



## Securing Microsoft Software on the Cisco Unity Server(s)

---

In this chapter, you will find descriptions of potential security issues related to the software 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, Exchange 2000, or Exchange 5.5 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](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, refer to the following:

- For Cisco Unity operating environment components, refer to *Cisco Unity System Requirements, and Supported Hardware and Software*, available at [http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html).

- For recommended service packs and updates, refer to *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).

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, refer to 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](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 a. through Step f.
- 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, refer to *Cisco Unity System Requirements, and Supported Hardware and Software*, available at

[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_installation\\_guides\\_list.html](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](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.”