

# IIS Deployment Procedures



## In This Appendix

Assign Additional IP Addresses to a Network Adapter .....	297
Assign a Server Certificate to a Web Site .....	297
Back Up and Restore Registry Entries.....	298
Back Up and Restore the IIS Metabase.....	298
Back Up and Restore the Web Server to a File or Tape.....	299
Configure an ASP.NET Application for ASP.NET .....	302
Configure Anonymous User Identity.....	304
Configure a Web Site to be FrontPage Extended .....	305
Configure Application Identity for IIS 5.0 Isolation Mode .....	306
Configure Application Isolation Modes.....	307
Configure Application Isolation Settings for IIS 5.0 Isolation Mode.....	308
Configure Application Pool Health .....	309
Configure Application Pool Identity .....	310
Configure Application Pool Performance .....	311
Configure Application Pool Recycling.....	313
Configure FrontPage Server Roles.....	315
Configure FTP Server Authentication.....	316
Configure IIS Components and Services .....	318
Configure IP Address Assigned to Web Sites.....	318
Configure IP Address and Domain Name Restrictions.....	319
Configure MIME Types.....	322
Configure NTFS Permissions.....	324
Configure the State Service on the ASP.NET State Server .....	325
Configure the Registry.....	326
Configure the Web Site Identification Number .....	327
Configure Web Server Authentication .....	328
Configure Web Service Extensions .....	330

Configure Web Site Permissions .....	332
Configure Windows Server 2003 Services .....	333
Convert Existing Disk Volumes to NTFS.....	334
Create a Service Account .....	335
Create A SQL Server Database for Storing ASP.NET Session State .....	337
Create a Virtual Directory.....	338
Create a Web Site.....	339
Debug Application Pool Failures .....	340
Determine Web Sites Uniquely Identified by IP Addresses .....	341
Disable Network Adapters.....	342
Enable ASP.NET.....	343
Enable Logging .....	344
Enable Network Adapters.....	345
Enable Security Auditing .....	345
Enable the WWW Service After Upgrade .....	347
Enable Web Site Content Auditing .....	347
Export a Server Certificate .....	350
Gather and Display WWW Service Uptime Data .....	351
Grant User Rights to a Service Account .....	353
Install a Server Certificate .....	355
Install IIS 6.0.....	357
Install Subauthentication.....	357
Isolate Applications in Worker Process Isolation Mode.....	358
Make a Service Account a Member of the Local Administrators Group.....	359
Migrate CDONTS.....	360
Modify the IIS Metabase Directly .....	361
Monitor Active Web and FTP Connections .....	362
Pause Web or FTP Sites.....	364
Publish Web Site Content with FrontPage .....	365
Remove Virtual Directories .....	368
Request a Server Certificate.....	369
Secure the Root Folder of Each Disk Volume .....	370
Secure Windows Server 2003 Built-in Accounts .....	370
Set Processor Affinity .....	371
Stop the WWW Service .....	373
Upgrade FrontPage Extended Web Sites .....	373
View Application Isolation Configuration .....	374
View Web Site and Application Process Identities.....	375

## Assign Additional IP Addresses to a Network Adapter

You can configure a network adapter to have additional IP addresses. When you assign a specific IP address to a network adapter, you can uniquely identify a Web site or application by associating the Web site or application with that unique IP address.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

#### ► To assign additional IP addresses to a network adapter

1. In Control Panel, click **Network Connections**, right-click the network adapter that connects to the client computers, and then click **Properties**.
2. On the **General** tab, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
3. On the **General** tab, click **Advanced**.
4. On the **Advanced TCP/IP Settings** dialog box, click **Add**.
5. On the **TCP/IP Address** dialog box, enter the **IP address** and the **Subnet mask**, and then click **Add**.
6. Click **OK** twice, and then click **Close**.

---

## Assign a Server Certificate to a Web Site

Server certificates contain information about the server that allows the client to positively identify the server before sharing sensitive information. After you obtain a server certificate from a trusted certification authority and install the server certificate on the Web server, you need to assign the server certificate to the Web site.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

▶ **To assign a server certificate to a Web site**

1. In IIS Manager, expand the local computer, and then expand the **Web Sites** folder.
2. Right-click the Web site or file that you want, and then click **Properties**.
3. Depending on whether you are configuring a Web site or a file, select either the **Directory Security** or **File Security** tab, and under **Secure communications**, click **Server Certificate**.
4. In the Web Server Certificate Wizard, click **Assign an existing certificate**.
5. Follow the steps in the Web Server Certificate Wizard, which guides you through the process of installing a server certificate.
6. You can view the information about the certificate by clicking the **View Certificate** button on the **Directory Security** or **File Security** tab of the Web site's **Properties** page.

---

## Back Up and Restore Registry Entries

Some COM objects, COM+ objects, Internet Server API (ISAPI) extensions, and other components save configuration information in the Windows registry. If no setup program or provisioning script exists to make the appropriate registry updates during migration, you must manually identify the registry entries and then recreate them on the target server. To accomplish this, once you have identified the registry entries required by the applications currently running on the source server, back up the registry entries on the source server by using the registry editor Regedit.exe. Modify the registry entries in the backup files created by the registry editor to reflect changes in disk volume drive letters or paths to directories, and then restore the updated registry backups to the target server. Restoring the registry entries is accomplished by merging the backup files into the registry on the target server.



### Caution

The registry editor bypasses standard safeguards, allowing settings that can damage your system, or even require you to reinstall Windows. If you must edit the registry, back it up first and see the Registry Reference on the *Microsoft® Windows® Server 2003 Deployment Kit* companion CD or on the Web at <http://www.microsoft.com/reskit>.

▶ **To back up registry entries by using the registry editor**

1. In the **Run** dialog box, type **regedit**, and then click **OK**.
2. In the registry editor, right-click the registry key or subkey that contains the registry entries that you want to back up, and then click **Export**.
3. In the **Export Registry File** dialog box, select a location for the backup registry file. Click **Save** to save the registry file to that location.
4. Close the Registry Editor.

► **To restore registry entries**

1. Copy the backup registry file to any location on the target server.
2. In Windows Explorer, navigate to the backup registry file on the target server, and right-click the file name.
3. Click **Merge**. In the **Registry Editor** message box, click **Yes** to add the information in the file to the registry.
4. Click **OK** to finish.

---

## Back Up and Restore the IIS Metabase

Metabase backup files are copies of the metabase configuration file (MetaBase.xml) and the matching metabase schema file (MBSchema.xml). The metabase can be restored from the backup files by using the metabase configuration backup and restore feature. You can create backup files by using IIS Manager or the command-line script **iisback.vbs**, which is stored in *systemroot\System32*.

The administrator can create a *portable backup* by providing a password that is used by IIS to encrypt the secure metabase properties in the backup files. Encrypting the secure properties in this way allows the backup files to be restored to another computer by using the password. Once a backup is created, the password within the backup file cannot be changed.

When creating a *non-portable backup*, the administrator does not provide a password. Instead, the machine key is used to encrypt secure metabase properties. Because a machine key is unique to the computer it belongs to, a backup created this way can only be restored to the original computer.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc, Iisback.vbs

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

► **To create a portable backup (password required)**

1. In IIS Manager, right-click the local computer, click **All Tasks**, and then click **Backup/Restore Configuration**.
2. Click **Create Backup**.
3. In the **Configuration backup name** box, type a name for the backup file.

4. Select the **Encrypt backup using password** check box, type a password into the **Password** box, and then type the same password in the **Confirm password** box.
5. Click **OK**, and then click **Close**.

The IIS metabase is created in the `systemroot\system32\inetsrv\MetaBack` folder.

▶ **To create a non-portable backup (password not required)**

1. In IIS Manager, right-click the local computer, click **All Tasks**, and click **Backup/Restore Configuration**.
2. Click **Create Backup**.
3. In the **Configuration backup name** box, type a name for the backup file.
4. Click **OK**, and then click **Close**.

The IIS metabase is created in the `systemroot\system32\inetsrv\MetaBack` folder.

▶ **To restore the metabase backup**

1. In IIS Manager, right-click the local computer, click **All Tasks**, and click **Backup/Restore Configuration**.
2. In the **Backups** list box, click the version of the **Automatic Backup** file that you want to restore, and click **Restore**. If prompted for a password, type the password you chose to secure the backup.

The IIS metabase is restored to the location from which it was backed up.

---

## Back Up and Restore the Web Server to a File or Tape

You should back up a Web server before upgrading it or making configuration changes to it. A complete Web server backup includes all Web sites, applications, and data stored on the Web server. For example, before an upgrade, or before you enable client access to a target Web server, perform a complete image backup before you change any of the configuration settings on the existing Web server. The image backup provides a point-in-time snapshot of the Web server. If unforeseen problems occur during the upgrade or configuration process, you can use this backup to restore the Web server to a known configuration.

A backup file can be saved to a hard disk, a floppy disk, or to any other nonremovable or removable media on which you can save a file. Backup files usually have the extension `.bkf`, but you can change it to any extension you prefer.

You should back up all boot and system volumes, including the System State, when you back up the Web server.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** `ntbackup.exe`

## Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

### ► To back up to a file or tape

1. Open **Accessories**, click **System Tools**, and then click **Backup**.
2. Click the **Advanced Mode** link on the Backup or Restore Wizard.
3. Click the **Backup** tab, and then on the **Job** menu, click **New**.
4. In the **Click to select the check box for any drive, folder, or file that you want to back up** text box, click the box next to **System State** and any other items you would like to backup. You should back up all boot and system volumes along with the System State.
5. In **Backup destination**, do one of the following:
  - Choose **File** if you want to back up files and folders to a file. This is selected by default. You will not be able to choose any other option if you do not have a tape drive on your system.
  - or-
  - Click a tape device from the drop-down list if you want to back up files and folders to a tape. You cannot use this option if you do not have a tape device on your system.
6. In **Backup media or file name**, do one of the following:
  - If you are backing up files and folders to a file, type a path and file name for the backup (.bkf) file, or click the **Browse** button to find a file.
  - If you are backing up files and folders to a tape, select the tape you want to use from the drop-down list box.
7. Click **Tools**, and then click **Options** to select any backup options you want, such as the backup type and the log file type. When you have finished selecting backup options in the **Options** dialog box, click **OK**.
8. Click **Start Backup**, and then make any necessary changes to the **Backup Job Information** dialog box.
9. Click the **Advanced** tab if you want to set advanced backup options such as data verification or hardware compression. When you have finished setting advanced backup options, click **OK**.
10. Click **Start Backup** to start the backup operation.

► **To restore the Web server from a file or tape**

1. Open **Accessories**, point to **System Tools**, and then click **Backup**.
2. Click the **Advanced Mode** link on the Backup or Restore Wizard.
3. Click the **Restore and Manage Media** tab, and then in **Expand the desired media item**, **then check the box for the items to restore**, expand the media item that contains the backup file you wish to use, and select the check box next to **System State** for that file. This will restore the System State data along with any other data you have selected for the current restore operation.
4. In **Restore files to**, do one of the following:
  - Click **Original location** if you want the backed up files and folders to be restored to the folder or folders they were in when they were backed up. Skip to step 6.
  - or-
  - Click **Alternate location** if you want the backed up files and folders to be restored to a folder that you designate. This option will preserve the folder structure of the backed up data; all folders and subfolders will appear in the alternate folder you designate.
  - or-
  - Click **Single folder** if you want the backed up files and folders to be restored to a folder that you designate. This option will not preserve the folder structure of the backed up data; the files will appear only in the folder that you designate.
5. If you selected **Alternate location** or **Single folder**, type a path for the folder under **Alternate location**, or click the **Browse** button to find the folder.
6. On the **Tools** menu, click **Options**, click the **Restore** tab, and then do one of the following:
  - Click **Do not replace the file on my computer** if you do not want the restore operation to copy over files that are already on your hard disk.
  - or-
  - Click **Replace the file on disk only if the file on disk is older** if you want the restore operation to replace older files on your disk with newer files from your backup.
  - or-
  - Click **Always replace the file on my computer** if you want the restore operation to replace files on your disk regardless of whether the backup files are newer or older.
7. Click **OK** to accept the restore options you have set.
8. Click **Start Restore**.
9. Click the **Advanced** tab if you want to change any advanced restore options, such as restoring security settings and junction point data. When you are done setting advanced restore options, click **OK**.
10. Click **OK** to start the restore operation.



## Configure an ASP.NET Application for ASP.NET

By default, when the Microsoft®.NET Framework is installed on a computer with an existing .NET Framework installation, most Microsoft ASP.NET applications are automatically updated to use the newly installed version. The exceptions are applications that are bound to an incompatible or later version of the .NET Framework. Although later versions of the .NET Framework are designed to be backward compatible, you might need to configure an ASP.NET application to use an earlier version, if it cannot run successfully on a later version of the .NET Framework.

When multiple versions of the .NET Framework are executing side-by-side on a single computer, the ASP.NET ISAPI version script that is mapped to an ASP.NET application determines which version of the common language .NET Framework is used for the application. The following sections describe the process for configuring an ASP.NET application to target a specific version of the .NET Framework.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

### Viewing the Script Map for an ASP.NET Application

When managing a computer with multiple versions of the .NET Framework installed, it is often useful to view the script map for an ASP.NET application to determine which version is used by the application.

#### ► To view the script map for an ASP.NET application

1. Open IIS Manager, expand the local computer, and navigate to the Web site folder that contains the ASP.NET application.
2. Right-click the Web site folder, and then click **Properties**.

3. In the **Properties** dialog box, on the **Home Directory** tab, click the **Configuration** button.
4. In the **Application Configuration** dialog box, on the **Mappings** tab, select an ASP.NET application extension, such as .asmx or .aspx.

The **Executable Path** column of the dialog box lists the path to the ASP.NET ISAPI version used by the selected application type. By default, the ASP.NET ISAPI is installed in the following location:

*systemroot\Microsoft.NET\Framework\versionNumber*

The version number shown in the path indicates the version number of the ASP.NET ISAPI used by the application type. The first two digits of the ASP.NET ISAPI version number are the same as the first two digits of the version number of the .NET Framework used by the application.

## Configure an ASP.NET Application for ASP.NET

When the .NET Framework is installed on a computer with an existing .NET Framework installation, by default all ASP.NET application script maps are automatically updated to use the newly installed version. To make it easier to reconfigure the script map for an ASP.NET application, each installation of the .NET Framework comes with an associated version of the ASP.NET IIS Registration tool (Aspnet\_regiis.exe). Administrators can use Aspnet\_regiis.exe to remap an ASP.NET application to the correct version of ASP.NET.



### Note

Because Aspnet\_regiis.exe is linked to a specific version of the .NET Framework, administrators must use the appropriate version of Aspnet\_regiis.exe to reconfigure the script map for an ASP.NET application.

Aspnet\_regiis.exe can also be used to display the status of all installed versions of ASP.NET, register the associated version of ASP.NET, create client-script directories, and perform other configuration operations.

### ► To use Aspnet\_regiis.exe to update a script map for an ASP.NET application

1. In the **Run** dialog box, type **cmd**, and then click **OK**.
2. At the command prompt, use the **cd** command to change to the directory of the Aspnet\_regiis.exe version you want to use. Remember that each version of the .NET Framework comes with its own version of Aspnet\_regiis.exe. By default, Aspnet\_regiis.exe is located in the following directory:

*systemroot\Microsoft.NET\Framework\versionNumber*

You can check to see which version you are running by using the procedure “To view the script map for an ASP.NET application” earlier in this section.

