, distributing to trusted root store [10-7](#)

RSA SecurID overview [8-12](#)

RTP stream, modification threat [6-1](#)

S

secure messaging

installing [11-6](#)

limitations [11-4](#)

overview [11-2](#)

sending and receiving [11-2](#)

setting user expectations [11-4](#)

Secure Real Time Protocol (SRTP) [6-3](#)

securing

passwords [9-1](#)

Windows [1-1](#)

security mode settings

best practice [6-4](#)

voice messaging ports [6-4](#)

security policy, Windows, applying [1-2](#)

security template, Windows, applying [1-2](#)

security updates, installing Microsoft [2-6](#)

server

identity theft [6-2](#)

securing [1-1](#)

service packs, installing Microsoft [2-6](#)

services, changing the startup type [1-3](#)

SQL Server 2000, securing [2-2](#)

SSL

certificate, installing [10-5](#)

certificate, issuing [10-4](#)

certificate request, submitting [10-4](#)

redirection [10-10](#)

startup type for services, changing [1-3](#)

T

TCP ports, securing [1-6](#)

toll fraud

preventing by using restriction tables [5-1](#)

preventing with account policy [9-9](#)

Transport Layer Security (TLS) protocol [6-2](#)

trusted root store [10-7](#)

TUI

preventing unauthorized access [9-5](#)

private message handling [11-1](#)

U

UDP ports, securing [1-6](#)

URLScan tool, hardening the Cisco Unity server with [2-4](#)

user rights, changing [1-2](#)

V

ViewMail, private message handling [11-1](#)

voice messaging ports

best practice [6-4](#)

Cisco Unified CM security features [6-2](#)

identity theft [6-1](#)

security mode settings [6-4](#)

W

Windows

applying a security policy [1-2](#)

applying a security template [1-2](#)

securing [1-1](#)

Windows NT Challenge/Response authentication [8-2](#)