Windows 2000 Server

Users and Computers

This section covers:

- Managing servers remotely
- Accessing Windows 2000 Server Help remotely
- Windows Management Instrumentation
- Microsoft Management Console
- Group Policy
- Remote Installation Services
- User profiles

For information about managing users and computers in Active Directory, see Active Directory.

Managing servers remotely

With Windows 2000 Administration Tools, included on the Windows 2000 Server and Windows 2000 Advanced Server compact disc sets, you can manage a server remotely from any computer that is running Windows 2000. Windows 2000 Administration Tools contains Microsoft Management Console snap-ins and other administrative tools that are used to manage computers running Windows 2000 Server, and which are not provided on Windows 2000 Professional.

To install Windows 2000 Administration Tools on a local computer, open the I386 folder on the applicable Windows 2000 Server disc, and then double-click the Adminpak.msi file. Follow the instructions that appear in the Windows 2000 Administration Tools Setup wizard. After Windows 2000 Administration Tools is installed, you can access the server administrative tools by clicking **Start**, pointing to **Programs**, and then pointing to **Administrative Tools**.

On Windows 2000 Server, you can use the Software Installation snap-in to deploy Windows 2000 Administration Tools to other computers in your organization in two ways:

- Assign Windows 2000 Administration Tools to other computers. It is then automatically installed on the remote computers.
- Publish Windows 2000 Administration Tools in Active Directory. Once this is done, an administrator can use **Add/Remove Programs** in Control Panel on the remote computer to install it when needed.

The following is a list of the server administrative tools included in Windows 2000 Administration Tools:

- Active Directory Domains and Trusts
- Active Directory Schema
- Active Directory Sites and Services
- Active Directory Users and Computers
- Certification Authority
- Cluster Administrator
- Connection Manager Administration Kit
- DHCP
- Distributed File System
- DNS
- Internet Authentication Service
- Internet Services Manager
- QoS Admission Control
- Remote Boot Disk Generator (part of Remote Installation Services)
- Remote Storage
- Routing and Remote Access
- Telephony
- Terminal Services Manager, Licensing, and Client Connection Manager
- WINS

For information on how to use the Software Installation snap-in to deploy Windows 2000 Administration Tools to other computers in your organization, see Checklist: Software installation.

Note

- You must have administrative permissions for the local computer to install and run Windows 2000 Administration Tools.

Accessing Windows 2000 Server Help remotely

This topic explains how to view Help for Windows 2000 Server or Windows 2000 Advanced Server from a location other than a local server.

The Windows 2000 Server Help files are typically located in C:\Winnt\Help. These files are interconnected to form an integrated Help system and they contain shortcuts that open various server administrative tools. The Help files use approximately 30 MB of disk space.

You can access server Help in several ways. Because each method has its own advantages and disadvantages, you should use the method that best fits your particular situation or best complies with the administrative policy for your organization:

- **Allow read-only access to the Help folder on a server**. If you grant Read permission for the Help folder on a server computer, authorized users or groups can access server Help. The Help shortcuts that open administrative tools will function, provided the user has the proper permissions. However, granting even read-only access to server resources may constitute a security risk. To start server Help in a shared Help folder, double-click Windows.chm or create a shortcut to that file.

  For more information on access control for Windows 2000, see Access control.

- **Copy all Help files to a shared folder on your network**. You can copy all files in the Help folder to another computer on your network. Then grant the Read permission for the shared folder to authorized users or groups. The Help shortcuts that open administrative tools will not function. To start server Help in a shared folder, double-click Windows.chm or create a shortcut to that file.

- **Copy all Help files to your local computer**. You can copy all files in the Help folder to your local computer. However, if the local computer is running Windows 2000 Professional, you will overwrite the Help system for that platform unless you copy the server

Help files to a location other than the local Winnt\Help folder. If the Help files are not located in Winnt\Help, or if Windows 2000 Administration Tools is not installed, the Help shortcuts that open administrative tools will not function. To start server Help in a folder on your local computer, double-click Windows.chm or create a shortcut to that file.

- **Install Windows 2000 Administration Tools on your local computer**. Windows 2000 Administration Tools adds server administrative tools and their associated Help files to Windows 2000 Professional. You can access the Help files through the menus of the individual tools. However, you do not obtain all the server Help, only the Help associated with the server tools that are included.

  For more information on Windows 2000 Administration Tools, see Managing servers remotely.

- **Print Help topics from a server**. You can print some, or all, topics listed in the table of contents for server Help. To do so, on the **Contents** tab, right-click a topic and then click **Print**. To print just the content that appears in the topic pane, click **Print the selected topic**. To print all content associated with a particular heading (book) in the table of contents, click **Print the selected heading and all subtopics**. Before printing all subtopics, you should view the subtopics to get an estimate of the size of the print job.

- **View the Help files on the Microsoft Web site.** You can view the latest Help for Windows 2000 Server and Windows 2000 Advanced Server on the Windows Home Pages Web site. For Windows 2000 Server, see the Microsoft Web site (http://www.microsoft.com/).

  For Windows 2000 Advanced Server, see the Microsoft Web site (http://www.microsoft.com/).

Note

- When copying files from the Help folder, be sure to copy all files (including any hidden files) in the folder, otherwise the Help system may not function correctly.

Windows Management Instrumentation overview

Windows Management Instrumentation (WMI) is the Microsoft implementation of Web-Based Enterprise Management (WBEM), an initiative to establish standards for accessing and sharing management information over an enterprise network. WMI is WBEM-compliant and provides integrated support for the Common Information Model (CIM), the data model that describes the objects that exist in a management environment.

WMI includes a CIM-compliant object repository, which is the database of object definitions, and the CIM Object Manager, which handles the collection and manipulation of objects in the repository and gathers information from the WMI providers. WMI providers act as intermediaries between components of the operating system and applications. For example, the registry provider draws information from the registry, while the SNMP provider provides data and events from SNMP devices.

In Windows 2000, several management tools have been WMI-enabled, including Logical Drives, System Properties, System Information, and the Dependencies component of Services. In addition, Windows 2000 provides a tool called the WMI Control that can be used to modify WMI configuration settings. These components are briefly described below:

- The WMI Control enables you to perform Windows Management configuration tasks, such as setting permissions for authorized users or groups, backing up the object repository, and turning error logging on or off. For more information about the WMI Control, see Using Windows Management Instrumentation Control.
- Logical Drives lets you manage mapped drives and local drives on a remote computer or a local computer. You can view drive properties, change drive labels, and configure security settings for drives. For more information about Logical Drives, see Using Logical Drives.
- System Properties lets you view and change system properties on a local or remote computer. You can restart a remote computer to apply settings changes or to detect new hardware, view the computer name and domain information for other computers on your network, or change the settings for the virtual memory paging file on a computer that might run programs requiring a lot of memory. For more information about System Properties, see Using System Properties.
- System Information collects and displays configuration information about your system. This is is especially useful when troubleshooting your system with a support technician. For more information, see Using System Information.
- Services helps you manage the services on your computer. Services dependencies identify the services upon which the current service is dependent and the services that are dependent upon it. For more information about Services, see Using Services.

For technical information about developing for the WMI system, see the WMI Software Development Kit (SDK). The WMI SDK is released by MSDN as part of the Microsoft Platform SDK.

Microsoft Management Console

Microsoft Management Console (MMC) hosts administrative tools that you can use to administer networks, computers, services, and other system components.

- For help with specific tasks, see How To.
- For general background information, see Concepts.
- For information about accessibility features, see Accessibility for MMC.
- For problem-solving instructions, see Troubleshooting MMC.

How to...

- Open MMC and saved console files
- Author an MMC console file
- Modify a saved MMC console file
- Work with MMC and saved console files
- Set policy for MMC and snap-ins

Open MMC and saved console files

- Open MMC
- Open a saved MMC console for a local computer
- Open a saved MMC console for a remote computer
- Create a desktop shortcut to open MMC

To open MMC

- Do one of the following:
  - Click **Start**, click **Run**, type **mmc**, and then click **OK**.
  - At a command prompt, type **mmc**, and then press ENTER.

The complete command-line syntax for MMC is:

mmc *path**filename.msc* [**/a**]

*path**filename.msc*

Starts MMC and opens a saved console. You need to specify the complete path and file name for the saved console file. If you do not specify a console file, MMC opens a new console.

You can use environment variables to create command lines or shortcuts that do not depend on the explicit location of console files. For instance, if the path to a console file is in the system folder (for example, **mmc c:\winnt\system32\console_name.msc**), you can use the expandable data string %systemroot% to specify the location (**mmc %systemroot%\system32\console_name.msc**). This may be useful if you are delegating tasks to people in your organization who are working on different computers.

/a

Opens a saved console in author mode. Used to make changes to saved consoles. When consoles are opened with this option, they are opened in author mode, regardless of their default mode. This does not permanently change the default mode setting for files; when you omit this option, MMC opens console files according to their default mode settings.

Notes

- After you open MMC or a console file in author mode, you can open any existing console by clicking **Open** on the **Console** menu.
- You can use the command line to create shortcuts for opening MMC and saved consoles. A command-line command works with the **Run** command on the **Start** menu, in any command-prompt window, in shortcuts, or in any batch file or program that calls the command.

To open a saved MMC console for a local computer

- Do one of the following:
  - Click **Start**, point to **Settings**, click **Control Panel**, double-click **Administrative Tools**, and then double-click the console.
  - Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click the console.
  - Click **Start**, point to **Programs**, and then click the console.
  - Open the folder where your console is located, and then double-click the console.

Notes

- By default, in Windows 2000 Professional, console files are not available from the Administrative Tools folder on the **Programs** menu. However, if you create a custom console and save it to the per-user Administrative Tools folder (in Windows 2000, located at *systemdrive*\Documents and Settings*user*\Start Menu\Programs\Administrative Tools), this folder appears on the **Programs** menu for that user.
- On computers running Windows 2000, you can also open console files by using **Run As**. With this command, you can log on to your computer with user rights to perform routine tasks, but open console files to perform administrative tasks with Administrator rights as necessary. You can use this command by typing **runas** at a command prompt or by right-clicking an .msc file, and then clicking **Run As**.

To open a saved MMC console for a remote computer

- Do one of the following:
  - Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click the console.
  - Open the folder where your console is located, and then double-click the console.

Notes

- By default, in Windows 2000 Professional, console files are not available from the Administrative Tools folder on the **Programs** menu. However, if you create a custom console and save it to the per-user Administrative Tools folder, this folder appears on the **Programs** menu.
- On computers running Windows 2000, you can also open console files by using **Run As**. With this command, you can log on to your computer with user rights to perform routine tasks, but open console files to perform administrative tasks with Administrator rights as necessary. You can use this command by typing **runas** a command prompt or by right-clicking an .msc file, and then clicking **Run As**.

To create a desktop shortcut to open MMC

1. Right-click an open area on the Windows desktop, point to **New**, and then click **Shortcut**.
2. Follow the instructions on your screen.

   A shortcut appears on your desktop.

Note

- You can drag a shortcut that you create on the desktop to other folders in the operating system, such as the folder where you keep your .msc files or the folder for the **Start** menu.

  You can also create a shortcut to MMC in folders by using Windows Explorer. To do so, click the folder where you want the shortcut, and on the **File** menu, point to **New**, click **Shortcut**, and then follow the instructions on your screen.

Author an MMC console file

- Add an item to a new MMC console for a local computer
- Add an item to a new MMC console for a remote computer
- Add a published snap-in to a new MMC console
- Add an extension snap-in to an MMC console
- Add a published extension snap-in to an MMC console
- Create a taskpad view in a saved MMC console
- Create tasks for a taskpad view in a saved MMC console
- Edit a taskpad view in a saved MMC console
- Edit tasks in a taskpad view in a saved MMC console
- Add an item to the Favorites list in an MMC console
- Organize the Favorites list in an MMC console
- Install a program managed by an MMC snap-in

- Set MMC console options
- Save an MMC console file

To add an item to a new MMC console for a local computer

1. Open MMC.
2. On the **Console** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. Under **Snap-in**, double-click the item you want to add, and, if prompted, do one of the following:
   - Click **Local computer: (the computer this console is running on)**, and then click **Finish**.
   - If a wizard appears, follow the instructions on your screen.
4. To add another item to the console, repeat step 3.

Notes

- To open MMC, click **Start**, click **Run**, type **mmc**, and then click **OK**.
- If you add a snap-in to a console, but then the snap-in becomes damaged, try adding another instance of the same snap-in to the console, configure it as needed, and then remove the first instance of the snap-in.
- If a console is saved to the per-user Administrative Tools folder (in Windows 2000, located at *systemdrive*\Documents and Settings*user*\Start Menu\Programs\Administrative Tools), it is then available in the Administrative Tools folder on the **Programs** menu for that user.
- If a snap-in does not appear in the list, you must first install the program, device, or service administered by the snap-in. In addition, if you are using Windows 2000 and are part of a domain, you can access snap-ins from the **Add/Remove Snap-in** dialog box that are not locally installed, but are available in the Active Directory directory service. For more information, see Windows 2000 Server Help.
- To make an item subordinate to an item in the console tree other than the console root, click the appropriate item in **Snap-ins added to** before you click **Add** in step 2.

To add an item to a new MMC console for a remote computer

1. Open MMC.
2. On the **Console** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. Under **Snap-in**, double-click the item you want to add, and do the following:
   - Click **Another computer**, type the name of the computer you want this item to manage, and then click **Finish**.
   - If a wizard appears, follow the instructions on your screen.
4. To add another item to the console, repeat step 3.

Notes

- To open MMC, click **Start**, click **Run**, type **mmc**, and then click **OK**.
- If you add a snap-in to a console, but then the snap-in becomes damaged, try adding another instance of the same snap-in to the console, configure it as needed, and then remove the first instance of the snap-in.
- If a snap-in does not appear in the list, you must first install the program, device, or service administered by the snap-in. In addition, if you are using Windows 2000 and are part of a domain, you can access snap-ins from the **Add/Remove Snap-in** dialog box that are not locally installed, but are available in the Active Directory directory service. For more information, see Windows 2000 Server Help.
- If a dialog box or a wizard does not appear in Step 3, you can only use the item to administer your local computer.
- If a console is saved to the per-user Administrative Tools folder (in Windows 2000, located at *systemdrive*\Documents and Settings*user*\Start Menu\Programs\Administrative Tools), it is then available in the Administrative Tools folder on the **Programs** menu for that user.
- To make an item subordinate to an item in the console tree other than the console root, click the appropriate item in **Snap-ins added to** before you click **Add** in step 2.

To add a published snap-in to a new MMC console

1. Open MMC.
2. On the **Console** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. Click the published snap-in you want to add, and then click **Add**.
4. If a wizard for Windows Installer appears, follow the instructions on your screen, and then do one of the following:
   - Click **Local computer: (the computer this console is running on)**, and then click **Finish**.
   - If a wizard for the snap-in appears, follow the instructions on your screen.
5. To add another item to the console, repeat step 3.

Notes

- To open MMC, click **Start**, click **Run**, type **mmc**, and then click **OK**.
- For snap-ins available from the Windows 2000 Active Directory directory service, **Not Installed** displays in the **Vendor** column.
- You can only access snap-ins published in the directory if the computer you are using is running Windows 2000 and is part of a Windows 2000 domain. For more information about publishing applications and Windows Installer, see Windows 2000 Server Help.
- If a console is saved to the per-user Administrative Tools folder (in Windows 2000, located at *systemdrive*\Documents and Settings*user*\Start Menu\Programs\Administrative Tools), it is then available in the Administrative Tools folder on the **Programs** menu for that user.
- To make an item subordinate to an item in the console tree other than the console root, click the appropriate item in **Snap-ins added to** before you click **Add** in step 2.

To add an extension snap-in to an MMC console

1. Open a saved console in author mode by doing one of the following:
   - Right-click the .msc file, and then click **Author**.
   - Click **Start**, click **Run**, type **mmc** *path**filename.msc* **/a**, and then click **OK**.
2. On the **Console** menu, click **Add/Remove Snap-in**, and then click the item that you want to extend.
3. On the **Extensions** tab, in **Available extensions**, select the check box next to the extension you want to add, and then click **OK**.

Notes

- To add every extension available for a given item, on the **Extensions** tab, select the **Add all extensions** check box. Conversely, if you want to add only certain extensions, clear this check box.
- You can also use this procedure to remove extensions from a console by clearing the check box for an extension that was previously selected.

To add a published extension snap-in to an MMC console

1. Open a saved console in author mode by doing one of the following:
   - Right-click the .msc file, and then click **Author**.
   - Click **Start**, click **Run**, type **mmc** *path**filename.msc* **/a**, and then click **OK**.
2. On the **Console** menu, click **Add/Remove Snap-in**.
3. On the **Extensions** tab, in **Snap-ins that can be extended**, click the snap-in that you want to extend.
4. In **Available extensions**, select the check box next to the published extension you want to add, and then click **Download**.
5. If one or more wizards appear, follow the instructions on your screen, and then click **OK**.

Important

- If you select the **Add all extensions** check box on the **Extensions** tab, only extension snap-ins that are locally installed and registered are added to the console. You must specifically download extension snap-ins from the directory service to make them available in a console. Thus, to add all published extensions for a given item, do not select the **Add all extensions** check box, but instead select the check box next to each published extension.

Notes

- For extension snap-ins that are available from the Windows 2000 Active Directory directory service, the snap-in names are followed by the phrase **(not installed)**.
- You can only access extension snap-ins published in the directory if the computer you are using is running Windows 2000 and is part of a Windows 2000 domain. For more information about publishing applications and Windows Installer, see Windows 2000 Server Help.

To create a taskpad view in a saved MMC console

1. Open a saved console in author mode by doing one of the following:
   - Right-click the .msc file, and then click **Author**.
   - Click **Start**, click **Run**, type **mmc** *path**filename.msc* **/a**, and then click **OK**.
2. In the console tree, click a snap-in item.
3. On the **Action** menu, click **New Taskpad View**.
4. Follow the instructions in the New Taskpad View wizard.
5. If you want to create tasks immediately after you create the taskpad view, select the **Start New Task wizard** check box in the final screen of the wizard.

Note

- You can also create a taskpad view in a new console, but you must first add a snap-in to the console.

To create tasks for a taskpad view in a saved MMC console

1. Open a saved console in author mode by doing one of the following:
   - Right-click the .msc file, and then click **Author**.
   - Click **Start**, click **Run**, type **mmc** *path**filename.msc* **/a**, and then click **OK**.
2. In the console tree, click an item associated with the taskpad view, and on the **Action** menu, click **Edit Taskpad View**.
3. On the **Tasks** tab, click **New**.
4. Follow the instructions in the New Task wizard.

Notes

- If you are creating a new taskpad view and want to add a task, you can start the New Task wizard by selecting the **Start New Task wizard** check box in the final screen of the New Taskpad View wizard.
- On the Shortcut Menu Command page of the New Task wizard, in **Command source**, if you selected **Tree item task** and cannot view all items in the console tree, you must expand the console tree manually before starting the New Task wizard.

To edit a taskpad view in a saved MMC console

1. Open a saved console in author mode by doing one of the following:
   - Right-click the .msc file, and then click **Author**.
   - Click **Start**, click **Run**, type **mmc** *path**filename.msc* **/a**, and then click **OK**.
2. On the **Action** menu, click **Edit Taskpad View**.
3. On the **General** tab, do the following:
   - To change the name for the taskpad view, in **Name**, type a new name. The name appears in the upper-left corner of the taskpad view and on the tab on the bottom edge of the taskpad view.
   - To change the description for a taskpad view, in **Description**, type a new description. The description appears under the name in the upper-left corner of the taskpad view.
   - To change the list format, or to configure the taskpad view to contain tasks only, under **Style for the details pane**, click a new list format, or click **No list**.
   - To configure task descriptions, under **Style for task descriptions**, click **Text** or **InfoTip**. Text descriptions are displayed to the right of a task. InfoTip descriptions are displayed as popups when a user points to tasks with the mouse.
   - To change the size of the list, in **List size**, click a new size for the width (Vertical list) or height (Horizontal list) of the list.
4. Click **Options**, and then do one of the following:
   - To associate the taskpad view with only the currently selected item in the console tree, click **Selected tree item**.
   - To associate the taskpad view with all items in the console tree of the same type as the currently selected item, click **All tree items that are the same type as the selected tree item**.

If you click this option and want the taskpad view to appear by default, instead of the view on the **Normal** tab, select the **Change default display to this taskpad view for these tree items** check box.

To edit tasks in a taskpad view in a saved MMC console

1. Open a saved console in author mode by doing one of the following:
   - Right-click the .msc file, and then click **Author**.
   - Click **Start**, click **Run**, type **mmc** *path**filename.msc* **/a**, and then click **OK**.
2. In the console tree, click an item associated with the taskpad view, and on the **Action** menu, click **Edit Taskpad View**.
3. On the **Tasks** tab, under **Display these tasks**, click a task, and then do the following:
   - To move the selected task up the display list in the taskpad view, click **Move Up**.
   - To move the selected task down the display list in the taskpad view, click **Move Down**.
   - To delete the task from the display list in the taskpad view, click **Remove**.
   - Click **Modify**, and then do the following:
     - To change the name of a task, on the **General** tab, in **Task name**, type a new name. The name appears under the task.
     - To change the description for a task, on the **General** tab, in **Description**, type a new description. Depending on how you configured the taskpad view, this appears either to the right of the task or as a popup when a user points to the task with the mouse.
     - To change the icon for the task, on the **Task Icon** tab, click a new icon, and then click **OK**.

To add an item to the Favorites list in an MMC console

1. Open a saved console in author mode by doing one of the following:
   - Right-click the .msc file, and then click **Author**.
   - Click **Start**, click **Run**, type **mmc** *path**filename.msc* **/a**, and then click **OK**.
2. In the console tree, click the item that you want to add to the Favorites list.
3. In the details pane, click either the **Normal** tab or the tab for the taskpad view you want to add.
4. On the **Favorites** menu, click **Add to Favorites**.
5. In **Create in**, do one of the following:
   - To add an item to an existing folder, click the folder where you want the item to appear, and then click **OK**.
   - To add an item to a new folder, click the folder you want as the parent, and then click **New Folder**. In **Folder name**, type a name, click **OK**, and then click **OK** again.

Note

- The **Normal** tab and tabs for taskpad views are only available in the details pane of a console if you click an item in the console tree that is configured with a taskpad view. Otherwise, no tabs are visible in the details pane.

To organize the Favorites list in an MMC console

1. Open a saved console in author mode by doing one of the following:
   - Right-click the .msc file, and then click **Author**.
   - Click **Start**, click **Run**, type **mmc** *path**filename.msc* **/a**, and then click **OK**.
2. On the **Favorites** menu, click **Organize Favorites**, and then do the following:
   - To add a folder, click **Create Folder**, type a name in **Folder name**, and then click **OK**.
   - To move an item to a folder, click the item under the Favorites folder, click **Move to Folder**, click the folder where you want the item to appear, and then click **OK**.
   - To change the name of an item, click the item under the Favorites folder, click **Rename**, type a new name, and then press ENTER.
   - To remove an item, click the item under the Favorites folder, and then click **Delete**.

To install a program managed by an MMC snap-in

1. Click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Add/Remove Programs**.
2. Follow the instructions on your screen.

To set MMC console options

1. Open a saved console in author mode by doing one of the following:
   - Right-click the .msc file and then click **Author**.
   - Click **Start**, click **Run**, type **mmc** *path**filename.msc* **/a**, and then click **OK**.
2. On the **Console** menu, click **Options**.
3. To change the icon for the console, click **Change Icon**, in **File Name** type the path to a file containing icons, under **Current icon** click an icon, and then click **OK**.
4. To change the title for the console, type a new title in the box to the right of the icon.
5. To change the default mode for the console, in **Console mode**, click the mode that you want the console to open in.
6. If the default console mode for the console is one of the user modes, do the following:
   - To allow a menu to appear when users right-click the contents of a taskpad view, select the **Enable context menus on taskpads in this console** check box.
   - To prevent users from editing the console, select the **Do not save changes to this console** check box.
   - To enable users to access the **Customize View** dialog box, select the **Allow the user to customize views** check box.

Notes

- If you change the title of a console, the title bar will not display the path of items clicked in the console tree. However, if you do not change the title or you delete the title, the paths are displayed.
- Many files contain icons that can be used for custom consoles. For instance, use Shell32.dll, located on Windows 2000 and Windows NT in the *systemroot*\System32 folder.
- To stop receiving the message **Save console settings to** *console name***?**, which appears each time you close a console opened in

author mode, set the default mode for the console to one of the user modes and clear the **Do not save changes to this console** check box. Then, any changes to the console will be saved by default.

To save an MMC console file

- In an MMC console opened in author mode, on the **Console** menu, click **Save**.

Notes

- If the console is not in author mode, the **Console** menu is not available. In this case, saving is determined by whether the **Do not save changes to this console** check box (available by clicking **Options** on the **Console** menu) was selected when the console was configured. If this check box was not selected, changes to the console are automatically saved when you close MMC; if it was selected, changes to the console are discarded when you close MMC.
- If a console is saved to the per-user Administrative Tools folder (in Windows 2000, located at *systemdrive*\Documents and Settings*user*\Start Menu\Programs\Administrative Tools), it is then available in the Administrative Tools folder on the **Programs** menu for that user.

Modify a saved MMC console file

- Rename an item on the console tree of an MMC console
- Remove a snap-in or other item from an MMC console
- Make a new console window from an MMC console
- Make a new console window from part of an MMC console tree

To rename an item on the console tree of an MMC console

1. Open a saved console in author mode by doing one of the following:
   - Right-click the .msc file, and then click **Author**.
   - Click **Start**, click **Run**, type **mmc** *path******filename.msc* **/a**, and then click **OK**.
2. In the console tree, click the item that you want to rename.
3. On the **Action** menu, click **Rename**, and then type the new name.

Note

- Not all items in the console tree can be renamed. If the **Rename** command does not appear on the **Action** menu, you cannot rename the item.

To remove a snap-in or other item from an MMC console

1. Open a saved console in author mode by doing one of the following:
   - Right-click the .msc file, and then click **Author**.
   - Click **Start**, click **Run**, type **mmc** *path******filename.msc* **/a**, and then click **OK**.
2. On the **Console** menu, click **Add/Remove Snap-in**.
3. On the **Standalone** tab, click the item you want to remove, and then click **Remove**.

To make a new console window from an MMC console

1. Open a saved console in author mode by doing one of the following:
   - Right-click the .msc file, and then click **Author**.
   - Click **Start**, click **Run**, type **mmc** *path******filename.msc* **/a**, and then click **OK**.
2. On the **Window** menu, click **New Window**.

Note

- The new console window is rooted at the console root of the saved console.

To make a new console window from part of an MMC console tree

1. Open a saved console in author mode by doing one of the following:
   - Right-click the .msc file, and then click **Author**.
   - Click **Start**, click **Run**, type **mmc** *path******filename.msc* **/a**, and then click **OK**.
2. In the console tree, click the item that you want to become the console root of the new console.
3. On the **Action** menu, click **New Window from Here**.

Work with MMC and saved console files

- Hide or display features of a saved MMC console
- Hide or display menus and toolbars for snap-ins
- Reorder columns in an MMC console
- Hide or display columns in an MMC console
- Filter rows in an MMC console
- Export columns in an MMC console to a text file
- View the associated snap-in and item for a property page

To hide or display features of a saved MMC console

1. Open a saved console.
2. On the **View** menu, click **Customize**.
3. Under **MMC**, do the following:
   - To display or hide the console tree, select or clear the **Console tree** check box.
   - To display or hide the **Action** and **View** menus, select or clear the **Standard menus (Action and View)** check box.
   - To display or hide the console toolbar, select or clear the **Standard toolbar** check box.
   - To display or hide the status bar at the bottom of the console window, select or clear the **Status bar** check box.
   - To display or hide the description bar along the top of the details pane, select or clear **Description bar**.
   - To display or hide the tabs along the bottom of the details pane, select or clear the **Taskpad navigation tabs** check box.

Important

- If you clear the **Standard menus (Action and View)** check box and close the **Customize View** dialog box, you cannot access commands on the **Action** and **View** menus, including the **Customize** command. In this situation, to access the **Customize View** dialog box, click the system menu (the icon in the upper-left corner of the console), and then click **Customize View**.

Notes

- As you select or clear check boxes, view the console to confirm that the changes you make are what you expected.
- If you hide the console tree, the **Favorites** tab, if applicable, still appears.
- If you hide the **Action** and **View** menus, the **Favorites** menu, if applicable, still appears.

To hide or display menus and toolbars for snap-ins

1. Open a saved console.
2. On the **View** menu, click **Customize**.
3. Under **Snap-in**, do one or more of the following:
   - To display or hide menus specific to snap-ins, select or clear the **Menus** check box.
   - To display or hide toolbars specific to snap-ins, select or clear the **Toolbars** check box.

Note

- When you select or clear the **Menus** and **Toolbars** check boxes, the menus and toolbars are displayed or hidden for all snap-ins in the console, not just the currently selected snap-in. If toggling the check boxes does not change the view, the currently selected snap-in does not have custom menus or toolbars.

To reorder columns in an MMC console

1. In an open MMC console, click an item in the console tree that displays columns in the details pane.
2. On the **View** menu, click **Choose Columns**.
3. In the **Modify Columns** dialog box, under **Displayed columns**, click a column name, and then click **Move Up** or **Move Down** to change the position of the column.

Notes

- You can also reorder columns in the details pane by using a mouse to drag a column heading to the left or right of its original position. As you drag a column, highlighting between the column headings indicates the new position of the column.
- You can resize columns by using the mouse to drag column headings.
- You cannot change the position of the leftmost column in the details pane.
- This feature is not enabled for all items. If you do not see the **Choose Columns** option on the **View** menu, you cannot use this feature for the selected item.

To hide or display columns in an MMC console

1. In an open MMC console, click an item in the console tree that displays columns in the details pane.
2. On the **View** menu, click **Choose Columns**.
3. In the **Modify Columns** dialog box, do the following:
   - To hide a column, in **Displayed columns**, click the column you want to hide, and then click **Remove**.
   - To display a column, in **Hidden columns**, click the column you want to display, and then click **Add**.

Notes

- You cannot hide the leftmost column in the details pane.
- This feature is not enabled for all items. If you do not see the **Choose Columns** option on the **View** menu, you cannot use this feature for the selected item.

To filter rows in an MMC console

1. In an open MMC console, click an item in the console tree that displays columns in the details pane.
2. On the **View** menu, click **Filtered**.

   Filters appear below the column headings in the details pane.

Note

- This feature is not enabled for all items. If you do not see the **Filtered** option on the **View** menu, you cannot use this feature for the selected item.

To export columns in an MMC console to a text file

1. In an open MMC console, click an item in the console tree that displays columns in the details pane.
2. To export only certain rows in the details pane, select the rows.

   If you want to export the entire contents of the details pane, skip this step.
3. On the **Action** menu, click **Export List**.
4. In the **Save As** dialog box, enter the following information:
   - To export only certain rows, select the **Save Only Selected Rows** check box.
   - In **Save in**, click a location to save the file.
   - In **File name**, type a name for the file.
   - In **Save as type**, click a file format in the list.
5. Click **Save**.

Notes

- Some snap-ins do not provide the ability to select more than one row in the details pane. For these snap-ins, you can export all the rows in the details pane, but not selected rows only.
- In **Save as type**, Unicode file formats are only available if you are using Windows NT or Windows 2000.

To view the associated snap-in and item for a property page

1. In the console tree or details pane of an open MMC console, right-click an item for which you want to view properties and then click **Properties**.

2. In the properties dialog box, do the following:
   - To view which snap-in provided a particular property page in the dialog box, hold down the CTRL key and point to the label of the tab.
   - To view the location in the console tree for the item associated with the properties dialog box, hold down the CTRL key and point to the title bar of the properties dialog box.

Set policy for MMC and snap-ins

- Restrict access to author mode in MMC
- Restrict access to author mode in MMC for a domain
- Restrict access to a permitted list of snap-ins
- Restrict access to a permitted list of snap-ins for a domain
- Permit or restrict access to a snap-in
- Permit or restrict access to a snap-in for a domain

To restrict access to author mode in MMC

1. Open MMC.
2. On the **Console** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. Under **Snap-in**, click **Group Policy**, and then click **Add**.
4. In the **Select Group Policy Object** dialog box, do one of the following:
   - To edit the local Group Policy object, click **Local Computer**.
   - To edit a different Group Policy object, click **Browse**.
5. Click **Finish**, click **Close**, and then click **OK**.

   The Group Policy snap-in opens the specified Group Policy object.
6. In the console tree, click **Microsoft Management Console**.

   Where?
   - *PolicyName* Policy
   - User Configuration
   - Administrative Templates
   - Windows Components
   - Microsoft Management Console
7. In the details pane, double-click **Restrict the user from entering author mode**.
8. On the **Policy** tab, do one of the following:
   - To allow the user to use author mode in MMC, click **Not Configured** or **Disabled**.
   - To restrict the user from using author mode in MMC, click **Enabled**.

Notes

- To open MMC, click **Start**, click **Run**, type **mmc**, and then click **OK**.
- You must be an Administrator, or have equivalent rights, to configure Group Policy.
- You must be using Windows 2000 to configure Group Policy for MMC; this feature is not available for MMC running on other versions of Windows.
- For more information, click the **Explain** tab in the **Restrict the user from entering author mode properties** dialog box and see Windows 2000 Help.

To restrict access to author mode in MMC for a domain

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the organizational unit for which you want to configure policy, and then click **Properties**.
3. On the **Group Policy** tab, click **Edit**.

   The Group Policy console appears.
4. In the console tree, click **Microsoft Management Console**.

   Where?
   - *PolicyName* Policy
   - User Configuration
   - Administrative Templates
   - Windows Components
   - Microsoft Management Console
5. In the details pane, double-click **Restrict the user from entering author mode**.
6. On the **Policy** tab, do one of the following:
   - To allow the user to use author mode in MMC, click **Not Configured** or **Disabled**.
   - To restrict the user from using author mode in MMC, click **Enabled**.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- You must be a domain Administrator, or have equivalent rights, and use a computer configured as a domain controller to configure Group Policy for a domain.
- You must be using Windows 2000 to configure Group Policy for MMC; this functionality is not available for MMC running on other versions of Windows.
- For more information, click the **Explain** tab in the **Restrict the user from entering author mode properties** dialog box and see Windows 2000 Help.

To restrict access to a permitted list of snap-ins

1. Open MMC.

2. On the **Console** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. Under **Snap-in**, click **Group Policy**, and then click **Add**.
4. In the **Select Group Policy Object** dialog box, do one of the following:
   - To edit the local Group Policy object, click **Local Computer**.
   - To edit a different Group Policy object, click **Browse**.
5. Click **Finish**, click **Close**, and then click **OK**.

   The Group Policy snap-in opens the specified Group Policy object.
6. In the console tree, click **Microsoft Management Console**.

   Where?
   - *PolicyName* Policy
   - User Configuration
   - Administrative Templates
   - Windows Components
   - Microsoft Management Console
7. In the details pane, double-click **Restrict users to the explicitly permitted list of snap-ins**.
8. On the **Policy** tab, do one of the following:
   - To permit the user to access snap-ins that are not explicitly restricted, click **Not Configured** or **Disabled**.
   - To restrict the user from accessing any snap-in that is not explicitly permitted, click **Enabled**.

Notes

- To open MMC, click **Start**, click **Run**, type **mmc**, and then click **OK**.
- You must be an Administrator, or have equivalent rights, to configure Group Policy.
- You must be using Windows 2000 to configure Group Policy for MMC; this functionality is not available for MMC running on other versions of Windows.
- If you enable this policy, only permitted snap-ins appear in the list of available snap-ins in the **Add Standalone Snap-in** dialog box in MMC.
- For more information, click the **Explain** tab in the **Restrict users to the explicitly permitted list of snap-ins properties** dialog box and see Windows 2000 Help.

To restrict access to a permitted list of snap-ins for a domain

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the organizational unit for which you want to configure policy, and then click **Properties**.
3. On the **Group Policy** tab, click **Edit**.

   The Group Policy console appears.
4. In the console tree, click **Microsoft Management Console**.

   Where?
   - *PolicyName* Policy
   - User Configuration
   - Administrative Templates
   - Windows Components
   - Microsoft Management Console
5. In the details pane, double-click **Restrict users to the explicitly permitted list of snap-ins**.
6. On the **Policy** tab, do one of the following:
   - To permit the user to access snap-ins that are not explicitly restricted, click **Not Configured** or **Disabled**.
   - To restrict the user from accessing any snap-in that is not explicitly permitted, click **Enabled**.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- You must be a domain Administrator, or have equivalent rights, and use a computer configured as a domain controller to configure Group Policy for a domain.
- You must be using Windows 2000 to configure Group Policy for MMC; this functionality is not available for MMC running on other versions of Windows.
- If you enable this policy, only permitted snap-ins appear in the list of available snap-ins in the **Add Standalone Snap-in** dialog box in MMC.
- For more information, click the **Explain** tab in the **Restrict users to the explicitly permitted list of snap-ins properties** dialog box and see Windows 2000 Help.

