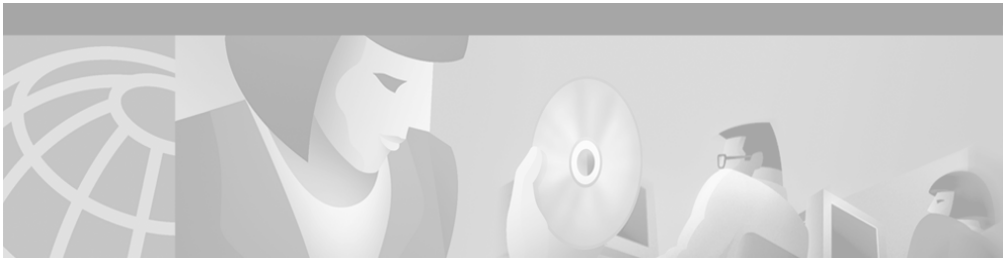

White Paper: Security Best Practices for Cisco Unity 3.0

Revised May 24, 2002

Introduction

This document provides the best practices recommended to "harden" a Cisco Unity 3.0 server. The term "server hardening" is used to describe the process of making a server less susceptible to unwanted or unauthorized access and viruses.

This document does not provide instructions for installing a Cisco Unity server. Instead, it should be used in conjunction with the *Cisco Unity Installation Guide* to harden the Cisco Unity server during installation and normal operations. The recommendations presented in this document will be evaluated on a regular basis, and updated as necessary.

The following sections in this document address the main security concerns for the Cisco Unity server:

- Securing the Cisco Unity Operating Environment—Several third-party products make up the Cisco Unity operating environment. Each of these products should be secured by following the security guidelines published by the product manufacturer. These guidelines, along with specific

Cisco Systems

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

recommendations for using each component with Cisco Unity, are summarized in this section, and can be used to harden the Cisco Unity operating environment during or after installation.

- Securing the Cisco Unity Application—Once the Cisco Unity application is installed, it can be secured by following the recommendations detailed in this section.
- Cisco Unity Server Security Policies—This section suggests the security policies that you can implement to further harden your server after installation is complete.

Finally, the Online References section offers a list of sites referenced in this document.

Securing the Cisco Unity Operating Environment

The Cisco Unity operating environment is comprised of all the third-party components that Cisco Unity utilizes to service subscribers. These components consist mainly of Microsoft products, though other third-party products such as Dialogic software (installed when voice boards are used to connect a Cisco Unity server to a traditional phone system) may be employed as well.

The following Microsoft products are the primary components of the Cisco Unity operating environment:

- Windows 2000 with Service Pack 2
- SQL Server 2000 with Service Pack 1 or MSDE 2000
- Internet Explorer (IE) 5.5 or 6.0 with current security patches
- Microsoft Message Queuing 2.0
- Internet Information Server (IIS) 5.0 with current security patch
- Exchange 2000 with Service Pack 1

For a detailed list of Cisco Unity operating environment components, refer to *Cisco Unity System Requirements, and Supported Hardware and Software* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/index.htm.

Each component in the Cisco Unity operating environment presents a security risk, because each may prevent Cisco Unity from running reliably and effectively if compromised. By default, however, most of these components are installed with minimum security, and thus, can be reconfigured with increased security in mind.

As appropriate, use the guidelines presented in the following sections in conjunction with the *Cisco Unity Installation Guide* (see http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity30/inst/index.htm) to harden the Cisco Unity operating environment during or after a new Cisco Unity installation.

Securing Windows

Until the Windows 2000 installation on the Cisco Unity server is complete, IIS is vulnerable once its services have started. You can disable its services or wait to install it until after the Windows 2000 Service Pack 2 is applied. However, the most secure approach to installing Windows is to use the integrated method of burning a Windows 2000 CD with Service Pack 2. Detailed instructions are provided in the article, "Installing and Securing a New Windows 2000 System," available on the Microsoft Web site. This article is impossible to find! It is on TechNet, but searching there will not find it. You can find it from ms.com, but the link goes to the wrong article.In addition, refer to the Microsoft Security Home page for the most current hardening and security guide for Windows 2000 and IIS 5.0.