3. Run **Aspnet\_regiis.exe** using the **-s** or **-sn** option along with the path to the application to set up the script maps. The following command-line example updates the script maps for an application called SampleApp1.

```
Aspnet_regiis.exe -s W3SVC/1/ROOT/SampleApp1
```



#### Note

The **-s** and **-sn** options allow you to install scriptmaps for ASP.NET at the specified path recursively (**-s**), which copies the scriptmaps to the subfolders, or nonrecursively (**-sn**), which does not copy the scriptmaps to the subfolders.

#### ► To get a list of the options available for Aspnet\_regiis.exe

- At the command prompt in the folder where **Aspnet\_regiis.exe** is installed, type:

```
aspnet_regiis ?.
```

A list of options available for use with **Aspnet\_regiis.exe** displays.

## Configure Anonymous User Identity

When the Web sites and applications running on the Web server require anonymous access, IIS must be configured with a user account specifically for anonymous access. This user account can be stored in the local account database on the Web server or in a domain.

If, prior to upgrade, the anonymous user identity is configured to use an account stored in a domain you must configure the anonymous user identity to use the same domain-based account after the upgrade. This is necessary because the upgrade process automatically configures IIS to use the default anonymous user account **IUSR\_computername**, where *computername* is the name of the computer on which IIS is running. You can configure the anonymous user identity to use the domain-based user account through IIS Manager. If the anonymous user identity does not use an account stored in a domain, it can be configured to use an account stored in the local account database on the Web server.

#### ► To configure the account used for Anonymous authentication

1. In IIS Manager, expand the local computer, right-click the site, directory, or file that you want to configure, and then click **Properties**.
2. Click the **Directory Security** or **File Security** tab, depending on the level for which you are changing the security settings.
3. In the **Authentication and access control** section, click **Edit**.
4. Select the **Enable anonymous access** check box.
5. Type the valid Windows user account you want to use for Anonymous access, or click **Browse** to locate it.
6. Click **OK** twice.

## Configure a Web Site to be FrontPage Extended

FrontPage 2002 Server Extensions from Microsoft provides Web-based and command-line administration for extending Web sites. *Extending* a Web site means enabling various FrontPage 2002 Server Extensions features to improve how you manage the content development and security of your site. Extending Web sites with FrontPage 2002 Server Extensions enables the Web site owner to author the site in the Microsoft® FrontPage® web site creation and management tool and delegate Web site ownership and administration credentials. After a Web site is extended, a FrontPage client can open the Web site and author it in FrontPage.

Before you can use FrontPage 2002 Server Extensions, you must create one or more Web sites to contain them. An extended Web site, formerly known as a virtual server, is an IIS Web site that receives additional functionality when it is extended by FrontPage Server Extensions. By default, IIS provides a working extended Web site called **Default Web Site**. This extended Web site points to the content directory `systemroot\inetpub\Wwroot`.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** `iis.msc`.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetpub\iis.msc"**.

Before extending a site, check to make sure that the FrontPage 2002 Server Extensions optional component is installed. In Control Panel, click **Add or Remove Programs**, and then click Windows Components Wizard. If the FrontPage 2002 Server Extensions component is not installed, add it by using the following procedure.

#### ► To add the FrontPage 2002 Server Extensions component

1. In the **Windows Components Wizard** select **Application Server**, and then click **Details**.
2. In the **Application Server** subcomponents list, select **Internet Information Services**, and then click **Details**.
3. In the IIS subcomponents list, select the check box for **FrontPage 2002 Server Extensions**, and then click **OK** to complete the Windows Components Wizard and install FrontPage 2002 Server Extensions. You might need your Windows Server 2003 installation CD to complete the installation.

► **To extend a site by using the FrontPage Server Extensions 2002 Server Administration tool**

1. Open Administrative Tools, and then click **Microsoft SharePoint Administrator**.  
If the FrontPage 2002 Server Extensions optional component is not installed IIS returns error 404, "The page cannot be found." In this case, add the FrontPage 2002 Server Extensions component by using the procedure described earlier in this section.
2. On the **FrontPage Server Extensions 2002 Server Administration** site, verify that the extended Web site you created is listed in the **Virtual Servers** section.
3. To extend the Web site, click the **Extend** link next to the extended Web site name.
4. Click **Submit**. The **FrontPage Server Extensions 2002 Server Administration** tool adds FrontPage 2002 Server Extensions template directories to the content directory of your extended Web site, and adds other files that contain metadata.

---

## Configure Application Identity for IIS 5.0 Isolation Mode

If you are running Internet Information Services (IIS) 6.0 in IIS 5.0 isolation mode, you also need to configure application identities for IIS 5.0 isolation mode. On your Microsoft® Windows® Server 2003–based server running in IIS 5.0 isolation mode, configure the application identity to the same settings as were set up on your server running IIS 5.0. You can do this by modifying the identity property of the COM+ object created for the Web site.

► **To configure Web site and application process identities in IIS 5.0**

1. In the **Run** dialog box, type **mmc**, and then click **OK** to start the Microsoft Management Console (MMC).  
If the Component Services Snap-in is not already loaded, on the **File** menu, click **Add/Remove Snap-in**, and then click **Add**. Under **Available Standalone Snap-ins**, click **Component Services**, and then click **Add**. Click **Close** and then click **OK**.
2. In MMC, in the console tree, expand **Component Services**, expand **Computers**, expand **My Computer**, and then expand **COM+ Applications**.
3. Right-click **IIS Out-of-Process Pooled Applications** and then click **Properties**.
4. Click the **Identity** tab.
5. In **User**, type the user name. In the **Password** and **Confirm password** text boxes, enter the password for the user account. To look up a valid user name, click **Browse**.
6. Click **OK**.

## Configure Application Isolation Modes

You can run Internet Information Services (IIS) 6.0 in one of two modes: *worker process isolation mode* or *IIS 5.0 isolation mode*. Worker process isolation mode is the default mode the Web server runs in after a clean installation of the Microsoft® Windows® Server 2003 operating system. IIS 5.0 isolation mode is the default mode when you upgrade to IIS 6.0 from a previous version of IIS. Administrators should only run IIS in IIS 5.0 isolation mode when applications on the server are determined to be incompatible with worker process isolation mode.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

## Configuring IIS for Worker Process Isolation Mode

To complete the following procedure, you must restart IIS, which will temporarily interrupt the World Wide Web Publishing Service (WWW service).

### ► To configure IIS for worker process isolation mode

1. In IIS Manager, expand the local computer, right-click **Web Sites**, and then click **Properties**.
2. Click the **Service** tab, clear the **Run WWW service in IIS 5.0 isolation mode** check box, and then click **OK**.
3. To start the WWW service, click **Yes** when asked if you want to restart IIS now.

If the switch to worker process isolation mode is successful, a folder named Application Pools appears in the IIS Manager listing for your local computer. You can quickly determine which isolation mode IIS is running because the Application Pools folder is present in worker process isolation mode and absent in IIS 5.0 isolation mode.

## Configuring IIS for IIS 5.0 Isolation Mode

After you complete the following procedure, you must restart the WWW service, which will temporarily interrupt the service.

### ► To configure IIS for IIS 5.0 isolation mode

1. In IIS Manager, expand the local computer, right-click **Web Sites**, and then click **Properties**.
2. Click the **Service** tab, select the **Run WWW service in IIS 5.0 isolation mode** check box, and then click **OK**.
3. To start the WWW Service, click **Yes** when asked if you want to restart IIS now.

## Configure Application Isolation Settings for IIS 5.0 Isolation Mode

*Isolating* applications means configuring them to run in a process (memory space) that is separate from the Web server core (the core components required to run Internet Information Services (IIS), such as IISAdmin, the metabase, and so on) and other applications. You can configure applications into one of three levels of application protection:

- Low (IIS process)
- Medium (pooled)
- High (isolated)

Note that server-side includes (SSI), Internet Database Connector (IDC), and other InProcessISAPIApps applications (special applications that must be run in process) cannot be run in medium or high isolation.

### Requirements

- **Mode:** This feature of IIS 6.0 is available only when IIS is running in IIS 5.0 isolation mode.
- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

#### ► To set or change the level of application protection

1. In IIS Manager, expand the local computer, right-click the Web site or the starting-point directory for the application you want to configure, and then click **Properties**.
2. Click the **Home Directory**, **Virtual Directory**, or **Directory** tab, depending on whether you are configuring a Web site, a virtual directory, or an application.
3. In the **Application protection** box, click the appropriate level of protection, and then click **OK**.

The Web server finishes processing any current requests for the application before it creates a separate process. At the next request for the application, the application will run in the appropriate memory space.

## Configure Application Pool Health

Monitoring the health of a worker process includes detecting whether the worker process is able to serve requests and then taking appropriate action. For example, if a worker process fails to respond to a ping request by the World Wide Web Publishing Service (WWW service), the worker process probably does not have threads available for processing incoming requests. You can monitor the health condition of an application pool by pinging the worker processes assigned to it at regular intervals. When a configurable unhealthy condition occurs, you can also set the following features to take corrective action:

- Rapid-fail protection
- Startup time limit
- Shutdown time limit

### Requirements

- **Mode:** This feature of Internet Information Services (IIS) 6.0 is available only when IIS is running in worker process isolation mode.
- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** `iis.msc`.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

Consider the following when setting the configuration for recycling the worker processes assigned to an application pool:

- Worker process pinging is enabled by default. Adjust the ping interval to get timely information about application pool health without triggering false unhealthy conditions.
- When the WWW service detects that a worker process fails more than a set maximum number of times in a set time period, it places the worker process in a rapid-fail protection state. Placing application pools in rapid-fail protection state protects the availability of other applications on the server.
- When the WWW service detects that a worker process is unhealthy, it marks the worker process for termination. Within configured time limits, IIS terminates the worker process. It is important to tune the shutdown time period to fit the load characteristics of the applications that are being processed.
- After IIS terminates an unhealthy worker process, it starts a new worker process to replace the unhealthy one. It is important to tune the startup time period to fit the overlap desired between the unhealthy worker process and the new worker process.



- ▶ **To configure worker process pinging**
  1. In IIS Manager, expand the local computer, right-click the application pool you want to configure, and then click **Properties**.
  2. On the **Health** tab, select the **Enable pinging** check box.
  3. In the text box to the right of **Ping worker process every (frequency in seconds)**, type the number of seconds to elapse before the worker process is pinged, and then click **OK**.
- ▶ **To configure rapid-fail protection**
  1. In IIS Manager, expand the local computer, right-click the application pool you want to configure, and then click **Properties**.
  2. On the **Health** tab, select the **Enable rapid-fail protection** check box.
  3. In the text box to the right of **Failures**, type the maximum number of failures allowed.
  4. In the box to the right of **Time period (in minutes)**, type the elapsed time, in minutes, during which the number of failures is counted, and then click **OK**.
- ▶ **To configure startup and shutdown time limits**
  1. In IIS Manager, expand the local computer, right-click the application pool you want to configure, and then click **Properties**.
  2. On the **Health** tab, under **Startup time limit**, in the text box to the right of **Worker process must startup within (time in seconds)**, type the time, in seconds, to elapse before starting up a new worker process.
  3. On the **Health** tab, under **Shutdown time limit**, in the text box to the right of **Worker process must shutdown within (time in seconds)**, type the time, in seconds, to elapse before shutting down a failing worker process, and then click **OK**.

---

## Configure Application Pool Identity

The identity of an application pool is the name of the service account under which the application pool's worker process runs. By default, application pools operate under the Network Service user account, which has low-level user access rights. You can configure application pools to run under the Local System user account, which is an account with more user rights than the Network Service or Local Service user accounts. However, be mindful that running an application pool under an account with increased user rights presents a high security risk.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- This feature of Internet Information Services (IIS) 6.0 is available only when IIS is running in worker process isolation mode.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

By default, application pools operate under the Network Service user account, which has low-level user access rights. Consequently, this account provides better security against attackers or malicious users who might attempt to take over the computer on which the World Wide Web Publishing Service (WWW service) is running. The Local Service user account has low access rights as well, and is useful for situations that do not require access to resources on remote computers. You can, however, configure application pools to run under the Local System user account, which is an account with more user rights than the Network Service or Local Service user accounts.

► **To change the service account that an application pool runs under**

1. In IIS Manager, expand the local computer, and expand **Application Pools**.
2. Right-click the application pool you want to configure, and then click **Properties**.
3. Click the **Identity** tab, and click either **Predefined** or **Configurable**.

**Predefined** refers to standard service accounts, such as Network Service (the default), which has low-level user access rights that can be used for access to resources on remote computers, Local Service, which has low-level access rights, and is used for situations that do not require access to resources on remote computers, or, Local System, which is an account with more user rights than the Network Service or Local Service account.

**Configurable** refers to registered user names.

4. If you click **Predefined**, click a predefined account in the list box.
5. If you click **Configurable**, in the **User name** and **Password** boxes, type the user name and password of the account under which you want the worker process to operate.
6. Click **OK**.

---

## Configure Application Pool Performance

In worker process isolation mode, Internet Information Services (IIS) 6.0 can be configured to optimize the performance of an application pool, allowing you optimize the performance of your Web applications. Some of the ways to accomplish this include configuring an application pool to limit the size of its request queue, enabling CPU monitoring to allow the server to take action when CPU usage exceeds maximum CPU use, configuring the server to shut down a worker process after being idle for a specified number of minutes, and creating a Web garden, which is an application pools with more than one worker process assigned. Setting these configurations helps you manage the resources on a Web server.

## Requirements

- **Mode:** This feature of IIS 6.0 is available only when IIS is running in worker process isolation mode.
- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

## Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

When performance is degraded by too many requests or by problem applications, and you want to configure the application pool to improve the performance of the worker processes assigned to the pool, consider the following:

- When an application pool receives requests faster than it can handle them, the requests might consume all of the application pool's memory. This could happen when the requests queue size limit is large and legitimate requests are coming in at a rapid rate, or during a denial of service attack. To prevent requests from consuming all of an application pool's memory, limit the size of the request queue for the application pool.
- When problem applications consume excessive CPU resources, you need a way to manage them. In worker process isolation mode, you can enable CPU monitoring, configure CPU limits, and direct IIS to take action when a worker process exceeds the CPU limit set for it.
- Web gardens are application pools with more than one worker process assigned. Create a Web garden to achieve more robust performance when resources often get tied up with a single worker process, or when you need to smooth out the handling of a workload.

### ► To configure idle timeout

1. In IIS Manager, expand the local computer, right-click the application pool you want to configure, and then click **Properties**.
2. On the **Performance** tab, under **Idle Timeout**, select the **Shutdown worker process after being idle for (time in minutes)** check box.
3. In the text box to the right of **Shutdown worker process after being idle for (time in minutes)**, type the number of minutes to elapse before the worker process is recycled, and then click **OK**.

### ► To configure a request queue limit

1. In IIS Manager, expand the local computer, right-click the application pool you want to configure, and then click **Properties**.
2. On the **Performance** tab, select the **Limit the kernel request queue (number of requests)** check box.
3. In the text box to the right of **Limit the kernel request queue (number of requests)**, type the maximum number of requests to allow in the request queue, and then click **OK**.

▶ **To configure CPU monitoring**

1. In IIS Manager, expand the local computer, right-click the application pool you want to configure, and then click **Properties**.
2. On the **Performance** tab, select the **Enable CPU monitoring** check box.
3. In the box to the right of **Maximum CPU use (percentage)**, type the percent maximum CPU threshold.
4. In the text box to the right of **Refresh CPU usage numbers (in minutes)**, type the number of minutes before the CPU usage numbers are refreshed.
5. In the drop-down list box below **Action performed when CPU usage exceeds maximum CPU use**, select the action to take, and then click **OK**.