To permit or restrict access to a snap-in

1. Open MMC.
2. On the **Console** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. Under **Snap-in**, click **Group Policy**, and then click **Add**.
4. In the **Select Group Policy Object** dialog box, do one of the following:
   - To edit the local Group Policy object, click **Local Computer**.
   - To edit a different Group Policy object, click **Browse**.
5. Click **Finish**, click **Close**, and then click **OK**.

   The Group Policy snap-in opens the specified Group Policy object.
6. In the console tree, click **Restricted/Permitted snap-ins**.

   Where?
   - *PolicyName* Policy
   - User Configuration

└Administrative Templates
└Microsoft Management Console
└Restricted/Permitted snap-ins

7. In the details pane, double-click the snap-in that you want to permit or restrict, and then do one of the following:
   - To enable the user to access this snap-in unless the user is restricted by the **Restrict users to the explicitly permitted list of snap-ins** policy, click **Not Configured**.
   - To permit the user to access this snap-in, click **Enabled**.
   - To restrict the user from accessing this snap-in, click **Disabled**.

Notes

- To open MMC, click **Start**, click **Run**, type **mmc**, and then click **OK**.
- You must be an Administrator, or have equivalent rights, to configure Group Policy.
- You must be using Windows 2000 to configure Group Policy for MMC; this functionality is not available for MMC running on other versions of Windows.
- For more information, click the **Explain** tab in the *snap-in* **Properties** dialog box and see Windows 2000 Help.

To permit or restrict access to a snap-in for a domain

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the organizational unit for which you want to configure policy, and then click **Properties**.
3. On the **Group Policy** tab, click **Edit**.

   The Group Policy console appears.
4. In the console tree, click **Restricted/Permitted snap-ins**.

   Where?
   └*PolicyName* Policy
   └User Configuration
   └Administrative Templates
   └Microsoft Management Console
   └Restricted/Permitted snap-ins
5. In the details pane, double-click the snap-in that you want to permit or restrict, and then do one of the following:
   - To enable the user to access this snap-in unless the user is restricted by the **Restrict users to the explicitly permitted list of snap-ins** policy, click **Not Configured**.
   - To permit the user to access this snap-in, click **Enabled**.
   - To restrict the user from accessing this snap-in, click **Disabled**.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- You must be a domain Administrator, or have equivalent rights, and use a computer configured as a domain controller to configure Group Policy for a domain.
- You must be using Windows 2000 to configure Group Policy for MMC; this functionality is not available for MMC running on other versions of Windows.
- When you restrict or explicitly permit access to a snap-in, the snap-in is added to a list of restricted or permitted snap-ins. The restricted list takes precedence over the permitted list, so that if the same snap-in exists on both lists, access to the snap-in is restricted.
- For more information, click the **Explain** tab in the *snap-in* **Properties** dialog box and see Windows 2000 Help.

Concepts

This section covers:

- MMC overview
- Understanding MMC
- Using MMC
- Resources

MMC overview

You can use Microsoft Management Console (MMC) to create, save, and open administrative tools (called MMC consoles) that manage the hardware, software, and network components of your Windows system. MMC is a feature of the Windows 2000 operating system, but you can also run MMC on Windows NT, Windows 95, and Windows 98 operating systems. In addition, MMC is a feature of several software applications designed to run on Windows.

MMC does not perform administrative functions, but hosts tools that do. The primary type of tool you can add to a console is called a snap-in. Other items that you can add include ActiveX controls, links to Web pages, folders, taskpad views, and tasks.

There are two general ways that you can use MMC: in *user mode*, working with existing MMC consoles to administer a system, or in *author mode*, creating new consoles or modifying existing MMC consoles. For more information about the differences between user and author mode, see Console access options.

Understanding MMC

This section covers:

- MMC consoles
- Group Policy and MMC
- MMC in author mode

MMC consoles

A new MMC console consists of a window divided into two panes. The left pane contains two tabs: the **Tree** tab and the **Favorites** tab. The right pane contains the details pane. The **Tree** tab, also called the console tree, shows the items that are available in a given console. The details pane shows information about, and functions pertaining to, these items. As you click different items in the console tree, the information in the details pane changes. The details pane can display many types of information including Web pages,

graphics, charts, tables, and columns.

Each console has its own menus and toolbar, separate from those of the main MMC window, that help a user perform tasks. For more information about the main MMC window, see The MMC window.

The operating system you are using may already have preconfigured and saved console files available on the **Programs** menu or in the Administrative Tools folder in Control Panel.

Group Policy and MMC

In Windows 2000, administrators can use Group Policy to restrict or allow access to specific snap-ins or restrict the ability of a user or group to use author mode in MMC. To set policies for users of a particular computer, you must be an administrator for that computer or have equivalent rights. To set policies for an organizational unit in a domain, you must be an administrator for that domain or have equivalent rights. You cannot use this version of MMC to create computer policies; you can only create user policies.

For more information about Group Policy in Windows 2000, see Windows 2000 Help.

For more information about applying Group Policy to MMC, see Setting Group Policy in MMC.

MMC in author mode

You can use MMC in author mode to create new consoles or modify existing consoles. To create an administrative tool, you add snap-ins and other items to a console. You can create additional console windows that provide views of the various items that make up a console. You can also create taskpad views that contain shortcut links to run menu commands from different locations and tools in the console, as well as run command-line functions. After a console is saved, you can distribute it to users.

This section covers:

- The MMC window
- Snap-ins
- Taskpad views and tasks
- The console tree and console root
- The Favorites list
- Console access options

In addition, for a tutorial about creating and customizing consoles, see the Microsoft Web site (http://www.microsoft.com/).

The MMC window

The components of an MMC console are contained in the MMC window. This window has several menus and a toolbar that provide commands to open, create, and save MMC consoles. The menu and toolbar on the MMC window are called the *main menu bar* and the *main toolbar*, respectively. In addition, there is a *status bar* at the bottom of the window and a *description bar* along the top of the details pane. Open MMC to view the MMC window.

When you open a new MMC console, a *console window* appears in the workspace in the MMC window. In the console window, you can assemble and configure a new console and then work with the tools in the console. After you add items to a console, you can hide the main menu bar, main toolbar, description bar, and status bar to prevent users from making unnecessary changes to the console. For more information, see To hide or display features of a saved MMC console and To hide or display menus and toolbars for a snap-in.

Snap-ins

A snap-in is the basic component of an MMC console. Snap-ins always reside in a console; they do not run by themselves.

When you install a component that has a snap-in associated with it on a computer running Windows, the snap-in is available to anyone creating a console on that computer (unless restricted by a user policy). For information about user policies, see Group Policy and MMC.

Stand-alone and extension snap-ins

MMC supports two types of snap-ins: stand-alone snap-ins and extension snap-ins. You can add a stand-alone snap-in, usually called a snap-in, to a console tree without adding another item first. An extension snap-in, usually called an extension, is always added to a stand-alone or extension snap-in that is already on the console tree. When extensions are enabled for a snap-in, they operate on the objects controlled by the snap-in, such as a computer, printer, modem, or other device.

When you add a snap-in or extension to a console, it may appear as a new item in the console tree, or it may add context menu items, additional toolbars, additional property pages, or wizards to a snap-in already installed in the console.

Adding snap-ins to a console

You can add a single snap-in or multiple snap-ins and other items to a console. In addition, you can add multiple instances of a particular snap-in to the same console to administer different computers or to repair a damaged console. Each time you add a new instance of a snap-in to a console, any variables for the snap-in are set at default values until you configure the snap-in. For instance, if you configure a particular snap-in to manage a remote computer and then add a second instance of the snap-in, the second instance will not automatically be configured to manage the remote computer.

In general, you can only add snap-ins that are installed on the computer you are using to author a console. However, in Windows 2000, if your computer is part of a domain, you can use MMC to download any snap-ins that are not locally installed, but that are available in the Active Directory directory service. For more information about adding published snap-ins and extensions to a console, see Creating consoles. For more information about distributing software by using Active Directory in Windows 2000, see Windows 2000 Server Help.

Taskpad views and tasks

Taskpad views are pages to which you can add views of the details pane of a console, as well as shortcuts to functions both inside and outside a given console. You can use these shortcuts to run tasks such as starting wizards, opening property pages, performing menu commands, running command lines, and opening Web pages. You can configure a taskpad view so that it contains all the tasks a given user might need. In addition, you can create multiple taskpad views in a console, so that you can group tasks by function or user.

A taskpad view may make it easier for novice users to perform their jobs. For instance, you can add applicable tasks to a taskpad view and then hide the console tree, so that a user can begin using tools before they are familiar with the location of particular items in the console tree or operating system.

You may also use taskpad views to make complex tasks easier. For instance, if a user must frequently perform a task that involves multiple snap-ins and other tools, you can present tasks in a single location that open or run the necessary dialog boxes, property pages, command lines, and scripts.

For more information about creating taskpad views and tasks, see Creating consoles.

The console tree and console root

The console tree is a hierarchical structure in the left pane of an MMC console on the **Tree** tab. The console tree shows the items that are available in a console. These items can include folders, snap-ins, controls, Web pages, and other tools.

Open MMC to view the console tree of a new console.

In a new console, the only item on the console tree is a folder labeled Console Root. You can create the administrative functions of the console by adding items to the console. For instructions about adding items to a console, see Creating consoles.

You do not need to root a console window on the console root; you can root a console window on any item in the console tree. This hides items in the console tree above the root and focuses the window on the new console root and any administrative tools under it.

For instructions about changing where a console is rooted, see To make a new console window from part of an MMC console tree.

Containers on the console tree

A container is any item on the console tree to which objects are added. You click the plus sign ⊞ to expand a container and view its contents, and the minus sign ⊟ to collapse the container. The obvious container is a folder  , which you can use to group related items on a console tree. However, you can also use MMC to add tools to items other than folders, which then also become containers.

The console root is a container; its only function is to contain the console tree. The top item in a snap-in is usually a folder or another container.

Another type of item that can contain other items is a viewable item. When you click a viewable item, it displays a list, text, or graphic information in the details pane rather than additional items. Web pages are viewable items because they require a browser, which can open only in the details pane. You should not add items to viewable items because, if a user hides the console tree, they may be unaware that a viewable item contains others items. Instead, if you have a collection of viewable items, you can add a folder to the console tree and group the viewable items in the folder. Then a user can select from all the items when the console tree is hidden.

For instructions about hiding the console tree, see To hide or display features of a saved MMC console.

One type of item that cannot contain other items is a leaf. When you click a leaf, it lists items in the details pane. These are normally items that are individually contained on the console tree. However, when items number in the hundreds or thousands, a snap-in uses a leaf rather than a container.

Adding new functionality to a console

You may find that none of the snap-ins provided by the **Add/Remove Snap-in** command provide exactly the capabilities you require. You can try the following possible solutions:

- Check for additional snap-ins or extensions that may have been posted on the Web by Microsoft or other vendors.
- Author your own extension to augment an existing snap-in, or author a new stand-alone snap-in.

For more information about these options, see Resources.

The Favorites list

The Favorites list is located on the **Favorites** tab in the left pane of a new MMC console. The tab appears automatically if you open a console in author mode, or if you already added an item to the Favorites list in a console.

You can use the Favorites list to create shortcuts to items in the console tree. For your convenience, you can add shortcuts to tools that you use often or tools that are several levels down in the console tree. You can also use the Favorites list to make it easier for novice users to complete tasks. For instance, you can create a console that has shortcuts in the Favorites list to only the items in the console tree that a given user needs to perform a job. You can then hide the console tree to further simplify the view.

You can also use the Favorites list to organize taskpad views. For example, a complex console may have multiple taskpad views distributed among the multiple items in the console tree. However, you can add all these taskpad views to the Favorites list, which enables users to access them from a single location.

For more information, see Creating consoles.

Console access options

When building a custom console, you can assign the console one of two general access options: author mode or user mode. There are, in turn, three levels of user mode, so that there are four options for default access to a console:

- Author mode
- User mode - full access
- User mode - limited access, multiple window
- User mode - limited access, single window

You can configure these options in the **Options** dialog box in MMC. For instructions about opening this dialog box, see To set MMC console options.

You can assign author mode to a console to grant full access to all MMC functionality, including the ability to add or remove snap-ins, create new windows, create taskpad views and tasks, add items to the Favorites list, and view all portions of the console tree. By selecting one of the user mode options, authoring features that a user may not need are eliminated. For instance, if you assign the **User mode - full access** option to a console, all window management commands and full access to the console tree are provided, but a user is prevented from adding or removing snap-ins or changing the console properties.

Changes made to consoles in author mode and consoles in user mode are saved differently. If you work with a console in author mode, when you close the console you will be prompted to save your changes. However, if you work with a console in user mode and have cleared the **Do not save changes to this console** check box, available by clicking **Options** on the **Console** menu, changes will be automatically saved when you close the console.

If any of the following conditions apply, the default mode for a console is ignored and a console is opened in author mode:

- MMC is already open when a console is opened.
- A console is opened by using the shortcut menu command **Author**.
- A console is opened at a command prompt with the **/a** option.

For more information about console modes and command-line syntax for MMC, see To open MMC.

Author mode access for MMC is unnecessary for users who do not need to create or change MMC consoles. A system administrator can configure user profile settings to prevent users from opening MMC in author mode, by inhibiting the **/a** option or the shortcut menu option. In addition, in Windows 2000, an administrator can use Group Policy settings to prevent users from opening MMC and saved consoles in author mode. For more information, see Group Policy and MMC.

Using MMC

This section covers:

- Using MMC consoles
- Setting Group Policy in MMC

- Using the MMC Help system
- Authoring MMC consoles

Using MMC consoles

You may need to use only saved MMC consoles that are part of your operating system or an application; you may never need to build custom consoles of your own. Such preconfigured consoles are usually available in the Administrative Tools folder in Control Panel or from the **Start** menu. If you save a custom console to a per-user Administrative Tools folder (in Windows 2000, located at *systemdrive*\Documents and Settings*user*\Start Menu\Programs\Administrative Tools), it is then available in the Administrative Tools folder on the **Programs** menu for that user.

It is likely that any preconfigured consoles that came as part of your operating system are configured to open in one of the three user modes. In Windows 2000, the default mode is **User mode - limited access, single window**. For more information about default console mode settings, see Console access options.

Customizing the view for MMC and saved consoles

You can use the **Customize View** dialog box accessed from the **Customize** command on the **View** menu to hide or display elements for a console. One of the elements that you can hide is the **View** menu itself. If you do this, but then want to reconfigure the view, you can also access the **Customize View** dialog box from the **Customize View** command on the System menu. For more information, see To hide or display features of a saved MMC console and To hide or display menus and toolbars for a snap-in.

Working with columns in saved consoles

In saved consoles that display columns in the details pane, you can customize how the columns and rows appear. For instance, you can reorder or hide columns. You can also reorder rows alphabetically or chronologically by clicking the column heading. In addition, with certain snap-ins, you can filter columns based on additional attributes. If this feature is enabled, a row of drop-down list boxes that contain options for filtering is displayed beneath the column headings. For more information, see To reorder columns in an MMC console, To hide or display columns in an MMC console, and To filter rows in an MMC console.

You can also export the contents of columns to a text file. For more information, see To export columns in an MMC console to a text file.

If you customize the columns in a console, your settings are automatically saved from session to session.

Using property pages in saved consoles

Much of the work done using consoles is performed from property pages. In fact, certain snap-ins or extensions may be accessed in a console only from a property page. You can determine which snap-in provided a particular property page if you hold down the CTRL key while you point with the mouse to the label of the tab for the property page. Also, if you hold down the CTRL key while you point to the title bar of a particular properties dialog box, you can determine the path in the console tree to the item associated with the property page. For more information, see To view the associated snap-in and item for a property page.

As with properties dialog boxes for other applications and tools, the properties dialog boxes for consoles often become hidden behind consoles and other tools. If you cannot find a property page that you were working on, simply reopen the properties dialog box or minimize the other tools on your screen.

Setting Group Policy in MMC

In Windows 2000, you can use Group Policy to restrict access to particular snap-ins or functions of MMC. You can enable Group Policy for users of a computer or for organizational units of a domain.

Enabling Group Policy for users of a computer

To set MMC or snap-in policies for users of a particular computer, you must first add the Group Policy snap-in to a new console. For more information, see To add an item to a new MMC console for a local computer or To add an item to a new MMC console for a remote computer. When you add the Group Policy snap-in to a new console, you need to confirm that the **Administrative Templates (Users)** check box is selected (under **Available extensions** on the **Extensions** tab in the **Add/Remove Snap-in** dialog box). This is enabled by default on a new installation of Windows 2000. For information about configuring Group Policy, see Windows 2000 Help.

Enabling Group Policy for an organizational unit in a domain

To set MMC or snap-in policies for a domain, you must use a computer that is configured as a domain controller and you must be an Administrator for that domain or have equivalent rights. For information about configuring a domain controller, see Windows 2000 Help.

After you configure your computer as a domain controller, the Active Directory Users and Computers console appears in the Administrative Tools folder on the **Programs** menu. You can use this tool to set policies for organizational units in the domain. Before you begin, you need to confirm that **Group Policy** is selected (on the **Extensions** tab in the **Add/Remove Snap-in** dialog box). Then, as in setting policies for users of an individual computer, you need to confirm that the **Administrative Templates (Users)** extension is selected for Group Policy.

Setting policies

You can set policies for users, groups, and organizational units that restrict or permit access to specific snap-ins. You can also set policies that restrict users, groups, and organizational units from using snap-ins that are not explicitly permitted (all snap-ins are restricted except those on the permitted list). This second option is the best choice if you are planning to restrict access for a user, group, or organizational unit to most of the snap-ins. For more information, see To permit or restrict access to a snap-in, To permit or restrict access to a snap-in for a domain, To restrict access to a permitted list of snap-ins and To restrict access to a permitted list of snap-ins for a domain.

You can also set policies that restrict users, groups, and organizational units from using author mode in MMC to create new consoles or customize existing consoles. For more information, see To restrict access to author mode in MMC and To restrict access to author mode in MMC for a domain.

The following table describes the behavior of MMC and snap-ins when you implement a policy for a user or group:

Policy	Action	Result
Enable **Restrict the user from entering author mode**.	Open MMC or open a console in author mode: • Type **mmc** at a command prompt. • Type **mmc** *path******filename.msc* **/a** at a command prompt. • Right-click an .msc file, and then click **Author**. • Open a console file that is configured to open in author mode.	An error message appears.

Disable or do not configure **Restrict the user from entering author mode**.	Open MMC or open a console in author mode: • Type **mmc** at a command prompt. • Type **mmc** *path**filename.msc* **/a** at a command prompt. • Right-click an .msc file, and then click **Author**. • Open a console file that is configured to open in author mode.	Use of author mode is unrestricted.
Enable **Restrict users to the explicitly permitted list of snap-ins**.	Open a console that contains a snap-in that is not on the permitted list, or a snap-in that is extended by a snap-in that is not on the permitted list: • Type **mmc** *path**filename.msc* at a command prompt. • Double-click an .msc file. • Right-click an .msc file, and then click **Open**.	An error message appears. **Note** • If you enable this policy, only explicitly permitted snap-ins appear in the list of available snap-ins in the **Add Standalone Snap-in** dialog box in MMC—all other snap-ins are restricted.
Disable or do not configure **Restrict users to the explicitly permitted list of snap-ins**.	Open a console that contains a snap-in that is not on the permitted list, or a snap-in that is not extended by a snap-in on the permitted list: • Type **mmc** *path**filename.msc* at a command prompt. • Double-click an .msc file. • Right-click an .msc file, and then click **Open**.	Use of the console that contains the snap-in is unrestricted.
Explicitly permit a snap-in.	Open a console that contains the snap-in, or a snap-in that is extended by the permitted snap-in: • Type **mmc** *path**filename.msc* at a command prompt. • Double-click the .msc file. • Right-click the .msc file, and then click **Open**.	Use of the console that contains the snap-in is unrestricted.
Explicitly restrict a snap-in.	Open a console file that contains the snap-in, or contains a snap-in that is extended by the restricted snap-in: • Type**mmc** *path**filename.msc* at a command prompt. • Double-click the .msc file. • Right-click the .msc file, and then click **Open**.	An error message appears.
Do not configure the policy to permit or restrict a snap-in.	Open a console file that contains the snap-in, or contains a snap-in that is extended by this snap-in: • Type **mmc** *path**filename.msc* at a command prompt. • Double-click the .msc file. • Right-click the .msc file, and then click **Open**.	Use of the console that contains the snap-in is unrestricted unless the user, group, or organizational unit is restricted to a list of explicitly permitted snap-ins.

Using the MMC Help system

You can access Help for MMC from the **Help** menu on the main toolbar, from the  button on the toolbar of a console window, on the system menu of the MMC window or a console window, by right-clicking an item in the console tree or details pane, or by pressing the F1 key.

Help for MMC displays a combined table of contents that includes general Help for MMC and Help specific to each snap-in included in the console. Snap-in Help is provided only for existing Help files that were associated to snap-ins by their authors. If you are authoring a console, you may want to provide additional documentation for tasks associated with the console or provide information specifically related to your network.

Authoring MMC consoles

This section covers:

- Creating consoles
- Saving consoles
- Using custom consoles

For more information about author mode, see MMC in author mode.

Creating consoles

Before you author a console, you should identify the tasks the console will perform, the components to be administered, and the snap-ins and controls that are needed to perform the tasks. You should also consider whether you need to create a taskpad view and tasks. After you make these decisions, you can open a new console and start adding items to the console tree. For a tutorial about creating and customizing consoles, see the Microsoft Web site (http://www.microsoft.com/).

To create or edit a console, open the console in author mode (use the command-line option **/a**). To view the complete command-line syntax, see To open MMC.

Adding items to the console tree

You can help users locate the components they need in the console by arranging items hierarchically or in groups on the console tree. To add items to the console tree, you can use the **Add/Remove Snap-in** command on the **Console** menu of the main toolbar of MMC.

In the **Add/Remove Snap-in** dialog box, **Snap-ins added to** determines the item on the console tree under which new items are added. The default value is **Console Root**. You can click an item in **Snap-ins added to** to locate an object elsewhere on the console tree.

The **Add Standalone Snap-in** dialog box displays a list of available snap-ins. For computers running Windows 2000 that are members of a domain, this list includes both locally-installed snap-ins and snap-ins published in the Active Directory directory service. For snap-ins that are available in Active Directory, **Not Installed** appears in the **Vendor** column.

If you have already installed a snap-in, and you want to enable one of its extension snap-ins, you can use the **Extensions** tab in the **Add/Remove Snap-in** dialog box. On this tab, you can select any item in the console tree that can be extended and view the extension snap-ins that you can enable or disable. When you enable an extension snap-in, it is automatically inserted in the console tree under the selected item. If there is more than one instance of a snap-in on the console tree, all instances of the snap-in are extended.

After an extension snap-in is enabled, you may notice that it appears in **Snap-ins that can be extended** along with the stand-alone snap-ins. This means that the extension snap-in also has extensions that you can enable.

Like stand-alone snap-ins, an administrator can also publish extension snap-ins in the Windows 2000 Active Directory directory service. Extension snap-ins available to a user from Active Directory appear in the list of available extension snap-ins with any locally installed extension snap-ins, except that they are followed by the phrase **(not installed)**. You must specifically download extension snap-ins from the directory service to make them available in a console. Thus, to download all extensions for a given item, do not select the **Add all extensions** check box on the **Extensions** tab of the **Add/Remove Snap-in** dialog box. Instead, clear this check box and select the check boxes next to each extension that you want to download.

You can add multiple instances of the same snap-in to a console either to manage multiple remote computers from the same console or to repair a damaged console. As an example of the latter situation, you may notice that a tool is behaving differently than expected, that its configuration is outdated, or that it is timing out because resources have been removed. To fix the console, try adding a new instance of the snap-in to the console, configure it as needed, and then remove the old instance of the snap-in from the console.

For information about adding items to the console tree, see To add an item to a new MMC console for a local computer, To add an item to a new MMC console for a remote computer, To add a published snap-in to a new MMC console, To add an extension snap-in to an MMC console, and To add a published extension snap-in to an MMC console.

Adding taskpad views and tasks

Before you add taskpad views and tasks to a console, determine how many taskpad views you need. If you need multiple taskpad views, you also need to determine how the tasks are divided among the taskpad views. In addition, you should decide what kind of taskpad view you want to use—one that displays a list and tasks, or one that displays tasks only.

To create a taskpad view for a console, the console must contain at least one snap-in. You can use the New Taskpad View wizard to configure the titles, headings, and lists that appear in the taskpad view, and to define whether a taskpad view is associated with a single item or multiple items in the console tree.

After you complete the New Taskpad View wizard, you can use the New Task wizard to add tasks to the taskpad view. Tasks can include menu commands for the items in the console, as well as commands that are run from a command prompt. You can create commands to act on part of the console tree or details pane, or to open another component on your computer. However, if you create a task from a menu command for an item in the console tree, and then you remove that item, the task is disabled.

For information about creating and editing taskpad views and tasks, see To create a taskpad view in a saved MMC console, To create tasks for a taskpad view in a saved MMC console, To edit a taskpad view in a saved MMC console, and To edit tasks in a taskpad view in a saved MMC console.

Viewing the console tree in a console window

When the console tree is visible, it appears in the left pane of a console window. You can also hide the console tree. For information about hiding the console tree, see To hide or display features of a saved MMC console.

What you view in a console window is determined by where the console window is rooted on the console tree. The initial window in a new console is rooted at Console Root, as are any windows you create with the **New Window** command on the **Window** menu on the main toolbar.

You can close console windows to hide the console root or entire portions of the console tree. You can then configure the console to prevent users from viewing hidden portions of the tree. However, the entire console tree is always saved when you save a console.

Rooting console windows on items in the console tree

While you can use MMC to make consoles that meet every administrative need for a group, you can also design simple consoles for less experienced users. For instance, after you add items to a console tree, you can open additional console windows rooted on any item in the console tree. You can use this method to create console windows that display specific administrative components of the console tree. You can then close windows that show portions of the console tree that users do not need.

Closing a window does not remove any items from the console tree; when you close a window, you remove only that view of the console tree. The entire tree is still saved when you save the console, and you can always view the console root.

For information about changing the console root, see To make a new console window from part of an MMC console tree.

For information about viewing a console root that is hidden, see To make a new console window from an MMC console.

Adding items to the Favorites list

You can use the Favorites list to create shortcuts to items in the console tree and to taskpad views. You can then access these items from both the **Tree** tab and the **Favorites** tab.

For more information about creating the Favorites list, see To add an item to the Favorites list in an MMC console and To organize the Favorites list in an MMC console.

Configuring console options

You can use the **Options** dialog box, available from the **Console** menu, to choose an icon for, change the title of, and choose the default mode for a console.

Icons are available from many sources including Shell32.dll, located on Windows 2000 and Windows NT in the *systemroot*\system32 folder.

When changing the title of a console, keep in mind that by default, as you click items in the console tree, the title bar displays the path to the selected item. But if you change the title of a console, the title bar will not display this path. However, if you delete the title, the default behavior is restored.

When considering which mode to set as the default for a console, remember that if you use one of the user modes, you can open the console at any time using the **Author** or **Run As** commands—you will not need to use author mode for most management tasks.

For more information about console options, see To set MMC console options and Console access options.

Saving consoles

Saving an MMC console to a file preserves the list of loaded snap-ins for the console, the arrangement and contents of console windows in the main MMC window, the default mode, and information about permissions. All the configuration settings for the tools and controls

are saved with the console and restored when the console file is opened. You can open a console file on different computers or even different networks and restore the saved settings for all the tools.

Console files have an .msc (management saved console) extension. The operating system you are using may already have preconfigured and saved console files that are available from the Administrative Tools folder in Control Panel. If you create console files and save them in your per-user Administrative Tools folder (in Windows 2000, located at *systemdrive*\Documents and Settings*user*\Start Menu\Programs\Administrative Tools), they are available from the Administrative Tools folder on the **Programs** menu for you only—the console files are not available for other users of the computer. After you save a console, you can distribute it by using a floppy disk, e-mail, or your network.

If you are working with a console in author mode, you can save changes to the console by using the **Save** command on the **Console** menu. If you are working with a console in one of the user modes, saving changes to the console is determined by whether the **Do not save changes to this console** check box (available by clicking **Options** on the **Console** menu) was selected when the console was configured. If this check box was not selected, changes to the console are automatically saved when you close MMC; if it was selected, changes to the console are discarded when you close MMC. For more information about saving consoles, see To save an MMC console file. For more information about console modes, see Console access options.

Using custom consoles

After you create and save an MMC console, you can use it on your local computer, send it to other users in e-mail, post it on your network or the Web, or copy it to a floppy disk and install it on other computers. In addition, in Windows 2000, you can use MMC and the Active Directory directory service to publish consoles or assign consoles to users. For more information about distributing software by using Active Directory in Windows 2000, see Windows 2000 Server Help.

Requirements to use a console

To use a console, you must have access to the services and administrative tools included in the console, either installed on the local computer or available on the network. You must also have administrative permissions for the components on the system that is administered by the console.

Opening a saved console

If you save a console to the per-user Administrative Tools folder (in Windows 2000, located at *systemdrive*\Documents and Settings*user*\Start Menu\Programs\Administrative Tools), it is then available in the Administrative Tools folder on the **Programs** menu.

If you know the name and location of a console file, you can open it as you would any other document:

- By double-clicking the .msc file.
- By right-clicking the .msc file, and then clicking **Open**.
- From a command prompt.

In addition, on computers running Windows 2000, you can log on to your computer with user rights and perform routine tasks, but use the **Run As** command to open console files and perform administrative tasks that require Administrator rights. You can use this command by typing **runas** at a command prompt or by right-clicking an .msc file, and then clicking **Run As**.

For more information about opening consoles, see To open a saved MMC console for a local computer, To open a saved MMC console for a remote computer, and To open MMC.

Resources

For more information about MMC, try the following resources:

- The Personal Support Center Web site at the Microsoft Web site (http://www.microsoft.com/) contains general support information and articles written by support professionals at Microsoft.
- The Microsoft Management Console Web site at the Microsoft Web site (http://www.microsoft.com/) contains information for snap-in authors and developers.
- The Windows 2000 Web site at the Microsoft Web site (http://www.microsoft.com/) provides a tutorial for creating and customizing MMC consoles.

Accessibility for MMC

In addition to Microsoft Windows accessibility products and services, MMC provides keyboard shortcuts for selecting commands and for navigating in and between console windows:

- Navigation in MMC
- MMC main window keyboard shortcuts
- MMC console window keyboard shortcuts

Snap-ins and other items that are added to an MMC console may also provide accessibility features. For more information, refer to the Help or other documentation for the console item.

Navigation in MMC

You can move through an MMC console tree by expanding and collapsing branches as needed with the plus sign ⊞ and minus sign ⊟ keys or by clicking and double-clicking with the mouse. The following table lists the keystrokes you can use to move in and between console windows.

Keystroke action	Result
TAB or F6	Moves forward between panes in the active console window.
SHIFT+TAB or SHIFT+F6	Moves backward between panes in the active console window.
CTRL+TAB or CTRL+F6	Moves forward between console windows.
CTRL+SHIFT+TAB or CTRL+SHIFT+F6	Moves backward between console windows.
PLUS SIGN (+) on the numeric keypad	Expands the selected item.
MINUS SIGN (-) on the numeric keypad	Collapses the selected item.
Asterisk (*) on the numeric keypad	Expands the entire console tree below the root item in the active console window.
UP ARROW	Moves the selection up one item in a pane.

DOWN ARROW	Moves the selection down one item in a pane.
PAGE UP	Moves the selection to the top item visible in a pane.
PAGE DOWN	Moves the selection to the bottom item visible in a pane.
HOME	Moves the selection to the first item in a pane.
END	Moves the selection to the last item in a pane.
RIGHT ARROW	Expands the selected item. If the selected item does not contain hidden items, behaves like DOWN ARROW.
LEFT ARROW	Collapses the selected item. If the selected item doesn't contain exposed items, behaves like UP ARROW.
ALT+RIGHT ARROW	Moves the selection to the next item. Performs the same function as the Forward arrow on the toolbar.
ALT+LEFT ARROW	Moves the selection to the previous item. Performs the same function as the Back arrow on the toolbar.

The following table lists the mouse actions you can use to move through an MMC console tree.

Mouse action	**Result**
Click	Selects an item.
Double-click	Displays or hides items contained by the selected item. Displays properties for or opens an item.
Right-click	Displays the **Action** shortcut menu for the selected item.

Note

- If the mouse buttons do not behave as indicated here, the right and left buttons may have been switched. The computer you are using may be configured so that the default actions obtained with the left and right mouse buttons are reversed.

MMC main window keyboard shortcuts

The following table lists keyboard shortcuts for the menu commands that act on the entire console or the main window of a console.

Action	**Result**
CTRL+O	Opens a saved console.
CTRL+N	Opens a new console.
CTRL+S	Saves the open console.
CTRL+M	Adds or removes a console item.
CTRL+W	Opens a new window.
F5	Refreshes the content of all console windows.
ALT+SPACEBAR	Displays the MMC window menu.
ALT+F4	Closes the active console window.

Note

- The CTRL+W keyboard shortcut is available for consoles opened in author mode or user mode - full access. Other CTRL+ shortcuts are only available for consoles opened in author mode.

MMC console window keyboard shortcuts

The following table lists keyboard shortcuts for the menu commands that act on the active console window in a console or on the contents of a console window.

Action	**Result**
CTRL+P	Prints the current page or active pane.
ALT+MINUS SIGN	Displays the window menu for the active console window.
SHIFT+F10	Displays the **Action** shortcut menu for the selected item.
ALT+A	Displays the **Action** menu for the active console window.
ALT+V	Displays the **View** menu for the active console window.
ALT+F	Displays the **Favorites** menu for the active console window.
F1	Opens the Help topic, if any, for the selected item.
F5	Refreshes the content of all console windows.
CTRL+F10	Maximizes the active console window.
CTRL+F5	Restores the active console window.
ALT+ENTER	Displays the properties dialog box, if any, for the selected item.
F2	Renames the selected item.
CTRL+F4	Closes the active console window. When a console has only one console window, this closes the console.

Troubleshooting

What problem are you having?

Help for a snap-in cannot be found.

Cause: You can usually access Help for MMC from the **Help** menu on the main toolbar, from the icon on the toolbar of a console window, on the system menu of the MMC window or a console window, by right-clicking an item in the console tree or details pane, or by pressing the F1 key. However, if you add a snap-in to a console, but cannot find Help for the snap-in by using the standard methods, the snap-in may not provide a Help file to merge into the MMC Help table of contents. Instead, the snap-in may use a different method to provide Help.

Solution: Open a console in author mode that contains the snap-in, click the item in the console tree for which you want Help, and then click the **Help** menu. A separate command for the snap-in Help may be displayed on the **Help** menu above the **Help Topics** command. If you do not see a separate command, view the contents of the toolbars and details pane for a Help button or additional icon. If you do not see a separate command, button, or icon, then no Help is available from MMC for the snap-in.

A snap-in is not listed in the Add Standalone Snap-in dialog box.

Cause: The corresponding service or software may not be installed on your computer.

Solution: You must install the component to view its snap-in.

See also: To install a program managed by an MMC snap-in

Cause: If you are using a computer running Windows 2000, an administrator may have set a policy that restricts you from accessing the snap-in.

Solution: See your system administrator.

See also: Setting Group Policy in MMC

When using a console, one or more of the following occurs: the console is not behaving as expected, the console is timing out, or error messages are displayed that you have not seen before.

Cause: The console may have become damaged, or because of changes to your network, the configuration of the console may have become outdated.

Solution: Determine which snap-in is causing the problem in the console and then refer to the troubleshooting information in the documentation for that snap-in to find out how to repair or reconfigure the snap-in. To determine which snap-in is causing the problem, right-click the item in the console tree or the details pane and then click **Properties**. Hold down the CTRL key and point to the labels of the tabs in the dialog box.

If you cannot directly repair or reconfigure the console, try adding another instance of the snap-in you are using to the console, configure it as needed, and then remove the old version of the snap-in.

See also: To add an item to a new MMC console for a local computer, To add an item to a new MMC console for a remote computer, Snap-ins, and To view the associated snap-in and item for a property page.

Group Policy

You use Group Policy to define settings that are applied to computers or users as they are initialized.

- Before using Group Policy, see Checklists.
- To find features that have been moved in Windows 2000, see New ways to do familiar tasks.
- For tips on using Group Policy, see Best practices.
- For help with specific tasks, see How to.
- For general background information, see Concepts
- For problem-solving instructions, see Troubleshooting.

