



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 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 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,” refer to 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, refer to the article “Checklists; Windows Server 2003, Standard Edition,” and for Windows 2000 Server, refer to the article “Installing and Securing a New Windows 2000 System,” both available on the Microsoft website.
- Refer to 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 “[Changing Windows 2000 Server Audit Policies and User Rights](#)” section on page 1-2. 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 Startup Type for Services on the Cisco Unity Server

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
Application Management	Manual*
Automatic Updates	Automatic*
Background Intelligent Transfer Service	Manual*
Clipboard	Disabled
COM+ Event System	Manual*
Computer Browser	Disabled
CsBridgeConnector	Manual*
DHCP Client	Disabled

Table 1-3 Services Settings (continued)

Setting	Recommended Startup Type
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*
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*

Table 1-3 Services Settings (continued)


Setting	Recommended Startup Type
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*
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*

Table 1-3 Services Settings (continued)

Setting	Recommended Startup Type
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

See the following sub-sections:

- [TCP and UDP Ports Used by Cisco Unity 4.0\(x\), page 1-6](#)
- [Restricting DCOM Dynamic Port Allocation, page 1-9](#)
- [Configuring Windows TCP/IP Filtering, page 1-10](#)

TCP and UDP Ports Used by Cisco Unity 4.0(x)

Table 1-4 shows the TCP and UDP ports that are used by Cisco Unity, with the following details:

- The TCP and UDP ports used by Cisco Unity 4.0(x) and by Cisco Unity-CM TAPI service provider (TSP) version 7.0(1) and later.
- The protocols and services that use the ports.
- The direction of the traffic: outbound (to a port on a remote host) or inbound (to a local port).
- A description of port usage.

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.)



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 1-9](#).

Table 1-4 TCP and UDP Ports Used by Cisco Unity 4.0(x)

Server Source Port	Protocol or Service	Direction	Port Usage
TCP 25	SMTP	Both directions	Used by Microsoft Exchange when Exchange is installed on the Cisco Unity server.
TCP and UDP 53	DNS	Outbound	Used to access the DNS server for name resolution.
		Inbound	Used when the DNS server is running on the Cisco Unity server.
UDP 67	DHCP/BOOTP (when Cisco Unity is a DHCP client)	Outbound	If you are using DHCP instead of static IP addresses, used by the Cisco Unity server to send DHCP or BOOTP requests.
	DHCP/BOOTP (when Cisco Unity is a DHCP server)	Inbound	Used by the Cisco Unity server to receive DHCP or BOOTP requests.
UDP 68	DHCP/BOOTP (when Cisco Unity is a DHCP client)	Inbound	If you are using DHCP instead of static IP addresses, used by the Cisco Unity server to receive DHCP or BOOTP replies.
	DHCP/BOOTP (when Cisco Unity is a DHCP server)	Outbound	Used by the Cisco Unity server to send DHCP or BOOTP replies.
TCP 80	HTTP	Both directions	Used to access the Cisco Unity Administrator, the Cisco Personal Communications Assistant, and Microsoft Internet Information Services (IIS).
TCP 135	MS-RPC	Both directions	Used to negotiate access to the Media Master, Cisco Unity ViewMail for Microsoft Outlook, the Exchange server, and other DCOM services.
UDP 137	NetBIOS	Both directions	NetBIOS Name Service. Used for NetBIOS name resolution or WINS resolution.
UDP 138	NetBIOS	Both directions	NetBIOS Datagram Service. Used when browsing Windows networks.
TCP 139	NetBIOS	Outbound	Used to access Windows file shares and perform NetBIOS over TCP/IP connections.
		Inbound	Used to access Cisco Unity reports and Microsoft Windows file shares.
UDP 161	SNMP	Both directions	Used to send SNMP notifications and to provide SNMP information when the host agent is queried.
UDP 162	SNMP Trap	Outbound	Used to send SNMP Traps.
TCP 389	LDAP with AD-DC	Outbound	Used to access LDAP directory services.
		Inbound	Used when Cisco Unity is running on the domain controller that is providing LDAP directory services.
Configurable (We recommend TCP 390 or any unused TCP port.)	LDAP with Exchange 5.5	Outbound	Used to access LDAP directory services.
		Inbound	Used when Cisco Unity is running on the domain controller that is providing LDAP directory services.

Table 1-4 TCP and UDP Ports Used by Cisco Unity 4.0(x) (continued)