▶ **To configure a Web garden**

1. In IIS Manager, expand the local computer, right-click the application pool you want to configure, and then click **Properties**.
2. On the **Performance** tab, under **Web garden**, in the **Maximum number of worker processes** text box, type the number of worker processes to assign to the application pool., and then click **OK**

---

## Configure Application Pool Recycling


Internet Information Services (IIS) can be configured to periodically restart worker processes assigned to an application pool, which recycles faulty Web applications. Recycling keeps problematic applications running smoothly, especially when it is not feasible to modify the application code. Recycling helps ensure that problematic applications do not cause other applications to fail, and that system resources can be recovered from unhealthy applications. Use the “Configure Application Pool Health” procedure earlier in this appendix to configure worker process shutdown and startup times to ensure that applications do not experience downtime.

### Requirements

- **Mode:** This feature of IIS 6.0 is available only when IIS is running in worker process isolation mode.
- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname “mmc %systemroot%\system32\inetmgr\iis.msc”**.

- ▶ **To recycle a worker process immediately on demand**
    1. In IIS Manager, expand the local computer.
    2. Expand **Application Pools**.
    3. Right-click the appropriate application pool you want to recycle, and then click **Recycle**.
  - ▶ **To configure a worker process to be recycled after a set elapsed time**
    1. In IIS Manager, expand the local computer, and expand **Application Pools**.
    2. Right-click the application pool you want to configure, and then click **Properties**.
    3. On the Recycling tab, select the **Recycle worker processes (in minutes)** check box.
    4. In the text box to the right of the **Recycle worker processes (in minutes)**, type the number of minutes that you want to elapse before the worker process is recycled, and then click **OK**.
  - ▶ **To configure a worker process to be recycled after a set number of processing requests**
    1. In IIS Manager, expand the local computer, and expand **Application Pools**.
    2. Right-click the application pool you want to configure, and then click **Properties**.
    3. On the **Recycling** tab, select the **Recycle worker process (number of requests)** check box.
    4. In the text box to the right of the **Recycle worker process (number of requests)**, type the number of requests to be processed before the worker process is recycled, and then click **OK**.
  - ▶ **To configure a worker process to be recycled at scheduled times**
    1. In IIS Manager, expand the local computer, expand **Application Pools**.
    2. Right-click the application pool you want to configure, and then click **Properties**.
    3. On the Recycling tab, select the **Recycle worker processes at the following times** check box.
    4. Click **Add** to add a time to the list, **Remove** to delete a time, or **Edit** to change an existing time when the worker process is recycled, and then click **OK**.
- 
- Note**
- When recycling is set to occur at scheduled times, it may occur off-schedule if the system time is manually altered. To avoid unintended changes in the time that recycling occurs, recycle the scheduled worker processes soon after the system time is changed.
- ▶ **To configure a worker process to be recycled after consuming a set amount of memory**
    1. In IIS Manager, expand the local computer, and expand **Application Pools**.
    2. Right-click the application pool you want to configure, and then click **Properties**.

3. On the Recycling tab, under Memory recycling, select the Maximum virtual memory (in megabytes) check box.
4. In the text box to the right of **Maximum virtual memory (in megabytes)**, type the maximum amount of virtual memory allowed before the worker process is recycled.
5. Select the Maximum used memory (in megabytes) check box.
6. In the text box to the right of **Maximum used memory (in megabytes)**, type the maximum amount of memory allowed before the worker process is recycled, and then click **OK**.

---

## Configure FrontPage Server Roles

The configuration of Internet Information Services (IIS) and the Web sites on the source server might reference user accounts that are stored in the local account database on the source server. These accounts stored locally on the Web server are known as *local user accounts*. Local user accounts are only valid on the Web server where they exist, not on other Web servers. When you migrate your Web site to another server, these local user accounts must be recreated on the target server. Once the user accounts have been created, the roles that were assigned to the user accounts on the source server must be assigned to the user accounts on the target server.

You can manage roles from the **Site Administration** page for your Web site. On this page you can view a list of roles, change which rights are included in a role, add a new role, and delete a role.

- ▶ **To add a user account and assign FrontPage server roles to it**
  1. Open Administrative Tools, and click **Microsoft SharePoint Administrator**.
  2. On the **Server Administration** page, click the name of the extended Web site for which you want to assign user roles.
  3. On the **Site Administration** page for the Web site, click **Manage users**.
  4. On the **Manage Users** page, click **Add a user**.
  5. On the **Add a User** page, in the **User** section, click **Add user or group name (For example, DOMAIN\name)**, and enter a user name in the format *LocalComputerName\UserAccountName*.
  6. In the **User Role** section, select the check boxes for all roles that apply to this user account, and then click **Add User**.
- ▶ **To assign FrontPage server roles to an existing user account**
  1. Open Administrative Tools, and click **Microsoft SharePoint Administrator**.
  2. On the **Server Administration** page, click the name of the extended Web site for which you want to assign user roles.
  3. On the **Site Administration** page for the Web site, click **Manage users**.

4. On the **Manage Users** page, click the name of the user for which you need to change the roles.
5. On the **Edit User Role Membership** page, next to **User Role**, select the check box for every role that applies to this user, and then click **Submit**.

---

## Configure FTP Server Authentication

Internet Information Services (IIS) supports the following File Transfer Protocol (FTP) authentication methods:

- Anonymous FTP authentication
- Basic FTP authentication

Available authentication settings must be set at the site level for FTP sites. FTP service is not enabled by default in IIS 6.0.



### Important

If you change the security settings for your FTP site or virtual directory, your Web server prompts you for permission to reset the security settings for the child nodes of that site or directory. If you choose to accept these settings, the child nodes inherit the security settings from the parent site or directory.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

## Enable Anonymous FTP Authentication

If you select Anonymous FTP authentication to secure FTP resources, all requests for that resource are accepted without prompting the user for a user name or password. For Anonymous authentication, IIS automatically creates a Windows user account called IUSR\_*computername*, where *computername* is the name of the server on which IIS is running. If you have both Anonymous FTP authentication and Basic FTP authentication enabled, IIS tries to use the Anonymous FTP authentication user account first.

### ► To enable the Anonymous FTP authentication method

1. In IIS Manager, right-click the FTP site, directory, virtual directory, or file you want to configure, and click **Properties**.
2. Click the **Security Accounts** tab.

3. Select the **Allow anonymous connections** check box.
4. To allow your users to gain access by Anonymous authentication only, select the **Allow only anonymous connections** check box.
5. In the **User name** and **Password** boxes, enter the Anonymous logon user name and password you want to use, and then click OK

The user name is the name of the anonymous user account, which is typically designated as **IUSR\_computername**.



#### Note

If the default **IUSR\_computername** account will not be used for Anonymous FTP authentication, you must create a Windows user account appropriate for the authentication method. For more information about creating a new user account, see the procedure “Create a Service Account” in this chapter.

6. Set the appropriate NTFS permissions for the anonymous account.

For more information about setting NTFS permissions, see the procedure “Configure NTFS Permissions” earlier in this appendix.

## Enable Basic FTP Authentication

If you select the Basic FTP authentication method to secure your FTP resources, users must log on with a user name and password corresponding to a valid Windows user account. If the FTP server cannot verify a user’s identity, the server returns an error message. Basic FTP authentication provides only low security because the user transmits the user name and password across the network in an unencrypted form.

### ► To enable the Basic FTP authentication method

1. Create a Windows user account appropriate for the authentication method. If appropriate, add the account to a Windows user group.

For more information about creating a new user account, see the procedure “Create a Service Account” earlier in this appendix.

2. Configure NTFS permissions for the directory or file for which you want to control access.

For more information about setting NTFS permissions, see the procedure “Configure NTFS Permissions” earlier in this appendix.

3. In IIS Manager, right-click the FTP site, directory, virtual directory, or file you want to configure, and click **Properties**.
4. Click the **Security Accounts** tab.
5. Clear the **Allow anonymous connections** check box, and then click **OK**.



## Configure IIS Components and Services

**Add or Remove Programs** helps you manage programs and components on Microsoft® Windows® Server 2003 and Internet Information Services (IIS) 6.0. As you enable and disable the IIS protocols and services, you correspondingly increase and decrease the attack surface of the Web server.



### Tip

You can also add Windows components by using the Configure Your Server Wizard.

### ► To configure IIS components and services

1. In Control Panel, open **Add or Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. On the Windows Components Wizard page, under **Components**, click **Application Server**, and then click **Details**.
4. Click **Internet Information Services (IIS)**, and then click **Details**.
5. Enable or disable the appropriate IIS components and services by selecting the check box to add the component or clearing the check box to remove the component.
6. Complete the Windows Components Wizard by following the instructions in the wizard.

---

## Configure IP Address Assigned to Web Sites

You can configure your Web site to use a unique IP address that uniquely identifies the Web site.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

### ► To configure the IP address assigned to a Web site

1. In IIS Manager, expand the local computer, right-click the Web site you want to configure, and then click **Properties**.
2. Click the **Web Site** tab, and then click the drop-down arrow next to **IP Address**.
3. Click the IP address you want to use from the drop-down list of IP addresses, and then click **OK**.

## Configure IP Address and Domain Name Restrictions

You can configure your Web site to grant or deny specific computers, groups of computers, or domains access to Web sites, directories, or files.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

## Configure Restrictions Based on IP Address

You can use IIS Manager to grant or deny access to Web sites or applications for a computer or group of computers.

### Grant or deny access to resources for a single computer

You can either deny or grant access for a single computer based upon its IP address.

#### ► To grant access to resources for a computer

1. In IIS Manager, expand the local computer, right-click a Web site, directory, or file you want to configure, and click **Properties**.
2. Click the **Directory Security or File Security** tab. In the IP address and domain name restrictions section, click **Edit**.
3. Click **Granted access**.
4. When you select **Granted access**, you grant access to all computers and domains, except to those that you specifically deny access.
5. Click **Add**.
6. Click **Single computer**.
7. Click **DNS Lookup** to search for computers or domains by name, rather than by IP address.

8. Type the DNS name for the computer. IIS searches on the current domain for the computer, and if found, enters its IP address in the IP address box.

The following information is important to remember when using the **DNS Lookup** feature:

- Server performance decreases while DNS addresses are being looked up.
- A user accessing your Web server through a proxy server will appear to have the IP address of the proxy server.
- Some user server access problems can be corrected by using the “\*.domainname.com” syntax rather than the “domainname.com” syntax.

9. Click **OK** three times.

### ► To deny access to resources for a computer

1. In IIS Manager, expand the local computer, right-click a Web site, directory, or file you want to configure, and click **Properties**.
2. Click the **Directory Security** or **File Security** tab. In the **IP address and domain name restrictions** section, click **Edit**.
3. Click **Denied access**.

When you select **Denied access**, you deny access to all computers and domains, except to those that you specifically grant access.

4. Click **Add**.
5. Click **Single computer**.
6. Click **DNS Lookup** to search for computers or domains by name, rather than by IP address.
7. Type the DNS name for the computer.

IIS searches on the current domain for the computer, and if found, enters its IP address in the **IP address** box.

The following information is important to remember when using the **DNS Lookup** feature:

- Server performance decreases while DNS addresses are being looked up.
- A user accessing your Web server through a proxy server will appear to have the IP address of the proxy server.
- Some user server access problems can be corrected by using the “\*.domainname.com” syntax rather than the “domainname.com” syntax.

8. Click **OK** three times.

### **Grant or deny access to resources for a group of computers**

A group of computers can be either denied or granted access based upon their network ID and a subnet mask. The network ID is the IP address of a host computer, usually a router for the *subnet*. The subnet mask determines which part of the IP address is a subnet ID, and which part is a host ID. All computers in a subnet have the same subnet ID, but have their own unique host ID. By specifying a network ID and a subnet mask, you can select a group of computers.

▶ **To grant access to resources for a group of computers**

1. In IIS Manager, expand the local computer, right-click a Web site, directory, or file you want to configure, and click **Properties**.
2. Click the **Directory Security** or **File Security** tab. In the **IP address and domain name restrictions** section, click **Edit**.
3. Click **Granted access**.  
When you select **Granted access**, you grant access to all computers and domains, except to those that you specifically deny access.
4. Click **Add**.
5. Click **Group of computers**.
6. In the **Network ID** box, type the IP address of the host computer.
7. In the **Subnet mask** box, type the subnet ID for the computer you want grant or deny access to.
8. Click **OK** three times.

▶ **To deny access to resources for a group of computers**

1. In IIS Manager, expand the local computer, right-click a Web site, directory, or file you want to configure, and click **Properties**.
2. Click the **Directory Security** or **File Security** tab. In the **IP address and domain name restrictions** section, click **Edit**.
3. Click **Denied access**.  
When you select **Denied access**, you deny access to all computers and domains, except to those that you specifically grant access.
4. Click **Add**.
5. Click **Group of computers**.
6. In the **Network ID** box, type the IP address of the host computer.
7. In the **Subnet mask** box, type the subnet ID for the computer you want grant or deny access to.
8. Click **OK** three times.

## **Configure Restrictions Based on Domain**

Access to resources for a domain can be granted or denied by using IIS Manager.

▶ **To grant access to resources for a domain**

1. In IIS Manager, expand the local computer, right-click a Web site, directory, or file you want to configure, and click **Properties**.
2. Click the **Directory Security** or **File Security** tab. In the **IP address and domain name restrictions** section, click **Edit**.

3. Click **Granted access**.

When you select **Granted access**, you grant access for all computers and domains, except for those that you specifically deny access.

4. Click **Add**.
5. Click **Domain name**. You will see a warning message saying that “Restricting access by domain name requires a DNS reverse lookup on each connection. This is a very expensive operation and will dramatically affect server performance.” Click **OK** to close the message dialog box.
6. In the **Domain name** box, type the domain name.
7. Click **OK** three times.

► **To deny access to resources for a domain**

1. In IIS Manager, expand the local computer, right-click a Web site, directory, or file you want to configure, and click **Properties**.
2. Click the **Directory Security** or **File Security** tab. In the **IP address and domain name restrictions** section, click **Edit**.
3. Click **Denied access**.

When you select **Denied access**, you deny access for all computers and domains, except for those that you specifically grant access.

4. Click **Add**.
5. Click **Domain name**.
6. In the **Domain name** box, type the domain name.
7. Click **OK** three times.

---

## Configure MIME Types

Internet Information Services (IIS) serves only static files with extensions registered in the Multipurpose Internet Mail Exchange (MIME) types list. IIS is preconfigured to recognize a default set of global MIME types, and also allows you to configure additional MIME types and change or remove MIME types. These MIME types are recognized by all Web sites you create in IIS.

MIME types can also be defined at the Web site and directory levels, independent of one another or the types defined globally. When you view MIME types at the Web site or directory level, only the types unique to that level are displayed, not all types inherited from the next level up. If you apply a MIME type at the global level after modifying the same MIME type at a lower level, the global-level MIME type overrides the modified MIME type at the lower level.

When IIS delivers a mail message to a mail application, or a Web page to a client Web browser, it also sends the MIME type of the data it is sending. If there is an attached or embedded file in a specific format, IIS tells the client application the MIME type of the embedded or attached file. The client application then knows how to process or display the data being received from IIS. IIS returns error 404.3 if a client request refers to a file name extension that is not defined in the MIME types.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

#### ► To add a global MIME type

1. In IIS Manager, right-click the local computer, and click **Properties**.
2. Click the **MIME Types** button.
3. Click **New**.
4. In the **Extension** box, type the file name extension.
5. In the **MIME type** box, type a description that exactly matches the file type defined on the computer.



#### Note

You can also create a MIME type for files without an extension or for undefined MIME types. This is not recommended.