Checklists

This section covers:

- Checklist: Implementing Group Policy in Active Directory
- Checklist: Implementing local Group Policy
- Checklist: Opening the Software Installation snap-in

Checklist: Implementing Group Policy through Active Directory

	Step	References
☐		
Review key concepts about Active Directory and Group Policy.	Group Policy overview; Active Directory Users and Computers	
☐	Install Windows 2000 on the client computers.	Remote Installation Services
☐	Install a Windows 2000 Server domain controller.	To install a domain controller
☐	Determine the Active Directory structure that you want to use.	Best Practices; Planning site structure; Planning your domain structure; Planning your DNS structure
☐	Open Group Policy.	Open the Group Policy snap-in; Ways to open the Group Policy snap-in

Checklist: Implementing local Group Policy

	Step	Reference

☐	Review key concepts about local Group Policy.	Group Policy objects; Local Group Policy
☐	Install Windows 2000 Server or Windows 2000 Professional on the local computer.	Getting Started
☐	Open Group Policy to edit the local Group Policy snap-in.	Open the Group Policy snap-in; Ways to open the Group Policy snap-in

Checklist: Opening the Software Installation snap-in

	Step	References
☐		

Review key concepts about Software Installation, Group Policy, and Active Directory.	Active Directory Users and Computers; Group Policy overview; Software Installation	
☐	Set up Group Policy in your organization.	Checklist: Implementing Group Policy in Active Directory
☐	Open Group Policy to apply to the site, domain, or organizational unit containing the users and computers that should receive the software.	Open Group Policy; Ways to open the Group Policy snap-in
☐	Obtain Windows Installer (.msi) packages for your software.	Contact the software vendor
☐	Open the Software Installation snap-in.	To open the Software Installation snap-in

New ways to do familiar tasks

Windows NT 4.0 introduced the System Policy Editor, which you could use to create a system policy to control user work environment and actions, and to enforce system configuration settings for all computers running Windows NT 4.0. Policies define the various components of the desktop environment, including the applications available to users, the applications that appear on users' desktops, and the options displayed on the **Start** menu.

Users upgrading from Windows NT 4.0 will find that Group Policy and its extensions provide a unified replacement for many of the tools they are familiar with.

If you want to	In Windows NT 4.0 use	In Windows 2000 use
Set policies on users and computers in a site	Not applicable	Group Policy accessed through Active Directory Sites and Services
Set policies on users and computers in a domain	System Policy Editor (poledit.exe)	Group Policy accessed through Active Directory Users and Computers
Set policies on users and computers in an organizational unit	Not applicable	Group Policy accessed through Active Directory Users and Computers
Use security groups to filter the scope of policy	Not applicable	Edit the permission entry for **Apply Group Policy** on the security tab of the Group Policy object's properties sheet.
Manage software	For an administrator, Systems Management Server. For a user, Add/Remove Programs in Control Panel.	Systems Management Server and the three Software Installation and Maintenance tools: • Software Installation, an extension to the Group Policy snap-in • Windows Installer • Add/Remove Programs in Control Panel
Create a safe user interface for editing the registry	Windows NT 4.0–style Administrative Templates for System Policy Editor	Windows 2000–style Administrative Templates for Group Policy See The role of Administrative Templates concerning how the use of .adm files has changed in Windows 2000.
Perform general administrative tasks	Administrative wizards, User Manager, and Server Manager	Microsoft Management Console (MMC) snap-ins, particularly Active Directory Users and Computers, Active Directory Sites and Services, and Group Policy and its extensions.

Best practices

Group Policy

- **Disabling unused parts of a Group Policy object**
  If a Group Policy object has, under the User Configuration or Computer Configuration node of the console, only settings that are **Not Configured**, then you can avoid processing those settings by disabling the node. This expedites startup and logon for those users and computers subject to the Group Policy object. For more information, see To disable the User Configuration settings in a Group Policy object and To disable the Computer Configuration settings in a Group Policy object.
- **Using the Block Policy Inheritance and No Override features sparingly**
  Routine use of these feature makes it difficult to troubleshoot policy.

- **Minimizing the number of Group Policy objects associated with users in domains or organizational units**
  The more Group Policy objects are applied to a user, the longer it takes to log on.
- **Filtering policy based on security group membership**
  Users who do not have an Access Control Entry (ACE) directing that a particular Group Policy object be applied to them can avoid the associated logon delay, because the Group Policy object will not be processed for those users.

  Filtering can only be done using membership in security groups.

  The ACEs appear on the **Security** tab on the **Properties** page of a Group Policy object.
- **Overriding user-based Group Policy with computer-based Group Policy only when necessary**
  Do this only if you need the desktop configuration to be the same regardless of who logs on.
- **Avoiding cross-domain Group Policy object assignments**
  The processing of Group Policy objects will slow logon and startup if Group Policy is obtained from another domain.

Software Installation and management

- **Specifying application categories for your organization**
  Using categories makes it easier for users to find an application in Add/Remove Programs in Control Panel. For example, you could define categories such as Sales Applications, Accounting Applications, and so on. For more information, see To specify categories for applications.
- **Making sure Windows Installer packages are correctly transformed before they are published or assigned**
  Remember that transforms are applied to packages at the time of assignment or publication. Transforms, or .mst files, are customizations applied to Windows Installer packages. A transform is applied at the time of assignment or publication, not at the time of installation. In practical terms, this means that you should make sure the **Modifications** tab of the package properties dialog box is set up as you intend before you click **OK**. If you neglect to do this, and assign or publish a transformed package before you have completely configured it, then you can either remove the software and republish or reassign it or upgrade the software with a completely transformed version. For procedures on how to do this, see To remove a managed application and To upgrade a managed application.
- **Assigning or publishing just once per Group Policy object**
  A Windows Installer package should be assigned or published no more than once in the same Group Policy object. For example, if you assign Microsoft Office to the computers affected by a Group Policy object, then do not assign or publish it to users affected by the Group Policy object.
- **Taking advantage of authoring tools**
  Developers familiar with the files, registry entries, and other requirements for an application to work properly can author native Windows Installer packages using tools available from various software vendors.
- **Repackaging existing software**
  You can use commercially available tools to create Windows Installer packages for software that does not include natively authored .msi files. These work by comparing a computer's state before and after installation. For best results, install onto a computer free of other application software (clean install).
- **Using SMS and Dfs**
  Microsoft Systems Management Server (SMS) and the Windows 2000 Distributed File System (Dfs) are helpful in managing the software distribution points (the network shares from which users install their managed software).
- **Assigning or publishing at a high level in the Active Directory hierarchy**
  Because Group Policy settings apply by default to child Active Directory containers, it is efficient to assign or publish by linking a Group Policy object to a parent organizational unit or domain. Use security descriptors (access control entries or ACEs) on the Group Policy object for finer control over who receives the software. For more information, see Using security groups to filter Group Policy.

  Notes

  - Authenticated Users need the **Read** and **Apply Group Policy** ACEs to be able to install from the software distribution point.
  - Administrators need **Full Control** to manage software.
- **Using Software Installation properties for widely scoped control**
  In the Group Policy console, right-click **Software Installation** and on the context menu click **Properties**.

  Where?
  Group_Policy_object_name
  Computer Configuration (or User Configuration)
  Software Settings
  Software Installation

  This spares administrative keystrokes when assigning or publishing a large number of packages with similar properties in a single Group Policy object—for example, when all the software is published and it all comes from the same software distribution point.
- **Using Windows Installer package properties for fine control**
  Proceed to the Software Installation node as described previously, but right-click the package in the details pane and click **Properties**. Use this for assigning or publishing a single package.

Folder Redirection

- **Enabling client-side caching**
  This is especially important for users with laptops.
- **Incorporating %username% into fully qualified universal naming convention (UNC) paths**
  This allows users to have their own folders. For example, \\server\share\%username%\My Documents
- **Having My Pictures follow My Documents**
  This is advisable unless there is a compelling reason not to, such as file share scalability.
- **Policy removal considerations**
  Keep in mind the behavior your Folder Redirection policies will have upon policy removal, as described in Caution.
- **Accepting defaults**
  In general, accept the default Folder Redirection settings.

How to...

- Open the Group Policy snap-in
- Use Administrative Templates
- Use scripts

- Use the Software Installation snap-in
- Use the Folder Redirection snap-in
- Configure Group Policy

Open the Group Policy snap-in

- Open Group Policy from Active Directory Users and Computers
- Open Group Policy from Active Directory Site and Services
- Open Group Policy as a stand-alone MMC snap-in

If you're not sure which way you should open Group Policy, see Ways to open the Group Policy snap-in.

To open Group Policy from Active Directory Users and Computers

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the domain or organizational unit you want to set Group Policy for.

   Where?
   - Active Directory Users and Computers [*domain_controller_name.domain_name*]
   - *domain*
   - *organizational_unit*
   - *child_organizational_unit...*
3. Click **Properties**, and then click the **Group Policy** tab.
4. Click **Edit** to open the Group Policy object you want to edit. (Or, click **New** to create a new Group Policy object, and then click **Edit**.)

Note

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.

To open Group Policy from Active Directory Sites and Services

1. Open Active Directory Sites and Services.
2. In the console tree, right-click the site you want to set Group Policy for.

   Where?
   - Active Directory Sites and Services [*domain_controller_name.domain_name*]
   - Sites folder
   - Site
3. Click **Properties** and then click the **Group Policy** tab.
4. Click an entry in the **Group Policy object links** list to select an existing Group Policy object, and then click **Edit**.

   Or, you can click **New** to create a new Group Policy object, and then click **Edit**.

Note

- To open Active Directory Sites and Services, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Sites and Services**.

To open Group Policy as a stand-alone MMC snap-in

1. Open Microsoft Management Console.
2. On the MMC console's menu bar, click **Console**, and then click **Add/Remove Snap-in**.
3. On the **Standalone** tab, click **Add**.
4. In the **Add Standalone Snap-in** dialog box, click **Group Policy**, and then click **Add**.
5. In the **Select Group Policy object** dialog box, click **Local Computer** to edit the local Group Policy object, or browse to find the Group Policy object you want.
6. Click **Finish**, and then click **OK**. The Group Policy snap-in now opens the specified Group Policy object for editing.

Note

- To open an MMC console, click **Start**, click **Run**, type **mmc**, and then press ENTER.

Work with Group Policy objects

- Edit a Group Policy object
- Edit the local Group Policy object
- Create a new Group Policy object
- Delete a Group Policy object
- Link a Group Policy object to a site, domain, or organizational unit
- Block policy inheritance
- Disable a Group Policy object for a site, domain, or organizational unit
- Prevent a Group Policy object from being overridden

To edit a Group Policy object

1. Open the Group Policy object you want to edit.
2. Double-click items in the details pane to change their settings.

Notes

- You need Read and Write permissions on a Group Policy object to open it.
- Because changes to a Group Policy object take place immediately, you might want to disable the Group Policy object while you are editing it.

To edit the local Group Policy object

1. Open Group Policy.
2. Make whatever policy setting you want in the Group Policy console.

Notes

- To open Group Policy to edit the local Group Policy object, click **Start**, click **Run**, type **gpedit.msc**, and then press ENTER.

To create a new Group Policy object

1. Open Active Directory Users and Computers to create a Group Policy object linked to a domain or an organizational unit.

   or

   Open Active Directory Sites and Services to create a Group Policy object linked to a site.
2. In the console, right-click the site, domain, or organizational unit to which the newly created Group Policy object will be linked. (It will be stored in the current domain.)
3. Click **Properties** and then click the **Group Policy** tab.
4. Click **New**, type a name for the Group Policy object, and then click **Close**.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- To open Active Directory Sites and Services, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Sites and Services**.
- The newly created Group Policy object is linked by default to the site, domain, or organizational unit that was selected in the Microsoft Management Console when it was created. Therefore its settings apply to that site, domain, or organizational unit. You might want to unlink the Group Policy object from the site, domain, or organizational unit, so that its settings do not apply.

To delete a Group Policy object

1. Open Active Directory Users and Computers.
2. In the console, right-click the domain or any organizational unit in the domain.
3. Click **Properties**, and then click the **Group Policy** tab.
4. To find all the Group Policy objects stored in the domain, click **Add** to open the **Add a Group Policy object Link** dialog box, and then click the **All** tab.
5. Right-click the Group Policy object to delete, and then click **Delete**.
6. When asked if you are sure, click **Yes**, and then click **OK**.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- When you delete a Group Policy object, any sites, domains, or organizational units to which it is linked are no longer affected by it. You might want to disable the Group Policy object instead.

To link a Group Policy object to a site, domain, or an organizational unit

1. Open Active Directory Users and Computers to link to a domain or an organizational unit, or Active Directory Sites and Services to link to a site.
2. In the console, right-click the site, domain, or organizational unit to which the Group Policy object should be linked.
3. Click **Properties**, and then click the **Group Policy** tab.
4. To add the Group Policy object to the **Group Policy object Links** list, click **Add**. The **Add a Group Policy object Link** dialog box appears.
5. Click the **All** tab, click the Group Policy object you want, and then click **OK**.
6. In the **Properties** dialog box for the site, domain, or organizational unit, click **OK**.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- To open Active Directory Sites and Services, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Sites and Services**.
- You link a Group Policy object to specify that its settings should be applied to users and computers in the site, domain, or organizational unit, and to users and computers in Active Directory containers that inherit from the site, domain, or organizational unit.

To block policy inheritance

1. To block policy inheritance in a site, open Active Directory Sites and Services.

   To block policy inheritance in a domain or organizational unit, open Active Directory Users and Computers.
2. In the console, right-click the site, domain, or organizational unit in which you want to block Group Policy inheritance, and then click **Properties**.
3. Click the **Group Policy** tab, make sure the **Block Policy inheritance** check box is selected, and then click **OK**.

Notes

- To open Active Directory Sites and Services, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Sites and Services**.
- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- The **Block Policy inheritance** setting blocks Group Policy objects that apply higher in the Active Directory hierarchy of sites, domains, and organizational units. It does not block Group Policy objects if they have **No Override** enabled.
- The **Block Policy inheritance** setting is set only on sites, domains, and organizational units, not on individual Group Policy objects.

To disable a Group Policy object for a site, domain, or organizational unit

1. Open Active Directory Users and Computers to disable a Group Policy object for a domain or organizational unit.

   or

   Open Active Directory Sites and Services to disable a Group Policy object for a site.
2. In the console, right-click the site, domain, or organizational unit from which to unlink the Group Policy object (which disables it for

that site, domain, or organizational unit).

3. Click **Properties**, and then click the **Group Policy** tab.
4. Select the Group Policy object you want to disable, and then click **Delete**. The **Delete** dialog box appears.
5. Make sure **Remove the link from the list** is selected, click **OK** on the **Delete** dialog box.

Important

- If you select **Remove the link and delete the Group Policy object permanently**, then all sites, domains, and organizational units to which the Group Policy object is linked will no longer have those Group Policy settings applied to them.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- To open Active Directory Sites and Services, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Sites and Services**.

To prevent a Group Policy object from being overridden

1. Open Active Directory Users and Computers for a Group Policy object linked to a domain or organizational unit, or open Active Directory Sites and Services for a Group Policy object linked to a site.
2. In the console, right-click the site, domain, or organizational unit to which the Group Policy object is linked.
3. Click **Properties**, and then click the **Group Policy** tab.
4. Right-click the Group Policy object link you want to enforce, click **No Override** on the context menu, and then click **OK**. (This toggles the No Override state to Active, and a check appears in the **No Override** column.)

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- To open Active Directory Sites and Services, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Sites and Services**.
- Setting **No Override** on a Group Policy object link results in the enforcement of those Group Policy settings on all users or computers in the site, domain, or organizational unit, and on all users and computers in Active Directory containers that inherit Group Policy from it.
- Group Policy settings enforced by way of **No Override** cannot be blocked.

Work with Group Policy object properties

- Filter the scope of Group Policy according to security group membership
- Find the sites, domains, and organizational units to which a Group Policy object is linked
- Disable the User Configuration settings in a Group Policy object
- Disable the Computer Configuration settings in a Group Policy object

To filter the scope of Group Policy according to security group membership

1. Open the Group Policy object whose scope is to be filtered.
2. Right-click the root node of the console, which shows a Group Policy icon followed by a label that appears as follows: *Group_Policy_object_name* [*domain_controller_name.domain_name*] **Policy**
3. Click **Properties**, click the **Security** tab, and then click the security group through which to filter this Group Policy object.

   If you need to change the list of security groups through which to filter this Group Policy object, you can add or remove security groups using **Add** and **Remove**.
4. Set the permissions as shown in the following table, and then on the property sheet for the Group Policy object, click **OK**.

Your intention	Set these permissions	Result
Members of this security group should have this Group Policy object applied to them.	Set **Apply Group Policy** to **Allow**. Set **Read** to **Allow**.	This Group Policy object applies to members of this security group unless they are members of at least one other security group that has **Apply Group Policy** set to **Deny**, or **Read** set to **Deny**, or both.
Members of this security group are exempt from this Group Policy object.	Set **Apply Group Policy** to **Deny**. Set **Read** to **Deny**.	This Group Policy object never applies to members of this security group regardless of the permissions those members have in other security groups.
Membership in this security group is irrelevant to whether the Group Policy object should be applied.	Set **Apply Group Policy** to neither **Allow** nor **Deny**. Set **Read** to neither **Allow** nor **Deny**.	This Group Policy object applies to members of this security group if and only if they have both **Apply Group Policy** and **Read** set to **Allow** as members of at least one other security group. They also must not have **Apply Group Policy** or **Read** set to **Deny** as members of any other security group.

Notes

- Group Policy objects are applied only to sites, domains, and organizational units. Group Policy settings affect only the users and computers they contain. In particular, Group Policy objects are not applied to security groups.
- The location of a security group in Active Directory has no relation to, and no effect on, filtering through that security group as described in this procedure.
- If a user or computer is not contained in a site, domain, or organizational unit that is subject to a Group Policy object either directly through a link, or indirectly through inheritance, then there is no combination of permissions on any security group that can cause those Group Policy settings to affect that user or computer.
- Filtering at the Group Policy object level, as described in this procedure, causes the Group Policy object to be processed or not processed as a whole. The Software Installation and Folder Redirection extensions use security groups to refine control beyond the Group Policy object level. Except for Folder Redirection and Software Installation, security groups are not used to filter individual settings, or subsets, of a Group Policy object. For control over individual settings, edit or create a Group Policy object instead.

To find the sites, domains, and organizational units to which a Group Policy object is linked

1. Open Group Policy with the Group Policy object of interest at the root node of the console.

2. Right-click the root node of the console, and then click **Properties**.
3. Click the **Links** tab, and then click **Find Now**. The sites, domains, and organizational units to which the Group Policy object is linked are listed in the **Sites, Domains or Organizational Units found** field.

Notes

- If the Group Policy object is linked to more than one domain, then you can limit your search for organizational units to one domain at a time using the **Domain** drop-down menu.

To disable the User Configuration settings in a Group Policy object

1. Open the Group Policy object you want to edit.
2. Right-click the console root, which appears as follows:
   Group_Policy_object_name [*domain_name*] **Policy**
3. Click **Properties**, make sure **Disable User Configuration settings** is selected, and then click **OK**.

Notes

- The User Configuration settings in this Group Policy object will no longer affect any site, domain, or organizational unit to which this Group Policy object is linked.

To disable the Computer Configuration settings in a Group Policy object

1. Open the Group Policy object you want to edit.
2. Right-click the console root, which appears as follows:
   Group_Policy_object_name [*domain_name*] **Policy**
3. Click **Properties**.
4. Make sure **Disable Computer Configuration settings** is selected, and then click **OK**.

Notes

- After you disable the Computer Configuration settings in a Group Policy object, they no longer affect any site, domain, or organizational unit to which this Group Policy object is linked.

Use Administrative Templates

- Add or remove an Administrative Template (.adm file)
- Use the view provided by Administrative Templates

To add or remove an Administrative Template (.adm file)

1. Open the Group Policy object you want to edit, and then right-click **Administrative Templates**.

   Where?
   - *Group_Policy_object_name*
   - Computer Configuration (or User Configuration)
   - Administrative Templates
2. Click **Add/Remove Templates**, and then in the **Add/Remove Templates** dialog box, click **Add**.
3. If you want to remove a template, click it, and then click **Remove**.

   If you want to add a template, click **Add**. Click the template you want to add in the **Add/Remove Templates** dialog box and then click **Open**.
4. In the **Add/Remove Templates** dialog box, click **Close**.

Notes

- Because the role of Administrative Templates has changed from Windows NT 4.0 to Windows 2000, it is not recommended to use Windows NT 4.0–style .adm files on Windows 2000 clients.

  If you do use the older .adm files to create namespaces in the Group Policy console, you can control whether the Windows NT 4.0 System Policy settings are visible in the details pane as follows: in the console tree click the Administrative Templates node, on the console menu bar click **View**, and then click **Show Policies Only** to select or clear that menu item. You can also use the Group Policy setting **Enforce Show Policies Only** to do this:

  Where?
  - *Group_Policy_object_name*
  - User Configuration
  - Administrative Templates
  - System
  - Group Policy
    - It is also recommended that you use the **Disable System Policy (use Group Policy only)** setting, which prevents System Policy settings from ever applying to Windows 2000 clients.

      Where?
      - *Group_Policy_object_name*
      - Computer Configuration
      - Administrative Templates
      - System
      - Group Policy

To use the view provided by Administrative Templates

1. Open Group Policy and click the folder under Administrative Templates containing the policies you want, such that **Policies** and **Settings** for those policies appear in the details pane.

   Where?
   - *policy_name* Policy
   - Computer Configuration (or User Configuration)
   - Administrative Templates
   - *policy_folder*
2. Double-click a policy, or right-click and choose **Properties**, to bring up the property sheet for the policy.
3. Click the **Explain** tab to see a description of the policy, if the author of the .adm file has included one.
4. Click the **Policy** tab and set the policy using the button shown in the following table.

Button	Result
Not Configured	The registry is not modified.
Enabled	The registry reflects that the policy setting is selected.
Disabled	The registry reflects that the policy setting is not selected.

5. Set any additional parameters on the **Policy** tab and then click **Apply**.
6. Use **Previous Policy** and **Next Policy** to access other policies in the current folder, and set them in the same way. Click **OK** when you are finished.

Notes

- Group Policy can have two Administrative Templates nodes. Settings for HKEY_LOCAL_MACHINE are under Computer Configuration, and settings for HKEY_CURRENT_USER are under User Configuration.
- If computer policies conflict with user policies, computer policies take precedence in Windows 2000, as they did under Windows NT 4.0 System Policy.

Use scripts

- Set up scripts on the domain controller
- Assign computer startup scripts
- Assign computer shutdown scripts
- Assign user logon scripts
- Assign user logoff scripts

To set up scripts on the domain controller

- Copy the script and dependent files to the Netlogon share, or other share, of the domain controller from which you want the script to run.

To assign computer startup scripts

1. Open the Group Policy snap-in.
2. In the console tree, click the Scripts node.

   Where?
   └ *policy_name* Policy
   └ Computer Configuration
   └ Windows Settings
   └ Scripts (Startup/Shutdown)
3. In the details pane, double-click the **Startup** icon.
4. In the **Startup** properties page, click **Add**.
5. In the **Add a Script** dialog box, set the options you want to use, and then click **OK**:

   Script Name: Type the path to the script, or click **Browse** to search for the script file in the Netlogon share of the domain controller.

   Script Parameters: Type any parameters you want to use as you would type them on the command line. For example, if your script included parameters called //logo (display banner) and //I (interactive mode), you would type the following:
   //logo //I
6. In the **Startup** properties page, specify any options you want to use:

   Startup Scripts for: Lists all scripts currently assigned to the selected Group Policy object. If you assign multiple scripts, the scripts are processed according to the order you specify. To move a script up in the list, click it and then click **Up**; to move it down, click **Down**.

   Add: Opens the **Add a Script** dialog box, where you can specify any additional scripts to use.

   Edit: Opens the **Edit Script** dialog box, where you can modify script information such as name and parameters.

   Remove: Removes the selected script from the **Startup Scripts** list.

   Show Files: Select to view the script files stored in the selected Group Policy object.

Note

- Startup scripts are run as Local System.

To assign computer shutdown scripts

1. Open the Group Policy snap-in.
2. In the console tree, click the Scripts node.

   Where?
   └ *policy_name* Policy
   └ Computer Configuration
   └ Windows Settings
   └ Scripts (Startup/Shutdown)
3. In the details pane, double-click the **Shutdown** icon.
4. In the **Shutdown** properties page, click **Add**.
5. In the **Add a Script** dialog box, set the options you want to use, and then click **OK**:

   Script Name: Type the path to the script, or click **Browse** to search for the script file in the Netlogon share of the domain controller.

   Script Parameters: Type any parameters you want to use as you would type them on the command line. For example, if your script included parameters called //logo (display banner) and //I (interactive mode), you would type the following:
   //logo //I
6. In the **Shutdown** properties page, specify any options you want to use:

   Shutdown Scripts for: Lists all scripts currently assigned to the selected Group Policy object. If you assign multiple scripts, the scripts are processed according to the order you specify. To move a script up in the list, click it and then click **Up**; to move it down,

click **Down**.

Add: Opens the **Add a Script** dialog box, where you can specify any additional scripts to use.

Edit: Opens the **Edit Script** dialog box, where you can modify script information such as name and parameters.

Remove: Removes the selected script from the **Shutdown Scripts** list.

Show Files: Select to view the script files stored in the selected Group Policy object.

Notes

- Shutdown scripts are run as Local System.

To assign user logon scripts

1. Open the Group Policy snap-in.
2. In the console tree, click the Scripts node.

   Where?
   policy_name Policy
   User Configuration
   Windows Settings
   Scripts (Logon/Logoff)
3. In the details pane, double-click the **Logon** icon.
4. In the **Logon** properties page, click **Add**.
5. In the **Add a Script** dialog box, set the options you want to use, and then click **OK**:

   Script Name: Type the path to the script, or click **Browse** to search for the script file in the Netlogon share of the domain controller.

   Script Parameters: Type any parameters you want to use as you would type them on the command line. For example, if your script included parameters called //logo (display banner) and //I (interactive mode), you would type the following:
   //logo //I
6. In the **Logon** properties page, specify any options you want to use:

   Logon Scripts for: Lists all scripts currently assigned to the selected Group Policy object. If you assign multiple scripts, the scripts are processed according to the order you specify. To move a script up in the list, click it and then click **Up**; to move it down, click **Down**.

   Add: Opens the **Add a Script** dialog box, where you can specify any additional scripts to use.

   Edit: Opens the **Edit Script** dialog box, where you can modify script information such as name and parameters.

   Remove: Removes the selected script from the **Logon Scripts** list.

   Show Files: Select to view the script files stored in the selected Group Policy object.

Notes

- Logon scripts are run as User, not Administrator.

To assign user logoff scripts

1. Open the Group Policy snap-in.
2. In the console tree, click the Scripts node.

   Where?
   policy_name Policy
   User Configuration
   Windows Settings
   Scripts (Logon/Logoff)
3. In the details pane, double-click the **Logoff** icon.
4. In the **Logoff** dialog box, click **Add**.
5. In the **Add a Script** dialog box, set the options you want to use, and then click **OK**:

   Script Name: Type the path to the script, or click **Browse** to search for the script file in the Netlogon share of the domain controller.

   Script Parameters: Type any parameters you want to use as you would type them on the command line. For example, if your script included parameters called //logo (display banner) and //I (interactive mode), you would type the following:
   //logo //I
6. In the **Logoff** properties page, specify any options you want to use and then click **OK**:

   Logoff Scripts for: Lists all scripts currently assigned to the selected Group Policy object. If you assign multiple scripts, the scripts are processed according to the order you specify. To move a script up in the list, click it and then click **Up**; to move it down, click **Down**.

   Add: Opens the **Add a Script** dialog box, where you can specify any additional scripts to use.

   Edit: Opens the **Edit Script** dialog box, where you can modify script information such as name and parameters.

   Remove: Removes the selected script from the **Logoff Scripts** list.

   Show Files: Select to view the script files stored in the selected Group Policy object.

Note

- Logoff scripts are run as User, not Administrator.

Use the Software Installation snap-in

- Open the Software Installation snap-in
- Set options for Software Installation
- Work with applications
- Set application properties
- Work with package modifications

To open the Software Installation snap-in

1. Open Group Policy from Active Directory Users and Computers, from Active Directory Sites and Services, or as a stand-alone Microsoft Management Console snap-in.
2. To assign software to computers, double-click Computer Configuration. To assign or publish software to users, double-click User Configuration.
3. Double-click Software Settings.
4. In the console tree, click Software Installation.

   Where?
   - *policy_name* Policy
   - [Computer | User] Configuration
   - Software Settings
   - Software Installation

Set options for Software Installation

- Set Software Installation defaults
- Specify automatic installation options based on file name extension
- Specify categories for applications to be managed

To set Software Installation defaults

1. Open the Software Installation snap-in.
2. Right-click the Software Installation node, and then click **Properties**.

   Where?
   - *Group_Policy_object_name*
   - Computer Configuration (or User Configuration)
   - Software Settings
   - Software Installation
3. Click the **General** tab and then select the settings you want:

   Default Package Location: Specify the default software distribution point.

   New packages. Packages can either be published or assigned by default (to computers, only assigned). If you want to make these decisions for each package, select **Display the Deploy Software dialog box**. For finer control on a per-package basis, select **Advanced assign or publish**.

   Installation user interface options: Click **Basic** or **Maximum**, depending on how apparent you want the installation process to be to the users.

   Uninstall the applications when this Group Policy object no longer applies to Users or Computers: Use this option if you want software to be removed at logon (for users) or startup (for computers) if the user or computer moves to a site, domain, or organizational unit for which the software is not managed.

To specify automatic installation options based on file name extension

1. Open the Software Installation snap-in, and then in the console right-click the **Software Installation** node.

   Where?
   - *Group_Policy_object_name*
   - Computer Configuration (or User Configuration)
   - Software Settings
   - Software Installation
2. Click **Properties**, and then click the **File Extensions** tab.
3. On the **File Extensions** property sheet, specify the options you want to use, and then click **OK**:

   Select file extension: Displays a list of all available file name extensions for the managed software. When an extension is selected, all applications in Active Directory associated with the selected file name extension are displayed in the **Application precedence** list box. For example, for an .htm extension, many applications can be associated, such as Microsoft Word 97, Microsoft Internet Explorer 5, Netscape Communicator 5.0, and so on.

   Application precedence: Lists all the applications associated with the selected extension. The application with the highest precedence by default is listed at the top of the list.

   Up: Moves the selected application higher in the priority list. The application at the top of the list is automatically installed if a document with the selected file name extension is invoked before the application has been installed. This option is unavailable when the selected application is at the top of the list.

   Down: Moves the selected application lower in the priority list. This option is unavailable when the selected application is at the bottom of the list.

Note

- When you upgrade an application, make sure to turn off the autoinstall option for the older version.

To specify categories for applications to be managed

1. Open the Software Installation snap-in.
2. Right-click the Software Installation node, and then click **Properties**.

   Where?
   - *Group_Policy_object_name*
   - Computer Configuration (or User Configuration)
   - Software Settings
   - Software Installation
3. Click the **Categories** tab.
4. Create or change the list of categories under which programs appear in Add/Remove Programs in Control Panel, using the available buttons:

   Add: Opens a dialog box where you can type text to define the new category. The option is unavailable if you do not have permission to add categories.

   Modify: Opens a dialog box where you can change the text of the selected category. The option is unavailable if you do not have permission to edit categories.

Remove: Removes the selected category from the **Categories** list.

Notes

- The changes you make to the application categories apply throughout the domain in which this Group Policy object is stored.
- To perform this procedure, you need to be a domain administrator or have equivalent rights.

Work with applications

- Assign an application
- Publish an application
- Upgrade applications
- Remove a managed application

To assign an application

1. Open the Software Installation snap-in, and in the console click the **Software Installation** node.

   Where?
   └*Group_Policy_object_name*
   └Computer Configuration (or User Configuration)
   └Software Settings
   └Software Installation
2. Right-click the details pane, click **New**, and then click **Package**.
3. In the **Open** dialog box, click the Windows Installer package to be assigned, and then click **Open**. (The **Open** dialog box shows those packages located at the software distribution point you specify as the default.)

   If the Windows Installer package is located on a different network share, click **Browse** to find the software distribution point for the package.
4. In the **Deploy Software** dialog box, click **Assigned**, and then click **OK**.

To publish an application

1. Open the Software Installation snap-in, and in the console click the Software Installation node.

   Where?
   └*Group_Policy_object_name*
   └User Configuration
   └Software Settings
   └Software Installation
2. Right-click the details pane, click **New**, and then click **Package**.
3. In the **Open** dialog box, click the Windows Installer package to be published, and then click **Open**. (The **Open** dialog box shows those packages located at a software distribution point you specify as the default.)

   If the Windows Installer package is located on a different network share, click **Browse** to find the software distribution point for this package.
4. In the **Deploy Software** dialog box, click **Published**, and then click **OK**.

   The application is available for users to install either by using Add/Remove Programs in Control Panel, or by opening a file with a file name extension that you have associated with the application.

Notes

- Packages can be published only to users, not to computers.

To upgrade applications

1. Open the Software Installation snap-in and click the **Software Installation** node.

   Where?
   └g*roup_Policy_object_name*
   └Computer Configuration (or User Configuration)
   └Software Settings
   └Software Installation
2. In the details pane, right-click the Windows Installer package that will function as the upgrade (not the package to be upgraded). You will have previously assigned or published this package.
3. Click **Properties** and then click the **Upgrades** tab.
4. Click **Add** to create or add to the list of packages that are to be upgraded by the current package.
5. In the **Add Upgrade Package** dialog box, specify either **Current Group Policy object** or **A specific GPO** as the source of the package to be upgraded. In the latter case, click **Browse**, click the Group Policy object you want, and then, in the **Browse for a Group Policy object** dialog box, click **OK**.

   A list of all the other packages assigned or published within the selected Group Policy object appears under the heading **Package to upgrade**. Depending on the Group Policy object, this list may have zero or more entries.
6. Click the package to upgrade.
7. Click either **Uninstall the existing package, then install the upgrade package** or **Package can upgrade over the existing package**. Typically the uninstall option is for replacing an application with a completely different one (perhaps from a different vendor). The upgrade option is for installing a newer version of the same product while retaining the user's application preferences, document type associations, and so on.
8. Enable the check box for **Required upgrade for existing packages** if you want the upgrade to be mandatory, and then click **OK**.

   If this is an upgrade under the Computer Configuration node of the Group Policy console, the check box appears dimmed and selected, because packages can only be assigned to computers, not published.

To remove a managed application

1. Open the Software Installation snap-in, and in the console click the **Software Installation** node.

   Where?
   └*Group_Policy_object_name*
   └Computer Configuration (or User Configuration)

└Software Settings
└Software Installation

2. In the details pane, right-click the application you want to remove.
3. Click **All Tasks**, and then click **Remove**.
4. In the **Remove Software** dialog box, select one of the following removal options, and then click **OK**:

   Immediately uninstall software from users and computers: Select this option to specify that the application is removed the next time a user logs on or restarts the computer.

   Allow users to continue to use the software but prevent new installations: Select this option to specify that users can continue to use the application if they have already installed it. If they remove the application or have never installed it, they will not be able to install it.

Set application properties

- View properties for managed applications
- Edit Software Installation options for applications
- Specify categories for Add/Remove Programs in Control Panel
- Set autoinstall for an application
- Set permissions for installing software

To view properties for managed applications

1. Open the Software Installation snap-in.
2. In the details pane, right-click the application icon you want to view properties for, and then click **Properties**.

To edit installation options for applications

1. Open the Software Installation snap-in, and in the console click the **Software Installation** node.

   Where?
   └*Group_Policy_object_name*
   └Computer Configuration (or User Configuration)
   └Software Settings
   └Software Installation
2. In the details pane, right-click the application for which you want to set installation options, and then click **Properties**.
3. On the application's **Properties** sheet, click **Deployment**.
4. On the **Deployment** property sheet, click one of the following deployment types in the **Deployment type** box:

   Published: Users in the selected site, domain, or organizational unit can install the application using either Add/Remove Programs in Control Panel, or by file activation.

   Assigned: Users in the selected site, domain, or organizational unit receive this application the next time they log on (for assignment to users) or when the computer restarts (for assignment to computers).
5. In the **Deployment options** frame, select among these options:

   Auto-install this application by file extension activation: Select this option if you want to use the application precedence for the file name extension as determined on the **File Extensions** tab of the **Software Installation Properties** dialog box.

   If the software is not already installed, selecting this option causes it to be installed when the user opens a file with this file association; for example, by double-clicking it.

   Uninstall this application when this Group Policy object no longer applies to users or computers: Select this option if you want the application to be removed at logon (for users) or startup (for computers) if they move to a site, domain, or organizational unit for which the application is not deployed.

   Do not display this package in Add/Remove Programs in Control Panel: This option removes the most obvious way for users to uninstall the program. This may be useful from time to time during the software life cycle.
6. In **Installation user interface options**, click one of the following options:

   Basic: Only progress bars and errors are displayed.

   Maximum: The entire user interface supported by the package is displayed.
7. If you want to set advanced options, click **Advanced**:

   Ignore language when deploying this package: Use this option if you are installing an application whose locale differs from that of the operating system.

   Remove previous installs of this product from computers, if the product was not installed by Group Policy–based Software Installation: This may be useful if, for example, company policy is to not allow users to install from their own compact discs.

Notes

- The **Advanced Deployment Options** form that appears when you click **Advanced** provides the following advanced diagnostic information, which can be useful for troubleshooting.

