



# 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 2000 Server system. For detailed information, see:

- The article “Installing and Securing a New Windows 2000 System,” available on the Microsoft website.
- The Microsoft Security Home page for the most current hardening and security guide for Windows 2000 Server and for the *IIS 5.0 Baseline Security Checklist*.

To check an existing Windows 2000 Server 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](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 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 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)**

<b>Setting</b>	<b>Recommended Startup Type</b>
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 Search	Automatic*
MSSQLSERVER	Automatic*
MSSQLServerADHelper	Manual*
Net Logon	Automatic*
NetMeeting Remote Desktop Sharing	Disabled
Network Connections	Manual*
Network DDE	Manual*
Network DDE DSDM	Manual*

**Table 1-3 Services Settings (continued)**

Setting	Recommended Startup Type
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
 <b>Caution</b> 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)	Disabled
Smart Card	Manual*
Smart Card Helper	Manual*
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*

**Table 1-3 Services Settings (continued)**

Setting	Recommended Startup Type
Windows Time	Automatic*
Workstation	Automatic*
World Wide Web Publishing Service	Automatic*

\* 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 by a firewall from:

- Domino servers on which mailboxes for Cisco Unity subscribers are homed.
- Domino servers on which Cisco Unity accesses Domino address books.
- The Domino server that the installer specified while installing IBM Lotus Notes on the Cisco Unity server. (Cisco Unity delivers all voice messages to Mail.box this server for routing.)
- The domain controller on which the Cisco Unity installation and services accounts were created.

In addition, when failover or standby redundancy is configured, do not separate the Cisco Unity servers by a firewall from one another.



### 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 3-6.