To check an existing Windows 2000 installation for vulnerabilities, first confirm that Service Pack 2 is installed on the server. Then, query the Microsoft TechNet Web site for the latest information on securing an existing Windows 2000 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 Web site, or the Windows 2000 online Help.

Caution Applying certain security templates can render Cisco Unity inoperable. If you apply security templates, make sure that they use the suggested security settings outlined in the Cisco Unity Server Security Policies section of this document. These settings enable the Cisco Unity server to maintain full functionality.

Securing SQL

While the installation of SQL on the Cisco Unity server provides a fully functioning SQL server, its intended use is as a back-end database for Cisco Unity. As a best practice, it should be used for no other purpose.

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

Install SQL using Windows security only

Although you can use a domain user account or the Local System account to run the SQL services, it is best to use the Local System account, which is the default.

Assign a password to the SQL administrator (SA) account

Note the password and keep it in a secure location.

Restrict client access to SQL

Grant access to SQL directories, folders, and files only to the Unity service accounts and to a highly privileged account designated for use by a system administrator (see Best Practices for Cisco Unity Accounts for more details). The Cisco Unity installation process gains access to the SQL server by its membership in the local server administrators group.

Securing Internet Explorer

At a minimum, IE 5.5 with Service Pack 1 must be installed on the Cisco Unity server. As a best practice, use IE on the Cisco Unity server for Cisco Unity administration only, and for no other purpose.

Perform the following steps to reduce the chance of being exposed to a worm like the recent Code Red and Nimda viruses. For additional information on preventing exposure to and recovering from the Nimda virus on the Cisco Unity server, refer to http://www.cisco.com/warp/customer/788/AVVID/vmum.shtml.

To disable active scripting

Note that Microsoft recommends that you subscribe to the Security Notification Service. To do so, however, you must set IE to use less secure settings than those suggested in this procedure. Therefore, as a best practice, confirm that at least one

computer at your site—other than a Cisco Unity server—is subscribed to the Security Notification Service, and perform the following procedure on remaining workstations.

In this way, you can receive updates about the latest hotfixes and security issues without seriously compromising Cisco Unity security.

Step 1 Start Internet Explorer.

Step 2 For each of the four security levels, perform the following actions:

- Click **Tools > Internet Options**.
- From the Internet Options dialog box, click the appropriate icon for the security level that you want to customize (Internet, Intranet, Trusted, Untrusted).
- Click **Security > Custom Level**.
- Under Scripting, check the **Prompt** field.

Step 3 Click **OK**.

Step 4 Click **OK**, and exit Internet Explorer.

Securing Microsoft Message Queuing

Microsoft Message Queuing (MSMQ) 2.0 is used by Unity services to read changes from Active Directory and write them to the Cisco Unity back-end database. It is not used to connect the Cisco Unity server to Active Directory.

As a best practice, ensure that MSMQ is configured for Local Use Only. This means you should install the MSMQ so that it does not use Active Directory.

Securing IIS

This section contains guidelines that you can use to better secure the IIS 5.0 installation on the Cisco Unity server before the Cisco Unity application is installed, and reference information that you can use after the installation is complete.

IIS Configuration Guidelines

Confirm that the current patch level is MS01-044 (this is the cumulative update patch for IIS 5.0). If the operating system is installed or updated by using the method described in the Securing Windows section, then secure IIS 5.0 by removing the default settings.

In addition, use the following guidelines 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 guidelines as specified in the complete IIS 5.0 security checklist available on the Microsoft TechNet Web site.

Secure Cisco Unity Web components

Follow guidelines as specified in the complete IIS 5.0 security checklist available on the Microsoft TechNet Web site—except change the ACLs to allow only the Unity service accounts and/or the local server administrators group to have Full Control access to the Cisco Unity directories, folders, and files (see <driveletter>:\inetpub\wwwroot\…).

Disable all default IIS COM objects

Follow guidelines as specified in the complete IIS 5.0 security checklist available on the Microsoft TechNet Web site—except do not disable the “file system object” (FSO).

Remove unused script mappings

Cisco Unity uses only asa and asp script mappings. Remove all remaining unused script mappings.