Field	Data
Product code	Globally unique identifier (GUID) representing the product
Deployment count	Number of times the package has been deployed in this Group Policy object
Script name	The full network path, including GUIDs, to the application assignment script (.aas file)

To specify application categories for Add/Remove Programs in Control Panel

1. Open the Software Installation snap-in.
2. In the details pane, double-click the managed application you want to set categories for, and then, on the application's property sheet, click **Categories**.
3. On the **Categories** property sheet, set the following options you want to use, and then click **OK**:

   Available categories: Lists the application categories that have been defined for your organization.

   Select: Associates the selected application category with the application. To use this option, select a category from the **Available**

categories list and then click **Select**.

Remove: Removes a category from the **Selected categories** list. To use this option, select a category from the **Selected categories** list, and then click **Remove**.

Selected categories: Displays the categories that are associated with this application.

Notes

- The categories you set in this dialog box generally pertain to published applications only, because assigned applications do not appear in Add/Remove Programs in Control Panel. The application appears in the selected categories in Add/Remove Programs, which the user can use to install the application.
- This procedure is not used to create or destroy categories, but only to associate applications with existing categories.

To set the autoinstall option for an application

1. Open the Software Installation snap-in and then, in the console, click the **Software Installation** node.

   Where?
   - *Group_Policy_object_name*
   - User Configuration
   - Software Settings
   - Software Installation
2. In the details pane, right-click the application you want to be installed automatically.
3. Click **Properties**, and then click the **Deployment** tab.
4. Under **Deployment options**, make sure **Auto-install this application by file extension activation** is selected, and then click **OK**.

Notes

- When you upgrade an application, make sure to turn off the autoinstall option for the older version.

To set permissions for software installation

1. Open the Group Policy object you want to edit.
2. Right-click the console root, where you see a name that appears as follows:
   Group_Policy_object_name [*domain_name*] **Policy**
3. Click **Properties**, and then click the **Security** tab.
4. Click the security group on which to set permissions.

   You can add or remove security groups using the buttons provided if you need to change the set of security groups with permissions on this Group Policy object.
5. If the security group represents administrators (who manage software for users and computers in the organization), set **Full Control** to **Allow**.

   If the security group represents users (who use software assigned or published by an administrator), set both **Apply Group Policy** and **Read** to **Allow**.
6. On the Group Policy object property sheet, click **OK**.

Note

- The permissions that are set in this procedure pertain only to the Group Policy object. In addition, the network must have a shared folder (a software distribution point) containing the packages to be installed. Administrators must have Full Control of the software distribution point, and users must have Read permission.

Work with package modifications

Modifications (.mst files) are applied to Windows Installer packages (which have the .msi extension) in an order specified by the administrator. This order must be determined before the application is assigned or published.

Modifications are also called transforms.

For information on working with package modifications, see To add or remove modifications for an application package.

To add or remove modifications for an application package

1. Open the Software Installation snap-in, and in the console, click the Software Installation node.

   Where?
   - *Group_Policy_object_name*
   - Computer Configuration (or User Configuration)
   - Software Settings
   - Software Installation
2. In the details pane, right-click, click **New**, and then click **Package**.
3. In the **Open** dialog box, click the Windows Installer package, and then click **Open**.
4. In the **Deploy Software** dialog box, click **Advanced assign or publish**, and then click **OK**.
5. In the package's property sheet, click **Modifications**.
6. If you want to add modifications, in the **Modifications** dialog box, click **Add**. In the **Open** dialog box, browse to the transform file (.mst), and then click **Open**.
7. If you want to remove modifications, in the **Modifications** dialog box, click the modification you want to remove, and then click **Remove**. Repeat until each unwanted modification has been removed.
8. Make sure the modifications are configured exactly the way you want them, and then click **OK**.

Warning

- Do not click **OK** until you have finished configuring the modifications. When you click **OK**, the package is assigned or published immediately. If the modifications are not properly configured, you will have to uninstall the package, or upgrade the package with a correctly configured version.

Notes

- You can add multiple modifications (transforms). The transforms are applied according to the order you specify in the **Modifications** list, from top to bottom. To rearrange the list, select a transform from the list and then click **Move Up** or **Move Down**.

Use the Folder Redirection snap-in

- Redirect to one location for everyone in the site, domain, or organizational unit
- Redirect to different locations according to security group membership

To redirect special folders to one location for everyone in the site, domain, or organizational unit

1. Open a Group Policy object linked to the site, domain, or organizational unit containing the users whose special folders you want to redirect to a network location.
2. In the console tree, double-click the **Folder Redirection** node to show the special folder you want to redirect.

   Where?
   - *policy_name* Policy
   - User Configuration
   - Windows Settings
   - Folder Redirection
3. Right-click the special folder you want (such as Desktop, My Documents, and so on), and on the context menu click **Properties**.
4. On the **Setting** drop-down menu, click **Basic**, click **Browse**, and then browse to the location you want.

   If you enter a drive letter, such as **D:**, then this must represent a valid path on the user's local computer. It is recommended that you enter a full universal naming convention (UNC) path.

   If you want each user in the site, domain, or organizational unit to have his or her own subfolder at this location, then you can incorporate %username% into the UNC path, such as \\Win2000profiles\docs\%username%. Including %username% in the path is recommended.
5. In the **Browse for Folder** dialog box, click **OK**.
6. Click the **Settings** tab, and then set each of the following options. The defaults are recommended:

   Grant the user exclusive rights to the special folder: Enabled by default. The user and the local system have full rights to the folder, and no one else, not even administrators, has any rights. If this setting is disabled, no changes are made to the permissions on the folder. The permissions that apply by default remain in effect.

   Move the contents of the user's current special folder to the new location: Enabled by default.
7. Choose one of the following two options for policy removal. The default setting is recommended:

   Leave the files in the new location when policy is removed.

   Redirect the folder back to the local user profile location when the policy is removed.
8. On the special folder Properties dialog box, click **OK**.

Caution

- If the redirection policy specifies that the folder be redirected back to the local user profile location upon policy removal, but does not specify that the contents be moved during redirection, then the contents of the special folder that were visible to the user while the policy was in effect are no longer visible to the user upon policy removal. The user's files remain at the location that was specified when the policy was in effect. See Policy removal considerations for details.

Notes

- Special folders are those located in Documents and Settings under the root directory.
- The My Pictures special folder offers one further option. The default behavior, which is recommended, is for My Pictures to follow My Documents automatically. This can be changed by clicking the **Setting** drop-down list on **My Pictures Properties**, or the **Settings** tab of **My Documents Properties**.

To redirect special folders to different locations according to security group membership

1. Open a Group Policy object linked to the site, domain, or organizational unit containing the users whose special folders you want to redirect to a network location.
2. In the console tree, double-click the Folder Redirection node to show the folder you want to redirect.

   Where?
   - *policy_name* Policy
   - User Configuration
   - Windows Settings
   - Folder Redirection
3. Right-click the folder you want (such as Desktop, My Documents, and so on) and on the context menu click **Properties**.
4. On the **Setting** drop-down menu, click **Advanced**, and then click **Add**.
5. In the **Specify Group and Location** dialog box, under **Security Group Membership** click **Browse**.
6. In the **Select Group** dialog box, click the security group you want and then click **OK**.
7. In the **Specify Group and Location** dialog box, under **Target Folder Location**, click **Browse**.
8. On the **Browse for Folder** dialog box, select the redirect location you want for this security group.

   If you enter a drive letter, such as **D:**, then this must represent a valid path on the user's local computer. It is recommended that you enter a full universal naming convention (UNC) path.

   If you want each user in the site, domain, or organizational unit to have his or her own subfolder at this location, then you can incorporate %username% into the UNC path, such as \\Win2000profiles\docs\%username%. Including %username% in the path is recommended.
9. In the **Specify Group and Location** dialog box, click **OK**.
10. If you want to redirect folders for members of other security groups, repeat steps 2 through 9 until all the groups have been entered.
11. Click the **Settings** tab, and then set each of the following options. The defaults are recommended:

    Grant the user exclusive rights to the special folder: Enabled by default. The user and the local system have full rights to the folder, and no one else, not even administrators, has any rights. If this setting is disabled, no changes are made to the permissions on the folder. The permissions that apply by default remain in effect.

    Move the contents of the user's current special folder to the new location: Enabled by default.
12. Choose one of the following two options for policy removal. The default setting is recommended:

    Leave the files in the new location when policy is removed.

Redirect the folder back to the local user profile location when the policy is removed.

13. On the special folder Properties dialog box, click **OK**.

Caution

- If the redirection policy specifies that the folder be redirected back to the local user profile location upon policy removal, but does not specify that the contents be moved during redirection, then the contents of the special folder that were visible to the user while the policy was in effect are no longer be visible to the user upon policy removal. The user's files remain at the location that was specified when the policy was in effect. See Policy removal considerations for details.

Notes

- Special folders are those located in Documents and Settings under the root directory.
- The **My Pictures** folder offers one further option. The default behavior, which is recommended, is for My Pictures to follow My Documents automatically. This can be changed by clicking the **Setting** drop-down list on **My Pictures Properties**, or the **Settings** tab of **My Documents Properties**.

Configure Group Policy

- Extend the functionality of Group Policy
- Refresh Group Policy immediately
- Set permissions for managing Group Policy
- Set Group Policy refresh rate for computers
- Set other policies for Group Policy

To extend the functionality of Group Policy

1. Open Group Policy as a stand-alone MMC snap-in.
2. On the **Console** menu, click **Add/Remove snap-in**.
3. Click the **Extensions** tab, select the snap-in extensions you want, and then click **OK**.

To refresh Group Policy immediately

1. Click **Start** and then click **Run** to open the **Run** dialog box.
2. To refresh policies under the Computer Configuration node, type the following and then click **OK**:
   secedit /refreshpolicy MACHINE_POLICY

   To refresh policies under the **User Configuration** node, type the following and then click **OK**:
   secedit /refreshpolicy USER_POLICY

To set permissions for managing Group Policy

1. Open Group Policy.
2. In the Group Policy console root, right-click the Group Policy object for which you want to set permissions, click **Properties**, and then click **Security**.
3. In the **Properties** dialog box, set the options you want to use, and then click **OK**:

   Add: Opens the **Add Users and Groups** dialog box, where you can specify the users and groups for whom to assign permissions.

   Remove: Removes users or groups and their associated permissions from this object.

   Permissions: Lists the standard permissions that you can allow or deny to users; for example, Full Control, Read, Write, and so on.

   Advanced: Use this option to set special permissions, auditing information, and owner information for the selected object.

   Allow inheritable permissions from parent to propagate to this object: Specifies whether or not security permissions for this object are affected by inheritance.

To set Group Policy refresh rate for computers

1. Open Group Policy with System.adm installed under Computer Configuration\Administrative Templates. (Because System.adm is installed by default, you should not need to take any action.)
2. Open the Computer Configuration\Administrative Templates\System\Group Policy folder to reveal several policies, including **Group Policy refresh interval for computers**.

   Where?
   - *policy_name* policy
   - Computer Configuration
   - Administrative Templates
   - System
   - Group Policy
3. In the details pane, double-click the **Group Policy refresh interval for computers** icon.
4. Click the **Policy** tab and make sure the check box is selected and does not appear dimmed.
5. Use the drop-down lists to select the refresh interval and random offset, and then click **OK**.
6. Double-click the icon for **Disable background refresh of Group Policy**. Make sure that policy is **Disabled** by clearing the check box, and then click **OK**.

Notes

- Client computers request policy from a domain controller when any of these events occur:
  - Computer startup
  - User logon
  - An application requests a refresh by way of the **RefreshPolicy()** API.
  - The user requests an immediate refresh.
  - One of the Group Policy refresh interval policies is enabled, and the interval has transpired, as described previously.

  Policy is not imposed by the domain controller; it is requested by the client computer.
- The minimum setting of **Group Policy Refresh Interval** (zero minutes) actually takes about seven seconds between requests for a refresh. Very short settings should not be used in a production environment, except only briefly for testing.

The Software Installation and Folder Redirection extensions to Group Policy ignore policy refreshes.

Set other policies for Group Policy

1. Open Group Policy with System.adm installed. (Because System.adm is installed by default, you generally do not need to take any action.)
2. If you want to edit a user policy, in the console tree, click the Group Policy node for user policies.

   Where?
   └ *policy_name* Policy
   └ User Configuration
   └ Administrative Templates
   └ System
   └ Group Policy
3. If you want to edit a computer policy, in the console tree, click the Group Policy node for computer policies.

   Where?
   └ *policy_name* Policy
   └ Computer Configuration
   └ Administrative Templates
   └ System
   └ Group Policy
4. Double-click the icon for the policy you want to set.
5. On the **Policy** tab, make the setting you want, and then click **OK**.

Note

- Descriptions of the policies for Group Policy are provided on the **Explain** tab if the author of the .adm file has included them.

Concepts

This section consists of general background information about Group Policy.

- Group Policy overview
- Understanding Group Policy
- Using Group Policy
- Resources

Group Policy overview

To begin using Group Policy immediately, see Ways to open the Group Policy snap-in.

Group Policy settings define the various components of the user's desktop environment that a system administrator needs to manage; for example, the programs that are available to users, the programs that appear on the user's desktop, and **Start** menu options. To create a specific desktop configuration for a particular group of users, you use the Group Policy snap-in. Group Policy settings you specify are contained in a Group Policy object, which is in turn associated with selected Active Directory objects—sites, domains, or organizational units.

Group Policy includes settings for **User Configuration**, which affect users, and **Computer Configuration**, which affect computers.

Using Group Policy and its extensions, you can:

- **Manage registry-based policy through Administrative Templates.** Group Policy creates a file that contains registry settings that are written to the User or Local Machine portion of the registry database. User profile settings that are specific to a user who logs on to a given workstation or server are written to the registry under **HKEY_CURRENT_USER** (HKCU), and computer-specific settings are written under **HKEY_LOCAL_MACHINE** (HKLM).
- **Assign scripts** (such as computer startup and shutdown, and logon and logoff).
- **Redirect folders** from the Documents and Settings folder on the local computer to network locations.
- **Manage applications** (assign, publish, update, or repair). To do this, you use the Software Installation extension.
- **Specify security options.** To learn about setting security options, see the Security Settings online Help.

How and when Group Policy is applied

User and computer policy

User policy (settings located under the **User Configuration** node in Group Policy) is obtained when a user logs on.

Computer policy settings are located under **Computer Configuration**, and are obtained when a computer boots.

Users and Computers are the *only* types of Active Directory objects that receive policy. Specifically, security groups do not have policy applied to them. Instead, for performance reasons, security groups are used to filter the policy by way of an **Apply Group Policy** access control entry (ACE), which can be set to **Allow** or **Deny**, or left unconfigured.

Order of application

Policies are applied in this order:

1. The unique local Group Policy object.
2. Site Group Policy objects, in administratively specified order.
3. Domain Group Policy objects, in administratively specified order.
4. Organizational unit Group Policy objects, from largest to smallest organizational unit (parent to child organizational unit), and in administratively specified order at the level of each organizational unit.

By default, policies applied later overwrite previously applied policies when the policies are inconsistent. If the settings are not inconsistent, however, earlier and later policies both contribute to the effective policy.

Policy can be filtered by security group membership

A security group ACE on a Group Policy object can be set to **Not configured** (no preference), **Allowed**, or **Denied**. Denied takes precedence over allowed.

Blocking policy inheritance

Policies that would otherwise be inherited from higher site, domain, or organizational units can be blocked at the site, domain, or organizational unit level.

Enforcing policy from above

Policies that would otherwise be overwritten by policies in child organizational units can be set to **No Override** at the Group Policy object level.

Note

- Policies set to **No Override** cannot be blocked.

This section covers:

- User Configuration
- Computer Configuration
- Security Settings
- Administrative Templates
- Software Settings
- Windows Settings
- Software Installation
- Folder Redirection

User Configuration

You use the User Configuration node in Group Policy to set policies applying to users, regardless of which computer they log on to.

User Configuration typically contains subnodes for Software Settings, Windows Settings, and Administrative Templates, but because Group Policy can have snap-in extensions added to or removed from it, the exact set of subnodes you see may be different.

See also:

- Computer Configuration
- Administrative Templates
- Software Settings
- Windows Settings
- Assign user logon scripts
- Assign user logoff scripts
- Disable the User Configuration Settings in a Group Policy object

Computer Configuration

Administrators use the Computer Configuration node in Group Policy to set policies that are applied to computers, regardless of who logs onto them.

Computer Configuration typically contains the subnodes Software Settings, Windows Settings, and Administrative Templates. However, because Group Policy can have extensions added to or removed from it, the exact set of subnodes you see may be different.

See also:

- User Configuration
- Administrative Templates
- Software Settings
- Windows Settings
- Disable the Computer Configuration Settings in a Group Policy object
- Assign computer startup scripts
- Assign computer shutdown scripts

Security settings

Group Policy has two Security Settings nodes. **\Computer Configuration\Windows Settings\Security Settings** is for security settings applying to all users who log on to the computer. This node has two subnodes: IP Security Policies on Active Directory, and Public Key Policies.

\User Configuration\Windows Settings\Security Settings is for security settings applying to users regardless of which computer they log on to. This node has a Public Key Policies subnode.

For more information on using these nodes, see Security settings.

Administrative Templates

The Group Policy Administrative Templates node contains all registry-based policy information. User configurations are saved in HKEY_CURRENT_USER (HKCU), and computer configurations are saved in HKEY_LOCAL_MACHINE (HKLM). The software policy settings include Group Policy for programs as well as for the Windows 2000 operating system and its components.

The namespace under the Administrative Templates node is populated by using .adm files or by an extension to Group Policy. When you use this node for the first time, the .adm files are automatically installed.

If you plan to create entries for the Administrative Templates node, you should populate the namespace using the following naming convention, which is also used in the registry:
*****CompanyName******product******version (or *****CompanyName******product&version**)**
For example, the operating system settings for Windows 2000 are in \Microsoft\Windows 2000.

The user interface that is displayed under the Administrative Templates nodes is populated by using .adm files. For this purpose, Windows 2000 is shipped with several .adm files. For a description of these files, see .adm files included with Windows 2000.

For information on adding an .adm file, see To add or remove an Administrative Template (.adm file).

Registry.pol Files

The Administrative Templates extension of Group Policy saves information in Registry.pol files. These files contain the customized registry settings that you specify (by using Group Policy) to be applied to the computer or user portion of the registry. One of the Registry.pol files contains the registry settings to be applied to the HKEY_LOCAL_MACHINE registry key; it is stored in the GPT\Machine

folder. The other Registry.pol file contains registry settings specific to the HKEY_CURRENT_USER key; it is stored in the GPT\User subdirectory.

See also:

- Use the view provided by Administrative Templates
- The role of Administrative Templates
- Advanced topic: Creating custom .adm files

Software settings

Group Policy has two Software Settings nodes.

\Computer Configuration\Software Settings\ is for software settings applying to all users who log on to the computer. This node has a **Software Installation** subnode, and possibly other subnodes placed there by Independent Software Vendors.

\User Configuration\Software Settings is for software settings that applying to users regardless of which computer they log on to. This node has a **Software Installation** subnode, and possibly other subnodes placed there by Independent Software Vendors.

See also:

- Software Installation
- User Configuration
- Computer Configuration

Windows settings

Group Policy has two Windows Settings nodes.

\Computer Configuration\Windows Settings is for windows settings that apply to all users who log on to the computer. This node has two subnodes: Security Settings and Scripts.

\User Configuration\Windows Settings is for windows settings that apply to users regardless of which computer they log on to. This node has three subnodes: Folder Redirection, Security Settings, and Scripts.

See also:

- User Configuration
- Computer Configuration
- Security Settings
- Scripts
- Folder Redirection

Software Installation

Software Installation helps you specify how applications are installed and maintained within your organization.

You manage an application within a Group Policy object, which is in turn associated with a particular Active Directory container—either a site, domain, or organizational unit. Applications can be managed in one of two modes: assigned or published.

You *assign* an application when you want everyone to have the application on his or her computer. For example, suppose you want all users in a marketing department to have Microsoft Excel on their computers. A Group Policy object manages every user in marketing. When you assign Microsoft Excel within the marketing Group Policy object, Microsoft Excel is *advertised* on every marketing user's computer. When an assigned application is advertised, it is not actually installed on the computer. In this case, the application advertisement installs only enough information about Microsoft Excel to make the Microsoft Excel shortcuts appear on the **Start** menu and the necessary file associations (.xls) appear in the registry.

When these users log on to their computers, Microsoft Excel appears on their **Start** menu. When they select Microsoft Excel from the **Start** menu for the first time, Microsoft Excel is installed. A user can also install an advertised application by opening a document associated with the application (either by file name extension or by COM-based activation). If a user who has not yet activated Microsoft Excel from the **Start** menu clicks a Microsoft Excel spreadsheet to open it, then Microsoft Excel is installed and the spreadsheet opens.

A user can delete an assigned application, but the assigned application is advertised again the next time the user logs on. It will be installed the next time a user selects it from the **Start** menu.

You *publish* an application when you want the application to be available to people managed by the Group Policy object, should a user want the application. With published applications, it is up to each person to decide whether or not to install the published application.

For example, if you publish Microsoft Image Composer to users managed by the marketing Group Policy object and a marketing user wants to install Image Composer, the user can use **Add/Remove Programs** in Control Panel, click **Image Composer** from the list of published applications, and then install it. If users do not install Image Composer using **Add/Remove Programs** in Control Panel, and if the .jpg file name extension for the image document is associated with Image Composer, then Image Composer can be installed for users when they first open any .jpg document.

See also:

- Use the Software Installation Snap-in
- Understanding Software Installation

Folder Redirection

You use the Folder Redirection extension to Group Policy to redirect certain Windows 2000 special folders to network locations. Special folders are those folders such as My Documents and My Pictures that are located under Documents and Settings.

Folder Redirection is located under User Configuration in the Group Policy console.

Where?
└ *policy_name* Policy
└ User Configuration
└ Windows Settings
└ Folder Redirection

To individualize a user's redirected folder, it is recommended to incorporate %username% into the path; for example, *****server******share***\%username%\My Documents**

In addition, you can either redirect a special folder to the same network share for everyone (as described in To redirect special folders to one location for everyone in the site, domain, or organizational unit) or you can refine the redirection beyond the Group Policy object level. For example, members of the Users security group could have My Documents redirected to \\server1\share\%username%\My Documents, while members of the Guests security group could have My Documents redirected to

\\server2\share\%username%\My Documents. For more information, see To redirect special folders to different locations according to security group membership.

Windows 2000 allows the following folders to be redirected:

Special folder	Notes
Application Data	A Group Policy setting controls the behavior of Application Data when client side caching is enabled. Look in **User Configuration\Administrative Templates\Network\Offline Files** in the Group Policy console.
Desktop	
My Documents	See Advantages of redirecting My Documents for details.
My Documents\My Pictures	My Pictures can be redirected independently of My Documents, or it can be made to follow My Documents (to remain its subfolder whenever My Documents is redirected) as it does by default. The default behavior is recommended unless you have a specific reason (such as file share scalability) for separating My Pictures from My Documents. If they are separated, a shortcut takes the place of the My Pictures folder in My Documents.
Start Menu	When Start Menu is redirected, its subfolders always follow.

Advantages of redirecting My Documents

Some of the following benefits pertain to redirecting any folder, but redirecting My Documents can be particularly advantageous because this folder tends to become large over time.

- Even if a user logs on to various computers on the network, his or her documents are always available.
- Offline File technology gives users access to My Documents even when they are not connected to the network. For more information, see To make a file or folder available offline. This is particularly useful for those who use laptop computers.
- When roaming user profiles are used, only the network path to the My Documents folder is part of the roaming user profile, not the My Documents folder itself. Therefore, its contents do not have to be copied back and forth between the client computer and the server each time the user logs on or off, and the process of logging on or off can be much faster than it was in Windows NT 4.0.
- Data stored on a shared network server can be backed up as part of routine system administration. This is safer, because it requires no action on the part of the user.
- The system administrator can use Group Policy to set disk quotas, limiting the amount of space taken up by users' special folders.
- Data specific to a user can be redirected to a different hard disk on the user's local computer from the hard disk holding the operating system files. This makes the user's data safer if the operating system needs to be reinstalled.

For more information, see Best practices for Folder Redirection.

Default folder locations

The default locations for special folders that have not been redirected depend on the operating system that was in place previously:

Operating system	Location of special folders
Windows 2000 new installation (no previous operating system)	%systemdrive%\Documents and Settings; for example, C:\Documents and Settings
Windows 2000 upgrade of Windows NT 4.0 or Windows NT 3.51	%systemroot%\Profiles; for example, C:\WinNT\Profiles
Windows 2000 upgrade of Windows 95 or Windows 98 with user profiles disabled	%systemdrive%\Documents and Settings; for example, C:\Documents and Settings
Windows 2000 upgrade of Windows 95 or Windows 98 with user profiles enabled	%systemroot%\Profiles; for example, C:\Windows\System\Profiles

For more information on user profiles, see User profiles.

Policy removal considerations

The following table summarizes what happens to redirected folders and their contents when the Group Policy object no longer applies.

Move the contents of special folder to the new location setting	Policy Removal option	Results when policy is removed
Enabled	**Redirect the folder back to the user profile location when policy is removed**	• The special folder returns to its user profile location. • The contents are copied, not moved, back to the user profile location. • The contents are not deleted from the redirected location. • The user continues to have access to the contents, but only on the local computer.
Disabled	**Redirect the folder back to the user profile location when policy is removed.**	• The special folder returns to its user profile location. • The contents are not copied or moved to the user profile location. Caution • If the contents of a folder are not copied to the user profile location, the user can no longer see them.
Either **Enabled** or **Disabled**	**Leave the folder in the new location when policy is removed**	• The special folder remains at its redirected location. • The contents remain at the redirected location. • The user continues to have access to the contents at the redirected folder.

Understanding Group Policy

This section covers:

- Group Policy objects

- Policy inheritance
- Storage of Group Policy objects
- Group Policy precedence
- Understanding Software Installation

Group Policy objects

Policy settings are stored in Group Policy objects. The Group Policy snap-in can be thought of as an application whose document type is the Group Policy object, just as a word processor might use .doc or .txt files.

Local and nonlocal Group Policy objects

There are two kinds of Group Policy objects. Nonlocal Group Policy objects, which are stored on a domain controller, are available only in an Active Directory environment. They apply to users and computers in the site, domain, or organizational unit with which the Group Policy object is associated.

Local Group Policy objects are stored on each computer running Windows 2000. Only one local Group Policy object exists on a computer, and it has a subset of the settings available in a nonlocal Group Policy object. Local Group Policy object settings can be overwritten by nonlocal settings if they are in conflict; otherwise, both apply.

Policy inheritance

In general, Group Policy is passed down from parent to child containers. If you have assigned a specific Group Policy to a high-level parent container, that Group Policy applies to all containers beneath the parent container, including the user and computer objects in each container. However, if you explicitly specify a Group Policy setting for a child container, the child container's Group Policy setting overrides the parent container's setting.

If a parent organizational unit has policy settings that are not configured, the child organization unit doesn't inherit them. Policy settings that are disabled are inherited as disabled. Also, if a policy is configured for a parent organizational unit, and the same policy is not configured for a child organizational unit, the child inherits the parent's policy setting.

If a parent policy and a child policy are compatible, the child inherits the parent policy, and the child's setting is also applied. Policies are inherited as long as they are compatible. For example, if the parent's policy causes a certain folder to be placed on the desktop and the child's setting calls for an additional folder, the user sees both folders.

If a policy configured for a parent organizational unit is incompatible with the same policy configured for a child organizational unit, the child does not inherit the policy setting from the parent. The setting in the child is applied.

Blocking inheritance

You can block inheritance of policies at the site, domain, or organizational unit level using the **Block Inheritance** check box. If this option is selected for a child-level Group Policy object, the child does not inherit any policy from a parent-level Group Policy object.

Enforcing inheritance

The **No Override** check box forces all child policy containers to inherit the parent's policy even if those policies conflict with the child's policies, and even if **Block Inheritance** has been set for the child.

Storage of Group Policy objects

Each computer running Windows 2000 has exactly one local Group Policy object. It is stored in %systemroot%System32\GroupPolicy.

Group Policy objects other than the local Group Policy object consist of two parts, stored separately: the Group Policy container and the Group Policy template. Information that is small and infrequently changed resides in the Group Policy template, while information that is large or frequently changed is kept in the Group Policy container. The Group Policy user interface does not expose them separately.

Group Policy container

The Group Policy container is a directory service object. It includes subcontainers for computer and user Group Policy information. The Group Policy container contains the following data:

- **Version information.** This is used to make sure the information is synchronized with Group Policy template information.
- **Status information.** This indicates whether the Group Policy object is enabled or disabled for this site, domain, or organizational unit.
- **List of components**. This specifies which extensions to Group Policy have settings in the Group Policy object.

The Group Policy container stores information for the Software Installation snap-in and the Folder Redirection snap-in, two extensions of Group Policy.

Group Policy template

The Group Policy template is a folder of domain controllers for the storage domain of the Group Policy object. A typical Group Policy template folder might look like this example:

systemroot\Sysvol\SYSVOL\Streetmarket.com\Policies\
{34975054-fd77-df75-54fe-074936850457}

Subfolders of the Group Policy template

The Group Policy template folder contains subfolders including but not limited to the following:

- **adm.** Contains all of the .adm files for this Group Policy template.
- **Scripts.** Contains all the scripts and related files for this Group Policy template.
- **User.** Includes a Registry.pol file that contains the registry settings to be applied to users. When a user logs on to a computer, this Registry.pol file is downloaded and applied to the HKEY_CURRENT_USER portion of the registry. The User folder contains the following subfolders:
- **User\Applications.** Contains the .aas files (application advertisement scripts) used by the operating system–based installation service. These are applied to users.
- **Machine.** Includes a Registry.pol file that contains the registry settings to be applied to computers. When a computer initializes, this Registry.pol file is downloaded and applied to the **HKEY_LOCAL_MACHINE** portion of the registry. The Machine folder contains the following subfolders:
- **Machine\Applications.** Contains the .aas files used by the operating system–based installation service. These are applied to computers.

Group Policy precedence

In Windows 2000, Group Policy is applied to Group Policy objects that are in turn associated with Active Directory objects (sites, domains, or organizational units). Group Policy can be applied to either users or computers. It is important to note that although some settings are user interface settings—for example, the background bitmap, or the ability to use the **Run** command on the **Start** menu—they can be applied to computers.

Group Policy is applied hierarchically from the least restrictive group (site) to the most restrictive group (organizational unit). Group Policy is also cumulative. Child directory service containers inherit Group Policy from parent containers, and Group Policy processing occurs in the following order: site, domain, and organizational unit. This means that if you have assigned a specific Group Policy to a high-level parent container, that Group Policy applies to all containers beneath the parent container, including the user and computer objects in each container. However, if you explicitly specify a Group Policy for a child container, the child container's Group Policy overrides the parent container's Group Policy.

Optionally, you can enforce Group Policy on child directory containers by setting **No Override** on the Group Policy object. You can also prevent inheritance of Group Policy from parent directory containers.

Group Policies take precedence over profile settings in the event of a conflict.

This section covers:

- Order of events in startup and logon
- Order of processing settings
- The role of applications in Group Policy precedence

Order of events in startup and logon

The following sequence shows the order in which computer policy and user policy are applied when a computer starts and a user logs on:

1. Network starts. Remote Procedure Call System Service (RPCSS) and Multiple Universal Naming Convention Provider (MUP) are started.
2. An ordered list of Group Policy objects is obtained for the computer. The list might depend on these factors:
   - Whether the computer is part of a Windows 2000 domain, and is therefore subject to Group Policy through Active Directory.
   - The location of the computer in Active Directory.
   - If the list of Group Policy objects has not changed, then no processing is done. You can use a policy setting to change this behavior.
3. Computer policy is applied. These are the settings under Computer Configuration from the gathered list. This occurs synchronously by default, and in the following order: local, site, domain, organizational unit, child organizational unit, and so on. No user interface is displayed while computer policies are being processed.

   See Order of processing settings for details about the order in which settings are processed when user or computer policy is applied.
4. Startup scripts run. This is hidden and synchronous by default; each script must complete or time out before the next one starts. The default timeout is 600 seconds. You can use several policy settings to modify this behavior.
5. The user presses CTRL-ALT-DEL to log on.
6. After the user is validated, the user profile is loaded, governed by the policy settings in effect.
7. An ordered list of Group Policy objects is obtained for the user. The list might depend on these factors:
   - Whether the user is part of a Windows 2000 domain, and is therefore subject to Group Policy through Active Directory.
   - Whether loopback is enabled, and the state (**Merge** or **Replace**) of the loopback policy setting.
   - The location of the user in Active Directory.
   - If the list of Group Policy objects to be applied has not changed, then no processing is done. You can use a policy setting to change this behavior.
8. User policy is applied. These are the settings under User Configuration from the gathered list. This occurs synchronously by default, and in the following order: local, site, domain, organizational unit, child organizational unit, and so on. No user interface is displayed while user policies are being processed.

   See Order of processing settings for details about the order in which settings are processed when user or computer policy is applied.
9. Logon scripts run. Unlike Windows NT 4.0 scripts, Group Policy-based logon scripts are run hidden and asynchronously by default. The user object script (which, as in Windows NT 4.0, is run in a normal window) runs last.
10. Operating system user interface prescribed by Group Policy appears.

Important

- Three special cases deserve consideration during migration:
  - If the machine account object is in a Windows NT 4.0 domain and the user account object is in Active Directory, then only computer (not user) System Policy is processed when the user logs on. Then, user (not computer) Group Policy is processed.
  - If the machine account object is in Active Directory and the user account object is in a Windows NT 4.0 domain, then computer (not user) Group Policy is processed during computer startup. When the user logs on, user (not computer) System Policy is processed.
  - If the Windows 2000 computer and user accounts are members of a Windows NT 4.0 domain, then only System Policy (not Group Policy) for the computer and user is applied at user logon.

Notes

- Several of these events can be modified. You can set policies to:
  - Reverse the synchronize or asynchronize defaults of running scripts and applying policy.
  - Specify when scripts time out. By default scripts time out after 600 seconds.
  - Change whether scripts are run hidden, minimized, or in a normal window.

Order of processing settings

This section gives details about the order in which Group Policy settings for users and computers are processed in Windows 2000. See steps 3 and 8 in Order of events in startup and logon to see where the processing of policy settings fits into the framework of computer startup and user logon.

Group Policy settings are processed in the following order:

1. **Local Group Policy object**. Each Windows 2000 computer has exactly one Group Policy object stored locally.

2. **Site**. Any Group Policy objects that have been linked to the site are processed next. Processing is synchronous, and in an order specified by the administrator.
3. **Domain**. Multiple domain-linked Group Policy objects are processed synchronously, in an order specified by the administrator.
4. **Organizational units**. Group Policy objects linked to the organizational unit highest in the Active Directory hierarchy are processed first, then Group Policy objects linked to its child organizational unit, and so on. Finally, the Group Policy objects linked to the organizational unit that contains the user or computer are processed.

   At the level of each organizational unit in the Active Directory hierarchy, one, many, or no Group Policy objects can be linked. If several are linked to an organizational unit, then they are processed synchronously, and in an order specified by the administrator.

This order means that the local Group Policy object is processed first, and Group Policy objects linked to the organizational unit of which the computer or user is a direct member are processed last, overwriting the earlier Group Policy objects.

Exceptions to the default order

The default order of processing settings is subject to the following exceptions:

- Any Group Policy object linked to a site, domain, or organizational unit (not local Group Policy object) can be set to **No Override** with respect to that site, domain, or organizational unit, so that none of its policy settings can be overwritten. When more than one Group Policy object has been set to **No Override**, the one highest in the Active Directory hierarchy (or higher in the hierarchy specified by the administrator at each fixed level in Active Directory) takes precedence.

  Notice that **No Override** and **Disabled** are settings on Group Policy objects links, not the Group Policy objects. A Group Policy object can even be linked several times to the same organizational unit, and **No Override** and **Disabled** can be configured independently on each of the links. (Although multiple links from one Group Policy object to a single organizational unit would seldom be useful, this capability illustrates the flexibility of the Group Policy infrastructure.)

  For information on how to set links as **No Override** and **Disabled**, see To prevent a Group Policy object from being overridden and To disable a Group Policy object for a site, domain, or organizational unit.

- At any site, domain, or organizational unit, Group Policy inheritance can be selectively marked as **Block Policy inheritance**. Group Policy object links set to **No Override** are always applied, however, and cannot be blocked.

  The **Block Policy inheritance** setting is applied directly to the site, domain, or organizational unit. It is not applied to Group Policy objects, nor is it applied to Group Policy object links. Thus **Block Policy inheritance** deflects all Group Policy settings that would reach the site, domain, or organizational unit from above (by way of linkage to parents in the Active Directory hierarchy) no matter what Group Policy objects those settings originate from. However, **Block Policy inheritance** does not deflect Group Policy settings from Group Policy objects that have been directly linked to the site, domain, or organizational unit that has had **Block Policy inheritance** enabled.

- **Loopback** is an advanced Group Policy setting that is useful on computers in certain closely managed environments such as kiosks, laboratories, classrooms, and reception areas. For a description of loopback, see the **Explain** tab on the **User Group Policy loopback processing mode** properties sheet.