6. Click **OK**.

#### ► To add a MIME type to a Web site or directory

1. In IIS Manager, right-click the Web site or Web site directory for which you want to add a MIME type, and click **Properties**.
2. Click the **HTTP Headers** tab.
3. Click **Mime Types**.
4. Click **New**.
5. In the **Extension** box, type the file name extension.
6. In the **MIME type** box, type a description that exactly matches the file type defined on the computer. If you define a MIME type that has already been defined at a higher level, you are prompted to select the level where the MIME type should reside.
7. Click **OK**.

► **To remove a MIME type from a Web site or directory**

1. In IIS Manager, right-click the Web site or Web site directory from which you want to remove a MIME type, and click **Properties**.
2. Click the **HTTP Headers** tab.
3. Click **Mime Types**.
4. From the **Registered MIME types** list, click the MIME type you want to remove, and then click **Remove**.
5. Click **OK** three times.

---

## Configure NTFS Permissions

Use NTFS permissions to define the level of access to your directories and files that you want to grant to specific users and groups of users. Proper configuration of file and directory permissions is crucial for preventing unauthorized access to your resources.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

► **To secure a Web site by using NTFS permissions**

1. In IIS Manager, expand the local computer, right-click the Web site or file you want to configure, and click **Permissions**.
2. To add a group or user that does not appear in the **Group or user names** list box, click **Add**, and in the **Enter the object names to select** text box, type the name of the user or group. Click **OK**.  
-OR-
3. To change or remove permissions from an existing group or user, click the name of the group or user in the **Group or user names** list box.
4. To allow or deny a permission such as **Read & Execute**, **List Folder Contents**, **Read**, or **Write**, in the **Permissions for group or user name** list box, select the **Allow** or **Deny** check box next to the appropriate permission, and then click **OK**.



### Important

Inherited Deny permissions do not prevent access to an object if the object has an explicit Allow permission entry. Explicit permissions take precedence over inherited permissions, including inherited Deny permissions.

With NTFS permissions, you also have the choice of assigning special permissions to groups or users. Special permissions are permissions on a more detailed level. For better management, you should assign broad-level permissions to users or groups, where it is applicable. For descriptions of permissions, see “Permissions for files and folders” in Help and Support Center for Windows Server 2003.

▶ **To secure a Web site using NTFS special permissions**

1. In IIS Manager, expand the local computer, right-click a Web site or file you want to configure, and click **Permissions**.
2. Click **Advanced**, and then do one of the following on the **Permissions** tab:
  - To set special permissions for an additional group or user, click **Add**, and in the **Enter the object name to select** text box, type the name of the user or group. Click **OK**.
  - To view or change special permissions for an existing group or user, click the name of the group or user, and then click **Edit**.
  - To remove an existing group or user and its special permissions, click the name of the group or user and then click **Remove**. If the **Remove** button is unavailable, clear the **Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries exclusively defined here.** check box, and then click **Remove**. Click **OK** and skip steps 3-6 below.
3. To allow or deny a permission such as **Read & Execute**, **List Folder Contents**, **Read**, or **Write**, in the **Permissions** list box, select the **Allow** or **Deny** check box next to the appropriate permission.
4. In the **Apply onto** list box, click the folders or subfolders you want these permissions to be applied to.
5. To prevent the subfolders and files from inheriting these permissions, clear the **Apply these permissions to objects and/or containers within this container only** check box, and then click **OK** three times.



### Important

It is recommended that you assign permissions to the highest-level folders as possible and then apply inheritance to propagate the settings to lower-level subfolders and files. For more information on inheritance, see “How inheritance affects file and folder permissions” in Help and Support Center for Windows Server 2003.

---

## Configure the State Service on the ASP.NET State Server

The ASP.NET state service is used to manage session state on a computer. The ASP.NET state service is installed by default when Microsoft® Windows® Server 2003 is installed. The file `aspnet_state.exe` is installed on the remote server that will store session state information; the default location is `systemroot\Microsoft.NET\Framework\version\aspnet_state.exe`.



► **To configure the ASP.NET state service**

1. On the remote server that will store session state information, open Administrative Tools, and then click **Services**.
2. In the details pane, right-click **ASP.NET State Service**, and then click **Properties**.
3. On the **General** tab, in the **Startup type** list box, click **Automatic**.
4. Under **Service status**, click **Start**, and then click **OK**. The state service starts automatically when the Web server is restarted.

---

## Configure the Registry

If a registry entry must be created or modified to correctly configure the server, you can edit the entry directly using the registry editor Regedit.exe.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Regedit.exe.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr.msc"**.



### Caution

Do not edit the registry unless you have no alternative. The registry editor bypasses standard safeguards, allowing settings that can damage your system, or even require you to reinstall Windows. If you must edit the registry, back it up first and see the Registry Reference on the *Microsoft Windows Server 2003 Deployment Kit* companion CD or on the Web at <http://www.microsoft.com/reskit>.

► **To create a new registry entry by using the registry editor**

1. In the **Run** dialog box, type **regedit**, and then click **OK**.
2. In the registry editor, navigate to the key or subkey under which you wish to add an entry and select the name of the key or subkey by clicking on it.
3. On the **Edit** Menu, point to **New** and then click the data type for the entry, such as **String Value**, **Binary Value**, or **DWORD Value**.
4. In the details pane, type the name of the registry entry, and then press ENTER to create the entry.

5. To assign a value to the registry entry, right-click the entry and then click **Modify**. If the entry has been defined as **Binary Value**, click **Modify Binary Data** instead.
6. In the **Edit ValueType Value** dialog box, type an appropriate value in the **Value data** text box. Type or select the value of other options, such as the base (hexadecimal or decimal) for DWORD values, and then click **OK**.

► **To configure an existing registry entry by using the registry editor**

1. In the **Run** dialog box, type **regedit**, and then click **OK**.
2. In the registry editor, navigate to the registry entry that you want to modify.
3. In the details pane, right-click the entry, and click **Modify**. If the entry has been defined as **Binary Value**, then click **Modify Binary Data** instead.
4. In the **Edit ValueType Value** dialog box, type an appropriate value in **Value data**. Type or select the value of other options, such as the base (hexadecimal or decimal) for DWORD values, and then click **OK**.

---

## Configure the Web Site Identification Number

When a new site is created on Internet Information Services (IIS) 6.0, a Web site identification number is randomly generated based on the name of the Web site. In this way, Web sites of the same name usually generate the same Web site identification for IIS 6.0 servers in a Web farm. With IIS 5.0 and earlier versions, Web site identification numbers were incremental. For example, because the default Web site is created first, its site identification number is 1, and the next site to be created is identified as 2.

If you have administrative scripts that depend upon the IIS 5.0 method of generating Web site identification numbers, you can edit the registry entry **IncrementalSiteIDCreation** in the Windows registry to force IIS to use the incremental method of generating Web site identification numbers.



### Note

When you remotely administer a server running IIS, the value of the **IncrementalSiteIDCreation** registry entry on the local server is used to determine the generation of Web site identification numbers on the remote server.

### Requirements

- **Credentials:** Membership in the Administrators group on the local and on the remote computer is required to make changes to the remote computer's registry. Network policy settings might prevent you from completing this procedure.
- **Tools:** Regedit.exe.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.



#### Caution

Do not edit the registry unless you have no alternative. The registry editor bypasses standard safeguards, allowing settings that can damage your system, or even require you to reinstall Windows. If you must edit the registry, back it up first and see the Registry Reference on the *Windows Server 2003 Deployment Kit* companion CD or on the Web at <http://www.microsoft.com/reskit>.

#### ► To configure the IncrementalSiteIDCreation registry entry

1. To open the registry editor, in the **Run** dialog box, type **regedit**, and then click **OK**.
2. Expand **HKEY\_LOCAL\_MACHINE**, expand **SOFTWARE**, expand **Microsoft**, expand the **InetMGR** subkey, and then click **Parameters**.
3. Under **Parameters**, in the details pane, click **IncrementalSiteIDCreation**. If the entry does not exist, create it by doing the following:
  - Select **Parameters** by clicking on it.
  - On the **Edit** Menu, point to **New**, and then click **DWORD Value**.
  - Type **IncrementalSiteIDCreation** and press **ENTER** to create the entry.
4. With the entry **IncrementalSiteIDCreation** selected, on the **Edit** menu, click **Modify**.
5. In the **Value data** box, type **1** to force IIS to use the incremental method of generating Web site identification numbers, and then click **OK**.

---

## Configure Web Server Authentication

You can set the authentication method for your Web resources with property sheets at the Web site, directory, or file level by using IIS Manager.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** *Iis.msc*.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

► **To configure Web server authentication**

1. In IIS Manager, right-click the **Web Sites** folder, Web site, directory, virtual directory, or file, and click **Properties**.



**Note**

Configuration settings made at the Web Sites folder level can be inherited by all Web sites

2. Click the **Directory Security** or **File Security** tab, depending upon the level at which you are configuring security settings.
3. In **Authentication and access control**, click **Edit**.
4. To configure Integrated Windows authentication, in **Authenticated access**, select the **Integrated Windows authentication** check box.
5. To configure Digest authentication, in **Authenticated access**, select the **Digest authentication for Windows domain servers** check box.
6. To configure **Advanced Digest authentication**, in the **Realm** text box, type the realm name, or click **Select** to browse for a domain.



**Note**

If Basic authentication is enabled for the site, virtual directory, or folder you are configuring, the **Default domain** text box will also be available. However, **Realm** is only meaningful for **Advanced Digest authentication**.

7. To configure Basic authentication, In the **Authenticated access** section, select the **Basic authentication (password is sent in clear text)** check box. Because **Basic authentication** sends passwords over the network unencrypted, a dialog box appears asking if you want to proceed. Click **Yes** to proceed. In the **Default domain** box, either type the domain name you want to use, or click **Select** to browse to a new default logon domain.
8. To configure .NET Passport authentication, select the **.NET Passport Authentication** check box. When .NET Passport authentication is selected, all other authentication methods are unavailable. .NET Passport cannot be used with other authentication methods because it validates user credentials in a fundamentally different way.
9. Click **OK** twice.

## Configure Web Service Extensions

In order to take a more proactive stance against malicious users and attackers, Internet Information Services (IIS) is not installed on members of the Microsoft® Windows® Server 2003 family by default. Furthermore, when you initially install IIS, it is installed in a highly secure mode. By default, IIS serves only static content — features such as ASP, ASP.NET, server-side includes, WebDAV publishing, and FrontPage 2002 Server Extensions from Microsoft do not work unless they are specifically enabled. You can configure these features, also called Web service extensions, through the Web Service Extensions node in IIS Manager.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

#### ► To enable and disable a Web service extension

1. In IIS Manager, expand the local computer, and then click **Web Service Extensions**.
2. In the details pane, click the Web service extension that you want to enable or disable.
3. To enable a disabled Web service extension, click **Allow**.
4. To disable an enabled Web service extension, click **Prohibit**.

A message box with a list of applications that will be prevented from running on the IIS Web server displays.

5. Click **OK** to disable the Web service extension.

To use, or to deny the use of, an HTTP request handler that is not in the list of Web service extensions, you must first register it by adding the HTTP request handler to the list of Web service extensions.

#### ► To add new Web service extensions

1. In IIS Manager, expand the computer name, and then click **Web Service Extensions**.
2. In the details pane, click Add a new Web service extension.
3. In the **Extension name** text box, type the name of the new Web service extension, and then click **Add**.
4. In the **Path to file** text box, type the path or click **Browse** to navigate to any files that the new Web service extension requires, and then click **OK**.

5. Optionally, select the **Set extension status to Allowed** check box to automatically set the status of the new Web service extension to **Allowed**.
6. Click **OK** to add the new Web service extension.

▶ **To delete Web service extensions**



**Note**

You cannot delete built-in extensions. You can delete only extensions that you have added to the Web extension list.

1. In IIS Manager, expand the computer name, and then click **Web Service Extensions**.
2. In the details pane, right click the Web Service Extension you want to delete, and then click **Delete**.
3. Click **Yes** to confirm the deletion.

You can also use IIS Manager to specify the applications that are allowed to call Web service extensions.

▶ **To allow an application to call Web service extensions**

1. In IIS Manager, expand the local computer, and then click **Web Service Extensions**.
2. In the details pane, click **Allow all Web service extensions for a specific application**.
3. From the **Application** list box, click the name of the application.

The Web service extension that the application is allowed to call appears in the **Extensions to be allowed** box.

4. Click **OK** to allow the application to call Web service extensions.

You can disable all Web service extensions that are registered on the local computer with one setting in the Web Service Extension node of IIS Manager.

▶ **To disable all Web service extensions**

1. In IIS Manager, expand the local computer, and then click **Web Service Extensions**.
2. Click **Prohibit all Web service extensions**. The following message appears:  
If you prohibit all extensions, all Web service extensions in the list will be prohibited. This may prevent applications from running on your IIS Web server. Do you want to prohibit all extensions?
3. To disable all extensions, click **Yes**. To cancel the action, click **No**. For more information, click **Help**.
4. If you click **Yes**, the status of each Web service extension is **Prohibited**.

## Configure Web Site Permissions

You can configure access permissions for specific Web sites, directories, and files. Unlike NTFS permissions, Web permissions affect everyone who tries to access your Web site. Web site permissions are not meant to be used in place of NTFS permissions, but are used in conjunction with them.



### Note

If Web site permissions conflict with NTFS permissions for a directory or file, the more restrictive settings are applied.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

#### ► To set permissions for Web content

1. In IIS Manager, right-click the **Web Sites** folder, Web site, directory, virtual directory, or file you want to configure, and click **Properties**.
2. On the **Home Directory, Virtual Directory, or File** property sheet, select or clear any of the following check boxes (if available), depending on the type of access you want to grant or deny:
  - **Script Source Access.** Users can access source files. If **Read** is selected, source can be read, if **Write** is selected, source can be written to. **Script Source Access** includes the source code for scripts. This option is not available if neither **Read** nor **Write** is selected.
  - **Read** (selected by default). Users can view directory or file content and properties.
  - **Write.** Users can change directory or file content and properties.
  - **Directory browsing.** Users can view file lists and collections.
  - **Log visits.** A log entry is created for each visit to the Web site.
  - **Index this resource.** Allows Indexing Service to index this resource. This allows searches to be performed on the resource.

3. In the **Execute Permissions** list box, select the appropriate level of script execution:
  - **None** Do not run scripts or executables on the server.
  - **Scripts only** Run only scripts on the server.
  - **Scripts and Executables** Run both scripts and executables on the server.
4. Click **OK**. If child nodes for a directory have different Web site permissions configured, the **Inheritance Overrides** box appears.
 

If a child node belonging to the directory whose Web site permissions you have changed has also set the Web site permissions for a particular option, the permissions in the child node will override those you have set for the directory. If you want the Web site permissions at the directory level to apply to the child nodes, you must select those child nodes in the **Inheritance Overrides** box.
5. If the **Inheritance Overrides** box appears, select the child nodes in the **Child Nodes** list to which you want the directory's Web permissions to apply. You can also click **Select All** to set the property to apply the Web permissions to all child nodes.
6. You might see more than one **Inheritance Overrides** box if more than one property has been defined in the child nodes of the directory. Select the child nodes from the **Child Nodes** list or click **Select All**, and then click **OK** to apply the Web permissions for this property to the child nodes.

---

## Configure Windows Server 2003 Services

You can use Add or Remove Programs in Control Panel to add or remove Microsoft® Windows® Server 2003 services, and you can use the Services console to enable or disable services. As you add and remove Windows Server 2003 services and enable and disable services, you increase and decrease the attack surface of the Web server correspondingly.



### Tip

You can also add Windows Server 2003 services by using the Configure Your Server Wizard.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.