Do not disable Parent Paths

Do not follow the guidelines as specified in the complete IIS 5.0 security checklist on the Microsoft TechNet Web site to disable Parent Paths. By default, this option is enabled, and should remain so on the Cisco Unity server.

Additional IIS Reference Information

The following security tools can be used after IIS is installed to expose any existing vulnerabilities.

Caution Do not use these tools (or perform any procedures that are not referenced in this document) to alter the IIS configuration described in the previous section. If you do, you may render the Cisco Unity server inoperable.

Utilize IIS Lockdown and URLScan tools

You can use the Microsoft IIS Lockdown and URLScan tools to harden the IIS server. However, be careful not to disable support for active server pages (.asp) or the Scripts Virtual directory using IIS Lockdown.

Refer to the Security pages on the Microsoft TechNet Web site for download instructions and details on how to use these tools. For information on configuring these tools in an Exchange environment, refer to article #Q309508 (“XCCC: IIS Lockdown and URLScan Configurations in an Exchange Environment”) on the Microsoft Product Support Services Web site.

Follow Microsoft security checklists

In addition to the complete checklist, Microsoft offers a baseline security checklist for IIS on its TechNet Web site. Many of the checklist recommendations, such as subscribing to the Microsoft Security Notification Service, are necessary if you want to stay current with IIS security issues after installation.

Securing Exchange

You can install Exchange on the Cisco Unity server, or you can configure the Cisco Unity server to point to an Exchange server off-box. For details on the requirements for using Exchange, refer to *Cisco Unity System Requirements, and Supported Hardware and Software* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/index.htm. If you did not install Exchange on the Cisco Unity server, use the recommendations provided by Microsoft for securing your existing Exchange servers. Otherwise, use the following security guidelines, as appropriate for your version of Exchange.

Configuring Exchange 5.5

If Exchange 5.5 is installed on the Cisco Unity server, or if Cisco Unity is connected to an Exchange 5.5 server, change the LDAP port number to something other than the default, which is 389. Instead, assign it to a port that is seldom used, such as one in the 2000 range or higher. For most Cisco Unity configurations, you can change LDAP port settings by accessing the Protocol section in the Server container in Exchange Administrator. If Cisco Unity is installed as a unified messaging system, however, it might be necessary to change the setting in the Site Configuration container.

For more information on registered ports, search the Internet Engineering Task Force (IETF) Web site, or the Microsoft TechNet Web site.

Configuring Exchange 2000

If Exchange 2000 is installed on the Cisco Unity server, or if Cisco Unity is connected to an Exchange 2000 server, refer to the Microsoft Web site for recommendations on hardening an Exchange 2000 server.More to come with next revision.--ts 10/18

Securing the Cisco Unity Application

There are several ways that a Cisco Unity server can be hardened to minimize the risk of unwanted intrusion and viruses. See the following sections for details.

Best Practices for Cisco Unity Accounts

For the latest requirements for Cisco Unity service account usage and permissions, see the *Cisco Unity Installation Guide* for 3.0(2) available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity30/inst/inst302/index.htm. Additional information will be available in the upcoming white paper, “Cisco Unity 3.0 Account Permissions,” which outlines the minimal permissions and user rights assignments necessary to install and operate Cisco Unity (see http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/).

As a best practice, use the following guidelines to secure Cisco Unity accounts:

Limit account access to Cisco Unity

Access to the Cisco Unity server should be limited to the Unity service accounts and to one other highly privileged account designated for use by a system administrator. This account can have domain level administrative capabilities, access to Cisco Unity utilities, directories, files, and data, and should be able to administer Cisco Unity by using the Cisco Unity Administrator.

The Cisco Unity Administrator is the interface with which a system administrator performs most tasks. It is a Web site that the administrator can access by using Internet Explorer. The Cisco Unity Administrator is available from the following URL: http://<server name>/web/sa.

By default, only two administrative accounts have access to the Cisco Unity Administrator:

- **Installer**—When the installation process is complete, the account used to install Cisco Unity is automatically given proper security rights to access the Cisco Unity Administrator. It obtains access to the Cisco Unity Administrator by association with a built-in account currently called Unity Installer_<server name>.
- **Example Administrator**—Cisco Unity creates this account during installation. It serves as a default owner, message recipient, and member of several Cisco Unity entities.