  Where?
  └Group_Policy_object_name
  └Computer Configuration
  └Administrative Templates
  └System
  └Group Policy

  Loopback provides alternatives to the default method of obtaining the ordered list of Group Policy objects whose user configuration settings affect a user. By default, a user's settings come from a Group Policy object list that depends on the user's location in Active Directory. The ordered list goes from site-linked to domain-linked to organizational unit-linked Group Policy objects, with inheritance determined by the location of the user in Active Directory, and in an order specified by the administrator at each level.

  Loopback can be **Not Configured**, **Enabled**, or **Disabled** as can any other Group Policy setting. In the **Enabled** state, loopback can be set to **Merge** or **Replace**.

  Loopback with Replace. In this case, the Group Policy object list for the user is replaced in its entirety by the Group Policy object list already obtained for the computer at computer startup (during step 2 in Order of events in startup and logon). The User Configuration settings from this list are applied to the user.

  Loopback with Merge. In this case, the Group Policy object list is a concatenation. The default step 2 list for computers is appended to the default step 7 list for users, and the user gets the user configuration settings in the concatenated list. Notice that the Group Policy object list obtained for the computer is applied later and therefore has precedence if it conflicts with settings in the user's list.

- A computer that is a member of a workgroup processes only the local Group Policy object.

The role of applications in Group Policy precedence

The Group Policy infrastructure cannot force applications to use Group Policy. For example, applications that have always looked for registry entries in a particular place outside the approved registry trees reserved for Group Policy will continue to look there. Group Policy does not copy registry settings from the Group Policy areas to the Windows NT 4.0 System Policy areas, nor does it copy Windows NT 4.0 System Policy settings into the reserved Group Policy areas.

Guidelines for writing applications that take advantage of Group Policy are available in the software development kit documentation used by developers. Administrators, who need to anticipate the behavior of applications that they do not author, should be aware of the steps taken by properly written applications to obtain the registry data they need.

Initial state of the registry

After the computer starts and the user logs on, the Group Policy registry areas are rewritten to hold the cumulative Group Policy settings that are in effect from the local Group Policy object and Active Directory. If Windows NT 4.0 System Policy is enabled (not recommended for Windows 2000 clients), then other registry areas might also have changed during logon.

Sequence of events

1. The user launches the application.
2. A typical user-oriented application looks for registry data in the Group Policy reserved area HKEY_LOCAL_MACHINE \Software \Policies. If it finds what it needs, it looks no further.

   However, an application that changes or replaces features at the level of the operating system (such as the **Run** command) and which therefore affects the behavior of applications other than itself might look in the following Group Policy reserved key: HKEY_LOCAL_MACHINE \Software \Microsoft \Windows \CurrentVersion \Policies.
   If it finds what it needs, it looks no further.

3. The application looks for HKEY_LOCAL_MACHINE registry data outside the Group Policy reserved area, and if it finds what it needs, it looks no further.
4. The application looks for HKEY_CURRENT_USER registry data outside the Group Policy reserved area, and if it finds what it needs, it looks no further.
5. The application uses .ini files (not recommended) or default settings.

Newly authored native Windows 2000 applications might perform only the first three steps. Applications that use Group Policy under Windows 2000, but which remain compatible with earlier versions of Windows, continue on to step four when they run on the older operating systems. Applications that predate Windows 2000 never see steps two and three, and instead jump to step four.

The order of the sequence of events implies that:

- For properly written applications running on Windows 2000 clients, Group Policy takes precedence over Windows NT 4.0 System Policy.
- Older versions of applications (which are not aware of Active Directory and Group Policy) continue to function on Windows 2000 computers as they did under Windows NT 4.0.
- HKEY_LOCAL_MACHINE settings take precedence over HKEY_CURRENT_USER settings as they did under Windows NT 4.0.

Understanding Software Installation

The Software Installation snap-in, a software management feature of Windows 2000, is the administrator's primary tool for managing software throughout its life cycle within the organization.

Software Installation works in conjunction with Group Policy and Active Directory. It is one of the three Software Installation and Maintainance tools provided with Windows 2000 Server. These are described in the following table.

Component	Role
The Software Installation extension of the Group Policy snap-in	Used by administrators to manage software.
Windows Installer	Installs software packaged in Windows Installer files.
Add/Remove Programs in Control Panel	Used by users to manage software on their own computers.

Assigning to users

When you assign an application to a user, the application is advertised to the user the next time that user logs onto a workstation. The application advertisement follows the user regardless of which physical computer he or she actually uses. This application is installed the first time the user activates the application on the computer, either by selecting the application on the **Start** menu, or by activating a document associated with the application.

Assigning to computers

When you assign an application to the computer, the application is advertised and the installation is performed when it is safe to do so. Typically this happens when the computer starts up, so that there are no competing processes on the computer.

Publishing to users

When you publish the application to users, the application does not appear installed on the users' computers. No shortcuts are visible on the desktop or **Start** menu, and no changes are made to the local registry on the users' computers. Instead, published applications store their advertisement attributes in Active Directory. Then, information such as the application's name and file associations is exposed to the users in the Active Directory container. The application is then available for the user to install using Add/Remove Programs in Control Panel or by clicking a file associated with the application (such as an .xls file for Microsoft Excel).

Application assignment scripts

For every published or assigned application in a particular Group Policy object, an application assignment script (.aas file) is generated and is stored in that domain's Group Policy object. These script files contain the advertisement information about the application configuration.

Active Directory

Windows 2000 Active Directory consists of a hierarchical collection of containers and an extendable schema. The Active Directory containers include sites, domains, organizational units, users, computers, and printers. Because the schema defines the properties of Active Directory objects and can be extended to define new Active Directory objects, you can use it to store any arbitrary object.

Software management provides schema-extended objects in Active Directory. These objects store the information required to map various class settings to the application packages that support these class settings.

The user's view of software installation

At the user's computer, system components including Winlogon, the shell, object linking and embedding (OLE), the Lightweight Directory Access Protocol (LDAP) client, and the local registry provide the user's view of software installation. Winlogon is the privileged agent that applies software installation policy. The shell and OLE are enhanced to be Active Directory–aware and to communicate with Windows Installer to perform setup actions. The LDAP client provides the capability to search and query Active Directory.

Using Add/Remove Programs, users can browse for and install software from Active Directory in a managed environment, or from local media (in a non-managed environment, or if policy permits, installation from local media in a managed environment).

This section covers:

- The administrator's view of software installation
- Add/Remove Programs in Control Panel
- File types often encountered in Software Installation

The administrator's view of software installation

Administrators must complete the following phases to manage software for their organization: preparation, management, and removal.

Preparation

Before you can use Software Installation, you need a Windows Installer package for the program you want to install. The package is often supplied with the software. If a program does not have a Windows Installer package, you need to generate one. Third-party utilities are available for repackaging a program you plan to install. You can then use transforms to further customize a package.

The next step is creating a network share, called a software distribution point, that contains the packages, any transforms, and the program files and components. Administration is simpler if packages and program files are kept together, although they don't have to be. (Packages and transforms do have to be kept together.) Administrators might also benefit from using distributed file systems to help manage these software distribution points.

Finally, you need to make sure that users can read from the software distribution point, and write to the target of the installation, particularly if the program is being written to a network file server.

Management

To manage programs within your organization, you use Software Installation. You can assign a program to either computers or users, or publish programs to users.

Program assignment and publishing to users have the following software life cycle phases:

- **Evaluation phase:** For evaluation purposes, you might want to have only a few users try out and evaluate the new program. During this phase, the old version of the program is the default version, and the majority of users are still using it. A new user would install the assigned or published version. This is often called a pilot. The pilot is a good time to experiment with Software Installation options such as Assign/Publish, Auto Install/Not Auto Install, and Visible Installation/Hidden Installation.
- **Rollout phase:** During rollout, you begin making the new program available to more users. The new version of the program is now the default, and the majority of the users are using the new version. A new user would only have the option to install the new program. You can leave certain users unaffected if upgrading them at this time would impact their work.

Program removal phase

When administrators remove a program, they must select one of the following alternatives (the choices are mutually exclusive):

- **Immediately Uninstall:** This option requires that no one currently uses the program. Those users who still have the program on their computers receive an advertisement that removes the program.
- **Just prevent new installations:** This option allows users to continue using the software they already have.

Deletion from the server

When you are sure that an old version of a program is no longer needed by the organization, you can delete the Windows Installer package and the program files and components. You might want to archive the package and the program files and components and then delete the files from the software distribution point.

Add/Remove Programs in Control Panel

Using Add/Remove Programs in Control Panel, you can perform a number of tasks, primarily installing an application from local media such as a CD-ROM or floppy disk, a defined Active Directory location (assigned and published application on a corporate network), or the Internet. You can also use Add/Remove Programs to remove or modify an existing application, or repair a damaged application.

Add/Remove Programs also offers the following features:

- Provides users with a single user interface to use for managing and maintaining their programs.
- Provides an interface that is useful for users with both advanced and novice knowledge about Microsoft Windows.
- Supports installation of programs when a user has the program package (on local media), as well as installation from either a corporate or an Internet environment.
- Exposes the Windows Installer component while maintaining support for other installation technologies.

File types often encountered in Software Installation

Besides executables such as Setup.exe and Install.exe, administrators typically work with the following types of files.

File type	File name extension	Description
Windows Installer packages	.msi	These files are typically provided by the software vendor to facilitate installation of a specific application. You need to keep these files with any other necessary files at the software distribution point for the software being managed.
Transforms	.mst	Also called modifications, these files customize the installation of a Windows Installer package at the time of assignment or publication. For example, they might specify a subset of a suite of applications.
Patches	.msp	Bug fixes, service packs, and similar files can be distributed in this form. Patches should not be used for major changes, and their effects are limited in the following ways: • Cannot remove components or features • Cannot change product codes • Cannot remove or change names of shortcuts, files, or registry keys
.zap files	.zap	These files, which are similar to .ini files, are created with a text editor such as Notepad. They can only be published (not assigned), and they specify an executable setup program (such as *server**share*\Excel\Setup.exe) that appears in Add/Remove Programs in Control Panel for the user. The user has administrative rights on the local computer.
Application assignment scripts	.aas	These files contain instructions associated with the assignment or publication of a package.

Using Group Policy

This section covers:

- Ways to open the Group Policy snap-in
- Scripts
- Local Group Policy
- Advanced methods of extending Group Policy
- Administering Group Policy
- Group Policy and network infrastructure

- Policy for the Group Policy snap-in
- Migration issues
- Administrative Templates

Ways to open the Group Policy snap-in

You can open Group Policy in several ways, depending on what action you want to perform with the snap-in.

To apply Group Policy to	Do this
The local computer	In the Group Policy console, edit the local Group Policy object, as described in To edit the local Group Policy object.
Another computer	Open the local Group Policy object that is stored on the Windows 2000 network computer, as described in To open Group Policy as a stand-alone MMC snap-in, and then browse to the network computer. You must be an administrator of the network computer.
A site	Open Group Policy as described in To open Group Policy from Active Directory Sites and Services, and then link a Group Policy object to the intended site.
A domain	Open Group Policy as described in To open Group Policy from Active Directory Users and Computers, and then link a Group Policy object to the intended domain.
An organizational unit	Open Group Policy as described in To open Group Policy from Active Directory Users and Computers, and then link a Group Policy object to the intended organizational unit. You can also link a Group Policy object to an organizational unit higher in the Active Directory hierarchy, so that the organizational unit can inherit Group Policy settings.
Any existing Group Policy object or set of Group Policy objects	Create and save your own custom MMC console. For more information, see Microsoft Management Console.

Scripts

Group Policy includes two extensions for script deployment:

- **Scripts – Startup/Shutdown.** You use this extension, located under the Computer Configuration node, to specify scripts that are to run at computer startup or shutdown. These scripts run as Local System.
- **Scripts – Logon/Logoff.** You use this extension, located under the User Configuration node, to specify scripts that are to run when the user logs on or off the computer. These scripts are run as User, not Administrator.

Windows 2000 includes Windows Script Host, a language-independent scripting host for 32-bit Windows platforms that includes both Visual Basic Scripting Edition (VBScript) and JScript scripting engines. You can use Windows Script Host to run .vbs and .js scripts directly on the Windows desktop or command console, without the need to embed those scripts in an HTML document.

For more information about Windows Script Host, see Windows Script Host Overview. To learn about Windows Script Host, the Object Model, and to obtain script samples, see the Windows Script Host Web site at the Microsoft Web site (http://www.microsoft.com/).

Local Group Policy

Each computer running Windows 2000 has exactly one local Group Policy object. Using these objects, Group Policy settings can be stored on individual computers whether or not they are part of an Active Directory environment or a networked environment.

Because its settings can be overwritten by Group Policy objects associated with sites, domains, and organizational units, the local Group Policy object is the least influential one in an Active Directory environment. In a non-networked environment (or in a networked environment lacking a Windows 2000 domain controller), the local Group Policy object's settings are more important because they are not overwritten by other Group Policy objects.

You can open the Group Policy snap-in to edit the local Group Policy object stored on your local computer. For information on how to do this, see To open the local Group Policy object.

If you want to edit the local Group Policy object stored on another computer on the network, open Group Policy as a stand-alone Microsoft Management Console (MMC) snap-in and browse to the Group Policy object you want. For information on how to do this, see To open Group Policy as a stand-alone MMC snap-in.

The local Group Policy object resides in *SystemRoot*\System32\GroupPolicy.

Computers running Windows NT 4.0 or earlier do not have a local Group Policy object.

Advanced methods of extending Group Policy

You can use the following advanced methods to extend Group Policy functionality.

Method	Advantages	Disadvantages
An advanced option for administrators: write an .adm file.	• Easier option. • Everything you need is included in Windows 2000. • The .adm files are ASCII files and can be edited in Notepad. • You can write from scratch or modify existing templates to suit your purpose.	• Only suitable for registry-based policies. • The user interface is limited. Finding where to set individual policies might be difficult.
An option for software developers only: write an extension to Group Policy.	• Richer user interface. • The full Group Policy API is available to the developer. • Not limited to registry-based policies.	• Because writing an extension takes considerable development time, this option is not worthwhile unless it will be used widely or often. • Requires Software Development Kit material not included with Windows 2000.

Creating custom .adm files

Administrators can consider creating custom .adm files if the supplied template, System.adm, is inadequate. However, you should try to use the supplied template if possible.

Administrative Templates propagate registry settings to a large number of computers without requiring you to have detailed knowledge of the registry. In Windows 2000, you use Group Policy to set registry-based policies. In Windows NT 4.0, you used the System Policy Editor (Poledit.exe) to set System Policy.

For more information, see Creating custom .adm files.

Creating Microsoft Management Console (MMC) snap-in extensions

This is a task for software developers, not administrators.

Developers can create MMC snap-in extensions to provide program-specific user interfaces for setting Group Policy.

For information about Microsoft Management Console (MMC), see the Microsoft Platform SDK documentation (http://msdn.microsoft.com) for components for setup and Systems Management Services developers.

Administering Group Policy

This section covers:

- Default permissions
- Delegating control of Group Policy
- Policy for Microsoft Management Console
- Using security groups to filter Group Policy

Default permissions

The default permissions on Group Policy objects are as follows:

Security group	Default settings
Authenticated users	Read, Apply Group Policy (AGP)
Local system	Full Control (includes AGP)
Domain administrators	Read, Write, Create Child, Delete Child, AGP
Administrators	Read, Write, Create Child, AGP

The **Default Domain Policy** Group Policy object cannot be deleted by any administrator, by default. This is to prevent the accidental deletion of this Group Policy object, which contains important and required settings for the domain. If it truly needs to be deleted—for example, because the policies have been set in other Group Policy objects—then the **Delete** access control entry (ACE) must be given back to the appropriate group.

Delegating control of Group Policy

To delegate control of Group Policy, you first create and save Group Policy Microsoft Management Consoles (.msc files). Next, you need to determine which users and groups have access permissions to the Group Policy object and the site, domain, and organizational unit.

Setting read and write permissions for Group Policy

The security access control list (ACL) editor tab for a Group Policy object is hosted in the Properties form of that Group Policy object. To access the ACL editor, right-click the root node of Group Policy, click **Properties**, and then click **Security**. You use the **Security** property page to set permissions on a selected Group Policy object. These permissions allow or deny access to the Group Policy object by specified groups.

Your organization's top network administrators (members of the Domain Administrators group) can also use the ACL editor to determine which administrator groups can modify policies in Group Policy objects. To do this, the network administrator can define groups of administrators (for example, Accounting Administrators), and then provide them Read/Write access to selected Group Policy objects. In this way, the network administrator can delegate control of the Group Policy object policies.

Note

A user or administrator who does not have Write access (but does have Read access) to a Group Policy object cannot use the Group Policy snap-in to see the settings that it contains. Every extension to Group Policy assumes that it has Write access to the Group Policy object storage locations. Therefore Group Policy does not open a Group Policy object when the current user does not have Write access to it.

Policy for Microsoft Management Console

Several Group Policy settings provided in System.adm governing use of Microsoft Management Console (MMC). This is significant, because saving previously configured consoles is a way to delegate administrative rights.

In the console tree, click Group Policy.

Where?
└ Group_Policy_object_name
└ User Configuration
└ Administrative Templates
└ Windows Components
└ Microsoft Management Console
└ Restricted/Permitted snap-ins
└ Group Policy

Double-click each extension to Group Policy for which you want to set an administrative Group Policy setting that governs use of the extension in MMC consoles.

For more information, see Delegating control of Group Policy and Microsoft Management Console.

Using security groups to filter Group Policy

Because Group Policy can apply settings from more than one Group Policy object to a site, domain, or organizational unit, you can add Group Policy objects that are associated with other directory objects. You can also prioritize how these Group Policy objects affect the directory object to which they are applied.

In Windows 2000, computers can belong to security groups. Administrators can use security groups to further refine which computers and users a Group Policy object influences. For any Group Policy object, administrators can filter the Group Policy object's effect on computers that are members of specified security groups. This filtering occurs using the standard access control list (ACL) editor. To use the ACL editor, click a Group Policy object's property sheet, and then click **Security**. The ACL editor can also be used by administrators to delegate who can modify the Group Policy object.

Group Policy and network infrastructure

This section covers:

- Group Policy in replicated environments

- Group Policy over slow links
- Group Policy on sites

Group Policy in replicated environments

In a domain containing more than one domain controller, Active Directory information takes time to propagate from one domain controller to another. This section describes the replication mechanism as it relates to Group Policy.

An administrator using Active Directory Users and Computers can create an organizational unit on any domain controller.

By default, Group Policy objects are created or edited only on the domain controller that is holding the primary domain controller emulator operations master token. This token moves from one domain controller to another over time, as Active Directory information is replicated to keep the domain controllers synchronized.

An organizational unit must be replicated to the domain controller holding the token before the Group Policy object created there can be linked to it, allowing the Group Policy settings to be applied.

These considerations are more significant if the intra-domain links are slow.

Options governing selection of a domain controller

The Group Policy **View** menu contains an entry called **DC Options**, which opens the **Options for domain controller selection** dialog box, where you can specify a domain controller to use for editing Group Policy. The available options for the **Options for domain controller selection** dialog box are:

- **The one with the Operations Master token for the PDC emulator.** This is the default and preferred option, and is safest from the standpoint of data safety.
- **The one used by the Active Directory snap-ins.** Uses the domain controller that the utility from which the Group Policy console was invoked is currently using, if Group Policy was started in this way.
- **Use any available domain controller.** Allows the Group Policy snap-in to choose any available domain controller. This is the least safe option, because different administrators could theoretically edit a Group Policy object simultaneously, with indeterminate outcome. On the other hand, when this option is used it is likely that a domain controller in the local site will be selected. If only one administrator can administer Group Policy on a large domain with several sites, then the performance gain might be worthwhile.

Domain controller selection set through Group Policy

In addition to the **View** menu option described previously, there is also a Group Policy setting for domain controller selection. This is part of the System.adm Administrative Template that is loaded into the Group Policy console by default.

To access this setting, in the console tree, click the Group Policy node.

Where?
└ *Group_Policy_object_name*
└ User Configuration
└ Administrative Templates
└ System
└ Group Policy

In the details pane, double-click the **Group Policy domain controller selection** icon, and then select the appropriate setting from the drop-down list.

Group Policy over slow links

Group Policy is applied remotely, provided the computer is a member of the domain that the Routing and Remote Access server belongs to or is trusted to. This is true whether logging on by way of Routing and Remote Access, or logging on with cached credentials and then establishing a Routing and Remote Access connection.

Group Policy is not applied to computers that are members of a foreign domain (a domain not containing the computer, and not in a trust relationship with the computer's domain), or a workgroup. Although the connection may still be made, access to domain resources may be adversely affected because of mismatched IPSEC security.

By default, registry-based polices are always applied, and cannot be turned off. Security Settings are also applied by default, but all others are not applied. For all but the registry settings, the default behavior can be toggled to apply or not.

A remote access connection is not necessarily a slow link, nor is a local area network (LAN) necessarily a fast link. By default, the fast or slow status of a link is based on a test ping to the server. If it takes less than 2000 milliseconds (two seconds), then it's considered a fast link; more and it's considered a slow link. You can set this value using the Group Policy setting **Slow network connection timeout for user profiles Properties**.

Where?
└ group_policy_object_name
└ Computer Configuration
└ Administrative Templates
└ System
└ Logon

Several other Group Policy settings related to slow links appear there as well. Also, see the Group Policy setting **Group Policy slow link detection**.

Where?
└ group_policy_object_name
└ Computer Configuration
└ Administrative Templates
└ System
└ Group Policy

Group Policy on sites

Group Policy objects applied to Active Directory site objects affect all computers in the site. Directory information is replicated among and available between all the domain controllers in the site and to any domain controllers in sites for which a site link has been established. Therefore, any Group Policy object linked to a site is applied to all computers in that site regardless of which domain (in the forest) contains the computers.

This allows for multiple domains within a forest to get the same Group Policy object (and included policies), although the Group Policy object exists only as a stored entity on a single domain and must be read from that domain when the affected clients read their site-linked Group Policy.

If child domains are set up across wide area network (WAN) boundaries, the site setup should take this into account. If not, the computers in a child domain will be accessing a site-linked Group Policy object across a WAN link. This will increase the processing time for Group Policy.

Policy for the Group Policy snap-in

This section covers:

- Policy for Group Policy: Computer Configuration
- Policy for Group Policy: User Configuration

Policy for Group Policy: Computer configuration

This topic describes policies concerned with managing computers through Group Policy. Because these policies are included in System.adm, they should be present by default. To configure these policies, see Open the Group Policy snap-in. In the console tree, click the **Group Policy** node.

Where?
└ *policy_name* Policy
└ Computer Configuration
└ Administrative Templates
└ System
└ Group Policy

Disable background refresh of Group Policy

Prevents Group Policy from being updated while the computer is in use. This policy applies to Group Policy settings for computers, users, and domain controllers. If you enable this policy, the system waits until the current user logs off the system before updating the computer and user policies.

If you disable this policy, updates can be applied while users are working. The frequency of updates is determined by the **Group Policy refresh interval for computers** and **Group Policy refresh interval for users** policies.

Apply Group Policy for computers synchronously during startup

Directs the system to wait for updates to Group Policy to be completed before it displays the logon prompt. This policy applies only to Group Policy settings in the Computer Configuration folder.

If you enable this policy, users cannot log on until Group Policy for computers has been updated.

If you disable this policy, the system does not wait for Group Policy updates to complete before inviting the user to log on. As a result, the logon dialog box might appear sooner, but the Windows interface can appear to be ready before all Group Policy settings have been applied.

To determine whether the system synchronizes user Group Policy settings and Windows Explorer, see the **Apply Group Policy for user synchronously during startup** policy.

Apply Group Policy for users synchronously during startup

Directs the system to wait for updates to Group Policy to finish before it displays the logon prompt. This policy applies only to Group Policy settings that appear in the User Configuration folder. If you enable this policy, users cannot log on until user Group Policy settings have been updated.

If you disable this policy, the system does not wait for policy updates to complete before inviting users to log on. As a result, the **Log on to Windows** dialog box might appear sooner, but the Windows interface can appear to be ready before all policies have been applied. To determine whether the system synchronizes computer policies and Windows Explorer, see the **Apply Group Policy for computers synchronously during startup** policy.

Group Policy refresh interval for computers

Specifies how often Group Policy for computers is updated while the computer is in use (in the background). This policy specifies a background update rate only for Group Policy settings in the Computer Configuration folder.

In addition to background updates, Group Policy for the computer is always updated when the system starts.

If you disable this policy, Group Policy is updated every 90 minutes (the default), with a random offset of 0 to 30 minutes. You can specify an update rate from 0 to 64,800 minutes (45 days). If you select 0 minutes, the computer tries to update Group Policy every 7 seconds. However, because updates might interfere with users' work and increase network traffic, very short update intervals are not appropriate for most installations.

To specify that Group Policy should never be updated while the computer is in use, select the **Disable background refresh of Group Policy** policy.

You can also use the **Group Policy refresh interval for computers** policy to specify how much the actual update interval varies. To prevent clients with the same update interval from requesting updates simultaneously, the system varies the update interval for each client by a random number of minutes. The number you type in the random time box sets the upper limit for the range of variance. For example, if you type 30 minutes, the system selects a variance of 0 to 30 minutes. Typing a large number establishes a broad range and makes it less likely that client requests overlap. However, updates might be delayed significantly.

This policy establishes the update rate for computer Group Policy. To set an update rate for user policies, use the **Group Policy refresh interval for users** policy (located in User Configuration\Administrative Templates\System\Group Policy).

This policy is used only when the **Disable background refresh of Group Policy** policy is not enabled.

Note

- Consider notifying users that their policy is updated periodically so that they recognize the signs of a policy update. When Group Policy is updated, the Windows desktop is refreshed; it flickers briefly and closes open menus. Also, restrictions imposed by Group Policy settings, such as those that limit the programs users can run, might interfere with tasks in progress.

Group Policy refresh interval for domain controllers

Specifies how often Group Policy is updated on domain controllers while they are running (in the background). The updates specified by this policy occur in addition to updates performed when the system starts.

By default, Group Policy on the domain controllers is updated every five minutes.

You can specify an update rate from 0 to 64,800 minutes (45 days). If you select 0 minutes, the domain controller tries to update Group Policy every 7 seconds. However, because updates might interfere with users' work and increase network traffic, very short

update intervals are not appropriate for most installations.

If you disable this policy, the domain controller updates Group Policy every five minutes (the default). To specify that Group Policy settings for users should never be updated while the computer is in use, select the **Disable background refresh of Group Policy** policy.

You can also use this policy to specify how much the actual update interval varies. To prevent domain controllers with the same update interval from requesting updates simultaneously, the system varies the update interval for each controller by a random number of minutes. The number you type in the random time box sets the upper limit for the range of variance. For example, if you type 30 minutes, the system selects a variance of 0 to 30 minutes. Typing a large number establishes a broad range and makes it less likely that update requests overlap. However, updates might be delayed significantly.

Note

- This policy is used only when you are establishing policy for a domain, site, organizational unit, or customized group. If you are establishing policy for a local computer only, the system ignores this policy.

User Group Policy loopback processing mode

Applies alternate user policy settings when a user logs on to a computer affected by this policy setting. The possible settings are **Normal**, **Merge**, and **Replace**.

This policy directs the system to apply the set of Group Policy objects for the computer to any user who logs on to a computer affected by this policy setting. It is intended for special-use computers, such as those in public places, laboratories, and classrooms, where you must modify the user policy setting based on the computer that is being used.

By default, the user's Group Policy objects determine which user policy settings apply. If this policy is enabled, then, when a user logs on to this computer, the computer's Group Policy objects determine which set of Group Policy objects applies.

To use this policy, select one of the following policy modes from the **Mode** box:

Replace indicates that the user policy settings defined in this computer's Group Policy objects replace the user policy settings normally applied to the user.

Merge indicates that the user policy setting defined in this computer's Group Policy objects and the user policy settings normally applied to the user are combined. If the policy settings conflict, the user settings in this computer's Group Policy objects take precedence over the user's normal policy settings.

If you disable this policy or do not configure it, the user's Group Policy objects determine which user policy settings apply.

Group Policy slow link detection

Defines a slow connection for purposes of applying and updating Group Policy settings.

If the rate at which data is transferred from the domain controller providing a policy update to the computers in this group is slower than the rate specified by this policy, the system considers the connection to be slow.

The system's response to a slow policy connection varies among policies. The program implementing the policy can specify the response to a slow link. Also, you can use the policy-processing policies in this folder to override the programs's specified responses to slow links.

To use this policy, in the **Connection speed** box, type a decimal number between 0 and 4,294,967,200 (0xFFFFFFA0), indicating a transfer rate in kilobits per second. Any connection slower than this rate is considered to be slow. If you type 0, all connections are considered to be fast.

If you disable this policy or do not configure it, the system uses the default value of 500 kilobits per second.

This policy appears in the Computer Configuration and User Configuration folders. The policy in Computer Configuration defines a slow link for policies in the Computer Configuration folder. The policy in User Configuration defines a slow link for policies in the User Configuration folder.

Registry policy processing

If this policy is configured, the choices are **Do not apply during periodic background processing** and **Process even if the Group Policy objects have not changed**. These are independent of each other.

This policy determines when registry policies are updated, and it affects all policies in the Administrative Templates folder and any other policies that store values in the registry. It overrides customized settings that the program implementing a registry policy set when it was installed.

If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.

The **Do not apply during periodic background processing** option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.

The **Process even if the Group Policy objects have not changed** option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a setting if a user changes it.

Folder Redirection policy processing

If this policy is configured, the choices are **Do not apply across a slow network connections** and **Process even if the Group Policy objects have not changed**. These are independent of each other.

This policy determines when folder redirection policies are updated, and it affects all policies that use the Folder Redirection component of Group Policy, such as those in Windows Settings\Folder Redirection. You can set folder redirection policy only for Group Policy objects stored in Active Directory, not for Group Policy objects on the local computer.

This policy overrides customized settings that the program implementing the folder redirection policy set when it was installed.

If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.

The **Allow processing across a slow network connection** option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.

The **Process even if the Group Policy objects have not changed** option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a setting if a user changes it.

Disk Quota policy processing

If this policy is configured, the independent choices are **Allow processing across a slow network connection**, **Do not apply during periodic background processing**, and **Process even if the Group Policy objects have not changed**.

This policy determines when disk quota policies are updated, and it affects all policies that use the disk quota component of Group Policy, such as those in Computer Configuration\Administrative Templates\System\File System\Disk Quotas. It also overrides customized settings that the program implementing the disk quota policy set when it was installed.

If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system

The **Allow processing across a slow network connection** option updates the policies even when the update transmits across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.

The **Do not apply during periodic background processing** option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.

The **Process even if the Group Policy objects have not changed** option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a setting if a user changes it.

Scripts policy processing

If this policy is configured, the independent choices are **Allow processing across a slow network connection**, **Do not apply during periodic background processing**, and **Process even if the Group Policy objects have not changed**.

This policy determines when policies that assign shared scripts are updated, and it affects all policies that use the Scripts component of Group Policy, such as those in WindowsSettings\Scripts. It also overrides customized settings that the program implementing the scripts policy set when it was installed.

If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.

The **Allow processing across a slow network connection** option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.

The **Do not apply during periodic background processing** option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.

The **Process even if the Group Policy objects have not changed** option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a setting if a user changes it.

Security policy processing

If this policy is configured, the independent choices are **Do not apply during periodic background processing** and **Process even if the Group Policy objects have not changed**.

This policy determines when security policies are updated, and it affects all policies that use the security component of Group Policy, such as those in Windows Settings\Security Settings. It also overrides customized settings that the program implementing the security policy set when it was installed.

If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.

The **Allow processing across a slow network connection** option updates the policies even when the update transmits across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.

The **Do not apply during periodic background processing** option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.

The **Process even if the Group Policy objects have not changed** option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a setting if a user changes it.

EFS recovery policy processing

If this policy is configured, the independent choices are **Allow processing across a slow network connection**, **Do not apply during periodic background processing**, and **Process even if the Group Policy objects have not changed**.

This policy determines when encryption polices are updated, and it affects all policies that use the encryption component of Group Policy, such as policies related to encryption in Windows Settings\Security Settings. It also overrides customized settings that the program implementing the encryption policy set when it was installed.

If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.

The **Allow processing across a slow network connection** option updates the policies even when the update transmits across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.

The **Do not apply during periodic background processing** option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.

The **Process even if the Group Policy objects have not changed** option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a setting if a user changes it.

Software Installation policy processing

If this policy is configured, the independent choices are **Allow processing across a slow network connection** and **Process even if the Group Policy objects have not changed**.

This policy determines when software installation polices are updated, and it affects all policies that use the Software Installation component of Group Policy, such as policies in Software Settings\Software Installation. You can set software installation policy only for Group Policy objects stored in Active Directory, not for those on the local computer.

This policy overrides customized settings that the program implementing the software installation policy set when it was installed.

If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.

The **Allow processing across a slow network connection** option updates the policies even when the update transmits across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.

The **Process even if the Group Policy objects have not changed** option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a setting if a user changes it.

IP security policy processing

If this policy is configured, the independent choices are **Allow processing across a slow network connection**, **Do not apply during periodic background processing**, and **Process even if the Group Policy objects have not changed**.

This policy determines when IP security polices are updated, and it affects all policies that use the IP security component of Group Policy, such as policies in Computer Configuration\Windows Settings\Security Settings\IP Security Policies on Local Machine. It also overrides customized settings that the program implementing the IP security policy set when it was installed.

If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.

The **Allow processing across a slow network connection** option updates the policies even when the update transmits across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.

The **Do not apply during periodic background processing** option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.

The **Process even if the Group Policy objects have not changed** option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a setting if a user changes it.

Download missing COM components

Directs the system to search Active Directory for missing Component Object Model (COM) components that a program requires.

Many Windows programs, such as the Microsoft Management Console snap-ins, use the interfaces provided by the COM. These programs cannot perform all of their functions unless Windows 2000 has internally registered the required components.

If you enable this policy and a component registration is missing, the system searches for it in Active Directory and, if it is found, downloads it. The resulting searches might make some programs start or run slowly.

If you disable this policy or do not configure it, the program continues without the registration. As a result, the program might not perform all of its functions, or it might stop.

This policy applies to computers. To set this policy for users, use the **Download missing COM components** policy in UserConfiguration\AdministrativeTemplates\System\Group Policy.

Policy for Group Policy: User configuration

This topic describes policies you use to manage users through Group Policy. Because these policies are included in System.adm, they should be present in the console by default. To configure these policies, open Group Policy as described in To open the Group Policy snap-in. In the console tree, click the Group Policy node.

Where?
└ *policy_name* Policy
└ User Configuration
└ Administrative Templates
└ System
└ Group Policy

Group Policy refresh interval for users

Specifies how often Group Policy for users is updated while the computer is in use (in the background). This setting specifies a background update rate only for the Group Policy settings in the User Configuration folder.

In addition to background updates, Group Policy for users is always updated when users log on.

By default, user Group Policy is updated in the background every 90 minutes, with a random offset of 0 to 30 minutes.

You can specify an update rate from 0 to 64,800 minutes (45 days). If you select 0 minutes, the computer tries to update user Group Policy every 7 seconds. However, because updates might interfere with work and increase network traffic, very short update intervals are not appropriate for most installations.

If you disable this setting, user Group Policy is updated every 90 minutes (the default). To specify that Group Policy for users should never be updated while the computer is in use, select the **Disable background refresh of Group Policy** setting.

You can also use this setting to specify how much the actual update interval varies. To prevent clients with the same update interval from requesting updates simultaneously, the system varies the update interval for each client by a random number of minutes. The number you type in the random time box sets the upper limit for the range of variance. For example, if you type 30 minutes, the system selects a variance of 0 to 30 minutes. Typing a large number establishes a broad range and makes it less likely that client requests overlap. However, updates might be delayed significantly.

This setting establishes the update rate for user Group Policies. To set an update rate for computer Group Policies, use the **Group Policy refresh interval for computers** setting (located in Computer Configuration\Administrative Templates\System\Group Policy).

This setting is used only when the **Disable background refresh of Group Policy** setting is not selected.

Note

- Consider notifying users that their Group Policy is updated periodically so that they recognize the signs of a policy update. When Group Policy is updated, the Windows desktop is refreshed; it flickers briefly and closes open menus. Also, restrictions imposed by Group Policies, such as those that limit the programs a user can run, might interfere with tasks in progress.

Group Policy slow link detection

Defines a slow connection for purposes of applying and updating Group Policy.

If the rate at which data is transferred from the domain controller providing a policy update to the computers in this group is slower

than the rate specified by this setting, the system considers the connection to be slow.

The system's response to a slow policy connection varies among policies. The program implementing the policy can specify the response to a slow link. Also, the policy processing policies in this folder let you override the program's specified responses to slow links.

To use this policy, in the **Connection speed** box, type a decimal number between 0 and 4,294,967,200 (0xFFFFFFA0), indicating a transfer rate in kilobits per second. Any connection slower than this rate is considered to be slow. If you type 0, all connections are considered to be fast.

If you disable this policy or do not configure it, the system uses the default value of 500 kilobits per second.