▶ **To add or remove Windows Server 2003 services**

1. From Control Panel, click **Add or Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. On the Windows Components Wizard page, in the **Components** box, select or clear the check box next to the component to enable or disable the appropriate Windows Server 2003 services. You may need to select a higher level component and then click **Details** to locate the component you wish to add or remove.
4. Click **Next** to run the Windows Components Wizard.
5. Follow the instructions in the Windows Components Wizard to complete the addition or removal of the component.



**Note**

You may need to have your Windows Server 2003 CD-ROM available to complete the installation of the component.

▶ **To enable or disable Windows Server 2003 services**

1. Open Administrative Tools, and then click **Services**.
2. In the details pane, right-click the Windows Server 2003 service that you want to change, and then click **Properties**.
3. On the **General** tab, in the **Startup type** list box, click one of the following:
  - **Automatic.** The service starts automatically when the Web server is restarted.
  - **Manual.** The service can be started manually by an administrator or by another service.
  - **Disabled.** The service cannot be started by an administrator or by another service unless the startup type is changed to **Automatic** or **Manual**.
4. Click **OK** to save the changes.

---

## Convert Existing Disk Volumes to NTFS

The command-line tool **Convert.exe** converts FAT and FAT32 volumes to the NTFS file system, leaving existing files and folder intact. Volumes converted to the NTFS file system cannot be converted back to FAT or FAT32.

**Requirements**

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Convert.exe

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

#### ► To convert FAT and FAT32 volumes to NTFS

- In the **Run** dialog box, type **convert** followed by the appropriate syntax, and then click **OK**.

### Syntax

```
convert [Volume] /fs:ntfs
```

### Parameters

Volume

Specify the drive letter (followed by a colon), mount point, or volume name to convert to NTFS. Required if the volume to be converted is not the current volume.

/fs:ntfs

Required. Converts the volume to NTFS.

## Create a Service Account

A service account is a user account that is created explicitly to provide a security context for services running on Microsoft® Windows® Server 2003. Application pools use service accounts to assign permissions to Web sites and applications running on Internet Information Services (IIS). Administrators can manage service accounts individually to determine the level of access for each application pool in a distributed environment.

Use Active Directory Users and Computers to create service accounts in the Active Directory® directory service. Use Computer Management to create local service accounts on a local computer.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Active Directory Users and Computers; Computer Management.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

#### ► To create a service account in Active Directory

1. Open Administrative Tools, and then click **Active Directory Users and Computers**.
2. In the console tree, double-click the **Domain** node.

3. In the **Details** pane, right-click the organizational unit where you want to add the service account, point to **New**, and then click **User**.
4. In **First name**, type a first name for the service account.
5. In **Last name**, type a last name for the service account.
6. Modify **Full name** as desired.
7. In **User logon name**, type the name that the service account will log on with and, from the drop-down list, click the UPN suffix that must be appended to the service account logon name (following the @ symbol). Click **Next**.
8. In **Password** and **Confirm password**, type a password for the service account.
9. Select the appropriate password options, and then click **Next**.
10. Click **Finish** to complete creating a service account.

▶ **To create a service account on the local Web server**

1. Open Administrative Tools, and then click **Computer Management**.
2. In the console tree, expand **System Tools**, expand **Local Users and Groups**, and then click **Users**.
3. On the **Action** menu, click **New User**.
4. Type a **User name**, **Full name**, and a **Description** of the user account.
5. In **Password** and **Confirm password**, type a password for the user account.
6. Set the user account access by selecting the check box to set the option or clearing the check boxes to remove the option for:
  - **User must change password at next logon**
  - **User cannot change password**
  - **Password never expires**
  - **Account is disabled**
7. Click **Create**, and then click **Close**.

▶ **To create a service account for IIS\_WPG Group**

1. Open Administrative Tools, and then click **Computer Management**.
2. In the console tree, expand **System Tools**, expand **Local Users and Groups**, and click **Groups**.
3. Click the IIS\_WPG group and, on the **Action** menu, click **Add to Group**.
4. Under **Description**, type the name of the account and click **Add**.
5. In the **Select Users** dialog box, click the **Object Types** button, and select or clear the check box for the object types you want to find. Click **OK**.

6. Click the **Locations** button to select the location of the service account. Click **OK**.
7. Enter the name of the object under **Enter the object names to select**.
8. Click **OK**, and then click **OK** again.

---

## Create A SQL Server Database for Storing ASP.NET Session State

ASP.NET SQL state server is used to manage session state on a computer running Microsoft® SQL Server™. All versions of Microsoft ASP.NET that are installed on the same computer share the same SQL state server. The SQL state server version of session state that is used is always the one that is installed with the latest version of ASP.NET. When this version of ASP.NET is uninstalled, the latest remaining version on the computer is then registered and used in its place.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

### ► Create an ASP.NET session state database with SQL Server Enterprise Manager

1. On the **Start** menu, point to **Programs**, point to **Microsoft SQL Server**, and then click **Enterprise Manager**.
2. In **SQL Server Enterprise Manager**, connect to the server running SQL Server that will store the session state.
3. On the **Tools** menu, click **SQL Query Analyzer**.
4. In SQL Query Analyzer, on the **File** menu, click **Open**, and navigate to **InstallSqlState.sql** (the SQL script that builds the ASP.NET session state database).

The InstallSqlState.sql file is located on the Web server in **systemroot\Microsoft.NET\Framework\version** (where *version* is the most recent version number of the .NET Framework installed on the Web server).

5. On the **Query** menu, click **Execute**.  
Ensure the query completed with no errors by reviewing the status in the lower window of the SQL Query Analyzer.
6. Close SQL Query Analyzer.
7. In **SQL Server Enterprise Manager**, in the console tree, expand the server node, and then click **Databases**.
8. In the details pane, verify that **ASPState** is listed.
9. Close SQL Server Enterprise Manager.

## Create a Virtual Directory

In most cases, the content you publish to your Web site is located in a home directory on your computer, such as C:\inetpub\Wwwroot\. However, there might be instances when the content is located in another directory, or even on a remote computer.

To be able to publish content from any directory not contained within your home directory, you must create a *virtual directory*. A virtual directory is a directory that is not contained in the home directory but appears to client browsers as though it were. You can create a virtual directory by using IIS Manager or by using Windows Explorer.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

#### ► To create a virtual directory by using IIS Manager

1. In IIS Manager, expand the **Web Sites** folder, and expand the Web site to which you want to add a virtual directory.
2. Right-click the Web site or folder within which you wish to create the virtual directory, select **New**, and then click **Virtual Directory**. The Virtual Directory Creation Wizard appears.
3. Click **Next**.
4. In the **Alias** box, type a name for the virtual directory. This is the name the user types, and should be short and easy to type.
5. Click **Next**.
6. In the **Path** box, type the name of the physical directory or click **Browse** to navigate to the physical directory in which the content for the virtual directory resides.
7. Click **Next**.
8. Under **Allow the following permissions**, select the check boxes for the access permissions you want to assign to your users, and then click **Next**.



#### Note

For security purposes, when selecting access permissions, consider allowing only the default **Read** permission. By restricting permissions in this way, you can mitigate potential attacks against your Web site by malicious users.

9. Click **Finish**. The virtual directory is created below the currently selected folder level.

► **To create a virtual directory by using Windows Explorer**

1. Open Windows Explorer.
2. Right-click the folder you want to be a virtual directory, and select **Sharing and Security**.
3. On the **Web Sharing** tab, click **Share this folder**.
4. On the **Edit Alias** dialog box, in the **Alias** box, type the name for the virtual directory.
5. Under **Access permissions**, select the check boxes for the type of access you want to assign to the virtual directory.
6. Under **Application permissions**, select the check boxes for the type of application access you want to assign to the virtual directory.
7. Click **OK**, and then click **OK** again.

---

## Create a Web Site

During installation of Internet Information Services (IIS), a default home directory and Web site configuration are created on your hard disk. Similarly, creating a Web site by using IIS Manager does not create content, but merely creates a directory structure and configuration files from which to publish the content. To publish your Web content, you can place content in the default home directory, or you can create a different home directory or virtual directory and place content there.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

► **To use the default Web site**

1. In IIS Manager, expand the local computer, and expand the **Web Sites** folder.
2. Right-click **Default Web Site**, and select **Properties**.
3. On the **Web Site** tab, under **Web site identification**, type the name of your Web site in the **Description** box.
4. Click **OK**. The new name of the site appears in IIS Manager.

► **To create a new Web site**

1. In IIS Manager, expand the local computer, and right-click the **Web Sites** folder.
2. Select **New**, and then click **Web Site**. The Web Site Creation Wizard appears.

3. Click **Next**.
4. In the **Description** box, type a name for your site, and then click **Next**.
5. Type or select the IP address (the default is **All Unassigned**), TCP port, and host header (for example, *www.mysite.com*) for your site.
6. Click **Next**.
7. In the **Path** box, type the name of the directory or click **Browse** to navigate to the directory that contains, or will contain, the site content.
8. Click **Next**.
9. Select the check boxes for the Web site access permissions you want to assign to your users, and then click **Next**.
10. Click **Finish**.
11. o change these and other settings later, right-click the Web site, and select **Properties**.

---

## Debug Application Pool Failures

To enable *orphaning* of a worker process serving an application pool (which keeps failed applications running while your diagnostic tools monitor them), and to attach a debugger to the worker process, you must change the values of three metabase properties. The values of these metabase properties, which are set by running a script, must be specified as follows:

- Set the **OrphanWorkerProcess** metabase property to TRUE to notify the WWW service to orphan the worker process when it fails.
- Set the **OrphanActionExe** metabase property to specify an executable to run when the worker process is orphaned.
- Set the **OrphanActionParams** metabase property to configure command-line parameters for attaching the debugger to the worker process.

Consider the following guidelines when you enable debugging of application pool failures:

- Debugging requires that you set all three metabase properties outlined above; enabling debugging is ineffective until you attach a debugger.
- When you no longer want to use the debugging feature, disable it. Putting an application in orphan state wastes resources if the diagnostics are not running or will not be used.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

#### ► To enable and configure debugging on a worker process

1. Copy the following ADSI script (written in VBScript) into a text editor or word processor.

```
set appPoolObj=GetObject("IIS://localhost/W3svc/AppPools/app pool name")
` Set the application pool properties:
appPoolObj.Put "OrphanWorkerProcess", TRUE
appPoolObj.Put "OrphanActionExe", "full path\ntsd.exe"
appPoolObj.Put "OrphanActionParams", "-g -p %1%"
` Save the property changes in the metabase:
appPoolObj.SetInfo
WScript.Echo "After: " & appPoolObj.OrphanWorkerProcess & ", " &
appPoolObj.OrphanActionExe & ", " & OrphanActionParams
```

2. Save the file with the extension .vbs.
3. In the **Run** dialog box, type **cmd**, and then click **OK**.
4. At the command prompt, run the script by typing the following command:

```
cscript //nologo filename
```

where *filename* is the fully qualified path of the script file.

– or –

You can call the script by using a batch file that contains the following command:

```
"cscript //nologo filename"
```

where *filename* is the fully qualified path of the script file.

---

## Determine Web Sites Uniquely Identified by IP Addresses

You can determine whether you have any Web sites that are uniquely identified with an IP address by viewing the Properties sheet of the Web sites on your source server.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.



**5.0** ▶ **To determine Web sites that are uniquely identified by an IP address in IIS**

1. Open Administrative Tools, and then click **Internet Service Manager**.
2. In IIS Manager, expand the server, right-click the Web site, and then click **Properties**.
3. On the **Web Site** tab, under **IP Address**, note whether there is a specific IP address assigned to this Web site. A specific IP address entry in this box denotes a uniquely identified Web site.

**4.0** ▶ **To determine Web sites that are uniquely identified by an IP address in IIS**

1. Click **Start**, click **Programs**, click **Windows NT 4.0 Option Pack**, click **Microsoft Internet Information Server**, and then click **Internet Service Manager**.
2. In Internet Service Manager, expand the server, right-click the Web site, and then click **Properties**.
3. On the **Web Site** tab, under **IP Address**, note whether there is a specific IP address assigned to this Web site. A specific IP address entry in this box denotes a uniquely identified Web site.

---

## Disable Network Adapters

To ensure that clients cannot connect to the Web server while it is being upgraded, disable the network adapter that connects the Web server to the clients before taking it offline for the upgrade.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** none

▶ **To disable the network adapter for IIS 5.0**

1. Click **Start**, click **Settings**, and then click **Network Connections**.
2. Locate the network adapter that connects the Web server to the clients.
3. Right-click the network adapter, and then click **Disable**.

▶ **To disable the network adapter for IIS 4.0**

1. In Control Panel, double-click **Network**.
2. On the **Bindings** tab, click the network adapter, click **Disable**, and then click **OK**.

## Enable ASP.NET

A server running a member of the Microsoft® Windows® Server 2003 family supports application server functionality, with Microsoft ASP.NET as an option that you can enable when configuring the application server role. To deploy ASP.NET Web applications to a production server, you must be sure to enable the ASP.NET and Internet Information Services (IIS) roles on the production server before you distribute the application.



### Note

If you want to install ASP.NET on a domain controller, there are special steps you must take to make the installation work properly. For more information, see article 315158, "ASP.NET Does Not Work with the Default ASPNET Account on a Domain Controller," in the Microsoft Knowledge Base. To find this article, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

ASP.NET, along with the .NET Framework version 1.1, is included with Windows Server 2003. You need to install it by using Add or Remove Programs, or enable it by using the Configure Your Server Wizard.



### Note

When you use the Configure Your Server Wizard or the **Add or Remove Programs** dialog box to install ASP.NET on a server running Windows Server 2003, ASP.NET is automatically enabled in IIS Manager. However, if you install ASP.NET from a Web download or as part of an application such as Microsoft® Visual Studio®.NET, you must enable ASP.NET manually, as described later in this section.

### ► To enable ASP.NET on a server running Windows Server 2003 by using the Configure Your Server wizard

1. Click **Start**, and then click **Manage Your Server**.
2. In the **Manage Your Server** window, click **Add or remove a role**.
3. In the Configure Your Server wizard, click **Next**.
4. In the **Server Role** dialog box, click **Application Server (IIS, ASP.NET)** and then click **Next**.
5. In the **Application Server Options** dialog box, select the **Enable ASP.NET** check box.
6. Click **Next**, and then click **Next** again.
7. If you are prompted to do so, insert your Windows Server 2003 installation CD in the CD-ROM drive, and then click **Next**.
8. When the installation is complete, click **Finish**.

► **To enable ASP.NET on a server running Windows Server 2003 by using Add or Remove Programs**

1. In Control Panel, click **Add or Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. In the **Components** box in the Windows Components Wizard, select the **Application Server** check box, and then click **Details**.
4. In the **Application Server** dialog box, select the **ASP.NET** check box, and then click **OK**.
5. In the Windows Components Wizard, click **Next** to begin installing ASP.NET.
6. When the Windows Components Wizard has finished configuring Windows Server 2003, click **Finish**.

---

## Enable Logging

You can enable logging for individual Web and File Transfer Protocol (FTP) sites. After you enable logging for a Web or FTP site, all traffic to the site (including virtual directories) is written to the corresponding file for each site. You can also enable logging for specific virtual directories.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

► **To enable logging on a Web or FTP site**

1. In IIS Manager, expand the local computer, expand the **Web or FTP Sites** directory, right-click the Web or FTP Site for which you want to enable logging, and then click **Properties**.
2. On the **Web Site** or **FTP Site** tab, click the **Enable logging** check box.