To allow domain accounts access to the Cisco Unity Administrator on multiple Cisco Unity servers, you can assign these accounts to Unity Installer_<server name>. This built-in account is a member of the Cisco Unity Default Administrator class of service (COS). For further guidelines on allowing access to the Cisco Unity Administrator, see the Best Practices for Class of Service Restrictions section.

Limit account access to Cisco Unity directories, files, and data

The Cisco Unity application is installed in the CommServer directory. This directory can be installed on any local drive selected during installation (the default is C:\CommServer).

By default, Unity service accounts have Full Control access to this directory due to their membership in the local server administrators group. You should also set the permissions for Cisco Unity directories, folders, files and data to allow Full Control access to the highly privileged account that you designate for use by a system administrator. In this way, the account can be used to perform advanced administrative and troubleshooting tasks.

As a best practice, other domain accounts used by Cisco Unity system administrators should be restricted to read-only access, while Cisco Unity subscribers, and all other domain accounts and groups should have no access rights to the directories, folders, or files on the Cisco Unity server. To do so, exclude the System Group Everyone from the default user permissions for C:\ or root of any other drive on the Cisco Unity server. Instead, assign authenticated users. In addition, confirm that no explicitly privileged assignments have been made to individual groups or accounts.

Do not use Unity service accounts to administer Cisco Unity

Unity service accounts may have more permissions than are necessary to perform most administrative tasks. For this reason, if you have one or more domain users who need access to the Cisco Unity Administrator, but who do not need access to the Cisco Unity server itself, do not allow them to use the Unity service accounts to do so.

Instead, you can grant their domain accounts access to the Cisco Unity Administrator by using GRANTUNITYACCESS, a command line tool found in the CommServer folder (the default location is C:\CommServer). You can choose to associate these domain accounts with either the Unity Installer_<server name> account, or an imported subscriber account that has class of service rights to the Cisco Unity Administrator. In this way, you can allow these domain users to administer Cisco Unity without giving them administrator permissions for the server itself. For further guidelines on allowing access to the Cisco Unity Administrator, see the Best Practices for Class of Service Restrictions section.

Restrict use and access to the GRANTUNITYACCESS

Offer use of and access to this command line utility only to the highly privileged account that you designate for use by a system administrator.

Best Practices for Class of Service Restrictions

A class of service (COS) defines limits and permissions for using Cisco Unity. A COS is specified in each subscriber template; thus, a subscriber is assigned to the COS which is specified in the template upon which the subscriber account is based.

Cisco Unity includes the following predefined classes of service, which you can modify but not delete:

- **Default Subscriber**—The Default Subscriber COS contains settings that are applicable to subscribers. By default, this COS is associated with the {Default Subscriber} template, and is excluded from accessing the Cisco Unity Administrator. It is recommended that all subscriber COS settings prevent access to the Cisco Unity Administrator.
- **Default Administrator**—The Default Administrator COS contains system access settings that specify which tasks, if any, subscribers can perform in the Cisco Unity Administrator. (Cisco Unity system administrators are simply subscribers who have access to the Cisco Unity Administrator.) By default, this COS allows full administrative access to Cisco Unity, including the ability to:
  - Access the Cisco Unity Administrator.
  - Create, edit, or delete class of service, restriction tables, routing tables, call handlers, schedules and holidays, subscribers, and public distribution lists.
  - Access the Status Monitor, reports, diagnostic tools, and technician functions.

To restrict access to the Cisco Unity Administrator, you cannot change COS settings in individual subscriber accounts; however, you can at any time reassign a subscriber to a different COS that you create.

When modifying COS settings and assignments, consider the following:

- Do not modify the Default Administrator COS system access settings. Instead, reassign subscriber accounts to another COS with little or no access to the Cisco Unity Administrator.
- Do not reassign *every* account which has access to the Cisco Unity Administrator to another COS that offers little or no access to the Cisco Unity Administrator.

Caution If you do not have at least one domain account with membership in a COS that offers access to the Cisco Unity Administrator, you may lose the ability to administer Cisco Unity, and be required to reinstall. As a best practice, make sure that at least one account is assigned to the Default Administrator COS.