This policy appears in the Computer Configuration and User Configuration folders. The policy in Computer Configuration defines a slow link for policies in the Computer Configuration folder. The policy in User Configuration defines a slow link for policies in that folder.

Group Policy domain controller selection

Determines which domain controller the system uses when applying Group Policy to users.

Use the Primary Domain Controller indicates that policy is applied by the primary domain controller in the domain in which the user is logged on.

Inherit from the Active Directory Snap-ins indicates that policy is applied by the domain controller hosting the Group Policy snap-in.

Use any available domain controller indicates that the system can use the first domain controller it finds available in the domain.

If you disable this policy or do not configure it, the primary domain controller applies Group Policy.

Create new Group Policy object links disabled by default

If you enable this policy, the **New Group Policy Object** check box on the Active Directory Users and Computers and the Active Directory Sites and Services snap-ins is cleared (not selected) by default. Administrators can still select the check box to select the option.

If you disable this policy or do not configure it, the **New Group Policy Object** option is selected by default and administrators must click to clear it.

Enforce Show Policies Only

This policy affects the **Show Policies Only** view menu option in the Administrative Templates node of the Group Policy.

Enabling this policy prevents the user from clearing the **Show Policies Only** menu item. Disabling this policy prevents the user from selecting this menu item.

In this context, policies refers to Windows 2000 Group Policy, not Windows NT 4.0–style system policies. See Windows NT 4.0 System Policies for an explanation of why this distinction is significant.

Disable automatic update of .adm files

Prevents the system from updating the Administrative Templates source files automatically when you open Group Policy.

By default, when you start Group Policy, the system loads the most recently revised copies of the Administrative Templates source files (.adm) in the %systemroot%\inf folder. The .adm files create the list of policies that appear under Administrative Templates in Group Policy.

If you enable this policy, the system loads the .adm files you used the last time you ran Group Policy. After this, you must update the .adm files manually.

Notes

- Upgrading your .adm files does not overwrite your policy configuration settings. The settings are stored in Active Directory, not in the .adm files.
- To upgrade your .adm files manually, in Group Policy, right-click **Administrative Templates** (either instance), and then click **Add/Remove Templates**.

Download missing COM components

Tells the system to search Active Directory for missing Component Object Model (COM) components that a program requires.

Many Windows programs, such as the MMC snap-ins, use the interfaces provided by the Component Object Model. These programs cannot perform all of their functions unless Windows 2000 internally registers the required components.

If you enable this policy and a component registration is missing, the system searches for it in Active Directory and, if it is found, downloads it. The resulting searches might make some programs start or run slowly.

If you disable this policy or do not configure it, the program continues without the registration. As a result, the program might not perform all of its functions, or it might stop.

This policy applies to users. To set this policy for computers, use the **Download missing COM components** policy in ComputerConfiguration\AdministrativeTemplates\System\Group Policy.

Migration issues

This section covers:

- Client operating systems
- The role of Administrative Templates
- The role of System Policy Editor
- Windows NT 4.0 System Policies

Client operating systems

This section describes several operating-system issues regarding clients for policy.

Windows 2000 Server

Computers running Windows 2000 Server can either be ordinary member servers of Active Directory or domain controllers. Group Policy fully supports both.

Windows 2000 Professional

Group Policy fully supports client computers running Windows 2000 Professional.

Windows NT 4.0 Workstation and Server

These clients continue to be fully supported by Windows NT 4.0 System Policy, for which the System Policy Editor (Poledit.exe) is provided. The administrator uses Poledit.exe to write Windows NT 4.0–style .adm files.

Windows NT 4.0 does not use Active Directory. Because computers running Windows NT 4.0 do not have local Group Policy objects, Group Policy does not apply.

Windows 95 and Windows 98

Windows 95 and Windows 98 clients should run System Policy Editor (Poledit.exe) on the local computer. This ensures that the Config.pol file created will be compatible with those operating systems. Copy the resultant Config.pol file to the SysVol folder of the Windows 2000 Server domain controller.

Group Policy does not apply.

Windows NT 3.51, Windows 3.1, and MS-DOS

Group Policy does not apply.

Note

- Exactly one local Group Policy object exists on each computer running Windows 2000, and the User Configuration settings it contains are the same for each user of that computer. To handle multiple user configurations using policy on a computer running Windows 2000 that is subject to only a single Group Policy object because it is not part of a Windows 2000 domain (for example, a stand-alone computer), the administrator uses System Policy through System Policy Editor (Poledit.exe). Poledit.exe is run on the local computer to create a correctly formatted .pol file. User profiles provide individually configured desktops for individual users if neither System Policy nor Group Policy is used.

The role of Administrative Templates

In Windows 2000, Administrative Templates have the .adm file name extension, as they did in Windows NT 4.0. However, their roles are slightly different.

Role in earlier versions of Windows

In previous versions of Windows, Administrative Templates were ANSI-encoded text files. They created a namespace within System Policy Editor for convenient editing of the registry. Administrative Templates provided a friendlier user interface than the Registry Editor (Regedit.exe). They also added a degree of safety by exposing only the registry keys explicitly mentioned in the .adm file.

Role in Windows 2000

Windows 2000 includes several .adm files, which are listed in .adm files included with Windows 2000. You can also write additional .adm files. The new version of the .adm language is a superset of the previous version—older templates can create a user interface in Group Policy, but new ones cannot in System Policy Editor. For more information on the new .adm language, see Creating custom .adm files.

Windows 2000 supports Unicode-based .adm files.

For cautionary information on using Windows NT 4.0–style .adm files in a Windows 2000 environment, see Windows NT 4.0 system policies.

The role of System Policy Editor

Although System Policy Editor (Poledit.exe) is largely replaced by Group Policy, it is still useful under some circumstances.

- **Management of computers running Windows 95 or Windows 98**. The Windows 2000 version of the System Policy Editor must be run locally on computers running Windows 98 or Windows 95 to create Config.pol files compatible with the local operating system.
- **Management of computers running Windows NT 4.0 Workstation and Windows NT 4.0 Server**. These computers also need their own style of .pol file: NTConfig.pol.
- **Management of stand-alone computers running Windows 2000**. A Windows 2000 computer that is not joined to any domain is therefore not subject to nonlocal Group Policy by way of Active Directory. The only Group Policy that applies to such a computer is local Group Policy, which contains settings for only one user. (For more information on local Group Policy, see Local Group Policy.) To provide settings for multiple users, use System Policy Editor to write a Registry.pol file. Only the Windows 2000 version of System Policy Editor is compatible with Windows 2000.

Although earlier versions of System Policy Editor worked only with ASCII-encoded .adm files, the Windows 2000 version also supports Unicode-encoded .adm files.

Windows NT 4.0 system policies

If a Windows NT 4.0 client computer managed by a Windows 2000 server is upgraded to Windows 2000, then afterward the computer receives only Computer Configuration Group Policy, and not Windows NT 4.0 machine System Policy. The policy received by the user who logs on will be User Configuration Group Policy if the user account is in Active Directory. If the user account is managed by a Windows NT 4.0 domain controller, then the user gets Windows NT 4.0 user System Policy.

Policies included with Windows 2000 only set registry keys and values in one of these four reserved trees:

- HKEY_LOCAL_MACHINE \Software \Policies
- HKEY_CURRENT_USER \Software \Policies
- HKEY_LOCAL_MACHINE \Software \Microsoft \Windows \CurrentVersion \Policies
- HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \Policies

The first two are preferred. All four trees are secure, and cannot be modified by a user who is not an administrator.

When Group Policy changes for any reason, these trees are wiped clean and the new policies are then rewritten.

Windows NT 4.0 policies do not respect these special trees, and can write to any part of the registry. After such a policy is applied, it persists until the value is intentionally reversed, either by a counteracting Windows NT 4.0–style policy, or by editing the registry.

Caution

- It is possible for an Administrative Template (.adm file) to be added to Group Policy that sets registry values outside of the

approved Windows 2000 Group Policy trees, although Windows 2000 does not include any such .adm file. The administrator who chooses to install Windows NT 4.0–style .adm files should be aware that this can lead to undesirably persistent registry settings.

Administrative Templates

Group Policy requires a source from which to generate the user interface settings an administrator can set. For this purpose, Group Policy can use either a Microsoft Management Console extension snap-in to Group Policy, or an ASCII file referred to as an Administrative Template (.adm file).

The .adm file consists of a hierarchy of categories and subcategories that together define how the options are displayed through Group Policy. This file also indicates the registry settings that can be modified through Group Policy in addition to:

- Registry locations where changes should be made if a particular selection is made.
- Options or restrictions (in values) that are associated with the selection.
- In some cases, a default value to use if a selection is activated.

This section covers:

- .adm files included with Windows 2000
- Advanced topic: Creating custom .adm files

.adm files included with Windows 2000

Five Administrative Templates are included with Windows 2000.

Administrative template	Description
System.adm	Installed in Group Policy by default. For Windows 2000 clients.
Inetres.adm	Installed in Group Policy by default. Internet Explorer policies for Windows 2000 clients.
Winnt.adm	User interface options specific to Windows NT 4.0. For use with System Policy Editor (Poledit.exe).
Windows.adm	User interface options specific to Windows 95 and Windows 98. For use with System Policy Editor (Poledit.exe).
Common.adm	User interface options common to Windows NT 4.0 and Windows 95 and 98. For use with System Policy Editor (Poledit.exe).

System.adm and Inetres.adm use the four reserved Group Policy registry areas. For the locations of those areas, see Windows NT 4.0 system policies. Although the last three .adm files can be loaded into Group Policy, you should limit their use to the administration of earlier versions of Windows through System Policy Editor.

Visibility of System Policy settings in the Group Policy console

When an .adm file is added to Group Policy as described in To add or remove an Administrative Template (.adm file), by default only the settings contained in the genuine Group Policy trees are visible in the console. To change this default user preference, on the **View** menu of the Group Policy console, clear the **Show Policies Only** check box. (For **Show Policies Only** to appear on the **View** menu, you need to select one of the Administrative Templates nodes.)

The ability to clear the **Show Policies Only** setting on the **View** menu is subject to a Group Policy setting called **Enforce Show Policies Only**.

Where?
└*Group_Policy_object_name* [*domain_controller_name.domain_name*] Policy
└User Configuration
└Administrative Templates
└System
└Group Policy

When System Policy settings are allowed to be visible in a Group Policy console, the icons for those settings appear red. The icons for true Group Policy settings appear blue.

Caution

- It is highly recommended that you do not use System Policy–type .adm files when you manage Windows 2000 clients because this leads to undesirably persistent registry settings.

Advanced topic: Creating custom .adm files

An .adm file defines how registry-related Group Policy settings are displayed under the Administrative Templates nodes in the Group Policy user interface. In addition, the .adm file:

- Specifies the registry locations where changes should be made if an administrator makes a particular selection. (These registry locations are not shown in the Group Policy user interface, because an administrator generally doesn't need to work with them directly.)
- Specifies any options or restrictions (in values) that are associated with the selection.
- Can specify a default value to use if a selection is activated.

The following sections describe the components of an .adm file.

- STRING
- CLASS
- CATEGORY
- POLICY
- EXPLAIN
- PART
- PartTypes
- NUMERIC

String variables

You use string variables in an .adm file if you want to use variables to define text strings for the user interface. This is useful if the strings are lengthy and are used in several locations throughout the .adm file. This method also allows easier conversion to other languages (localization).

You can use string variables for **CATEGORY**, **POLICY**, **PART**, and **DEFAULT**. Assign the variable name to the component by preceding it with two exclamation points (**!!**). Then, in the [strings] section of the file, link the variable with the actual string to be used in the user interface. The string must be enclosed in quotation marks.

component **!!***variable*

where *component* is **CATEGORY**, **POLICY**, **PART**, or **DEFAULT**, and *variable* is the variable you want to use for a given string.

Optionally, you can enclose a variable name in double quotation marks (**"**). Names with spaces must be enclosed by double quotation marks.

In the [strings] section of the file, you define the variable as follows:

variable **=** "*string*"

String variable example

Suppose you want to use the following category name several places throughout your user interface:

My First Category

You could assign the following variable to this string:

FirstCategory

You would use the following

```
CATEGORY !!FirstCategory
```

Then, in the **[strings]** section, you would define the **FirstCategory** variable:

```
FirstCategory="My First Category"
```

Result: The **My First Category** string would be displayed without quotation marks in the Group Policy user interface.

CLASS

Your first entry in an .adm file must be **CLASS *xxxx***, where *xxxx* can be one of the following:

MACHINE: This section includes entries found in the Computer Configuration node in Group Policy.

USER: This section includes entries found in the User Configuration node in Group Policy.

These are the only two valid classes within an .adm file. The Group Policy snap-in ignores non-valid classes.

The valid keywords for **CLASS** are

- CLASS
- CATEGORY
- StringsSect
- USER
- MACHINE

CATEGORY

The category name is displayed in Group Policy as a node in either the Computer Configuration or the User Configuration node, depending on whether it is defined under the MACHINE class or the USER class.

The **CATEGORY** syntax is as follows:

CATEGORY !!"*variable name***"**

[**KEYNAME "***key name***"**]

[... *policy definition statements* ...]

END CATEGORY

where:

variable name is the category name as it should appear in the Group Policy list box. Names with spaces must be enclosed by double quotation marks.

key name is the optional registry key name to use for the category. If a key name is specified, it will be used by all child categories, policies, and parts, unless they specifically provide a key name of their own. Names with spaces must be enclosed by double quotation marks.

A policy definition statement cannot appear more than once in a single category.

The following example shows a category name of MyNewCategory:

```
CATEGORY !!MyNewCategory
```

To close the category after filling in the options, use:

```
END CATEGORY ; MyNewCategory
```

Note that categories can be nested to create subcategories as in the following example:

```
CATEGORY !!FirstCategory
CATEGORY !!SecondCategory
CATEGORY !!ThirdCategory
...
...
END CATEGORY ; ThirdCategory
END CATEGORY ; SecondCategory
END CATEGORY ; FirstCategory
```

The valid keywords for CATEGORY are:

- KEYNAME
- CATEGORY
- POLICY
- END

POLICY

To identify the policy that the user can modify, you use the keyword **POLICY**:

```
POLICY !!MyFirstPolicy
...fill in all the policy specifics
...and then finish with:
END POLICY
```

You can use multiple **POLICY** key names under one **KEYNAME**. In the previous example, you must define the *MyFirstPolicy* variable in the **[strings]** section of the .adm file.

The valid keywords for POLICY are:

- KEYNAME
- VALUENAME
- PART
- VALUEON
- VALUEOFF
- ACTIONLISTON
- ACTIONLISTOFF
- END
- HELP
- CLIENTEXT
- POLICY

VALUENAME

Defines the options available within a policy. You must first identify the registry value that is to be modified as a result of using the keyword **VALUENAME**. For example, **VALUENAME MyFirstValue**.

Unless you specify otherwise, the value will be written in the following format when the user selects or clears the option:

- Selected: REG_DWORD with a value of 1.
- Cleared: remove the value completely.

Other options are available and are listed in the following sections. If the option is to be selected within the lower pane of the Group Policy snap-in, then the **VALUENAME** needs to be within a **PART** scope, as described in **PART**.

CLIENTEXT

The CLIENTEXT keyword is used to specify which client-side extension (a .dll on the user's computer, for example) to the Group Policy snap-in is needed to process particular settings on the client computer. By default, the Registry extension processes all settings configured under the Administartive Templates node. The CLIENTEXT keyword changes the default behavior and causes the specified extension to process these settings after the Registry extension has placed them in the registry.

CLIENTEXT must be used within either the POLICY scope or the PART scope and should follow the VALUENAME statement.

For example:

```
POLICY !!DQ_Enforce
EXPLAIN !!DQ_Enforce_Help
VALUENAME "Enforce"
CLIENTEXT {3610eda5-77ef-11d2-8dc5-00c04fa31a66}
PART !!DQ_EnforceTip1 TEXT
END PART
END POLICY
```

The GUID that follows the CLIENTEXT keyword is the GUID of the client-side extension. The client-side extensions are listed in the registry under HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \WindowsNT \CurrentVersion \Winlogon \GPExtensions.

VALUEOFF/VALUEON

You use **VALUEOFF/VALUEON** to write specific values based on the state of the option. You enable this functionality by writing the .adm file as shown in the following examples:

```
KEYNAME ....
POLICY !!MyPolicy
VALUENAME ValueToBeChanged
VALUEON "Turned On" VALUEOFF "Turned Off"
END POLICY
```

or:

```
KEYNAME ....
POLICY !!MyPolicy
VALUENAME ValueToBeChanged
VALUEON 5 VALUEOFF 10
END POLICY
```

Using simple policies and policies with the VALUEOFF/VALUEON statements

This section presents two examples that illustrate the difference between using the default policy states and specifying VALUEON/VALUOFF statements.

Example 1

In this example, no explicit VALUEON / VALUEOFF statements are used. This means that the Administrative Templates will use the default behavior when the user changes the state of this policy.

```
POLICY !!EnableSlowLinkDetect
EXPLAIN !!EnableSlowLinkDetect_Help
KEYNAME "Software\Policies\Microsoft\Windows\System"
VALUENAME "SlowLinkDetectEnabled"
END POLICY
```

The following table lists the default behavior.

State	Behavior

Policy setting enabled	A DWORD with the value 1 is written to the registry.
Policy setting disabled	The registry value is deleted.
Policy setting not configured	No change is made to the registry.

The important thing to note is the Policy **disabled** state. *The value is not written to the registry with the value of 0*; instead it is explicitly deleted. This means a component reading the policy will not find it in the registry, and will fall back to using the default in the code. Essentially, having the policy in the disabled state is the same as having it in the dimmed state.

Example 2
In this example, the state values are explicitly defined, so the Administrative Templates will use these values when the user changes the policy.

```
POLICY !!EnableSlowLinkDetect
EXPLAIN !!EnableSlowLinkDetect_Help
KEYNAME "Software\Policies\Microsoft\Windows\System"
VALUENAME "SlowLinkDetectEnabled"
VALUEON NUMERIC 1
VALUEOFF NUMERIC 0
END POLICY
```

The following table lists the behavior in this example.

State	Behavior
Policy setting enabled	A DWORD with the value 1 is written to the registry.
Policy setting disabled	A DWORD with the value 0 is written to the registry.
Policy setting not configured	No change is made to the registry.

EXPLAIN

You use the EXPLAIN keyword to provide Help text.

Each policy needs one EXPLAIN keyword with at least one space after it, followed by either the explain string in quotation marks or a reference to the explain string.

Example:

```
POLICY !!NetCache KEYNAME Software\Policies\Microsoft\Windows\NetCache #if VERSION >= 3
HELP !!IntelliMirrorExplain #endif ..... [Strings] IntelliMirrorHelp="Explanation for
Windows 2000 IntelliMirror\n\n You can use this policy to configure the file system
caching options."
```

\n\n creates a new line in the displayed text.

In the example, an explanation is offered for one of the **Offline Files** options. The following string means that this can be used with Windows 2000 (version 3) or later versions of Windows:

```
#if VERSION >= 3
```

PART

You can use **PART** to specify various options, including drop-down list boxes, text boxes, and text in the lower pane of the Group Policy snap-in.

The **PART** syntax is:

```
PART [!!]name PartType
type-dependent data
[KEYNAME KeyName ]
VALUENAME ValueName
END PART
```

where:

name is the part name as it should appear in the Group Policy list box. Names with spaces must be enclosed by double quotation marks. As a text string that is visible in the user interface, it should use the **[STRINGS]** variable **!!**.

PartType is the policy part flags. Flags are discussed individually in the **PartTypes** section.

type-dependent data is information about the part. Type-dependent data is discussed in the following section.

KeyName is the optional key name to use. If no key name is specified, the previous key name in the hierarchy is used.

ValueName is the value name to use to set the data for this part.

An example of **PART** use follows:

```
PART !!MyVariable FLAG(s) {one or more, defined later}
...
END PART
```

or:

```
PART !!MyVariable FLAG(s) END PART
```

The valid keywords for PART are:

- CHECKBOX
- TEXT
- EDITTEXT
- NUMERIC
- COMBOBOX
- DROPDOWNLIST
- LISTBOX
- END
- CLIENTEXT
- PART

PartTypes

The basic ADM language allows the creation of a simple .adm file that either creates a **VALUENAME** of **REG_DWORD** type with a value of **1** or removes the value completely. Using the following modifiers can provide additional options.

TEXT

Displays a line of static (label) text. No associated registry value exists for this part type. The **TEXT** part type accepts no type-specific data. This is useful for displaying a description.

The only valid keyword for TEXT is END.

EDITTEXT

Displays an edit field that accepts alphanumeric text. The text is set in the registry with the **REG_SZ** type. The **EDITTEXT** part type accepts the following options:

- **DEFAULT value.** Specifies the initial string to place in the edit field. If this option is not specified, the field is initially empty.
- **MAXLEN value.** Specifies the maximum length of a string. The string in the edit field is limited to this length.
- **REQUIRED.** Specifies that Group Policy will not allow a policy containing this part to be enabled, unless a value has been entered for this part.
- **OEMCONVERT.** Sets the **ES_OEMCONVERT** style in the edit field so that typed text is mapped from ANSI to OEM and back. ES_OEMCONVERT converts text entered in the edit control. The text is converted from the Windows character set (ASCII) to the OEM character set and then back to the Windows set. This ensures proper character conversion when the application calls the `CharToOem <JavaScript:hhobj_1.Click()>` function to convert an ASCII string in the edit control to OEM characters. This style is most useful for edit controls that contain file names.

The valid keywords for EDITTEXT are:

- KEYNAME
- VALUENAME
- DEFAULT
- REQUIRED
- MAXLENGTH
- OEMCONVERT
- END
- EXPANDABLETEXT
- CLIENTEXT

COMBOBOX

Displays a combo box. The **COMBOBOX** part type accepts the same options as **EDITTEXT**, as well as the following option:

SUGGESTIONS. Begins a list of suggestions to be placed in the drop-down list. **SUGGESTIONS** are separated with spaces and must be enclosed by double quotation marks when a value includes spaces. The list ends with **END SUGGESTIONS**.

For example:

```
SUGGESTIONS
Alaska Alabama Mississippi "New York"
END SUGGESTIONS
```

CHECKBOX

Displays a check box. The value is set in the registry with the **REG_DWORD** type. The value will be nonzero if the check box is selected by the user and zero if it is cleared. The **CHECKBOX** part type accepts the following options:

- **ACTIONLISTOFF.** Specifies an optional action list to be used if the check box is cleared.
- **ACTIONLISTON.** Specifies an optional action list to be used if the check box is selected.
- **DEFCHECKED.** Causes the check box to be initially selected.
- **VALUEOFF.** Overrides the default "off" behavior of the check box if specified.
- **VALUEON.** Overrides the default "on" behavior of the check box if specified.

The default behavior of a check box is to write the value **1** to the registry if it is selected and **0** if it is cleared. **VALUEON** and **VALUEOFF** are used to override this behavior. For example, the following option writes "Fred" to the registry when the check box is selected.

```
VALUEON "Fred"
```

The following option writes the value **12** to the registry when the check box is cleared.

```
VALUEOFF NUMERIC 12
```

The valid keywords for CHECKBOX are:

- KEYNAME
- VALUENAME
- VALUEON
- VALUEOFF
- ACTIONLISTON
- ACTIONLISTOFF
- DEFCHECKED
- CLIENTEXT
- END

DROPDOWNLIST

Displays a combo box with a drop-down list style. The user can choose from only one of the entries supplied. The main advantage of a combo box with a drop-down list is that a number of extra registry edits can be specified, based on the user's selection. The

DROPDOWNLIST part type accepts the **ITEMLIST** and **REQUIRED** options.

- **ITEMLIST.** Begins a list of the items in the drop-down list. The list must end with **END ITEMLIST**.

  Each item in the **ITEMLIST** option must be specified as follows:

  ```
  NAME name VALUE value
  [ACTIONLIST actionlist]
  ...
  ```

  where:

  name is the text to be displayed in the drop-down list for this item.

  value is the value to be written as the part's value if this item is selected. Values are assumed to be strings unless they are preceded by NUMERIC. The following example shows both string and numeric values.

  ```
  VALUE "Some value"
  VALUE NUMERIC 1
  ```

  If **VALUE** is followed by **DELETE** (for example, **VALUE DELETE**), the registry value name and value pair will be deleted.

  actionlist is the optional action list to be used if this value is selected.

- **REQUIRED** specifies that Group Policy will not allow a policy containing this part to be enabled unless a value has been entered for the part.

The valid keywords for DROPDOWNLIST are:

- KEYNAME
- VALUENAME
- REQUIRED
- ITEMLIST
- END
- NOSORT
- CLIENTEXT

LISTBOX

Displays a list box with **Add** and **Remove** buttons. This is the only part type that can be used to manage multiple values under one key. The **VALUENAME** option cannot be used with the **LISTBOX** part type because there is no single value name associated with this type. By default, only one column appears in the list box, and for each entry a value is created whose *name* and *value* are the same. For instance, a "Fred" entry in the list box would create a value named **fred** whose data was "fred".

The **LISTBOX** part type accepts the following options:

- **ADDITIVE.** By default, the content of list boxes overrides any values set in the target registry. This means that a control value is inserted in the policy file, which causes existing values to be deleted before the values set in the policy file are merged. If this option is specified, existing values are not deleted and the values set in the list box will be in addition to whatever values exist in the target registry.
- **EXPLICITVALUE.** This option makes the user specify the value data and the value name. The list box shows two columns, one for the name and one for the data. Note that this option cannot be used with the **VALUEPREFIX** option.
- **VALUEPREFIX prefix.** The prefix you specify is used in determining value names. If a prefix is specified, the prefix and an incremented integer are used instead of the default value-naming scheme described previously. For example, a prefix of "SomeName" will generate the value names **SomeName1**, **SomeName2**, and so on. The prefix can be empty (""), which will cause the value names to be **1**, **2**, and so on.

The valid keywords for LISTBOX are:

- KEYNAME
- VALUEPREFIX
- ADDITIVE
- NOSORT
- EXPLICITVALUE
- EXPANDABLETEXT
- END
- CLIENTEXT

NUMERIC

Displays an edit field with an optional spinner control (an up-down control) that accepts a numeric value. The value is set in the registry with the **REG_DWORD** type.

The **NUMERIC** part type accepts the following options:

- **DEFAULT value.** Specifies the initial numeric value for the edit field. If this option is not specified, the field is initially empty.
- **MAX value.** Specifies the maximum value for the number. The default value is 9999.
- **MIN value.** Specifies the minimum value for the number. The default value is 0.
- **REQUIRED.** Specifies that Group Policy will not allow a policy containing this part to be enabled unless a value has been entered for this part.
- **SPIN value.** Specifies increments to use for the spinner control.
- **SPIN 0** removes the spinner control. SPIN 1 is the default.
- **TXTCONVERT** writes values as **REG_SZ** strings ("1," "2," or "128") rather than as binary values.

For example:

```
PART !!MyVariable NUMERIC
VALUENAME ValueToBeChanged
END PART
```

The valid keywords for NUMERIC are:

- KEYNAME

- VALUENAME
- MIN
- MAX
- SPIN
- DEFAULT
- REQUIRED
- TXTCONVERT
- END
- CLIENTEXT

TEXT

Displays text only.

For example:

```
PART !!MyVariable TEXT
END PART
```

NUMERIC

Writes a value to registry with data type **REG_DWORD**. This is the default unless another type is specified.

For example:

```
PART !!MyVariable NUMERIC
VALUENAME ValueToBeChanged
END PART
```

EXPANDABLETEXT

Writes a value to registry with data type **REG_EXPAND_SZ**.

For example:

```
PART !!MyVariable EDITTEXT EXPANDABLETEXT
VALUENAME ValueToBeChanged
END PART
```

EDITTEXT

Writes a value to the registry with data type **REG_SZ**.

For example:

```
PART !!MyVariable EDITTEXT
VALUENAME ValueToBeChanged
END PART
```

REQUIRED

Generates an error if the user does not enter a value when required.

For example:

```
PART !!MyVariable EDITTEXT REQUIRED
VALUENAME ValueToBeChanged
END PART
```

MAXLEN

Specifies maximum length of text.

For example:

```
PART !!MyVariable EDITTEXT
VALUENAME ValueToBeChanged
MAXLEN 4
END PART
```

DEFAULT

Specifies a default value. This can be used for text or numeric data.

For example:

```
PART !!MyVariable EDITTEXT
DEFAULT !!MySampleText
VALUENAME ValueToBeChanged
END PART
```

or:

```
PART !!MyVariable NUMERIC
DEFAULT 5
VALUENAME ValueToBeChanged
END PART
```

MIN/MAX

Specifies lowest and highest valid values.

For example:

```
PART !!MyVariable NUMERIC
MIN 100 MAX 999 DEFAULT 55
VALUENAME ValueToBeChanged
END PART
```

DROPDOWNLIST

Displays a list box of options from which to choose.

For example:

```
PART !!MyVariable DROPDOWNLIST
VALUENAME ValueToBeChanged
ITEMLIST
NAME "First" VALUE NUMERIC 1
NAME "Second" VALUE NUMERIC 2
NAME "Third" VALUE NUMERIC 3
NAME "Fourth" VALUE NUMERIC 4
END ITEMLIST
END PART
```

ACTIONLIST

Optional action list to be used if this value is selected.

ACTIONLIST can be used only as part of an ITEMLIST. See the example in the ITEMLIST section.

Two variants of ACTIONLIST exist (ACTIONLISTON and ACTIONLISTOFF), and they may be used with the POLICY tag and the CHECKBOX tag. See the example in the CHECKBOX section.

Resources

For more information about Windows 2000, see the Microsoft Windows (http://www.microsoft.com/) Web site.

Troubleshooting

An important part of troubleshooting Group Policy problems is to consider dependencies between components. For example, Software Installation relies on Group Policy, and Group Policy relies on Active Directory. Active Directory relies on proper configuration of network services. When trying to fix problems that appear in one component, it is generally helpful to check whether components, services, and resources on which it relies are working correctly. Event logs are useful for tracking down problems caused by this type of hierarchical dependency.

Are you having trouble using the Group Policy snap-in?

I cannot open a Group Policy object in the console even though I have Read access to it.

Cause: An administrator must have not just Read but Full Control of the Group Policy object to open it in the Group Policy console.

Solution: Be a member of a security group with Full Control on the Group Policy object. For example, a domain administrator can manage Active Directory–based Group Policy. An administrator on a computer can edit the local Group Policy object on that computer.

When I try to edit a Group Policy object, I get the "Failed to open the Group Policy object" error.

Cause: This usually is due to a networking problem, specifically a problem with the domain name system (DNS) configuration.

Solution: Make sure DNS is working properly. For more information, see Domain name system (DNS).

Are Group Policy settings not taking effect?

Group Policy is not being applied to users and computers in a security group that contains those users and computers, even though a Group Policy object is linked to an organizational unit containing that security group.

Cause: This is correct behavior. Group Policy affects only users and computers contained in sites, domains, and organizational units. Group Policy objects are not applied to security groups.

Solution: Link Group Policy objects to sites, domains, and organizational units only. Keep in mind that the location of a security group in Active Directory is unrelated to whether Group Policy applies to the users and computers in that security group.

Group Policy is not affecting users and computers in a site, domain, or organizational unit.

Cause: Group Policy settings can be prevented, intentionally or inadvertently, from taking effect on users and computers in several ways. A Group Policy object can be disabled from affecting users, computers, or both. It also needs to be linked either directly to an organizational unit containing the users and computers, or linked to a parent domain or organizational unit so that the Group Policy settings apply through inheritance.

When multiple Group Policy objects apply, they are processed in this order: local, site, domain, organizational unit. By default, settings applied later have precedence. In addition, Group Policy can be blocked at the level of any organizational unit, or enforced through a setting of **No Override** applied to a particular Group Policy object link.

Finally, the user or computer must belong to one or more security groups with appropriate permissions set.

Solution: Make sure that the intended policy is not being blocked.

Make sure no overriding policy set at a higher level of Active Directory has been set to **No Override**.

If **Block** and **No Override** are both used, keep in mind that **No Override** takes precedence.

Verify that the user or computer is not a member of any security group for which the Apply Group Policy ACE is set to **Deny**.

Verify that the user or computer is a member of at least one security group for which the Apply Group Policy ACE is set to **Allow**.

Verify that the user or computer is a member of at least one security group for which the Read ACE is set to **Allow**.

Group Policy is not affecting users and computers in an Active Directory container.

Cause: Group Policy objects cannot be linked to Active Directory containers other than sites, domains, and organizational units.

Solution: Link a Group Policy object to an organizational unit that is a parent to the Active Directory container. Then, by default, those settings are applied to the users and computers in the container through inheritance.

Group Policy is not taking effect on the local computer.

Cause: Local policies are the weakest. Any Active Directory–based policy can overwrite them.

Solution: Check to see what Group Policy objects are being applied through Active Directory, and if those Group Policy objects have settings that are in conflict with the local settings.

Are you having trouble with the Software Installation snap-in?

Published applications do not appear in Add/Remove Programs in Control Panel.

Cause: Several causes are possible:

- Group Policy was not applied.
- Active Directory cannot be accessed.

- User does not have any published applications in the Group Policy objects that apply to them.
- Client is running Terminal Server.

Solution: Investigate each possibility in turn. Note that Software Installation is not supported for Terminal Server clients.

Document activation of a published application does not cause the application to install.

Cause: The administrator did not set autoinstall.

Solution: See To set autoinstall for an application.

The user receives an error message such as "The feature you are trying to install cannot be found in the source directory."

Cause: This could be caused by network or permissions problems.

Solution: Make sure the network is working correctly. Also see To set permissions for installing software, particularly the second note at the bottom of the page.

After removal of an application, the shortcuts for the application still appear on the user's desktop.

Cause: The user has created shortcuts, and Windows Installer has no knowledge of them.

Solution: The user needs to remove the shortcuts manually.

A user receives an error message such as "Another installation is already in progress".

Cause: An uninstallation might be taking place in the background with no user interface presented to the user, or perhaps the user has inadvertently triggered two installations simultaneously (which is not supported).

Solution: The user can try again later.

The user opens an already installed application, and the Windows Installer starts.

Cause: An application might be undergoing automatic repair, or a user-required feature is being added.

Solution: No action is required.

A user receives error messages such as: "Active Directory will not allow the package to be deployed" or "Cannot prepare package for deployment".

Cause: The package might be corrupted, or there might be a networking problem.

Solution: Investigate and take appropriate action.

Note

- For current information on troubleshooting, visit the Microsoft Personal Support Site on the World Wide Web. (http://support.microsoft.com)

Remote Installation Services

Remote Installation Services is an optional component of the Windows 2000 Server operating system that you can use to set up new client computers without the need to physically visit each client computer.

- Before you begin using Remote Installation Services, see Checklist: Installing Remote Installation Services.
- For tips about using Remote Installation Services, see Best practices.
- For help with specific tasks, see How to.
- For general background information, see Concepts.
- For problem-solving instructions, see Troubleshooting.

Checklist: Installing Remote Installation Services

	Step	Reference
☐	Review key concepts.	Concepts
☐	Make sure that both your server and client hardware meet the remote installation hardware requirements.	Remote Installation Services system requirements
☐	Make sure a Domain Name System (DNS) server exists on the network.	To install a DNS server; To configure a standard primary DNS server for a new zone
☐	Make sure an authorized DHCP server exists on the network.	To install a DHCP server; Checklist: Installing a DHCP server
☐	Make sure Active Directory exists on the network.	Active Directory Overview; Checklist: Installing a domain controller
☐	Install and configure Remote Installation Services.	To install Remote Installation Services

Best practices

- **Using the appropriate number of Remote Installation Service servers on your network.**
  In a small local area network (LAN)—for example, one physical subnet without a router—a single Remote Installation Services server can serve all PXE remote boot–enabled client computers up to the network bandwidth, or server resource limitations. In routed environments, use the prestaged client option to direct clients to the physically closest Remote Installation Services server for client servicing. In branch office situations, where only slow links exist to the branch site, physically locate a Remote Installation Services server at the branch site to avoid saturation of the slow link to that site.
- **Restricting the number of installation options and operating system choices a users has access to within the Client Installation wizard.**
  By restricting the installation options, you increase the percentage of successful operating system installations without requiring assistance from technical support or administrative staff. By default, Remote Installation Services ships with only one installation option and operating system choice, both of which are not offered to users by default. For more information on client installation image options, see Installation options.
- **Using the Remote Installation Preparation wizard (RIPrep) image format to deploy a Windows 2000 Professional standard corporate desktop configuration across different types of client hardware throughout your organization.**
  Using the Remote Installation Preparation wizard, an administrator can replicate the installation image of an existing Windows 2000 Professional client computer, including any locally installed applications and operating system configuration changes, to an available remote installation server on the network. After it is replicated, the installation image can be remotely installed by any supported client computer, regardless of the hardware differences between the source computer used to create the image and the destination

computer installing that image. For more information, see Creating an installation image.