3. In the **Active log format** list box, click a format. By default, the format is **W3C Extended Log File Format**.



#### Note

If you select Open Database Connectivity (ODBC) logging, click **Properties** and type the ODBC Data Source Name (DSN) and the name of the table within the database into the text boxes. If a user name and password are required to access the database, type the necessary credentials, and click **OK**.

4. Click **Apply**, and then click **OK**.

#### ► To enable logging for a specific virtual directory on a site

1. In IIS Manager, expand the local computer, expand the **Web Sites** directory, right-click the virtual directory, and click **Properties**.
2. On the **Virtual Directory** or **Directory** tab, select the **Log visits** check box if it is not selected. By default, the check box is selected.
3. Click **Apply**, and then click **OK**.

---

## Enable Network Adapters

After you have upgraded the Web server, you are ready to enable client access to the Web sites. During the upgrade process, you disabled the network adapter on the Web server to prevent users from accessing the Web server during the upgrade process. Now that you know the upgrade completed successfully, you can enable the network adapters.

#### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** none.

#### ► To enable the network adapter for IIS 6.0

1. In Control Panel, click **Network Connections**, and then click **Local Area Connection**.
2. The network adapter is automatically enabled.

---

## Enable Security Auditing

Microsoft® Windows® Server 2003 uses security and system logs to store collected security events. Before enabling the system and security logs, you need to enable auditing for the system log and establish the number of events you want recorded in the security log. You customize system log events by configuring *auditing*. Auditing is the process that tracks the activities of users and processes by recording selected types of events in the security log of the Web server. You can enable auditing based on categories of security events such as:

- Any changes to user account and resource permissions.
- Any failed attempts for user logon.

- Any failed attempts for resource access.
- Any modification to the system files.

The most common security events recorded by the Web server are associated with user accounts and resource permissions.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Microsoft Management Console (MMC); Local Security Policy

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

#### ► To define or modify auditing policy settings for an event category on the local Web server

1. Open Administrative Tools, and then click **Local Security Policy**.
2. In the console tree, click **Local Policies**, and then click **Audit Policy**.
3. In the details pane, double-click an event category for which you want to change the auditing policy settings.
4. On the **Properties** page for the event category, do one or both of the following:
  - To audit successful attempts, select the **Success** check box.
  - To audit unsuccessful attempts, select the **Failure** check box.
5. Click **OK**.

#### ► To define or modify auditing policy settings for an event category within a domain or organizational unit, when the Web server is joined to a domain

This procedure is run on the domain controller.

1. Open Administrative Tools, and then click **Active Directory Users and Computers**
2. Right-click the appropriate domain, site, or organizational unit and then click **Properties**.
3. On the **Group Policy** tab, select an existing Group Policy object to edit the policy.
4. In **Group Policy Object Editor**, in the console tree, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local policy**, and then click **Audit Policy**.
5. In the details pane, double-click an event category for which you want to change the auditing policy settings.
6. If you are defining auditing policy settings for this event category for the first time, select the **Define these policy settings** check box.

7. Do one or both of the following:
  - To audit successful attempts, select the **Success** check box.
  - To audit unsuccessful attempts, select the **Failure** check box.
8. Click **OK**.

---

## Enable the WWW Service After Upgrade

When you upgrade a Web server running Internet Information Services (IIS) 5.0 and the Microsoft® Windows® 2000 operating system, the World Wide Web Publishing Service (WWW service) is disabled unless, prior to upgrade, you elected to run the IIS Lockdown Tool or you added the entry **RetainW3SVCStatus** to the registry. However, if neither of those was done, then you need to enable the WWW service after the upgrade.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Microsoft Management Console (MMC); Local Security Policy.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

▶ **To enable the WWW Service after upgrade**

1. Open Administrative Tools, and then click **Services**.
2. In the **Services** pane, double-click **World Wide Web Publishing Service**.
3. On the **Properties** page, on the **General** tab, select **Automatic** from the **Startup Type** drop-down box.
4. Under **Service Status**, click the **Start** button.
5. Click **OK**.

---

## Enable Web Site Content Auditing

Once you have enabled security auditing, you must also enable auditing on the Web site content (files and folders) in order to track any modification or deletion of the content.

Before you set up auditing for files and folders, you must first enable object access auditing. This security setting determines whether to audit the event of a user accessing an object, such as a file, folder, or printer. Enabling object access auditing is accomplished by defining auditing policy settings for the object access event category of the Audit Policies in Local Security Settings. If you do not enable object access auditing, you receive an error message when you set up auditing for files and folders, and no files or folders are audited. After object access auditing is enabled, you can view the security log in Event Viewer to review the results of your changes. You can then set up Web site content auditing.



### Tip

Because the security log is limited in size, carefully select the files and folders to be audited. In addition, consider the amount of disk space that you want to devote to the security log. The maximum size for the security log is defined in Event Viewer.

If file or folder auditing has been inherited from the parent folder, you will see the following.

- In the **Auditing Entry for File or Folder** dialog box, in the **Access** box, the check boxes are unavailable.
- or-
- In the **Advanced Security Settings for File or Folder** dialog box, the **Remove** button is unavailable.

### Requirements

- **Credentials:** You must be logged on as a member of the Administrators group or you must have been granted the **Manage auditing and security log** right in Group Policy to perform this procedure.
- **Tools:** Windows Explorer
- **File system:** To enable auditing of Web site content, the disk volumes on which the Web site is stored must use the NTFS file system.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

- ▶ **To enable object access auditing**
  1. Open Administrative Tools, and then click **Local Security Policy**.
  2. Expand **Local Policies**, and then click **Audit Policy**.
  3. Right-click **Audit object access**, and then click **Properties**.

4. Enable auditing by clicking one of the following:
  - Click **Success** to generate an audit entry when a user successfully accesses an object.
  - Click **Failure** to generate an audit entry when a user unsuccessfully attempts to access an object.
  - If you clear both check boxes, object access auditing is turned off.
5. Click **OK**.

► **To apply or modify auditing policy settings for a local file or folder**

1. Open **Accessories**, and then click **Windows Explorer**.
2. Right-click the file or folder for which you want to set audit policy settings, click **Properties**, and then click the **Security** tab.
3. Click **Advanced**, and then click the **Auditing** tab.
4. Do one of the following:
  - To set up auditing for a new user or group, click **Add**. In **Enter the object name to select**, type the name of the user or group that you want to audit, and then click **OK**.
  - To remove auditing for an existing group or user, click the group or user name, click **Remove**, click **OK**, and then skip the rest of this procedure.
  - To view or change auditing for an existing group or user, click the name of the group or user, and then click **Edit**.
5. In the **Apply onto** box, click the location where you want auditing to take place.
6. In the **Access** box, indicate what actions you want to audit by selecting the appropriate check boxes:
  - To audit successful events, select the **Successful** check box.
  - To stop auditing successful events, clear the **Successful** check box.
  - To audit unsuccessful events, select the **Failed** check box.
  - To stop auditing unsuccessful events, clear the **Failed** check box.
  - To stop auditing all events, click **Clear All**.
7. If you want to prevent subsequent files and subfolders of the original object from inheriting these audit entries, select the **Apply these auditing entries to objects and/or containers within this container only** check box.



## Export a Server Certificate

Web server certificates contain information about the server that allows the client to positively identify the server over a network before sharing sensitive information, in a process called *authentication*. Secure Sockets Layer (SSL) uses these certificates for authentication, and uses encryption for message integrity and confidentiality. SSL is a public key–based security protocol that is used by Internet services and clients to authenticate each other and to establish message integrity and confidentiality.

If you use SSL to protect confidential information exchanged between the Web server and the client, you must migrate or export the certificates and the associated private keys from the source server to the target server.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

#### ► To export a server certificate

1. In the **Run** dialog box, type **mmc**, and then click **OK**. The Microsoft Management Console (MMC) appears.
2. If you do not have **Certificate Manager** installed in MMC, you need to install it.  
For more information on how to add the Certificate snap-in to an MMC console, see the procedure "To add the Certificates Snap-in to MMC" in "Install a Server Certificate" in this appendix.
3. In the console tree, click the logical store where the certificate you want to export exists. Usually this is in the **Certificates** folder in the **Personal** directory under **Certificates (Local Computer)** on the Console Root.
4. Right-click the certificate you want to export, click **All Tasks**, and click **Export** to start the Certificate Export Wizard.
5. Click **Next**.

6. On Export Private Key, click Yes, export the private key.



### Important

You must export the private key along with your certificate for it to be valid on your target server. Otherwise, you will have to request a new certificate for the target server.

7. In the **Export File Format** dialog box, click the format you want for the certificate. If the certificate has already been formatted, that format is selected as the default. Click **Next**.  
Do not select **Delete the private key if export is successful**, because this will disable the SSL site that corresponds to that private key.
8. Continue to follow steps in the wizard, and enter a password for the certificate backup file when prompted. Using a strong password is highly recommended because it ensures that the private key is well protected.
9. Type the name of the file you want to export, or click **Browse** to search for the file. Click **Next**.
10. Click **Finish** to complete the Certificate Export Wizard.

---

## Gather and Display WWW Service Uptime Data

You can use Internet Information Services (IIS) 6.0 Performance Monitor to record and display data about the uptime of World Wide Web Publishing Service (WWW service) and Web sites by using the Service Uptime performance counter. These procedures support the task of determining the availability of the WWW service and Web sites running on IIS.

Use the following procedures to:

- Create a log file to record WWW service uptime data.
- Select a performance counter to generate uptime data for the WWW service and your Web sites.
- Start the Service Uptime performance counter.
- Connect System Monitor to the data in the log file you are using to gather WWW service and Web site uptime data.
- Read the display window in the details panel of System Monitor to display WWW service and Web site uptime data.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Perfmon.msc; Iis.msc.

## Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

## Gathering WWW Service Uptime Data

You can use IIS 6.0 Performance Monitor to create a log file, and to select and start the Service Uptime performance counter.

### ► To gather uptime data on the WWW service and Web sites

1. Open Administrative Tools, and then click **Performance**.
2. In the console pane, click **Performance Logs and Alerts**, and then click **Counter Logs**.
3. Right-click in the details pane, and select **New Log Settings** from the menu.
4. Enter the name you want to use for the new log, for example, **WWWServiceUptime**, and then click **OK**.

The property sheets for the new counter log open.

5. On the **General** tab, click **Add Counters**.
6. In the **Add Counters** window, if the performance counters you want to monitor are on the local computer, click **Use local computer counters**. If the performance counters you want to monitor are on a remote computer, click **Select counters from computer**, and then click the remote computer in the drop-down list.
7. Under **Performance object**, click **Web Service** in the drop-down list.
8. Click **Select counters from list**, and then click the **Service Uptime** counter.
9. Click **All instances**.
10. Click **Add**, and then click **Close**.

The **Service Uptime** counter for the computer you selected displays in the **Counters** window on the **General** tab.

11. Click **OK**.
12. To start logging data, select the log file on the **Performance** detail pane and, on the **Action** menu, click **Start**.
13. The counter log you created displays in green on the **Computer Logs** detail pane.
14. To manually stop logging data, select the log file and, on the **Action** menu, click **Stop**.
15. To start logging data again, select the log file and, on the **Action** menu, click **Start**.

## Displaying WWW Service Uptime Data

Consider the following guidelines for displaying WWW service uptime data:

- This procedure reads a log file that gathers WWW service uptime data. Before you can read the log file, you must create the file and connect it to the performance counter, as described earlier in this section.
- The file logs data for all instances of the Service Uptime performance counter. One instance, named the Total instance, accumulates WWW service data. Each of the other instances accumulates data about a Web site. Each Web site is recorded by a separate instance.

### ► To display data for WWW service uptime and Web site uptime

1. Open Administrative Tools, and click **Performance**.
2. In the console pane, click **System Monitor**.
3. Right-click in the details pane, and then click **Properties**.
4. On the **Source** tab, under **Data Source**, click **Log files**, and then click **Add**.
5. In the **Select Log File** window, navigate to the log file that you created to gather WWW service and Web sites uptime data.
6. Select the log file name from the list, and then click **Open**.
7. Click the **Data** tab, and then click the **Add** button. Under **Performance object**, select **Web Service** from the drop-down list.
8. Click the **Select counter from list** button and click **Service Uptime**.
9. Click the **All instances** button.
10. Click **Add**, and then click **Close**.
11. On the **System Monitor Properties** window, click **OK**.  
The Service Uptime counter instances appear in the list in the **Performance** detail pane.
12. Select the instance desired to view the graph and statistics for WWW Service (“\_Total”), or for each Web site.

---

## Grant User Rights to a Service Account

Typically, the user rights assigned to the IIS\_WPG group is sufficient for most Web sites or applications. However, when a Web site or application requires additional user rights to run properly, you must assign the required rights to the service account that is used as the identity for the Web sites and applications.

You grant user rights based on where the account is stored. If the service account is created locally on the Web server, you make changes in user rights through Local Computer Policy by using the Group Policy Object Editor MMC snap-in. When the service account is created in Active Directory, make the changes on the appropriate Group Policy object in Active Directory.

## Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

## Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

### ► To add the Group Policy Object Editor to MMC

1. In the **Run** dialog box, type **mmc**, and then click **OK**.  
The Microsoft Management Console appears.
2. On the **File** menu, click **Add/Remove Snap-in**.
3. On the **Standalone** tab, click **Add**.
4. In the **Available Standalone Snap-ins** list box, click **Group Policy Object Editor**, and then click **Add**.
5. In the **Select Group Policy Object** dialog box, in **Group Policy Object**, select **Local Computer**, and then click **Finish**.
6. Click **Close**, and then click **OK**.

### ► To grant user rights to a service account when the service account is stored locally on the Web server

1. In MMC, open the **Group Policy Object Editor**.
2. In the console tree, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **User Rights Assignment**.
3. In the details pane, double-click the user right that you want to grant to the service account.
4. In the **user\_right Properties** dialog box (where *user\_right* is the user right you selected in Step 3), click **Add User or Group**.
5. In the **Select Users, Computers, or Group** dialog box, type the name of the service account, and then click **OK**.
6. In the **user\_right Properties** dialog box (where *user\_right* is the user right you selected in Step 3), click **OK**.

### ► To grant user rights to a service account when the service account is stored in Active Directory

1. In MMC, open **Active Directory Users and Computers**.
2. In the console tree, browse to the organizational unit that contains the Group Policy object that you want to modify, right click the organizational unit, and then click **Properties**.
3. In the **organizational\_unit Properties** dialog box (where *organizational\_unit* is the organizational unit you selected in Step 2), click the **Group Policy** tab.

4. Select the Group Policy object that you want to modify, and then click **Edit**.  
The Group Policy Object Editor appears.
5. In the console tree, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **User Rights Assignment**.
6. In the details pane, double-click the user right that you want to grant to the service account.
7. In the *user\_right* **Properties** dialog box (where *user\_right* is the user right you selected in Step 3), click **Add User or Group**.
8. In the **Select Users, Computers, or Group** dialog box, type the name of the service account, and then click **OK**.
9. In the *user\_right* **Properties** dialog box (where *user\_right* is the user right you selected in Step 3), click **OK**.
10. Close the Group Policy Object Editor
11. Click **OK**.

---

## Install a Server Certificate

Web server certificates contain information about the server that allows the client to positively identify the server over a network before sharing sensitive information. This process is called *authentication*. If you use Secure Sockets Layer (SSL) to protect confidential information exchanged between the Web server and the client and you have exported the certificates from the source server to the target server, the server certificate needs to be installed on the Web server. before you can assign the server certificate to Web sites for use with SSL

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Certificates MMC snap-in.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

#### ► To add the Certificates Snap-in to MMC

1. In the **Run** dialog box, type **mmc**, and then click **OK**.  
The Microsoft Management Console appears.
2. On the **File** menu, click **Add/Remove Snap-in**.
3. On the **Standalone** tab, click **Add**.