For more information about COS settings and assignments, see the *Cisco Unity System Administration Guide* available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity30/sag/index.htm.

Best Practices for Creating Subscriber Accounts

Anyone who has an account on Cisco Unity is a subscriber. Typically...However, if the password policy is set to a higher setting, the default password listed in the subscriber template is not used. Instead the process occurs as explained below. If you create new subscriber accounts by using either the Cisco Unity Administrator or the CSV option available with the Cisco Unity Import utility, each subscriber account is associated with an Exchange mailbox, and subsequently is given an account in Active Directory.

The password that is initially assigned during this process is a randomly generated password that meets complexity requirements. There is no way to determine what this password is when it is assigned. As a result, a system administrator—one who is assigned a highly privileged account that has domain level administrative capabilities—would have to reset the password in order for the subscriber to use the account to access the ActiveAssistant.

Best Practices for Subscriber Phone Access

When subscribers interact with Cisco Unity by phone, they hear the Cisco Unity conversation, or TUI (Telephone User Interface). To do so, subscribers dial a Cisco Unity pilot number (or their own extension if they use DIDs), and then log on to Cisco Unity by entering a password.

The account policy settings in the Cisco Unity Administrator allow you to define the characteristics of the phone passwords that subscribers use to log on to Cisco Unity. In addition, account lockout settings allow you to lock subscriber accounts when incorrect phone passwords are entered repeatedly. These settings specify the number of invalid logon attempts that are allowed before the account is locked, and specify whether a system administrator must unlock the account.

As a best practice, the default phone password and account lockout settings should be changed to provide more secure access to the Cisco Unity application, as suggested in the following sections.

Securing Phone Password Settings

Information in this section refers to the fields on the Subscribers > Account Policy > Phone Password Restrictions Page in the Cisco Unity Administrator. As a best practice, do not enable the following fields:

- Password Never Expires
- Permit Blank Password
- Do Not Keep Password History

Instead, use the following guidelines to tighten phone password security on the Cisco Unity server. For information on changing phone password settings, see the *Cisco Unity System Administration Guide* available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity30/sag/index.htm.

Maximum Phone Password Age

When the Days Until Password Expires field is selected, subscribers are prompted to change their passwords every X days. X is the value specified in the adjacent box.

Default Setting	More Secure Setting
42	30

Phone Password Length

When the Minimum Number of Characters in Password field is selected, subscribers are required to create a password at least X characters long. X is the value specified in the adjacent box. In general, shorter passwords are easier to use, but longer passwords are more secure. When you change the minimum password length, subscribers will be required to use the new length the next time they change their passwords.

Default Setting	More Secure Setting
3 characters	8 characters

Phone Password Uniqueness

When the Number of Passwords to Remember field is selected, Cisco Unity enforces password history by storing the specified number of previous passwords for a subscriber and comparing a new password with them. Cisco Unity rejects the new password if it matches a password stored in the history.

Note that by default, Cisco Unity does not keep password history, as this field is disabled. As a best practice, you should enable the Number of Passwords to Remember field to enforce phone password history, and consider the following values for the adjacent box.

Default Setting	More Secure Setting	Most Secure Setting
Disabled (when field is enabled, 1 password is remembered)	10 passwords remembered	24 passwords remembered

Check Against Trivial Passwords for Extra Security

When this box is checked, Cisco Unity verifies that a new password meets the following criteria:

- The password is not the same as previous passwords.
- The digits are not all the same (for example, 9999).
- The digits are not consecutive (for example, 1234).
- The password is not the same as the extension assigned to the subscriber.
- The password does not spell the name of the subscriber.

As a best practice, confirm that the Check Against Trivial Passwords for Extra Security field is enabled. Note that if the Permit Blank Password box is selected, the Check Against Trivial Passwords for Extra Security field is automatically disabled.

Securing Account Lockout Settings

Information in this section refers to the fields on the Subscribers > Account Policy > Unity Account Lockout page in the Cisco Unity Administrator. By default, Cisco Unity blocks phone access to a subscriber account when the limit

of logon attempts is reached. (However, the subscriber can still access the account by using the ActiveAssistant, and can play messages from the Inbox.) Once the account has been accessed with a valid logon, Cisco Unity resets the number of logon attempts to zero.