- **Using Remote Installation Services with computers that do not contain the PXE-based remote boot ROM.**
  Use the remote boot floppy generator (Rbfg.exe) to create a floppy disk for computers that do not contain the PXE-based remote boot ROM. You can then use the Remote Installation Services feature for these computers. For more information on the PXE-based remote boot ROM, see PXE architecture.
- **Using the Client Installation wizard and non-ASCII characters.**
  Limit the characters to only standard ASCII characters (OEM characters 32–127) for user name, password, or domain name information. The Client Installation wizard does not support extended ASCII character sets (such as those containing ü, é, and so on).

How to...

- Install Remote Installation Services
- Configure Remote Installation Services
- Manage server options
- Manage client installation images
- Manage client computers
- Manage security

To install Remote Installation Services

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Configure Your Server**.
2. In the **Configure Your Server** dialog box, click **Finish setup**.
3. In the **Configure Remote Installation Services** dialog box, click **Configure** to start the Remote Installation Setup wizard.
4. In the **Remote Installation Setup wizard** dialog box, click **Next**.
5. In the Remote Installation Services Setup wizard, you are prompted for the following information:

Remote Installation Services drive and directory

Enter the drive and directory where you want Remote Installation Services to be installed. The drive should be dedicated to the Remote Installation Services server and contain enough space to store as many client images as you plan to host with this server. The minimum should be a 4-gigabyte drive or partition.

Windows 2000 Professional Source Path

Enter the location of the Windows 2000 Professional files. This can be the Windows 2000 Professional compact disc or the network share that contains the installation files.

Friendly Description and Help Text

Enter the friendly description for the client computer installation. This description will be displayed to users or clients of this server. Help text is used to describe the operating system installation choice to users or clients of Remote Installation Services.

Notes

- To start the Remote Installation Services Setup wizard, click **Start**, point to **Run**, and type **RIsetup**.
- This procedure requires you to have Administrator privileges.
- A Windows 2000 server or servers with DNS and DHCP services must be available on your network before Remote Installation Services can be installed.
- The installation wizard might prompt you to restart the computer if Remote Installation Services was added after installing Windows 2000 server by way of the Add/Remove Windows Components feature of Control Panel.
- To install Remote Installation Services, either select the **Advanced** option from the Windows 2000 Configure Your Server window or from the Add/Remove Windows Components feature of Control Panel.
- Installation images that are stored in locations other than
  *Server_name**Share_name*\REMINST\Setup*Language*\Images
  and referenced through junction points are not acted on by the SIS groveler agent. These installation images must be installed on an NTFS-formatted drive.
- Remote Installation Services must be installed on an NTFS- formatted drive.
- Remote Installation Services currently does not support the Encrypting File System (EFS), or the distributed file system (Dfs).
- The remote install volume cannot be installed on the same drive that contains the Windows 2000 Server operating system.
- To make sure all of the services have started successfully, open the Windows Event Viewer and review the entries for System Log and Application Log.

Configure Remote Installation Services

- Configure Remote Installation Services
- Configure Remote Installation Services advanced settings
- Manage client installation images
- Manage troubleshooting tools

To configure Remote Installation Services

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the applicable remote installation server.

   Where?
   - Active Directory Users and Computers
   - *Applicable domain*
   - *Applicable organizational unit* (such as Computers or Domain Controllers)
   - *Applicable remote installation server*
3. Click **Properties**, and then in the **Properties** dialog box, click the **Remote Install** tab.
4. In the **Remote Install** dialog box, click one of the following options:
   - **Respond to client computers requesting service**
   - **Do not respond to unknown client computers**

For more information on these options, see Responding to client service requests.

Note

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.

To configure Remote Installation Services advanced settings

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the applicable remote installation server.

   Where?
   - Active Directory Users and Computers
   - *Applicable domain*
   - *Applicable organizational unit* (such as Computers or Domain Controllers)
   - *Applicable remote installation server*
3. Click **Properties**. In the **Properties** dialog box, click the **Remote Install** tab, and then click **Advanced Settings**.
4. In the **Advanced Settings** dialog box, click the **New Clients** tab.
5. Click the client computer naming format or click **Customize** to create a client computer naming format.
6. Click one of the following options to determine where the client computer account is created:
   - **Default directory service location**
   - **Same location as that of the user setting up the client computer**
   - **The following directory service location**
7. If you chose the last option, click **Browse** and specify where to create the computer accounts.

Important

- If the network has multiple remote installation servers, each server must be configured to respond to client computers in the same manner.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- If a user is setting up the client computer, he or she needs to have the appropriate permissions to create the computer account within the domain or organizational unit chosen.

To manage client installation images

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the applicable remote installation server.

   Where?
   - Active Directory Users and Computers
   - *Applicable domain*
   - *Applicable organizational unit* (such as Computers or Domain Controllers)
   - *Applicable remote installation server*
3. Click **Properties**.
4. In the **Properties** dialog box, click the **Remote Install** tab, and then click **Advanced Settings**.
5. In the **Remote Installation Services Properties** dialog box, click the **Images** tab.
6. In the **Images** dialog box, click the installation image or unattended setup answer file.
7. Click one of the following options:
   - **Add**
   - **Remove**
   - **Properties**
   - **Refresh**

Note

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.

To manage troubleshooting tools

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the applicable remote installation server.

   Where?
   - Active Directory Users and Computers
   - *Applicable domain*
   - *Applicable organizational unit* (such as Computers or Domain Controllers)
   - *Applicable remote installation server*
3. Click **Properties**, and then in the **Properties** dialog box, click the **Remote Install** tab.
4. Click **Advanced Settings**, and then click the **Tools** tab.
5. In the **Tools** dialog box, click **Tool**.
6. Click one of the following options:
   - **Remove**
   - **Properties**
   - **Refresh**

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.

- Remote Installation Services cannot add tools to this list.

Manage server options

- Create a remote installation preparation wizard image
- Create a remote boot disk
- Verify the Remote Installation Services configuration

To create a Remote Installation Preparation wizard image

1. Use Remote Installation Services to install the operating system on the client computer you want to use to create the installation image.
2. Install any additional applications and modify the local configuration settings of the source client computer.
3. Click **Start**, and then click **Run**.
4. Type the Universal Naming Convention (UNC) path of the RIPrep utility, and then click **OK**.
   Example:
   *Server_name**Share_name*\REMINST\Admin\I386\RIPrep.exe
5. Read the information in the Remote Installation Preparation wizard (RIPW) Welcome screen and then click **Next**.
6. Type the server name this image will be copied to, and then click **Next**. By default this is the current Remote Installation Services server that you are running the wizard from.
7. Type the folder name on the Remote Installation Services server to which this installation image will be copied, and then click **Next**.
8. Type the friendly description and the Help text, and then click **Next**. This is used in the Client Installation wizard during the request for network services by the remote install clients.
9. It is recommended that you stop all programs or services on the source computer before proceeding. Review the list of programs or services that are currently running on the source computer, close any running applications, and then click **Next**.
10. Review the settings summary, and then click **Next**.
11. Review the information from **Completing the Remote Installation Preparation wizard** and click **Next** to replicate the source computer installation image onto the Remote Installation Services server.

Notes

- This procedure requires you to have Administrator privileges.
- The source computer shuts down when the image replication process is complete.
- The abbreviated Setup program automatically runs when you restart the source computer; complete the setup process to use this client computer to create another installation image.
- You can create additional installation images by rerunning the RIPW utility.

To create a remote boot disk

1. Click **Start**, and then click **Run**.
2. Type the UNC path of the Rbfg.exe utility, and then click **OK**. Example:
   servername\REMINST\Admin\I386\RBFG.exe
3. Insert a formatted disk into the disk drive.
4. Click the **Destination drive** option, and then click **Create Disk**.
5. Click **Close** when the disk is ready, and then remove the disk from the disk drive.

Note

- You can use the boot disk only with computers that contain supported PCI-based network adapters. To view the list of supported network adapters, start the Rbfg.exe utility and then click **Adapter List**.

To verify the Remote Installation Services configuration

1. Open Active Directory Users and Computers.
2. In the console tree, click the folder that contains the computer whose configuration you want to verify, such as **Computers** or **Domain Controllers**.

   Where?
   - Active Directory Users and Computers
   - *Applicable domain*
   - *Applicable container*
3. In the details pane, right-click the applicable remote installation server and then click **Properties**.
4. Click the **Remote Install** tab, and then click **Verify Server**.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- This procedure requires you to have Administrator privileges.
- The **Verify Server** command is available only on the console of the server you want to verify.
- If you are verifying the server configuration because you need to restore a Remote Installation Services volume from backup, you must verify the server configuration before you restore the volume.

Manage client installation images

- Add a new client operating system installation image
- Associate unattended setup answer files

To add a new client operating system installation image

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the applicable remote installation server.

   Where?
   - Active Directory Users and Computers
   - *Applicable domain*

└ *Applicable organizational unit* (such as Computers or Domain Controllers)
└ *Applicable remote installation server*

3. Click **Properties**, and then, in the **Properties** dialog box, click the **Remote Install** tab.
4. Click **Advanced Settings**, and then click the **Images** tab.
5. Click **Add** to start the Add wizard.
6. Click **Add a new installation image**, and then click **Next** to start the Remote Installation Setup wizard.
7. Click **Next**, and then type the location of the Windows 2000 Professional installation files. The location can be either a compact disc or network share.
8. Enter the friendly description and Help text, and then click **Next**.
9. Review the installation summary, and then click **Finish**.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- This process requires Administrator privileges.
- The Remote Installation Services server volume must be formatted with the NTFS file system. The drive should be dedicated only to Remote Installation Services and contain enough free space to store as many client installation images as you plan to host with this server. The minimum should be a 4-gigabyte drive or partition.
- Remote Installation Services currently does not support the Encrypting File System (EFS), or the Distributed file system (Dfs).
- The Remote Installation Services server volume cannot be the system volume.
- Windows 2000 Professional is currently the only installation option supported by Remote Installation Services.

To associate unattended setup answer files

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the applicable remote installation server.

   Where?
   └ Active Directory Users and Computers
   └ *Applicable domain*
   └ *Applicable organizational unit* (such as Computers or Domain Controllers)
   └ *Applicable remote installation server*
3. Click **Properties**, and then in the **Properties** dialog box, click the **Remote Install** tab.
4. Click **Advanced Settings**, and then click the **Images** tab.
5. Click **Add** to start the Add wizard.
6. Click **Associate a new answer file to an existing image**, and then click **Next**.
7. Click one of the following options:
   - **Windows image sample files**
   - **Another remote installation server**
   - **An alternate location**
8. Select the installation image the answer file will be associated with, and then click **Next**.
9. Enter the friendly description and Help text, and then click **Next**.
10. Review the settings summary, and then click **Finish** to complete the wizard process.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- You need Administrator privileges to run the Add wizard.

Manage client computers

- Prestage client computers
- Remove existing client computers
- Find client computers
- Locate the GUID for client computers
- Invoke a network service boot

To prestage client computers

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the applicable organizational unit that will contain the new client computer.

   Where?
   └ Active Directory Users and Computers
   └ *Applicable domain*
   └ *Applicable organizational unit*
3. Click **New**, and then click **Computer**.
4. Type the client computer name, click **Next**, and then click **This is a managed computer**.
5. Type the client computer **GUID** into the text entry field, and then click **Next**.
6. Click one of the following options to determine which server will support this client computer:
   - **Any available remote installation server.** Selecting this option indicates this client computer can be serviced by any Remote Installation Services server.
   - **The following remote installation server.** Selecting this option designates a specific server.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click

Active Directory Users and Computers.

- Make sure you have the client computer unique identifier (GUID) before proceeding.
- You can predetermine how a specific client computer network account is identified by prestaging the client computer account object within Active Directory. This information is used to identify and route the client computers during the network service boot request.
- Make sure you set the appropriate access permissions for users of the prestaged client computer.
- When prestaging a client computer into a domain with multiple domain controllers, the replication delay of the client computer account (CAO) information can cause a client computer to be serviced by another Remote Installation server.

To remove existing client computers

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the applicable client computer account.

   Where?
   - Active Directory Users and Computers
   - *Applicable domain*
   - *Applicable organizational unit*(such as Computers or Domain Controllers)
   - *applicable client computer account*
3. Click **Delete**.

Note

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.

To find client computers

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the applicable remote installation server.

   Where?
   - Active Directory Users and Computers
   - *Applicable domain*
   - *Applicable organizational unit*(such as Computers or Domain Controllers)
   - *Applicable remote installation server*
3. Click **Properties**, and then in the **Properties** dialog box, click the **Remote Install** tab.
4. In the **Remote Install** dialog box, click **Show Clients**.
5. Enter the client computer Globally Unique Identifier (GUID), and then click **Find Now**.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- The Show Clients feature searches for all client computers that are prestaged for this Remote Installation Services server.
- When using the Show Clients feature in multiple Remote Installation Services server environments, the search result might contain client computers from multiple servers. For example, if you have multiple servers with computer names such as RISsvr1, RISsvr10, and RISsvr100, the search returns client computers from each of the servers that begin with the same computer name.
- You can limit the client computer search to a specific server by entering its name in the **RI server** field.

To locate the GUID for client computers

- The computer's globally unique identifier (GUID) appears in the following areas:
  - A label on the side of the computer case.
  - A label within the computer case.
  - The basic input/output system (BIOS) of the client computer.

Notes

- The computer's GUID is supplied by the manufacturer.
- The GUID must be in the form {*dddddddd-dddd-dddd-dddd-dddddddddddd*}, where *d* is a hexadecimal text digit.

  For example: 8 hexadecimal text digits, followed by 4, then 4, then 4, then 12, such as the following:

  `{921FB974-ED42-11BE-BACD-00AA0057B223}`
- Valid entries for the client GUID are restricted to the following:

  `0 1 2 3 4 5 6 7 8 9 a b c d e f – A B C D E F`
- The dashes are optional and spaces are ignored.
- The GUID can also be entered in the wire format. In this format, the initial 16 characters of the GUID are transposed. For example, if you entered the following GUID in wire format as follows:

  `0123456789ABCDEF0123456789ABCDEF`

  the display would be as follows:
  GUID in wire format:

  `01234567 89AB CDEF 0123456789ABCDEF`

  GUID in display format:

  `{67452301-AB89-EFCD-0123-456789ABCDEF}`

To invoke a network service boot

1. After the Client Installation wizard starts, press ENTER to continue the process.
2. Enter the user name, password, and domain name into the appropriate fields, using TAB to move between the fields.
3. The Client Installation wizard offers the following options:
   - **Automatic Setup.** Use this option if you want most installation options to be configured by the administrator. The user is not offered Client Installation wizard choices.
   - **Custom Setup.** Use this option to provide the ability to define a unique name for this computer and specify where the computer account will be created within Active Directory.

- **Restart a previous Setup attempt.** This option restarts an operating system installation attempt if it fails prior to completion.
- **Maintenance and Troubleshooting.** This option provides the ability to access tools from the Client Installation wizard.

Notes

- Make sure you have a valid user name, password, and domain name before initiating a network service boot request.
- To invoke a network service boot on client computers that are not remote boot–enabled, insert the boot disk into the disk drive and start the client computer.
- The client computer's BIOS must be configured to use the network adapter as its primary boot device.
- When running the Client Installation wizard, use only standard ASCII characters (OEM characters 32–127) for user name, password, or domain name information. The Client Installation wizard does not support extended ASCII character sets (such as those containing ü, é, and other extended characters).

Manage security

- Set permissions for prestaged computer accounts
- Set permissions for user-created computer accounts
- Allow computers created in the Computers container to join the domain
- Allow computers created in organizational units to join the domain
- Set Group Policy for client installation options

To set permissions for prestaged computer accounts

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the applicable client computer account.

   Where?
   - Active Directory Users and Computers
   - *Applicable domain*
   - *Applicable organizational unit*(such as Computers or Domain Controllers)
   - *Applicable client computer account*
3. Click **Properties**.
4. In the **Properties** dialog box, click the **Security** tab and then click **Add**.
5. Select the user or group from the list, click **Add**, and then click **OK**.
6. Click the user or group you have added.
7. In **Permissions**, click **Read**, **Write**, **Reset password**, and **Change password** permissions, and then click **OK**.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- To view this option you must enable the **Users, Groups and Computers as Containers** and **Advanced Features** from the **View** menu of the Active Directory Users and Computers console.
- If a group is allowed to have these permissions, remember to add users to that group.
- For client computer accounts that are prestaged in another Active Directory folder location, expand the Active Directory Users and Computer console and select the appropriate client computer account.

To set permissions for user-created computer accounts

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the applicable domain.

   Where?
   - Active Directory Users and Computers
   - *Applicable domain*
3. Click **Delegate control**.
4. In the Delegation of Control wizard, click **Next**.
5. In the **Delegation of Control** dialog box, type your domain information, and then click **Next**.
6. In the **Group or User Selection** dialog box, click **Add**.
7. In the **Select Users, Computers or Groups** dialog box, click the user account or security group (preferred) containing the users you are setting permissions for, click **Add**, click **OK**, and then click **Next**.
8. In the **Predefined delegations** dialog box, click **Join a computer to the domain**, and then click **Next**.
9. Review the delegation of control summary information, and then click **Finish**.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- If a group is allowed to have these permissions, you need to add users to that group.

To allow computers created in the Computers container to join the domain

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the applicable domain.

   Where?
   - Active Directory Users and Computers
   - *Applicable domain*
3. Click **Delegate control**.
4. In the Delegation of Control wizard, click **Next**.
5. In the **Delegation of Control** dialog box, type your domain information, and then click **Next**.
6. In the **Group or User Selection** dialog box, click **Add**.
7. In the **Select Users, Computers or Groups** dialog box, click the **User** account or the **Security Group** (preferred) containing the

users that will be joining client computers to the domain, click **Add**, click **OK**, and then click **Next**.

8. In the **Predefined delegations** dialog box, click **Join a computer to the domain**, and then click **Next**.
9. Review the delegation of control summary information, and then click **Finish**.

Note

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.

To allow computers created in organizational units to join the domain

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the applicable organizational unit.

   Where?
   - Active Directory Users and Computers
   - *Applicable domain*
   - *Applicable organizational unit*
3. Click **Properties**, and then click the **Group Policy** tab.
4. Click the Group Policy object in the **Group Policy** dialog box, and then click **Edit** to start Group Policy.
5. Click **Computer Configuration**, click **Windows Settings**, click **Security Settings**, click **Local policies**, and then click **User Rights Assignment**.
6. Double-click **Add workstations to domain**.
7. Select the User account or Security Group (preferred) containing the users who will be joining client computers to the domain, click **Add**, and then click **OK**.
8. Close Group Policy, and then, in the **Group Policy** dialog box, click **OK**.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- Security settings that have been set on a domain controller through Group Policy within the Active Directory Users and Computers console do not take affect for the user or group accounts defined for up to 8 hours.

To set Group Policy for client installation options

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the applicable organizational unit.

   Where?
   - Active Directory Users and Computers
   - *Applicable domain*
   - *Applicable organizational unit*(such as Computers or Domain Controllers)
3. Click **Properties**, and then click the **Group Policy** tab.
4. Click the Group Policy object in the **Group Policy** dialog box, and then click **Edit** to start Group Policy.
5. Click **User Configuration**, click **Windows Settings**, and then click **Remote Installation Services**.
6. Double-click the **Choice Options** object, and then click the following Client Installation wizard choices:
   - **Automatic Setup.** Use this option if you want most installation options to be configured by the administrator. The user is not offered Client Installation wizard choices.
   - **Custom Setup.** Use this option to provide the ability to define a unique name for this computer and specify where the computer account will be created within Active Directory.
   - **Restart a previous Setup attempt.** This option restarts an operating system installation attempt if it fails prior to completion.
   - **Tools.** This option provides the ability to access tools from the Client Installation wizard.
7. Click one of the following Group Policy options for each of the Client Installation wizard choices selected in the previous step:
   - **Allow.** Use this option if you want to offer the installation option to users that this policy applies to.
   - **Don't care.** Use this policy to accept the policy settings of the parent container. For example, if the administrator for the entire domain has set Group Policy that is specific to Remote Installation Service, and the administrator of this container has chosen the **Don't care** option, the policy that is set on the domain is applied to all users that are affected by that policy.
   - **Deny.** If this option is set for a specific installation option, the users that are affected by this policy cannot access that installation option within the Client Installation wizard.
8. Close Group Policy, and then, in the **Group Policy** dialog box, click **OK**.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- The **Don't care** installation choice is the default setting.
- Automatic Setup is the default display option for users of client computers during the Client Installation wizard process.
- Security settings that have been set on a domain controller through Group Policy within the Active Directory Users and Computers console do not take effect for the user or group accounts defined for up to 8 hours.

Concepts

This section provides general background information on Remote Installation Services:

- Remote Installation Services overview
- Understanding Remote Installation Services
- Using Remote Installation Services
- Resources

Remote Installation Services overview

Using Remote Installation Services, you can set up new client computers remotely without the need to physically visit each client

machine. Specifically, you can install operating systems on remote boot–enabled client computers by connecting the computer to the network, starting the client computer, and logging on with a valid user account.

Remote Installation Services and IntelliMirror are new change and configuration management features included in Windows 2000 Server. By combining Remote Installation Services with other IntelliMirror features—user documents and settings, Software Installation, and Group Policy—organizations benefit from improved disaster recovery with easier operating system and application management, resulting in a reduction of technical support service calls. For more information, see IntelliMirror.

Understanding Remote Installation Services

This section covers:

- Related components
- Remote Installation Services architecture

Related components

Using Remote Installation Services requires several components that ship as part of the Windows 2000 Server operating system. The following services can be installed either on individual servers or on the same server. They must be active and available:

- Domain Name System (DNS Service)
- Dynamic Host Configuration Protocol (DHCP)
- Active Directory

Remote Installation client computers connect to the Remote Installation server through the network and identify themselves by their unique machine identifier (GUID/UUID). This machine identifier, which is provided by the computer manufacturer, gives each computer a unique identity. To find a computer's machine identifier, see To locate the GUID for client computers.

When Remote Installation Services detects the client computer's request for service, it responds in one of the following two ways, according to how you have set up your network:

- The service recognizes the client computer from its machine identifier and responds with the available installation choices.
- The server answers all network services requests from client computers.

For more information on setting how Remote Installation Services responds to requests, see Responding to client service requests.

Remote Installation Services architecture

This section covers:

- Related technologies and services
- PXE architecture
- Remote Installation Services directory service planning
- Remote Installation Services system requirements
- Remote Installation Services boot disk
- Network service boot
- Creating an installation image

Related technologies and services

The Remote Installation Service environment consists of several technologies and services within a network containing an existing Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and Active Directory.

You use the Pre-Boot eXecution Environment (PXE) DHCP–based remote boot technology to install the operating system on the client computer from a remote source. The remote source—the Remote Installation Services server—contains the operating system image to be installed in either compact disc (CD) or Remote Installation Preparation wizard (RIPrep) image format. The CD-based option is similar to setting up a client directly from the Windows 2000 Professional CD, except that the source files reside on an available Remote Installation Services server. You use the RIPrep option if you want to install and configure a client computer to comply with specific corporate desktop standards that are unique to the organization. For more information, see Creating an installation image.

The client computer's request for a network service boot can be initiated by either the system BIOS or by a special remote boot disk provided for pre–Net PC/PC98 client computers. For more information, see Remote Installation Services boot disk. When a network service boot is requested, the client computer receives an IP address by way of DHCP. Remote Installation Services responds to the boot request and downloads the Client Installation wizard. After the user is prompted to log on, a menu offers the installation options customized specifically for the user, subject to Group Policy settings.

Remote Installation Services server

A Remote Installation Services server contains the following components:

- **Client Installation wizard.** Steps the user through the available installation choices for client computers. For more information on this component, see Client Installation wizard.
- **Remote Installation Preparation wizard.** Provides the combined ability to prepare an existing Windows 2000 Professional installation—including locally installed applications and specific configuration settings—and replicate that image to an available Remote Installation Services server on the network.
- **Remote boot disk.** Enables client computers that do not have a PXE remote boot–enabled network adaptor to request network services from the server. For more information, see Remote Installation Services boot disk.
- **Remote Installation Services administration.** Provides the ability to configure the Remote Installation Services server by using a set of property pages.

When Remote Installation Services is enabled, the following services are automatically added to the server:

Boot Information Negotiations Layer (BINL):

This service listens for client network service requests and provides overall management of the Remote Installation Services environment. The BINL service makes sure the client is passed the correct files and, in the case of a prestaged client, makes sure it is serviced by the correct Remote Installation Services server. If the client computer has not been prestaged, BINL creates the client computer account object within Active Directory.

Trivial File Transfer Protocol Daemon (TFTPD):

Remote Installation Services server uses this service to download the initial files needed to begin the remote installation process. The most common file downloaded to the client using TFTPD is Startrom.com, which is responsible for bootstrapping the Windows 2000 client computer. If the client is new, OSChooser is downloaded to begin the remote installation process.

Single Instance Store (SIS):

Single Instance Store is the method used to reduce the overall storage required on the Remote Installation Services volume. The SIS drivers contain a groveler agent that scans the Remote Installation Services volume for duplicate files. If it finds duplicate files, the SIS groveler copies the original file into the SIS store and leaves a link file in its place. The link file contains information about the original file, such as its current location (SIS store), size, and attributes. If a new Remote Installation Preparation image contains duplicate files, all duplicates are copied into the store to reduce the amount of disk space on the Remote Installation Service server.

Note

- Installation images that are stored in locations other than *server name**reminst**Setup**language**Images* and referenced through junction points are not acted on by the SIS groveler agent. These installation images must be installed on a drive that is formatted with the NTFS file system.

PXE architecture

Remote Installation Services uses the Dynamic Host Configuration Protocol (DHCP) following the Pre-Boot eXecution Environment (PXE) architecture for bootstrapping a client computer. When a new PXE remote boot–enabled client computer starts for the first time, the client requests an Internet protocol (IP) address and the IP address of an active Remote Installation Services server by way of the DHCP protocol. As part of the initial request, the client computer sends out its globally unique identifier (GUID), which is used to uniquely identify the client computer within Active Directory.

The client computer receives an IP address along with the IP address of the boot server that will service the client. The client is then passed the name of a boot image that the client requests when contacting the boot server for initial service. In the case of Windows 2000 Server, after the client request is made, the first Remote Installation Services server to respond checks the directory service to determine if the client has been prestaged. Remote Installation Services does this by checking within Active Directory for a computer account object (CAO) that has the unique GUID that was passed by the client in the initial Remote Installation Services request. If a computer account with that GUID does not exist, the server provides the client computer with the Client Installation wizard, which requests that the user log on to the network.

Remote Installation Services directory service planning

The Remote Installation Services environment relies on a well-designed and well-planned Active Directory architecture. Normally, determining the physical location of a server can be a challenge, especially when you have to configure several servers located in different offices, floors, or buildings. In a given domain, Active Directory provides organizational units or containers, which you can use to organize users and resources into logical administrative groups.

The Remote Installation Service server computer object is located in the domain controllers folder if this server is a domain controller. From this one location, an administrator can manage individual remote installation servers with regard to client computer servicing, server verification, locating client computers, and determining the operating system installation options.

Note

- The computer account object is located in the Computers container when the Remote Installation Services server is a member server of a domain.

Remote Installation Services system requirements

This section describes the system requirements for Remote Installation Services servers, client computers, and network adapters.

Server hardware requirements

- Personal computer with Pentium or Pentium II 200 MHz or faster processor (Pentium 166 minimum).
- 256 megabytes (MB) of RAM recommended minimum (128 MB minimum supported; 4 gigabytes (GB) maximum).
- 2-gigabyte (GB) disk drive for Remote Installation Services servers folder tree.
- 10 or 100 MB/sec network adapter (100 MB/sec recommended).
- CD-ROM drive.

Client computer hardware requirements

- Pentium 166 MHz or faster Net PC client computer.
- 32 MB of RAM minimum; 64 MB recommended.
- One 800-MB disk drive.
- PXE DHCP–based boot ROM version .99c or greater.

Supported client network cards

For a list of which network adapters are supported by Remote Installation Services, run the Rbfg.exe utility and review the list of supported network adapters. For more information, see To create a remote boot disk.

Notes

- Be aware that Remote Installation Services will require a significant amount of disk space. You should dedicate an entire hard drive partition to the Remote Installation Services folder tree.
- Remote Installation Services cannot be installed on the same drive as the system volume.
- The volume you choose to install Remote Installation Services onto must be formatted with the NTFS file system.
- Remote Installation Services does not support the Encrypting File System (EFS) or the distributed file system (Dfs).
- The Windows 2000 Hardware Compatibility List (HCL) is a compilation of systems and hardware that has been extensively tested with Windows 2000 for stability and compatibility. It is the guide used by Microsoft Product Support Services to determine whether a given system is supported for use with Windows 2000.
- Up-to-date versions of the HCL are available on the World Wide Web at the Microsoft Web site. (http://www.microsoft.com/)

Remote Installation Services boot disk

You use the Remote Installation Services boot disk with client computers that do not contain a remote boot–enabled ROM. The boot disk simulates the PXE boot process for machines lacking a formal remote boot ROM. For more information on the PXE boot process, see PXE architecture.

The boot disk is analogous to a boot ROM, which uses the floppy drive to install the operating system from the remote installation server. The remote boot disk–generating utility (Rbfg.exe) included with Windows 2000 Server is located in the following folder: *Server name**Share name*\REMINST\Admin\I386\Rbfg.exe

You insert the remote boot disk into the client computer during the startup process. The client computer must have a supported network adapter. To find out which network adapters Remote Installation Services supports, use the boot disk–generating utility. For

more information, see To create a remote boot disk.

You also use a remote boot disk to initiate a network service boot. For information on how to do this, see To invoke a network service boot.

Network service boot

A network service boot can be initiated by either the user of a PXE remote boot–enabled client computer or by a special remote boot disk provided for pre–Net PC/PC98 computers. To invoke the network service boot request, the user presses F12 when prompted during the client computer startup sequence. When a network service boot is requested, the client computer receives an IP address by way of DHCP server and downloads the Client Installation wizard. For more information, see PXE architecture.

The user is prompted for user name, password, and domain name during the initial phase of the Client Installation wizard process. Remote Installation Services uses Group Policy within Active Directory and determines which installation options are appropriate for the user. The user is then offered a list of operating system installation choices that is based on the user's credentials or security group membership.

Creating an installation image

You use the Remote Installation Preparation wizard to prepare an existing Windows 2000 Professional installation and to replicate that image to an available Remote Installation Services server on the network.

The image conversion process consists of the following steps:

1. You use Remote Installation Services to remotely install the base Windows 2000 Professional operating system.
2. You install client computer applications that do not adhere to the Windows Installer technology.
3. You configure the source computer to conform to any company desktop standards required. For example, you might want to define specific screen colors, set the background bitmap to a company-based logo, remove any games installed by the base operating system, and configure Internet Explorer proxy settings.
4. You close all applications and run the Remote Installation Preparation wizard. For more information, see To create a Remote Installation Preparation wizard image.
5. The wizard configures the source computer to a generic state, removing anything that is unique to the client installation, such as the computer's unique security ID (SID), computer name, and any registry settings unique to the client source computer.
6. The wizard prompts you for the installation information required by the image conversion process. This information includes the location where the client installation image should be replicated, the name of the directory it should be copied to on the server, and a friendly description and associated Help text describing the installation image to users running the Client Installation wizard.
7. After the replication is complete, the installation image is automatically added to the list of available operating system installation options and is available to client computers that use the remote boot technology.

One important feature of the Remote Installation Preparation wizard process is that a remote boot–enabled client computer does not need to contain hardware identical to that of the source computer used to create the installation image. The Remote Installation Preparation wizard uses the Plug and Play feature of Windows 2000 to detect any differences between the source and destination computer's hardware during the image installation process.

Notes

- This procedure requires you to have Administrator privileges.
- The length of the friendly description and Help text for each installation image limits the number of installation image choices for a client computer. The typical number of installation image choices for client computers is generally between 12 and 20.
- You can control the installation choices for client computers by setting the access control permissions for the installation image .sif files. For more information, see To set, view, change, or remove file and folder permissions.
- Windows 2000 Professional is the only supported operating system installation image that can be replicated. The Remote Installation Preparation wizard currently supports replication of a single disk and single boot partition of a Windows 2000 Professional installation to a single remote installation server. This requires the Windows 2000 Professional operating system and all of the applications that make up the standard installation image to reside on a single partition of the source client computer.
- The wizard allows source image replication only to available remote installation servers. Currently, source replication to alternate drives or media types is not supported.
- Replication of encrypted files is not supported.
- The destination computer's disk capacity must be equal to or larger than that of the source computer.
- Disk preparation of the destination computer is identical to that of the source computer, and any remaining disk capacity on the destination computer will be formatted. For example, if the source computer's disk capacity is 1 gigabyte (GB) and the disk capacity of the destination computer is 2 GB, the entire 2 GB will be formatted on the destination computer.
- Changes made in the source computer's registry before running the Remote Installation Preparation wizard are not maintained in the installation image.
- The RIprep installation image maintains the volume and partition characteristics of the source computer File Allocation Table (FAT). For example, if you create an installation image from a source computer with a 2-GB FAT volume and then install the image on a client computer with a 4-GB drive, the resulting installation will format the drive as a 4-GB volume with a FAT32 partition. The change in the destination computer file system type is caused by the limits of the FAT file system. For more file system information, see Windows file systems.
- By changing the information in the .sif file associated with an installation image, you can restrict the disk reformatting to be the same as what the source computer used to create the installation image. For example, open the Ristndrd.sif file located in the \\REMINST\Setup*Applicable language*\Images*Applicable image name*\I386\Templates\Ristndrd.sif folder and modify the **UseWholeDisk** parameter to equal **NO**. When a client computer installs this image, the disk will be formatted to match the capacity of the source computer and the balance of the destination computer's disk will be unformatted.
- When you use the Remote Installation Preparation wizard (RIPW) to create an installation image of a client computer that was originally installed using a retail version of Windows 2000 Professional, the Remote Installation Services (RIS) unattended setup answer file (SIF) will need to be modified to include the product identification number (PID). The PID is the unique identification number specific to each copy of Windows 2000.

  If the PID is not entered in the .sif file, the installation process will stop and prompt the user for the product identifier information during the installation of that RIPrep image. You can avoid prompting your users for the PID by adding the product identifier to the [UserData] section of the .sif file associated with this installation image. For example, type the following (including the dashes and quotation marks) into the [UserData] section of the .sif file:

  ProductID = "xxxxx-xxx-xxxxxxx-xxxxx"

  Each copy of the Windows 2000 Professional product contains a unique product identification number (PID). The PID is used to uniquely identify the operating system installation and track the number of copies installed throughout the organization. Depending

on the type of product (Retail, Select, or OEM), a different type of user experience might be encountered when installing a Remote Installation Preparation wizard (RIPW) installation image from a remote installation server.

- **Installation image created from the Retail CD.** Modify the RIPrep.sif file to avoid the client installation process from stopping and prompting the user for the product identifier when the operating system is installed on the source computer using the retail version of the Windows 2000 Professional CD. Enter a valid PID for Windows 2000 Professional in the [UserData] section of RIPrep.sif located at \\REMINST\Setup*applicable_language*\Images*applicable_image_name*\I386 \Templates\Riprep.sif. The PID for each client installation is randomly generated using the PID entered in the RIPrep.sif file.
- **Installation image created from the Select or OEM CD.** When the source computer operating system is installed from the Select or OEM version of the Windows 2000 Professional CD, the PID does not need to be modified in the .sif file.

- Modifications to replicated installation images are not supported.
- This source computer will shut down when the image replication process is complete.
- The abbreviated Setup program automatically runs when the source computer is restarted. You must complete the setup process to use this client computer to create another installation image.
- All copies of Microsoft software made or installed using Remote Installation Services must be properly licensed. All copies of other software made or installed using Remote Installation Services must be properly licensed, and it is the licensee's obligation to ensure that it is licensed to make any such copies.

Using Remote Installation Services

This section covers:

- Remote Installation Services server authorization
- Required permissions
- Running the setup wizard
- Remote Installation Services administration
- Client computers
- Advanced configuration settings
- The remote installation process

Remote Installation Services server authorization

This feature prevents unauthorized Remote Installation Service servers from being added to a network where Windows 2000 and Active Directory are in use.

Remote installation server authorization is performed by using the DHCP server management console. This console is used to authorize both the DHCP and RIS servers to provide services on the network. For more information, see To authorize a DHCP server in Active Directory.

When a remote installation server attempts to start on the network, Active Directory is queried and the server computer's name or IP address is compared to the list of authorized remote installation servers. If a match is found, the remote installation server is authorized and can start on the network. If a match is not found, the server is not authorized. In this case, Remote Installation Services will not answer.

Required permissions

To create new computer accounts in Active Directory, users need to have permissions and rights assigned to them, as described in To set permissions for user-created computer accounts.

To join new computer accounts to the domain, users need to have permissions and rights assigned to them, as described in To allow computers created in the Computers container to join the domain.

Note

- The administrator must determine which users will be creating new client computer accounts and modify the users' rights and privileges accordingly.

Running the setup wizard

Before running the Remote Installation Services setup wizard, make sure you have Administrator privileges and have completed all prerequisite steps outlined in Checklist: Installing Remote Installation Services.