4. In the **Available Standalone Snap-ins** list box, click **Certificates**, and then click **Add**.
5. Click the **Computer account** option, and then click **Next**.
6. Click the **Local computer (the computer this console is running on)** option, and then click **Finish**.
7. Click **Close**, and then click **OK**.

▶ **To install a server certificate on a Web server**

1. In MMC, open the **Certificates** snap-in.
2. In the console tree, click the logical store where you want to import the certificate.  
The default location of the logical store for certificates is on the Console Root in the **Certificates (Local Computer)/ Personal/Certificates** folder.
3. On the **Action** menu, point to **All Tasks**, and then click **Import** to start the Certificate Import Wizard.



**Important**

You should only import certificates obtained from trusted sources. Importing an altered or unreliable certificate could compromise the security of any system component that uses the imported certificate.

4. Click **Next**.
5. Type the name of the file that contains the certificate to be imported, or click **Browse** and navigate to the file.

Certificates can be stored in several different file formats. The most secure format is Public-Key Cryptography Standard (PKCS) #12, an encryption format that requires a password to encrypt the private key. It is recommended that you send certificates using this format for optimum security.

If the certificate file is in a format other than PKCS #12, skip to step 8.

If the certificate file is in the PKCS #12 format, do the following:

- In the **Password** box, type the password used to encrypt the private key. You must have access to the password that was originally used to secure the file.
- (Optional) If you want to be able to use strong private key protection, select the **Enable strong private key protection** check box, if available.
- (Optional) If you want to back up or transport your keys at a later time, select the **Mark key as exportable** check box.

6. Click **Next**.

7. In the **Certificate Store** dialog box, do one of the following:
  - If the certificate should be automatically placed in a certificate store based on the type of certificate, select **Automatically select the certificate store based on the type of certificate**.
  - If you want to specify where the certificate is stored, select **Place all certificates in the following store**, click **Browse**, and select the certificate store to use.
8. Click **Next**, and then click **Finish**.

The file from which you import certificates remains intact after you have completed importing the certificates. You can use Windows Explorer to delete the file if it is no longer needed.

---

## Install IIS 6.0

You can install Internet Information Services (IIS) 6.0 by using **Add/Remove Windows Components** from Add or Remove Programs in Control Panel.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

► **To install IIS 6.0 using Control Panel**

1. In Control Panel, double-click **Add or Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. In the **Components** list box, click **Application Server**, and then click **Details**.
4. In the **Subcomponents of Application Server** box, click **Internet Information Services (IIS)**.
5. Click **OK** to start the installation of IIS 6.0.

---

## Install Subauthentication

To use Digest authentication in Internet Information Services (IIS) 6.0 when the domain controller is running Microsoft® Windows® 2000, you must enable subauthentication, which is not installed by default on IIS 6.0. There are three requirements for enabling subauthentication:

- Install the subauthentication component, **iissuba.dll**.
- Set the **UseDigestSSP** metabase property to **False**.
- Set the identity of the application pool to **Local System**. For more information about setting application pool identity, see “Ensuring Application Availability” in this book.



Consider the following guidelines for enabling subauthentication:

- The requirement to use subauthentication applies to Digest authentication only. Using Advanced Digest authentication does not require subauthentication.
- When you no longer want to use subauthentication, unregister the sub-authentication component and set the identity of the application pool to Local System.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

#### ► To install and register the subauthentication component

1. In the **Run** dialog box, type **cmd**, and click **OK**.
2. At the command prompt, type:
 

```
rundll32 systemroot\system32\iissuba.dll,RegisterIISSUBA.
```
3. Press ENTER.
4. For any application pools that use Digest authentication, set the application pool identity to **Local System**.

For more information about Digest authentication, see “Configure Web Server Authentication” earlier in this appendix.

For more information on configuring application pool identity, see “Configure Application Pool Identity” earlier in this appendix.

#### ► To unregister the subauthentication component

1. In the **Run** dialog box, type **cmd**, and click **OK**.
2. At the command prompt, type:
 

```
rundll32 systemroot\system32\iissuba.dll,UnregisterIISSUBA
```
3. Press ENTER.

---

## Isolate Applications in Worker Process Isolation Mode

An *application pool* is a configuration that links one or more applications to a set of one or more worker processes. Because applications in an application pool are separated from other applications by worker process boundaries, an application in one application pool is not affected by problems caused by applications in other application pools.

By creating application pools and assigning Web sites and applications to them, you can improve the availability and reliability of your Web sites and applications.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

#### ► To create a new application pool

1. In IIS Manager, expand the local computer, right-click **Application Pools**, click **New**, and then click **Application Pool**.
2. If the ID that appears in the **Application pool ID** box is not the ID that you want, type a new ID.
3. Under **Application pool settings**, click one of the following options:
  - **Use default settings for the new application pool**
  - or-
  - **Use existing application pool as a template.**
4. If you click the **Use existing application pool as template** option, in the drop-down box, click the **Application pool name** of the application pool you want to use as a template..
5. Click **OK**.

#### ► To assign a Web site or application to an application pool

1. In IIS Manager, right-click the application that you want to assign to an application pool, and then click **Properties**.
2. Click the **Virtual Directory**, **Directory**, or **Home Directory** tab, depending on the type of application you have selected.
3. If you are assigning a directory or virtual directory, verify that **Application name** is filled in. If the **Application name** box is not filled in, click **Create**, and then type a name.
4. In the **Application pool** list box, click the name of the application pool to which you want to assign the Web site.
5. Click **OK**.

---

## Make a Service Account a Member of the Local Administrators Group

If an application requires specific user rights to run successfully, but the service account for the application cannot be assigned the appropriate permissions, make the service account a member of the local administrators group. This should give the service account sufficient user rights to allow the application to run successfully.

- **To add a service account to the local administrators group**
1. In Administrative Tools, click **Computer Management**.
  2. In the console tree, expand **Local Users and Groups**, and then click **Groups**.
  3. Right-click the **Administrators** group, and then click **Add to Group**.
  4. Click **Add**.
  5. Click **Look in** to display a list of domains from which users and groups can be added to the group.
  6. In **Location**, click the domain containing the users and computers you want to add, and then click **OK**.
  7. In **Enter the object names to select**, type the name of the user or group you want to add to the group, and then click **OK**.
  8. If you want to validate the user or group names that you are adding, click **Check Names**.

---

## Migrate CDONTS

Collaboration Data Objects (CDO) for Microsoft® Windows NT® Server (CDONTS) has been removed from Microsoft® Windows® Server 2003. If your Web applications use CDONTS, you can modify your code to use Collaboration Data Objects for Windows 2000 (CDOSYS), which is supported by Windows Server 2003. However, if you upgrade to Windows Server 2003, CDONTS remains on your server, because Cdonts.dll is not removed during an upgrade to Windows Server 2003. CDONTS is not installed when you perform a clean installation of Windows Server 2003, but if necessary, you can copy it to the computer running Windows Server 2003 and register it.

- **To copy CDONTS to a computer running Windows Server 2003**
1. On the source server, copy **Cdonts.dll** from the *%systemroot%\system32* folder to a floppy disk.
  2. On the target server, copy **Cdonts.dll** from the floppy disk to the folder *systemroot\system32*.
  3. To register CDONTS, on the target server, in the **Run** dialog box, type **cmd**, and then click **OK**.
  4. At the command prompt, change to the *systemroot\system32* directory, and then type:
 

```
regsvr32 %windir%\system32\cdonts.dll.
```

 If the process is successful, the following message displays:
 

```
DllRegisterServer in cdonts.dll succeeded.
```
  5. Click **OK**.

## Modify the IIS Metabase Directly

If you need to modify the Internet Information Services (IIS) metabase, you can do so directly in the Metabase.xml file by using a text editor. Before you can modify the Metabase .xml file, you must enable the edit-while-running feature of the metabase by using IIS Manager. Once you have made your changes and saved the Metabase.xml file, disable the edit-while-running feature of the metabase. To implement changes to some metabase properties, you might need to restart the server.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

#### ► **To enable the edit-while running feature of the metabase by using IIS Manager**

1. In IIS Manager, right-click the local computer, and then click **Properties**.
2. Select the **Enable Direct Metabase Edit** check box, and then click **OK**.

#### ► **To modify the IIS metabase**

1. Open the Metabase.xml file in a text editor. The default path to this file is `%systemroot%\system32\inetsrv\metabase.xml`
2. Modify the metabase properties that you wish to change in the Metabase.xml file.
3. Save the changes to the file, and close the text editor.

Most changes to metabase properties are automatically recognized by IIS; in some cases, you must restart IIS for the metabase property changes to go into effect.

#### ► **To disable the Edit-while running feature of the metabase by using IIS Manager**

1. In IIS Manager, right-click the local computer, and then click **Properties**.
2. Clear the **Enable Direct Metabase Edit** check box, and then click **OK**.

## Monitor Active Web and FTP Connections

To ensure that service to clients is not interrupted, monitor the Web server for any active Web and File Transfer Protocol (FTP) connections before taking the Web server offline. Internet Information Services (IIS) 4.0, IIS 5.0, and IIS 6.0 include performance monitor counters that can be used to monitor the active Web and FTP connections. Monitor the active Web and FTP connections to ensure one of the following is true:

- The number of active Web and FTP connections is zero.
- All active Web or FTP sessions can be accounted for and can be terminated.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Perfmon.msc, Perfmon.exe.

#### ► To monitor active Web and FTP connections in IIS 6.0

1. Open Administrative Tools, and then click **Performance**.
2. Right-click the **System Monitor details** pane, and then click **Add Counters**.
3. Do one of the following:
  - To monitor any computer on which the monitoring console is run, click **Use local computer counters**.
  - or-
  - To monitor a specific computer, regardless of where the monitoring console is run, click **Select counters from computer**, and specify a computer name or IP address.
4. In **Performance object**, click:
  - **Web Service** to monitor active Web connections.
  - or-
  - **FTP Service** to monitor active FTP connections.
5. Click **Select counters from list**, and select **Current Connections**.
6. Click **All instances**.
7. Click **Add**, and then click **Close**.

#### ► To monitor active Web and FTP connections in IIS 5.0

1. Open Administrative Tools, and then click **Performance**.
2. Right-click the **System Monitor details** pane and then click **Add Counters**.

3. Do one of the following:
  - To monitor any computer on which the monitoring console is run, click **Use local computer counters**.
  - or-
  - To monitor a specific computer, regardless of where the monitoring console is run, click **Select counters from computer**, and specify a computer name or IP address.
4. In **Performance object**, click:
  - **Web Service** to monitor active Web connections.
  - or-
  - **FTP Service** to monitor active FTP connections.
5. Click **Select counters from list**, and then click **Current Connections**.
6. Click **All instances**.
7. Click **Add**, and then click **Close**.

► **To monitor active Web and FTP connections in IIS 4.0**

1. Open Administrative Tools, and then click **Performance Monitor**.
2. Click **Edit**, and then click **Add to Chart**.
3. The local computer is listed in the Computers box. To monitor any other computer on which the monitoring console is run, click the button to the right of **Computers** and select a computer from the **Select Computer** list, and then click **OK**.
4. In **Performance object**, click:
  - **Web Service** to monitor active Web connections.
  - or-
  - **FTP Service** to monitor active FTP connections.
5. In **Counters**, click **Current Connections**.



**Note**

The performance counters are not installed when IIS 4.0 is installed on Microsoft® Windows NT® version 4.0. In this case, if the performance counters have not been manually enabled, they do not appear in the Counters list. For more information about enabling the performance counters, see article 226512, "HOW TO: Reinstall IIS 4.0 Performance Monitor Counters," in the Microsoft Knowledge Base. To find this article, see the Microsoft Knowledge Base link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

6. In **Instances**, click **\_Total**.
7. Click **Add**, and then click **Done**.

---

## Pause Web or FTP Sites

To ensure that service to clients is not interrupted, pause all Web and File Transfer Protocol (FTP) sites on the Web server before taking the server offline. Pausing a site prevents the site from accepting new connections, but does not affect requests that are already being processed. Stopping a site does not interfere with other Internet services that are running.

You can pause a Web or FTP site by using either IIS Manager or a command-line script.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

## Pausing Web Sites

If you pause a Web site, you can temporarily reduce the load on the computer that hosts the site, and can make changes to the folder or document structure of the Web site.

- ▶ **To pause a Web site by using Internet Services Manager in IIS 4.0**
  1. Click **Start**, click **Programs**, click **Windows NT 4.0 Option Pack**, click **Microsoft Internet Information Server**, and then click **Internet Services Manager**.
  2. In Internet Services Manager, right-click the Web site you want to pause, and then click **Pause**.
- ▶ **To pause a Web site by using Internet Services Manager in IIS 5.0**
  1. Open Administrative Tools, and then click **Internet Services Manager**.
  2. In Internet Services Manager, right-click the Web site you want to pause, and then click **Pause**.



### Note

If a site stops unexpectedly, Internet Services Manager might not correctly indicate the state of the site. In IIS, right-click the **Web Sites** folder and then click **Refresh** to see the current state of all Web sites.

## Pausing FTP Sites

- ▶ **To pause an FTP site by using Internet Services Manager in IIS 4.0**
  1. Click **Start**, click **Programs**, click **Windows NT 4.0 Option Pack**, click **Microsoft Internet Information Server**, and then click **Internet Services Manager**.
  2. In Internet Services Manager, right-click the FTP site you want to pause; and then click **Pause**.
  
- ▶ **To pause an FTP site by using Internet Services Manager in IIS 5.0**
  1. Open Administrative Tools, and then click **Internet Services Manager**.
  2. In Internet Services Manager, right-click the FTP site you want to pause, and click **Pause**.



### Note

If a site stops unexpectedly, Internet Services Manager might not correctly indicate the state of the site. In IIS, right-click the **FTP Sites** folder and click **Refresh** to see the current state of all FTP sites.

---

## Publish Web Site Content with FrontPage

FrontPage Server Extensions from Microsoft provides a Web-based administration tool for extending Web sites. *Extending* a Web site means implementing features of FrontPage Server Extensions that enable the site owner to author the site in Microsoft® FrontPage® and delegate Web site ownership and Web site administration credentials. Making content available on an extended Web site is called *publishing* the Web site. A Web site that is not extended cannot be opened or authored in FrontPage.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetrv\iis.msc"**.

### Extending a Web site

You can use the FrontPage 2002 Server Administration tool to extend a Web site.



## ► To extend a Web site by using the FrontPage 2002 Server Administration tool

1. Open Administrative Tools, and then click **Microsoft SharePoint Administrator**.



### Note

If IIS returns error 404, "The page cannot be found," check to make sure FrontPage 2002 Server Extensions is enabled by using **Add or Remove Programs** in Control Panel.

2. On the **FrontPage Server Extensions 2002 Server Administration** site, check to see that the Web site you created is listed in the **Virtual Servers** section.
3. To extend the Web site, click the **Extend** link next to the name of the Web site.
4. To specify an administrator account for the extended Web site, type the administrator name in **Administrator user name**.
5. Click **Submit**.

The **FrontPage 2002 Server Administration** tool adds FrontPage Server Extensions template directories to the content directory of your extended Web site, and adds other files that contain metadata.

## Publishing a Web site

If your Internet service provider (ISP) has FrontPage Server Extensions from Microsoft installed, you can publish to the Web server by using HTTP. Otherwise, you can use FrontPage to publish your Web site to a File Transfer Protocol (FTP) server.



### Note

If you publish to a location on your local computer, your Web site will not have the full FrontPage functionality unless your computer is a server that has FrontPage Server Extensions or SharePoint Team Services from Microsoft installed.