As a best practice, do not enable the No Account Lockout field. Instead, use the following guidelines to tighten account lockout security on the Cisco Unity server. For information on changing account lockout settings, see the *Cisco Unity System Administration Guide* available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity30/sag/index.htm.

Lock Account After __ Invalid Attempts field

This field contains the value for the number of unsuccessful logon attempts after which Cisco Unity will block phone access to a subscriber account.

Default Setting	More Secure Setting	Most Secure Setting
6 attempts	4 attempts	3 attempts

Reset Count After __ Minutes

This field contains the value for the number of minutes after which Cisco Unity will clear the count of logon attempts, unless the limit is reached and the account is locked.

Default Setting	More Secure Setting	Most Secure Setting
60 minutes	1440 minutes (one day)	Forever (Subscribers must contact a system administrator to change the password.)

Best Practices for Subscriber Web Access

Each subscriber account has numerous settings, which system administrators manage by using the Cisco Unity Administrator. Some subscriber settings can also be changed by subscribers by using the ActiveAssistant, which is a

Web-based interface similar to the Cisco Unity Administrator. Subscribers can access ActiveAssistant from the following URL: http://<Cisco Unity server name>/web/aa. Like the Cisco Unity Administrator, subscribers can use the ActiveAssistant only if their class of service allows access to it. See the *Cisco Unity System Administration Guide* available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity30/sag/index.htm for details.

When either the Cisco Unity Administrator or the ActiveAssistant site receives an access request, it uses the subscriber NT credentials to authorize access. By default, this process uses NTLM auto authentication. However, it is possible to force subscribers to use manual authentication when accessing these sites by performing the following procedure.

To force manual authentication

Perform this procedure on the Cisco Unity server, and then on each subscriber workstation.

Step 1 Start Internet Explorer.

Step 2 Click **Tools > Internet Options**.

Step 3 From the Internet Options dialog box, click the **Local Intranet** icon.

Step 4 Click **Security > Custom Level**.

Step 5 Under User Authentication, check **User Name and Password** for the Logon Prompt field.

Step 6 Click **OK**.

Step 7 Click **OK**, and exit Internet Explorer.

Best Practices for Using Text-To-Speech

The text-to-speech (TTS) feature allows Cisco Unity subscribers to listen to their e-mail 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.

In some sites, offering TTS to subscribers is considered a security risk. To minimize the risk, you can disable TTS in the subscribers' COS, or you can set up Cisco Unity subscriber accounts to use a secure logon method known as two-factor user authentication. Cisco Unity works with the RSA SecurID system to provide this method of enhanced phone security. In the Cisco Unity Administrator, you can assign subscribers to a class of service for which enhanced phone security is enabled.

Enhanced security has been available for use with Cisco Unity for some time, and provides a very secure way to validate subscriber access to Cisco Unity. The RSA ACE Server, ACE Agent, and SecurID Token fobs are not included with Cisco Unity systems, but must be purchased separately. For more information on how the RSA SecurID system works with Cisco Unity, or for setup details, see the *Cisco Unity System Administration Guide* available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity30/sag/index.htm.

Cisco Unity Server Security Policies

This section suggests some ways that you can further harden a default, "out-of-the-box" Cisco Unity server configuration. It is recommended that you implement the suggested changes in this section after you have completed the Cisco Unity installation. For details about changing the settings presented in this section, search the Microsoft Web site for the "Step-by-Step Guide to Using the Security Configuration Tool Set."

Changing Cisco Unity Server Security Settings

Use the following hardening settings to restrict access to the Cisco Unity server. If your site already has a security policy in place, review the following policy settings to determine the additional settings necessary for securing the Cisco Unity server. These settings can also be made manually without applying a security template.

It is important to turn on auditing in order to track how the Cisco Unity server is being accessed. Without using auditing, you will not be able to tell when someone has accessed your system.