Server Source Port	Protocol or Service	Direction	Port Usage
TCP 443	HTTP/SSL	Outbound	Used to perform system administration on a remote Cisco Unity server when it is configured for HTTP/SSL.
		Inbound	Used to access the Cisco Unity Administrator, IIS, or the Cisco PCA when the Cisco Unity server is configured for HTTP/SSL.
TCP 445	SMB	Outbound	Used to access Windows file shares and perform NetBIOS over TCP/IP connections.
		Inbound	Used to access Cisco Unity reports and Microsoft Windows file shares.
TCP 636	LDAP/SSL	Outbound	Used to access LDAP directory services over SSL.
		Inbound	Used when Cisco Unity is running on a domain controller that is providing LDAP directory services over SSL.
TCP 691	SMTP/LSA	Inbound	Used when the Exchange server is running on the Cisco Unity server and the Exchange server is accepting SMTP with LSA.
TCP 1432	TDS proxy (CiscoUnityTdsProxy)	Both directions	Used by local processes to access the SQL Server or MSDE database.
TCP 1433 (default)	MS-SQL-S	Both directions	Used to access the SQL Server or MSDE database, and to perform replication when Cisco Unity failover is configured.
UDP 1434	MS-SQL-M	Both directions	Used to access the SQL Server or MSDE database.
TCP 2000 (default)	Skinny (SCCP)	Outbound	Used to access Cisco CallManager.
TCP 3268	LDAP with AD-GC	Outbound	Used to access LDAP directory services when the global catalog server is on another server.
		Inbound	Used when Cisco Unity is running on the global catalog server that is providing LDAP directory services.
TCP 3269	LDAP/SSL with AD-GC	Outbound	Used to access LDAP directory services over SSL when the global catalog server is on another server.
		Inbound	Used when Cisco Unity is running on the global catalog server that is providing LDAP directory services over SSL.
TCP 3372	MSDTC	Both directions	Used to access the SQL Server or MSDE database when Cisco Unity failover is configured.
TCP 3389	Windows Terminal Services	Inbound	Used to remotely perform system administration on a Cisco Unity server.
TCP 3653	Node Manager	Both directions	Used to send manual keep-alive packets (or “pings”) between the primary and secondary servers when Cisco Unity failover is configured.
TCP 4444	Kerberos authentication	Both directions	Used to perform Kerberos authentication.
TCP 5060 (default)	SIP	Both directions	Used when the Cisco Unity server is connecting to SIP endpoints or SIP proxy servers.

Table 1-4 TCP and UDP Ports Used by Cisco Unity 4.0(x) (continued)

Server Source Port	Protocol or Service	Direction	Port Usage
TCP 5060+	SIP	Outbound	Used when the Cisco Unity server is connecting to PIMG units. Requires one port.
		Inbound	Used when the Cisco Unity server is connecting to PIMG units. Requires one port per PIMG unit.
TCP 8005	Server Life Cycle (JMX)	Outbound	Used to access the Tomcat server.
TCP 8009	AJP	Both directions	Used by IIS.
TCP and UDP dynamic (in the range of 1024–65535)	DCOM	Both directions	Used by the Media Master to play and record voice messages, and used when the Cisco Unity server is a domain controller supporting member servers.
UDP dynamic (in the range of 1024–65535)	MAPI notifications	Inbound	Used to notify Cisco Unity of changes to subscriber mailboxes when Exchange is the message store.
UDP dynamic (in the range of 22800–32767)	RTP	Both directions	Used when sending and receiving VoIP traffic with SCCP or SIP endpoints.
Not applicable	ICMP	Both directions	Used by Cisco Unity Telephony Integration Manager (UTIM) on the Cisco Unity server to ping Cisco CallManager.

**Note**

The Cisco PCA is a website that subscribers use to access the Cisco Unity Assistant and the Cisco Unity Inbox. In version 3.1(x) and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA; the Cisco Unity Inbox was known as the Visual Messaging Interface, or VMI.

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.

Configuring Windows TCP/IP Filtering

You can configure Windows TCP/IP filtering to allow access only to the TCP ports that your Cisco Unity configuration requires.



Caution

Do not use Windows TCP/IP filtering to filter UDP ports, or Cisco Unity may not function properly.

To Configure Windows TCP/IP Filtering

- Step 1** If you have not already restricted DCOM dynamic port allocations, do the [“To Restrict DCOM Dynamic Port Allocation” procedure on page 1-9](#).
- Step 2** From [Table 1-4](#), gather the TCP port numbers listed as “Inbound” or “Both directions” for your Cisco Unity configuration.
- Step 3** On the desktop, right-click **My Network Places** and then click **Properties**.
- Step 4** In the Network and Dial-up Connections dialog box, right-click **Local Area Connection** and then click **Properties**.
- Step 5** In the Local Area Connections Properties dialog box, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
- Step 6** In the Internet Protocol (TCP/IP) Properties dialog box, click **Advanced**.
- Step 7** On the Options tab of the Advanced TCP/IP Settings dialog box, click **TCP/IP Filtering**, and then click **Properties**.
- Step 8** In the TCP/IP Filtering dialog box, check the **Enable TCP/IP Filtering (All Adapters)** check box, and select **Permit Only for the TCP Ports**.
- Step 9** Click **Add**, enter a port number in the Add Filter dialog box, and click **OK**.
- Step 10** Repeat [Step 9](#) for each port that you want to allow access to.

Remember to include the static ports to which you restricted DCOM in the [“To Restrict DCOM Dynamic Port Allocation” procedure on page 1-9](#).



Note You may need to open additional ports to accommodate third-party software installed on the Cisco Unity server, such as virus-protection and backup software.

Step 11 Click **OK** four times, and then restart your computer.