## ► To publish to a Web server by using HTTP

1. In Microsoft FrontPage, on the **File** menu, click **Publish Web**.
2. In the **Publish Destination** dialog box, do one of the following:
  - Type the location of a Web server.
  - or-
  - Click the drop-down arrow to select a location to which you have already published another Web site.
  - or-
  - Click **Browse** to find the publishing location.

**Note**

If you have previously chosen a publishing destination for this Web site, the **Publish Destination** dialog box will not appear; proceed to step 4.

3. Click **OK**.
4. Specify the pages you want to publish by doing the following:
  - a. In the **Publish Web** dialog box, click **Options** in the lower left corner.
  - b. Click the **Publish** tab, and do one or more of the following:
    - Under **Publish**, specify whether you want to publish only pages that have changed, or all pages.
    - Under **Changes**, specify how you want FrontPage to determine which pages have been changed.
    - If you want to create a log file for changes made during publishing, select that check box.
  - c. Click **OK**.
5. To publish subwebs, select the **Include subwebs** check box.
6. Click **Publish**.

FrontPage publishes your Web site to the Web server you specified. If you want to verify that your Web site was successfully published, click the hyperlink that is displayed after the Web has been published — your Web browser will open to the Web site you just published.

**Note**

If you cancel publishing in the middle of the operation, files that have already been published remain on the destination Web server.

**► To publish to an FTP site**

1. In FrontPage, on the **File** menu, click **Publish Web**.
2. In the **Publish Destination** dialog box, type the location of the FTP server, or click the drop-down arrow to select a location to which you have already published another web site.

**Note**

If you have previously chosen a publishing destination for this web site, the **Publish Destination** dialog box will not appear; proceed to step 4,

3. Click **OK**.
4. To specify the pages you want to publish, in the **Publish Web** dialog box, click **Options** in the lower left corner.

5. Click the **Publish** tab, and do one or more of the following:
  - Under **Publish**, specify whether you want to publish only pages that have changed, or all pages.
  - Under **Changes**, specify how you want FrontPage to determine which pages have been changed.
  - If you want to create a log file for changes made during publishing, select that check box.
6. Click **OK**.
7. To publish subwebs, select the **Include subwebs** check box.
8. Click **Publish**.

**Note**

If you cancel publishing in the middle of the operation, files that have already been published remain on the destination FTP server.

FrontPage publishes your Web site to the FTP server you specified.

---

## Remove Virtual Directories

The Internet Information Services (IIS) Lockdown Tool works by turning off unnecessary IIS features and components to reduce the attack surface of the Web server. To assist in mitigating these potential risks, remove any unnecessary virtual directories.

▶ **To remove a virtual directory using IIS Manager**

1. In IIS Manager, expand the site containing the virtual directory you want to remove, right-click the virtual directory, and then click **Delete**.
2. Click **Yes**.

▶ **To remove a virtual directory using Windows Explorer**

1. In Windows Explorer, browse to the folder containing the virtual directory you want to remove, right-click the directory, and then click **Sharing and Security**.
2. Click the **Web Sharing** tab, click **Remove**, and then click **Yes**.
3. Click **OK**.

You can verify that the virtual directory was deleted by starting IIS Manager and expanding the Web site.

**Note**

The following method does not work for root virtual directories

► **To delete a virtual directory using the `iisvdir.vbs` administration script**

1. In the **Run** dialog box, type `cmd`, and then click **OK**.
2. At the command prompt, use the `cd` command to change to the directory where the `iisvdir.vbs` script is installed. The default location for this file is `systemroot\system32\iisvdir.vbs`.
3. At the command prompt, type:

```
cscript iisvdir.vbs /delete "Sample Web Site" VirtualDirectoryName.
```

Substitute your Web site name and virtual directory name as appropriate. If there are spaces in the Web site name, use quotation marks around the Web site name, as shown in the preceding example.

4. Click **OK**.

## Request a Server Certificate

To enable Secure Sockets Layer (SSL) on a Web site, you must first request a server certificate from a trusted certification authority. After you obtain the certificate, you need to install it on the Web server, and then assign it to one or more Web sites.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** `Iis.msc`.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type `runas /user:administrative_accountname "mmc %systemroot%\system32\inetrv\iis.msc"`.

► **To request a server certificate**

1. In IIS Manager, expand the local computer, and then expand the **Web Sites** folder.
2. Right-click the Web site or file that you want, and then click **Properties**.
3. On the **Directory Security** or **File Security** tab, under **Secure communications**, click **Server Certificate**.
4. In the Web Server Certificate Wizard, click **Next**, and then click **Create a new certificate**.
5. Follow the steps in the Web Server Certificate Wizard, which guides you through the process of requesting a new server certificate.

## Secure the Root Folder of Each Disk Volume

Immediately after a new installation of Microsoft® Windows® Server 2003, the special group Everyone has Read and Execute permissions on the root of the *system volume*, which is the disk volume where Windows Server 2003 is installed.

Any folders created beneath the root of the system volume automatically inherit the permissions assigned to the root of the system volume. This means that the Everyone group will have Read and Execute permissions on any new folders created immediately beneath the root of the system volume. To prevent an accidental breach in security, remove the permissions assigned to the special group “Everyone” on dedicated Web servers.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.
- **File System:** The system volume must use the NTFS file system if you want to set file and folder permissions.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname “mmc %systemroot%\system32\inetmgr\iis.msc”**.

#### ► To secure the root of the system volume by removing permissions

1. Open Accessories, and then click **Windows Explorer**.
2. In Windows Explorer, locate the root of the system volume.
3. Right-click the root of the system volume, click **Properties**, and then click the **Security** tab.
4. In the **Group or user names** list box, click **Everyone**, and then click **Remove**.
5. Click **OK**.

---

## Secure Windows Server 2003 Built-in Accounts

After the installation of Microsoft® Windows® Server 2003, the built-in accounts Administrator and Guest exist on the Web server. In some instances, potential attackers can exploit these well known accounts unless they are renamed or disabled.

The Administrator account can be renamed, but cannot be disabled. The Guest account can be renamed and disabled. To help prevent potential attackers from exploiting these accounts, do the following:

- Rename the Administrator account.
- Rename and disable the Guest account.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

#### ▶ To rename the Administrator user account

1. In Control Panel, click Administrative Tools, and then click **Computer Management**.
2. In the console tree, expand **Local Users and Groups**, and then click **Users**.
3. In the details pane, right-click **Administrator**, and then click **Rename**.
4. Type the new user name, and then press ENTER.

#### ▶ To disable and rename the Guest user account

1. In Control Panel, click Administrative Tools, and then click **Computer Management**.
2. In the console tree, expand **Local Users and Groups**, and then click **Users**.
3. In the details pane, right-click **Guest**, and then click **Properties**.
4. In the **Guest Properties** dialog box, on the **General** tab, click the **Account is disabled** check box, and then click **OK**.
5. In the **Details** pane, right-click **Guest**, and then click **Rename**.
6. Type the new user name, and then press ENTER.

---

## Set Processor Affinity

On a multi-CPU server, you can configure application pools to establish affinity between worker processes and CPUs in order to take advantage of more frequent CPU cache hits. You can use processor affinity to control processors when applications place demands on system resources.

Processor affinity is used when it is necessary to continue processing an application that is tied to a subset of the hardware, so that transitions from one processor to another are minimized. You can establish affinity on a server that is supporting multiple applications so that a processor is dedicated to each application.

Consider the following when setting processor affinity to enable debugging of application pool failures:

- By default, processor affinity is off, and the load is distributed across all available CPUs.
- Processor affinity is used in conjunction with the processor affinity mask setting that is used to specify the CPUs.

- The metabase property **SMPProcessorAffinityMask** is a hexadecimal number. The maximum value, FFFFFFFF, is equivalent to decimal 32, the largest number of processors currently allowed. The hexadecimal value, translated to binary, gives the processors that are connected to the worker process in the application pool. For example, the hexadecimal number FFFFFFFF translates to the binary number 1111 1111 1111 1111 1111 1111 11111111 . This means that all 32 processors are available to the worker processes in the application pool. If the hexadecimal value is 00000005, the binary value is 0000 0000 0000 0000 0000 0000 0000 0101, which means that processor 0 and processor 2 are connected to the worker processes in the application pool (processors are numbered from the right, beginning with 0).

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.
- **Mode:** The processor affinity feature of IIS 6.0 is available only when running in worker process isolation mode.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetmgr\iis.msc"**.

#### ► To set processor affinity

1. Copy the following ADSI script into a text editor or word processor. The script (written in VBScript) enables and configures processor affinity.

```
set appPoolObj=GetObject("IIS://localhost/W3svc/AppPools/app pool name")
` Set the properties. Enable processor affinity for processors 0,1,2,3:
appPoolObj.Put "SMPAffinitized", TRUE
appPoolObj.Put "SMPProcessorAffinityMask", &H0000000F
` Save the property changes in the metabase:
appPoolObj.SetInfo
WScript.Echo "After: " & appPoolObj.SMPAffinitized & ", " &
appPoolObj.SMPProcessorAffinityMask
```

2. In the text editor, change the value of the metabase property **SMPProcessorAffinityMask** to the hexadecimal value that corresponds to the CPU numbers of the CPUs that are used by the worker processes in the application pool.
3. Save the file with extension **.vbs**.
4. In the **Run** dialog box, type **cmd** and then click **OK**.

5. At the command prompt, run the script by typing:

```
cscript //nologo filename.vbs
```

where *filename* is the fully qualified path of the script file.

6. To ascertain that the metabase properties have changed, view the metabase properties in the **metabase.xml** file to see if the values have been correctly set. To do so, open the **metabase.xml** file in Notepad or another text editor. The default path to this file is `%systemroot%\system32\inetsrv\metabase.xml`.

---

## Stop the WWW Service

Once you have verified that no users are accessing your Web site, you can stop the World Wide Web Publishing Service (WWW service) on your source computer. You can then migrate your Web sites to the target server.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

### Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:administrative\_accountname "mmc %systemroot%\system32\inetsrv\iis.msc"**.

#### ▶ To stop the WWW Service in IIS 5.0

1. Open Administrative Tools, and then click **Services**.
2. In the **Services** pane, double-click **World Wide Web Publishing Service**.
3. On the **Properties** page, on the **General** tab under **Service Status**, click the **Stop** button, and then click **OK**.

#### ▶ To stop the WWW Service in IIS 4.0

1. Open Control Panel, and then double-click **Services**.
2. On the **Services** page, click **World Wide Web Publishing Service**, and then click the **Stop** button, and then click **Close**.

---

## Upgrade FrontPage Extended Web Sites

You can upgrade Web sites to FrontPage 2002 Server Extensions from Microsoft from any previous version of FrontPage Server Extensions. During the upgrade process, changes are made to your Web site metadata and background structure, and some content is added to your Web site to enable it to work with FrontPage 2002 Server Extensions.



After you have installed FrontPage 2002 Server Extensions, you can upgrade your extended Web sites from the command-line, or by using Microsoft® SharePoint™ Administrator. To upgrade an extended Web site from the command-line, use the upgrade command.

▶ **To upgrade an extended Web site from the command line**

1. In the **Run** dialog box, type **cmd**, and then click **OK**.
2. At the command prompt, change to the FrontPage Extensions directory by typing:  

```
cd %CommonProgramFiles%\Microsoft Shared\Web Server Extensions\50\bin
```
3. Then, at the command prompt, type:

```
owsadm -o upgrade -p Port -m WebSiteUrl
```

where *Port* is the optional port number of the site to be upgraded (defaults to port 80), and *WebSiteUrl* is the URL for the Web site you are upgrading.

▶ **To upgrade an extended Web site by using SharePoint Administrator**

1. On the server, open Administrative Tools, and then click **Microsoft SharePoint Administrator**.
2. In the list of extended Web sites, next to the extended Web site you want to upgrade, click **Upgrade**.
3. In the **Administrator user name** box, type the user name for the administrator of the extended Web site.
4. Click **Submit**.

---

## View Application Isolation Configuration

Before configuring Internet Information Services (IIS) 6.0 to run in worker process isolation mode, you need to document the configuration for existing Web sites and applications running on the source server so you can transfer the settings to the target server.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Iis.msc.

▶ **To view application isolation settings in IIS 5.0**

1. Open Administrative Tools, and then click **Internet Services Manager**.
2. Expand the local computer, right-click the Web site for which you are documenting the settings, and then click **Properties**.
3. Click the **Home Directory** tab.

4. Under **Application Settings**, note the settings for **Application Protection**. Available settings are:
  - Low (IIS Process)
  - Medium (Pooled)
  - High (Isolated)
5. Click **OK**.

► **To view application isolation settings in IIS 4.0**

1. Click **Start**, click **Programs**, click **Windows NT 4.0 Option Pack**, click **Microsoft Internet Information Server**, and then click **Internet Services Manager**.
2. In Internet Services Manager, expand **Internet Information Server**, expand the local computer, right-click the Web site for which you are documenting the settings, and then click **Properties**.
3. On the **Home Directory** tab, under **Application Settings**, note whether the check box **Run in separate memory space (isolated process)** is selected.
4. Click **OK**.

---

## View Web Site and Application Process Identities

Before configuring Internet Information Services (IIS) 6.0 to run in worker process isolation mode, you need to document the process identity used by the Web site and application. After configuring IIS 6.0 to run in worker process isolation mode, you will use the documented process identities to configure the application pools in worker process isolation mode.

### Requirements

- **Credentials:** Membership in the Administrators group on the local computer.
- **Tools:** Internet Service Manager (ISM) for IIS 4.0 and IIS 5.0, and IIS Manager for IIS 6.0

► **To view Web site and application process identities in IIS 6.0 running in IIS 5.0 Isolation Mode**

1. In the **Run** dialog box, type **mmc**, and then click **OK**.
2. If you do not have the Component Services Snap-in installed, in MMC, on the **File** menu, click **Add/Remove Snap-ins**, and then click **Add**. Under **Available Standalone Snap-ins**, click **Component Services**, and then click **Add**.
3. In MMC, in the console tree, expand **Component Services**, expand **Computers**, expand **My Computer**, and then click **COM+ Applications**.
4. Right-click **WebSiteName** and then click **Properties** (where **WebSiteName** is the name of the Web site or application).
5. Click the **Identity** tab.
6. Document the identity for the Web site or application found in the **User** text box.

▶ **To view Web site and application process identities in IIS 5.0**

1. In the **Run** dialog box, type **mmc**, and then click **OK**
2. If you do not have the Component Services Snap-in installed, in the **File** menu click **Add/Remove Snap-ins**, and then click **Add**. Under **Add Standalone Snap-ins**, click **Component Services**, and then click **Add**. Click **Close** and then click **OK**.
3. In MMC, in the console tree, expand **Computers**, expand **My Computer** and expand **COM+ Applications**.
4. Right-click **IIS-{WebSiteName//Root}** and then click **Properties** (where *WebSiteName* is the name of the Web site or application).
5. Click the **Identity** tab.
6. Document the identity for the Web site or application found in the **User** text box.

▶ **To view Web site and application process identities in IIS 4.0**

1. Click **Start**, click **Programs**, click **Windows NT 4.0 Option Pack**, click **Microsoft Internet Information Server**, and then click **Internet Services Manager**.
2. In the console tree, expand **Microsoft Transaction Server**, expand **Computers**, expand **My Computer**, expand **Packages installed**, right-click *WebSiteName* and then click **Properties** (where *WebSiteName* is the name of the Web site or application).
3. Click the **Identity** tab.
4. Document the identity for the Web site or application found in the **User** text box.