Table 1 Local Policies: Audit Policies and User Rights Assignments

Setting	Default Value	Recommended Value
Audit account login events	No auditing	Failure
Audit account management	No auditing	Success, Failure
Audit directory service access	No auditing	Failure
Audit login events	Failure	Failure
Audit object access	No auditing	No auditing
Audit policy change	No auditing	Success, Failure
Audit privilege use	Failure	Failure
Audit system events	No auditing	No auditing
Act as part of the operating system	Account used to install Cisco Unity	Account used to install Cisco Unity
Access this computer from the network	Backup Operators, Power Users, Users, Administrators, servername\IWAM, domainname\ISUR_servername, everyone	Same as default, except do not include everyone
Shut down the system	Backup Operators, Power Users, Administrators	Backup Operators, Administrators

Using Strong Passwords

As a part of a comprehensive security policy, you should use strong passwords. Strong passwords can be enforced in Windows 2000. Strong passwords can be turned on by enabling Password Must Meet Complexity Requirements in the domain password policy settings.

All Cisco Unity accounts should be required to use passwords at least 8 characters or greater. During installation of a Cisco Unity server, Cisco Unity entities, such as the Installer and Example Administrator accounts, are given 15 character

passwords, which are randomly generated to meet complexity requirements. These accounts must have their passwords reset by an administrator with the appropriate privileges before they can be used. See the Best Practices for Creating Subscriber Accounts for more information.

The following settings can be modified by using the Windows Local Security Policy utility on the Cisco Unity server.

Table 2 Local Policies: Security Options

Setting	Default Value	Recommended Value
Additional restrictions for anonymous connections	None, rely on default permissions	Do not allow enumeration of SAM accounts and shares
Allow system to be shut down without having to log on	Disabled	Disabled
Audit use of Backup and Restore privilege	Disabled	Disabled
Clear virtual memory pagefile when system shuts down	Disabled	Disabled
Digitally sign client communication (always)	Disabled	Disabled
Digitally sign client communication (when possible)	Enabled	Enabled
Digitally sign server communication (always)	Disabled	Disabled
Digitally sign server communication (when possible)	Disabled	Enabled
Disable Ctrl-Alt-Del requirement for login	Disabled	Disabled
Do not display last user name in logon screen	Disabled	Enabled

Table 2 Local Policies: Security Options (continued)

Setting	Default Value	Recommended Value
LAN manager authentication level	Send LM and NTLM responses	Send NTLM response only
Message text for users attempting to log on	(blank)	Customer-specific information indicating that the system is for authorized use only. This information is important as legal protection in the event unauthorized access occurs.
Message title for users attempting to log on	(blank)	Customer-specific information indicating that the system is for authorized use only. This information is important as legal protection in the event unauthorized access occurs.
Number of previous logons to cache (in case domain controller is not available)	10 logons	5 logons
Prevent system maintenance of computer account password	Disabled	Enabled
Prompt user to change password before expiration	14 days	7 days
Rename administrator account	Administrator	A value which is difficult to guess
Restrict CD-ROM access to locally logged-on users only	Disabled	Enabled

Table 2 Local Policies: Security Options (continued)

Setting	Default Value	Recommended Value
Restrict floppy access to locally logged-on users only	Disabled	Enabled
Secure Channel: Digitally encrypt or sign secure channel data (always)	Disabled	Enabled
Secure Channel: Require strong (Windows 2000 or later) session key	Disabled	Enabled
Send unencrypted password to connect to third-party SMB servers	Disabled	Disabled
Smart card removal behavior	No Action	Lock workstation
Unsigned driver installation behavior	Warn but allow installation	Do not allow installation
Unsigned non-driver installation behavior	Silently succeed	Silently succeed / Warn but allow installation

The following settings can be modified by using the Windows Local Security Policy utility on the Cisco Unity server.

Table 3 Event Log Settings

Setting	Default Value	Recommended Value
Maximum application log size	8192 kilobytes	Undefined
Maximum security log size	512 kilobytes	5120 kilobytes
Maximum system log size	512 kilobytes	1024 kilobytes

Table 3 Event Log Settings (continued)

Setting	Default Value	Recommended Value
Restrict guest access to application log	Disabled	Enabled
Restrict guest access to security log	Disabled	Enabled
Restrict guest access to system log	Disabled	Enabled
Retain system log	7 days	14 days
Retention method for application log	As needed	As needed
Retention method for security log	By days	As needed

The following services should be disabled on the Cisco Unity server with the exception of the IPSec Policy Agent setting. You can disable these services by accessing the Service Control Panel in the Administration Tools folder.

Table 0-4 System Services

Setting	Default Value	Recommended Value
Alerter	Automatic	Disabled
Clipbook	Manual	Disabled
Computer Browser	Automatic	Disabled
DHCP Client	Automatic	Disabled
Distributed File System	Automatic	Disabled
Distributed Link Tracking Client	Automatic	Disabled
Distributed Link Tracking Server	Manual	Disabled
Distributed Transaction Coordinator	Automatic	Disabled
Fax Service	Manual	Disabled

Table 0-4 System Services (continued)

Setting	Default Value	Recommended Value
Internet Connection Sharing	Manual	Disabled
IPSec Policy Agent	Automatic	Automatic
Messenger	Automatic	Disabled
NetMeeting Remote Desktop Sharing	(blank)	Disabled
Print Spooler	Automatic	Disabled
Remote Access Auto Connection Manager	Manual	Disabled
Remote Access Connection Manager	Manual	Disabled
Remote Registry Service	Automatic	Disabled
Task Scheduler	Automatic	Disabled

Securing Remote Access

Telnet access should not be allowed on the Cisco Unity server. In addition, while a modem is required by Cisco TAC to support a Cisco Unity server, as a best practice turn it off or disconnect it when not in use.

Securing the Physical Unit

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

Protecting Cisco Unity From Virus Attacks

To minimize the risk of virus attacks, install an anti-virus software package on the Cisco Unity server. Before doing so, however, you should address the following issues. For additional information on preventing exposure to and recovering from the Nimda virus on the Cisco Unity server, refer to http://www.cisco.com/warp/customer/788/AVVID/vmum.shtml.

Disable anti-virus software during installation of Cisco Unity

It is best to install anti-virus software only after Cisco Unity is installed. If it is already installed prior to installing the Cisco Unity application, disable it before proceeding. Note that in some cases, you may need to completely remove the anti-virus software, and reinstall it after you have completed the Cisco Unity installation.

Use Microsoft recommendations to protect Exchange

If Exchange is installed on the Cisco Unity server, refer to the Microsoft Web site for the latest information on protecting an Exchange server from virus attacks.

Use Microsoft recommendations to protect SQL

Since SQL Server 2000 is installed on the Cisco Unity server, refer to the Microsoft Web site for the latest information on protecting a SQL server from virus attacks.

Use caution when employing message scanning

Consider the impact that scanning has on the performance of the Cisco Unity server prior to scanning for viruses in a certain way. For instance, performing a complete file IO scan may have a negative impact on Cisco Unity server performance.

Do not employ any message scanning that could drastically impact the performance of the Cisco Unity server.

Protecting Cisco Unity From Hacker Attacks

Follow Microsoft recommendations on securing the server from unwanted or unauthorized access. You can obtain vulnerability scanners (such as Cisco Scanner, Nessus, and SAINT). These products identify security vulnerabilities on your network. As a best practice, do not install the scanner on the Cisco Unity server.

Additionally, the Cisco Host IDS (Intrusion Detection System) is currently being qualified for use on Cisco Unity servers. Refer to the latest Cisco Unity Release Notes to determine support status for the Cisco Host IDS.

Online References

For more information about topics referenced in this document, refer to the following sites.

Cisco Unity documentation

- Official Cisco Unity 3.0 product documentation is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity30/index.htm.
- Cisco Unity white papers and application notes are available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/.
- Technical tips on installing, maintaining, and using Cisco Unity are available at http://www.cisco.com/warp/customer/788/AVVID/vmum.shtml.

CERT Coordination Center (CERT/CC) Web site

- Available at http://www.cert.org/.

Internet Engineering Task Force (IETF) Web site

- Available at: http://ietf.org/.

Microsoft Web sites

- The Microsoft Home page is available at http://www.microsoft.com/.
- The Microsoft Security Home page is available at http://www.microsoft.com/security/default.asp.

- The Microsoft TechNet Home page is available at http://www.microsoft.com/techNet/.