When Remote Installation Services is selected as an optional component during the Windows 2000 Server installation process, the setup wizard guides you through the necessary steps of installation and configuration.

The setup wizard process provides the following options:

- **Respond to all clients requesting service.** Select this option if you want the server to respond to all clients requesting service and provide them with operating system installation options. If this option is not selected, this remote installation server will not respond to clients requesting service.
- **Do not respond to unknown clients computers.** This option determines whether this server responds to unknown client computers requesting a remote installation server. A client computer is known if the client computer has an existing computer account object (CAO) created within Active Directory. Select this option if you want services offered only to authorized client computers. Client computers are considered authorized when there is an existing computer account within Active Directory.
- You are prompted for the location of the Windows 2000 Professional installation files. This can be either the Windows 2000 Professional compact disc or a network location that contains the installation files.
- You are prompted for a directory name to which the Windows 2000 Professional installation files should be copied in the remote installation server. You should name the directory something that represents the operating system you are copying—for example, Win2000.pro.
- You are prompted for a friendly description and Help text describing this operating system installation image. The friendly description and Help text will be displayed to users within the client installation process on a remote boot–enabled client computer. Enter a description that describes the operating system installation choice—for example, if this operating system is for the sales staff, then a friendly description might be Windows 2000 Professional for Sales Staff. The Help text will be displayed when the user selects the friendly description within the Client Installation wizard.
- The setup wizard displays the summary information of the setup process. To change any of this information, click **Back**.

Note

- You can also install Remote Installation Services after the initial Windows 2000 Server installation by using the Add/Remove Programs utility. Open Add/Remove Programs. <SPAN CLASS="reuse" ID="para1"></SPAN>

Remote Installation Services administration

This section covers:

- Remote Installation Services administration overview
- Responding to client service requests

Remote Installation Services administration overview

You administer Remote Installation Services using property pages that reside on specific objects within Active Directory.

To access the property pages, right-click the server object you want to administrate, and then, from the context menu, click **Properties**. For more information on configuring Remote Installation Services, see To configure Remote Installation Services.

You can set the following options from the Remote Installation Services property page:

Client servicing

You can either specify that servers respond to all clients requesting service or that they respond only to known clients. For more information, see Responding to client service requests.

Verify Server

If you select this option, you can check the integrity of the Remote Installation Services–enabled server.

Select this option if you suspect that the server is failing or if you are currently seeing inconsistent behavior, or if you need to restore a Remote Installation Services volume from backup. This brings up a wizard that checks whether all of the settings, services, and configuration options are correctly set and functioning.

For more information, see To Verify the Remote Installation Services configuration.

Important

- If you are verifying the server configuration because you need to restore a Remote Installation Services volume from backup, you must verify the server configuration before you restore the volume.

Note

- Before you select this option, make sure you have the Windows 2000 Server and Windows 2000 Professional installation compact discs available. You might be prompted for them during the Verify Server procedure.

Show Clients

If you select this option, you can search for Remote Installation Services clients within Active Directory.

Selecting this option displays a list of client computers—sorted by their unique Globally Unique Identifier (GUID)—that this server has serviced. The list also includes client computers that have been prestaged to this server for operating system installation.

For more information, see Client computers.

Advanced Settings

If you select this option, you can control the way a client computer is installed. The advanced setting options include:

- **Automatic client computer account naming format**
- **Active Directory location of client computer accounts**
- **Manage the installation images and pre–operating system maintenance tools installed on this Remote Install server**

For more information, see Advanced configuration settings.

Responding to client service requests

You can determine how the Remote Installation Services server responds to requests for service from client computers.

- **Respond to clients requesting service.** If you select this option, Remote Installation Services is enabled and will respond to client computers requesting service.
- **Do not respond to unknown client computers.** If you select this option, Remote Installation Services will respond only to known client computers.

Client computers

This section covers:

- Finding client computers
- Client computer properties

Finding client computers

Each client computer is identified by its globally unique identifier (GUID). By using the Show Clients feature, you can search Active Directory for Remote Installation Services client computers using their GUID. The Show Clients feature searches for all client computers that are prestaged for this remote installation server. The search process can include the entire Active Directory structure or be limited to a specific domain. The Show Clients search process returns a list of the client computers and displays them by their computer name and GUID. For more information on GUIDs, see To locate the GUID for client computers.

The Show Clients search process uses a wildcard search attribute appended to the current remote installation server computer name. For example, if the remote installation server is named RISsvr1, the Show Clients feature will use RISsvr1* for the server name. When you use the Show Clients feature in multiple remote installation server environments, the search result might contain client computers from multiple servers. For example, if you have multiple remote installation servers with computer names such as RISsvr1, RISsvr10, and RISsvr100, the search will return, from each of the servers, client computers that begin with the same computer name.

You can also search Active Directory for Remote Installation Services client computer accounts by their computer name or their GUID. For more information, see To find client computers.

Note

- You can limit the client computer search to a specific remote installation server by entering the server name in the RI server field.

Client computer properties

Remote Installation Services uses property pages to contain information relating to Remote Installation Services client computers. To access this information, either click **Show Clients** on the Remote Installation Services server property page or right-click the client computer objects in the Active Directory Users and Computers console.

Computer's Unique ID: (GUID/UUID) The unique identifier is supplied by the client computer manufacturer.

Notes

- The GUID/UUID ID must be in the form {ddddddddd-dddd-dddd-dddd-dddddddddddd}, where *d* is a hexadecimal text digit.

  For example: 8 hexadecimal text digits, followed by 4, then 4, then 4, then 12, such as: {67452301-AB89-EFCD-0123-

456789ABCDEF}. For more information on using the GUID, see To locate the GUID for client computers.

- Valid entries for the client GUID are restricted to the following:

```
0 1 2 3 4 5 6 7 8 9
a b c d e f - A B C D E F
```

- The dashes are optional and spaces are ignored.
- The GUID can also be entered in the wire format. The initial 16 characters of the GUID are transposed when a GUID is entered in this format. For example, if you entered the following GUID in wire format as "0123456789ABCDEF0123456789ABCDEF", the display would be as follows:

  GUID in wire format: 01234567 89AB CDEF 0123456789ABCDEF

  GUID in display format: {67452301-AB89-EFCD-0123-456789ABCDEF}

Advanced configuration settings

This section covers:

- Advanced settings overview
- Advanced settings for new clients
- Advanced settings for installation images
- Advanced settings for tools
- Computer names

Advanced settings overview

Remote Installation Services advanced configuration settings determine how the service creates client computer names, manages operating system images, and manages diagnostic tool applications.

To access these settings, see To configure advanced settings.

Advanced settings for new clients

You use the advanced settings of Remote Installation Services to define a policy that provides each remote installation client computer with a name that is unique on the network. For information on how to do this, see Computer names.

You can also determine the default directory service container to store the client computer machine account objects. Using this feature, you can group client computers within a specific Active Directory domain or organizational unit.

Use the **Computer account location** option if you want to be able to define—prior to actual installation—the default Active Directory container for all remote installation client computer accounts. You can choose one of the following three options:

Default directory service location

Specifies that the client computer account object is created in the Computers container by default during the domain join operation. The client computer becomes a member of the same domain as the remote installation–enabled server installing the client.

Same location as that of the user setting up the client computer

Specifies that the client computer account object is created within the same Active Directory container as the user setting up the computer. For example, if a user logs on whose user account currently resides within the Users container, the client computer account is also created within the Users container.

The following directory location

You can predetermine where client computer account objects are created in Active Directory. This option affects all client computers installed from this server.

Note

- A user setting up the client computer needs to have the appropriate rights to create computer accounts within Active Directory. For more information, see To set permissions for user-created computer accounts.

Advanced settings for installation images

Using Remote Installation Services, you can manage the operating system installation options for Remote Installation Services users. During the base install of Remote Installation Services, you are prompted to add a default operating system installation image to the remote installation–enabled server. This operating system image installation process copies the Windows 2000 Professional compact disc contents and directory structure to the remote installation–enabled server.

The unattended installation process uses text files—called setup information (.sif) files—to store the configuration settings for the installation image. The information contained in the .sif file is processed each time a client computer chooses the installation image using the Client Installation wizard. By modifying the .sif file for the installation image, you can predetermine the configuration settings for each client installation image. For example, if all of your client computers have the same type of display devices, you can set the screen resolution prior to installation by modifying the [Display] information of the .sif file.

Another example of using a .sif file is changing the way the client computer disk drive is formatted. While the Client Installation wizard is running, the installation image that the user selects is copied to the client computer. The disk preparation of the destination computer is identical to that of the source computer, and any remaining disk capacity on the destination computer is formatted. For example, if the source computer disk capacity is 1 gigabyte (GB) and the disk capacity of the destination computer is 2 GB, the entire 2 GB are formatted on the destination computer.

By changing the information in the .sif file associated with an installation image, you can restrict the disk reformatting to be the same as the source computer used to create the installation image. For example, suppose you open the Ristndrd.sif file and modify the UseWholeDisk parameter to **NO**. When a client computer installs this image, the disk is formatted to match the capacity of the source computer. The rest of the destination computer's disk remains unformatted.

Advanced settings for tools

You use the tools options for Remote Installation Services if you want independent software vendors (ISVs) or original equipment manufacturers (OEMs) to be able to provide system maintenance and troubleshooting tools to administrators, technical support staff, and users of client computers during the request for network boot services. Because the client computer's hard disk might be empty prior to installing the operating system, these tools can be extremely helpful. The maintenance and troubleshooting tools also give administrators an easy way to update client computer systems—such as the system flash BIOS—before or after the operating system installation.

The Remote Installation Services tools feature has the following options:

Remove

Removes the template setup information file (.sif) associated with the currently selected tool. This file contains the friendly description text, which gives the tool's purpose to users of a remote installation client computer. If you choose this option, the template file is

deleted and the tool is not offered to Remote Installation Services clients when they run the Client Installation wizard.

Properties

This option provides access to the selected tool property information. You can change the friendly description text and retrieve specific details about the selected tool.

Refresh

This option refreshes the contents of the display window.

Note

- You cannot add a tool from the **Remote Installation Properties** dialog box. ISVs and OEMs provide an external setup program that adds their own tool to the \RemoteInstall directory tree. After the tool is added, it is displayed within the **Tools properties** tab and is available to administrators and users when running the Client Installation wizard.

Computer names

You use the advanced settings of Remote Installation Services to define the naming policy that provides each client computer with a unique name. This name, which is used to identify the client computer on the network, is similar to the NetBIOS name used in previous versions of Windows and Windows NT.

Use the **Automatic computer naming** option to make sure each client computer is provided a unique name during the remote installation request. The default format is the user name with an appended incremental number.

You can also create a custom naming policy; to do this, click **Customize**. You can then select one of the following options to automatically create the computer name:

%First

The user's first name is used as the computer name.

%Username

The user name is used as the computer name.

%#

The name includes an incremental number.

%Last

The user's last name is used as the computer name.

%MAC

The network card media access control address is used as the computer name.

To limit the length of the computer name, add a numerical value to the text string. For example, if the user's last name is Smith and you want to limit the name to three characters (Smi), use the following string:
%3Last

You can combine options. For example, if you want the computer name to consist of the first three letters of the user's first name followed by the first three letters of his or her last name, use the following string:
%3First%3Last%

The remote installation process

This section covers:

- Client Installation wizard
- Installation options
- Supported operating systems
- Controlling client installations through Group Policy

Client Installation wizard

Users of a remote boot–enabled client computer can use the Client Installation wizard to select installation options, operating systems, and maintenance and troubleshooting tools.

The wizard prompts the user for his or her user name, password, and domain name. After the user's credentials have been validated, the wizard displays the installation options that are available for the user. After the user selects an option, the selected operating system installation image is copied to the client computer's local hard disk. You can predetermine these installation options during the Remote Installation Services setup process, or by running the RIPrep utility. For more information, see Creating an installation image.

Important

- Because the client computer's hard disk is reformatted during the operating system installation, all locally stored files are removed during installation.

Note

- When you use the Client Installation wizard, use only standard ASCII characters (OEM characters 32–127) for user name, password, or domain name information. The Client Installation wizard does not support extended ASCII character sets (such as those containing ü, é, and other extended characters).

Installation options

The Client Installation wizard is a text-based setup wizard that guides the user through the remote installation process. You can control which installation options are offered to users by using Group Policy. For more information on doing this, see Controlling client installations through Group Policy.

You can use either automatic setup or custom setup.

Automatic setup

Automatic setup is available by default to users setting up a remote boot–enabled client computer. If you decide to set up multiple operating system choices for the user, the user can choose which installation image is appropriate for his or her needs or role within the company. Windows 2000 Remote Installation Services uses the unattended installation templates so administrators can determine the type of operating system image that the user installs. For more information, see Advanced configuration settings.

By using an unattended installation setup information (.sif) file, you can create several installation options based on one operating system installation image on the Remote Installation Services server. You can also customize which items are installed, as well how specific client computer options are configured during operating system installation. For example, you can create a specific operating system type that installs the TCP/IP protocol, sets the display resolution to 800 x 600, and sets the default company name. You can also provide a friendly description for this operating system type, such as Windows 2000 Professional for Sales Staff. The text for the

friendly description can be modified after the initial installation of the client computer operating system. When users log on and choose the automatic setup option, they see a listing of operating system installation types that they can choose from.

Because the installation process reformats the client computer's hard disk drive, the Client Installation wizard warns the user that any previously stored data will be deleted.

You can predefine the computer name and a location within Active Directory for the client computer accounts. For more information, see Advanced configuration settings.

Custom setup

Using this option, you can specify the computer name and Active Directory container for the computer account object during the operating system installation process. You use custom setup when you want to set up a computer for someone else within their organization. Remote Installation Services can be configured to automatically create computer names based on the user logging into the client computer prior to the installation of the operating system.

Restart a Previous Setup Attempt

Restarts a failed operating system installation attempt if the installation procedure fails prior to completion.

Maintenance and Troubleshooting

Provides access to maintenance and troubleshooting tools required to maintain and troubleshoot client computers. Examples include memory virus scanners, system flash BIOS updates, and computer diagnostic utilities.

Notes

- Windows 2000 Remote Installation Services does not fully support unattended installations on computers that contain ISA devices or those that are not Plug and Play aware.
- Users that are setting up a remote boot–enabled client computer are not offered installation choices when automatic setup is their only installation option. For more information, see Controlling client installations through Group Policy.
- The unattended installation setup answer files (.sif) are text files that describe the installation process for an installation image. You associate the .sif file with one of the available installation images. For more information on creating unattended installation setup answer files, see the Windows 2000 Resource Kit.
- By default, the Client Installation wizard uses the Welcome.osc file located in \RemoteInstall\OSChooser to manage client installation image choices. For multiple language installation image options, you need to remove the Welcome.osc file and rename the MultiIng.osc file to Welcome.osc. The Client Installation wizard then offers a menu of multiple language choices to the user. You can also edit Welcome.osc to create custom language options.

Supported operating systems

The Client Installation wizard supports two types of operating system images: compact disc (CD)–based install and the Remote Installation Preparation wizard (RIPrep) image formats. The CD-based option is similar to setting up a client directly from the Windows 2000 Professional installation CD, except that the operating system image source files reside on an available remote installation server. Using the RIPrep option, you can install the necessary client computer applications and configure the client computer settings, such as monitor settings and network printers. For more information, see To create a Remote Installation Preparation wizard image.

Both the CD-based and RIPrep image formats are displayed in the list of available installation options. The installation process is initiated when the user of the client computer selects one of the operating system image options.

Note

- Windows 2000 Professional is currently the only installation option supported by Remote Installation Services.

Controlling client installations through Group Policy

You can determine which choices the Client Installation wizard displays to a given user or group by using the Group Policy snap-in. Group Policy is applied to sites, domains, and organizational units and can be inherited within Active Directory. For more information on Group Policy, see Group Policy overview.

The Group Policy options are as follows:

Allow

Users that this policy applies to are offered this installation option.

Don't care

The policy settings of the parent container apply to this option. For example, if you choose **Don't care** and the administrator for the entire domain has set Group Policy specific to Remote Installation Services, the policy that is set on the domain is applied to all users who are affected by that policy.

Deny

Users affected by this policy cannot access this installation option. For procedural information on controlling access through Group Policy, see To set Group Policy for client installation options.

For information on the options offered by the Client Installation wizard, see Installation options.

Resources

- Updated technical information
- Windows 2000 Resource Kit

Troubleshooting Remote Installation Services

What problem are you having?

I am not sure whether I have the correct PXE ROM version.

Solution: When the Net PC or client computer containing a remote boot ROM starts, the version of the PXE ROM appears on the screen. Remote Installation Services supports .99c or greater PXE ROMs, except in a few situations that require the .99L version. You may be required to obtain a newer version of the PXE-based ROM code from your original equipment manufacturer (OEM) if you have problems with the existing ROM version installed on a client computer.

I am not sure whether the client computer has received an IP address and has contacted the Remote Installation Services server.

Solution: When the client computer boots, you will see the PXE boot ROM begin to load and initialize. The following sequence occurs with most PC98 and Net PCs, PXE ROM-based computers, and the computers using the Remote Installation Services boot disk.

Remote Boot ROM Load Sequence:

Step 1:

The client computer displays the message "DHCP", which indicates that the client is requesting an IP address from the DHCP server. This can also mean that the client has obtained an IP address from DHCP and is awaiting a response from the remote installation server. To verify that the client is receiving an IP address, check the IP leases that have been granted on your DHCP server.

Troubleshooting

If the client does not receive the message, an IP address might not have been received or the BINL server might not be responding. Consider the following:

- Is the DHCP server available and has the service started? DHCP and remote installation servers must be authorized in Active Directory for their services to start. Make sure the service has started and that other clients that are not remote boot–enabled are receiving IP addresses on this segment.
- Does the DHCP server have a defined IP address scope, and has it been activated?
- Is there a router between the client and the DHCP server that is not allowing DHCP packets through?
- Are there any error messages in the event log under the system log for DHCP?
- Can other client computers—that is, those that are not remote boot–enabled clients—receive an IP address on this network segment?

Step 2:

When the client receives an IP address from the DHCP server, the message may change to "BINL". This indicates that the client successfully leased an IP address and is now waiting to contact the remote installation server. The client will eventually time out and post the error message "No Bootfile received from DHCP, BINL, or Bootp."

Troubleshooting

If the client does not receive the BINL message, this indicates the client is not receiving a response from the remote installation server. Consider the following:

- Is the remote installation server available and has the Remote Installation Services service started? Remote Installation Services servers must be authorized to start on the network. Use the Dhcpmgmt.msc snap-in to authorize both DHCP and Remote Installation Services servers within Active Directory.
- Are other remote boot–enabled clients receiving the Client Installation wizard? If so, this client computer either is not supported or is having remote boot ROM–related problems. Check the version of the PXE ROM on the client computer. Also, check Active Directory to see whether the administrator has prestaged this client computer to a remote installation server that is offline or unavailable to the client computer.
- Is a router between the client and the remote installation server not allowing the DHCP-based requests or responses through? The Remote Installation Services server communicates by way of the DHCP packet type during the initial service request/response sequence. You may need to configure the router to forward the DHCP packets.
- Are there any error messages in the event log under the system or application logs specific to Remote Installation Services (BINLSVC), Domain Name System (DNS), or Active Directory?

Step 3:

The client then changes to TFTP or prompts the user to press F12. This indicates that the client has contacted the Remote Installation Services server and is waiting to receive the first image file–CIW. You might not see the BINL and TFTP message on some machines because this sequence can occur very rapidly.

Troubleshooting

If the client machine does not get a response from the remote installation server, the client will time out and send an error message saying that it did not receive a file from either DHCP, BINL, or TFTP. In this case, the Remote Installation Services server did not answer the client computer. Do the following:

- Stop and restart the BINLSVC service by clicking **Start**, and pointing to **Run**.
- In the **Run** dialog box, type **cmd** in the text field, and click **OK**.
- In the console window, type the following:
  Net Stop BINLSVC
  Net Start BINLSVC
- Check the remote installation server properties to make sure the **Respond to client computers requesting service** option is selected and that **Do not respond to unknown client computers** is cleared unless you have prestaged the client computer in Active Directory prior to starting the client computer.
- Check the event log to make sure no errors relating to DHCP, DNS, RIS (BINLSVC), or Active Directory exist. If the client machine does not receive an answer after attempting to stop and restart the service, and after checking the remote installation server object properties to ensure the correct settings have been set, you should check the event log on the Remote Installation Services server for any errors relating to DHCP, DNS, and RIS (BINLSVC).

Step 4:

At this point, the client should have downloaded and displayed the Client Installation wizard application with a Welcome screen greeting the user.

Does Remote Installation Services support the older remote boot protocol, Remote Program Load (RPL)–based ROMs?

Solution: The Remote Installation Service feature uses the PXE DHCP–based remote boot ROMs. As such, there is no support in Windows 2000 for the older RPL-based remote boot.

Does Remote Installation Services support remote installation of Windows 2000 Server CD–based or RIPrep operating system installation images?

Solution: No. Remote Installation Services does not support remotely installing the Windows 2000 Server operating system.

Is the Pre-Boot portion of the PXE-based remote boot ROM secure?

Solution: No. The entire boot ROM sequence and operating system installation or replication process is not secure with regard to packet type encryption, client/server spoofing, or wire sniffer–based mechanisms. As such, use caution when using Remote Installation Services on your corporate network. Make sure you allow only authorized Remote Installation Services servers on your network and that you control the number of administrators allowed to install and or configure remote installation servers.

Does Remote Installation Services preserve the file attributes and security settings defined on the source computer when using the RIPrep image feature?

Solution: Yes. The file attributes and security settings that are defined on the source computer are preserved on the destination computer that installs that image. However, the RIPrep feature does not support the encrypted file system if enabled and used on the source client computer.

Does the RIPrep feature of Remote Installation Services support different hardware between the source computer used to create the RIPrep-based operating system installation image and the destination computer that will install the image?

Solution: Yes. The hardware between the source computer and the destination computer can be different. The one exception to this is the hardware abstraction layer (HAL) driver used. For example, if the source computer is an Advanced Configuration Power Interface (ACPI)–based computer, it uses a specific ACPI HAL driver. If you attempt to install this RIPrep image on a computer that is not based or enabled on ACPI, the operating system installation process will fail.

Does the RIPrep wizard support multiple disks or multiple partitions on a given client computer?

Solution: No. The RIPrep utility supports only a single disk with a single partition (C:*drive*) in this release of Remote Installation Services.

How does the RIPrep wizard deal with disks that differ in size between the source computer used to create the image and the destination computer that will receive it?

Solution: Disk preparation of the destination computer is identical to that of the source computer, and any remaining disk capacity on the destination computer will be formatted. For example, if the source computer disk capacity is 1 gigabyte (GB) and the disk capacity of the destination computer is 2 GB, the entire 2 GB will be formatted on the destination computer. Remote Installation Services can support formatting the destination computer's hard disk to match the same physical size of the source computer. For more information on managing the client computer disk reformatting process, see Creating an installation image.

How do I replicate all of the operating system installation images currently located on one Remote Installation server to other Remote Installation servers on the network for consistency across all client installations?

Solution: Currently the Remote Installation Services feature does not provide a mechanism for replication of operating system images from one remote installation server to another, but there are several mechanisms you can use to solve this problem. Use the strong replication features of the Systems Management Server product. This product provides for scheduled replication, compression, and slow-link features. You can also use other vendor solutions for operating system image replication. Make sure the replication mechanism you choose supports maintaining the file attributes and security settings of the source images.

Can I have a Remote Installation Services server and another vendor remote boot server on the network at the same time? If so, what are the implications?

Solution: Yes, you can have multiple-vendor remote boot/installation (RB/RI) servers on one physical network. It is important to understand that currently the remote boot PXE ROM code does not know the difference between vendors' RB/RI servers. As such, when a remote boot–enabled client computer starts and requests the IP address of an RB/RI server, all of the available servers will respond to that client; thus, the client has no way to ensure it is serviced by a specific RB/RI server.

Remote Installation Services gives an administrator the ability to prestage client computers into Active Directory and determine which remote installation server will service a client computer. By configuring the remote installation server to answer only known client computers (prestaged), the administrator is assured that the client will be serviced by the correct remote installation server.

Not all of the other RB/RI vendors have implemented the ability to ignore service requests. You might need to isolate the specific vendors' servers on the network so that clients are not answered by these vendors' RB/RI servers.

Can I remotely manage the Remote Installation Services servers from Windows 2000 Professional computers on my network?

Solution: Yes. If you are an administrator in the domain, and you have installed the Administrator Tools MSI package, you can administer the majority of the Remote Installation Services configuration settings. There are some items that you cannot manage—for example, you cannot remotely add more operating system installation images to the remote installation servers from Windows 2000 Professional computers.

Can I add more network adapters to the Remote Installation Services boot disk?

Solution: No. The Rbfg.exe utility cannot be modified with regard to the number of supported network adapters for this release of Remote Installation Services. Microsoft will be adding network card adapters over time, and will make the updated Rbfg.exe utility available through normal distribution channels such as the World Wide Web, Windows updates, and future service or feature pack updates.

Can I use the Active Directory object attributes to create a naming format for use with the Remote Installation Services automatic computer naming feature?

Solution: No. Currently the existing attributes supported with the automatic computer naming feature use Active Directory. However, not all of the Active Directory object attributes are currently supported.

Where do I look on the client computer to find the GUID/UUID for prestaging client computers in Active Directory for use with Remote Installation Services?

Solution: The GUID/UUID for most client computers that are PC98 or Net PC–compliant can be found in the system BIOS of the computer. Computer manufacturers are encouraged to ship either a floppy disk containing a comma-separated file or spreadsheet that contains a mapping of serial numbers to GUID/UUIDs. This will allow you to script prestaging client computers within Active Directory.

The GUID/UUID can also be located on the outside of the computer case for easy identification and prestaging of computer accounts. If the GUID is not found in the locations described in the previous paragraph, you can use a network utility to sniff the network traffic of the client computer and locate the DHCPDiscover packet; within that field will be the 128-bit, 16-byte GUID/UUID.

Command settings are not being processed during the unattended installation.

Cause: When using the "OemPreinstall = yes" setting in a .sif file, the correct directory information is required.

Solution: Change the directory information to \\RemoteInstall\Setup*applicable_language*\Images*applicable_name*\oem.

Language choice options are not displayed during the Client Installation wizard session.

Cause: By default, Remote Installation Services uses the Welcome.osc file to manage the client installation image choices. For multiple language installation image options, you need to replace the default Welcome.osc file with the Multilng.osc file.

Solution: The Client Installation wizard uses the Welcome.osc file located in the \\RemoteInstall\OSChooser folder to manage client installation image choices. When you remove the Welcome.osc file and rename the Multilng.osc file to Welcome.osc, the Client Installation wizard will also offer a menu of multiple language choices to the user. You can edit the Welcome.osc file to create custom language options.

The client computer is prestaged to a remote installation server but is being serviced by a different server.

Cause: When you prestage a client computer into a domain with multiple domain controllers, the replication delay of the client computer account (CAO) information can cause a client computer to be serviced by another Remote Installation server.

Solution: You can wait for the computer account information to be propagated during the next scheduled replication session, or modify the replication frequency between your domain controllers. For more information on configuring replication, see Replication goals and strategies.

Following the restoration of a backup of a Remote Installation Services volume, Remote Installation Services no longer functions properly.

Cause: Backup restored the volume without a Single Instance Store (SIS) directory.

Solution: Verify the configuration of the Remote Installation Services volume and then restore the volume again.

For information about how to verify the configuration of a Remote Installation Services volume, see To verify the Remote Installation Services configuration.

User profiles

User profiles automatically create and maintain the desktop settings for each user's work environment on the local computer.

- To find features that have been moved in Windows 2000 Server, see New ways to do familiar tasks.
- For tips about using user profiles, see Best practices.
- For help with specific tasks, see How to.
- For general background information, see Concepts.

New ways to do familiar tasks

The following table compares familiar Windows NT 4.0 user profile tasks with the equivalent tasks in Windows 2000.

If you want to	In Windows NT 4.0 use	In Windows 2000 use
Add a path to a user profile	**User Manager** in **Administrative Tools**.	Active Directory Users and Computers and click **Users**.
View the contents of a user profile	The profile is stored in Profiles in Winnt, *User*.	Windows Explorer. The profile is stored in Documents and Settings, *User*.
Copy a user profile	**System** utility in Control Panel.	System Properties and click **User Profiles**.
Add a home directory to a path	**User Manager** in **Administrative Tools**.	Active Directory Users and Computers and click **Users**.
Add a logon script to a user profile	**User Manager** in **Administrative Tools**.	Group Policy accessed through Active Directory Users and Computers. For more information, see To assign user logon scripts.

Best practices

- **Allowing for different hardware configurations**

  Because user profiles can be used on various types of client computers, you should keep in mind that these client computers can have different hardware configurations, particularly different video cards and display monitors.

  Because a user profile determines screen placement and size of windows, a workstation's type of display hardware affects how well the user profile works. For example, the window setup in a user profile created for a computer with a Super VGA monitor might not look correct when loaded on a computer with a regular VGA monitor.

- **Creating and editing user profiles**

  When you create or edit a user profile for a single user, use a computer with the same type of video hardware as the computer the user typically uses.

- **Creating mandatory profiles for multiple users**

  When you create a mandatory user profile for several users, create a single user profile for the whole group of users only if they all use computers with the same type of video hardware.

How to...

- Create a roaming user profile
- Copy the user profile to the server
- Delete a user profile
- Create a preconfigured roaming user profile
- Create a mandatory user profile
- Add a home directory to a profile

To create a roaming user profile

1. Open Active Directory Users and Computers.
2. In the details pane, right-click the applicable user account.

   Where?
   - Active Directory Users and Computers
   - *applicable domain*
   - *applicable container* (such as Users)
   - *applicable user account*
3. Click **Properties**.
4. In the **Properties** dialog box, click the **Profile** tab.
5. In **Profile path**, type the path information.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- Use a full path in each user account:

  *****server******share******%username%
- The user profile path location can be on any server; it does not have to be a domain controller. When the user logs on, Windows checks the user's account to see if a user profile path exits. If it does, the user profile is located by the system and copied to the local computer.
- The user account can be created in any organizational unit or container within the domain. The default location for the user account is the Users folder.
- Windows 2000 does not support the use of encrypted files with roaming user profiles.

- Roaming user profiles used with Terminal Services clients are not replicated to the server until the interactive user logs off and the interactive session is closed.

To copy the user profile to the server

1. Open the System Properties dialog box, and then click the **User Profiles** tab.
2. In the **User Profiles** dialog box, click the user profile you want to copy.
3. Click **Copy To**, and then either type the name of the destination folder or browse the network for it.

Notes

- To open a Control Panel item, click **Start**, point to **Settings**, click **Control Panel**, and then double-click the appropriate icon.
- This location must match the **User Profile Path** entry for the user's account in Active Directory.
- You cannot use Windows Explorer or any other file management utility to copy user profiles.
- Use this procedure to issue a profile to a specific user, or prepare a network default user profile for all new users in the domain.
- When you copy the user profile, in the **Copy To** dialog box, share the profile with Everyone. This user profile is then downloaded to the Default User (Network) folder on every computer at startup.

To delete a user profile

1. Open the System Properties dialog box.
2. In the **System Properties** dialog box, click the **User Profiles** tab.
3. Click the user profile you want to delete, and then click **Delete**.

Notes

- To open a Control Panel item, click **Start**, point to **Settings**, click **Control Panel**, and then double-click the appropriate icon.
- To delete a roaming user profile, the administrator needs to take ownership of the folder and then delete it.

To create a preconfigured roaming user profile

1. Open the System Properties dialog box.
2. Under **System Properties**, click **User Profiles**.
3. In the **Profiles stored on this computer** list, click the profile you want to copy.
4. Click **Copy To**, and then either type the name of the destination folder or browse the network for it.
5. To change the user or group allowed to use a user profile, click **Change**.

Notes

- To open a Control Panel item, click **Start**, point to **Settings**, click **Control Panel**, and then double-click the appropriate icon.
- You must be logged on to Windows 2000 as an administrator to copy a user profile.
- Do not use this procedure to create a local user profile that points to the Documents and Settings folder.
- The first time the user logs on, instead of getting a copy of the default profile, the user gets a copy of the preconfigured user profile from the server. Thereafter, the user profile functions just as a standard roaming user profile does. Each time the user logs off, the user profile is saved locally and is also copied to the server.
- Windows 2000 does not support the use of encrypted files with roaming user profiles.
- Roaming user profiles used with Terminal Services clients are not replicated to the server until both the interactive user logs off and the interactive session is closed.

To create a mandatory user profile

1. Open Active Directory Users and Computers.
2. In the details pane, right-click the applicable user account.

   Where?
   - Active Directory Users and Computers
   - *applicable domain*
   - *applicable container* (such as Users)
   - *applicable user account*
3. Click **Properties**.
4. In the **Properties** dialog box, click the **Profile** tab.
5. In **Profile path**, type the path information ending with the .man file name extension.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- Use a full path in each user account:

  *****server******share*\%username%.man

  For *share*, create a Profiles folder if it does not already exist, and share the folder with authenticated users allowing read only permissions. The share must be created before the user profile is enabled.
- When creating a mandatory profile, make sure you set the appropriate access permissions for the user or groups of users that will use this profile.
- You can also create a mandatory user profile by using Windows Explorer to rename the ntuser.dat file to ntuser.man.
- A mandatory user profile is a preconfigured user profile. The user can still modify the desktop, but the changes are not saved when the user logs off. The next time the user logs on, the mandatory user profile is downloaded again. User profiles become mandatory when you rename the NTuser.dat file on the server to NTuser.man. This extension makes the user profile read-only.
- The administrator can assign the same mandatory user profile to as many users as needed.

To add a home directory to a profile

1. Open Active Directory Users and Computers.
2. In the details pane, right-click the applicable user account.

   Where?
   - Active Directory Users and Computers

└ *applicable domain*
└ *applicable container* (such as Users)
└ *applicable user account*

3. Click **Properties**.
4. In the **Properties** dialog box, click the **Profile** tab.
5. In **Home Directory**, type the directory information.

Notes

- To open Active Directory Users and Computers, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- Windows 2000 includes a desktop folder called My Documents, which offers a convenient alternative to home directories but does not replace them. All users have a My Documents folder in their user profile.
- A user can change the target folder location of his or her My Documents folder by right-clicking the desktop icon, clicking **Properties**, and then specifying a new location on the **Target** tab.
- You can use Group Policy to change the target folder location of any user's My Documents folder, disable a user's ability to change the target folder location, remove the My Documents icon from the desktop, and choose whether programs use My Documents or a different folder as the default location for opening and saving files.
- If no home directory is assigned here, the system assigns the default local home directory to the user account (\Users\Default on the user's local drive where Windows 2000 is installed as an upgrade, or the root directory where Windows 2000 is installed as the initial version). The home directory can use the same location as the My Documents folder.
- When using Windows 2000 Terminal Services, the user profile is the default home directory.

Concepts

This section provides general background information about user profiles.

- User profiles overview
- Understanding user profiles
- Using user profiles
- Resources

User profiles overview

On computers running Windows 2000, user profiles automatically create and maintain the desktop settings for each user's work environment on the local computer. A user profile is created for each user when he or she logs on to a computer for the first time.

User profiles provide several advantages to users:

- More than one user can use the same computer, and each receives desktop settings when he or she logs on.
- When users log on to their workstation, they receive the desktop settings as they existed when they logged off.
- Customization of the desktop environment made by one user does not affect another user's settings.
- User profiles can be stored on a server so that they can follow users to any computer running Windows NT 4.0 or Windows 2000 on the network. These are called *roaming user profiles*.

As an administrative tool, user profiles provide these options:

- You can create a default user profile that is appropriate for the user's tasks.
- You can set up a mandatory user profile that does not save changes made by the user to the desktop settings. Users can modify the desktop settings of the computer while they are logged on, but none of these changes are saved when they log off. The mandatory profile settings are downloaded to the local computer each time the user logs on. For more information on mandatory profiles, see To create a mandatory user profile.
- You can specify the default user settings that will be included in all of the individual user profiles.

User profile types

A user profile defines customized desktop environments, which include individual display settings, network and printer connections, and other specified settings. You or your system administrator can define your desktop environment.

Types of user profiles include:

- **Local user profile.** A local user profile is created the first time you log on to a computer and is stored on a computer's local hard disk. Any changes made to your local user profile are specific to the computer on which you made the changes.
- **Roaming user profile.** A roaming user profile is created by your system administrator and is stored on a server. This profile is available every time you log on to any computer on the network. Changes made to your roaming user profile are updated on the server.
- **Mandatory user profile.** A mandatory user profile is a roaming profile that can be used to specify particular settings for individuals or an entire group of users. Only system administrators can make changes to mandatory user profiles.

Understanding user profiles

This section covers:

- Contents of a user profile
- Settings saved in a user profile

Contents of a user profile

Every user profile begins as a copy of Default User, which is a default user profile stored on each computer running Windows 2000. The NTuser.dat file within Default User displays configuration settings from the Windows 2000 registry. Every user profile also uses the common program groups, contained in the All Users folder.

The user profile folders contain links to various desktop items.

User profile folder	Contents
Application data	Program-specific data—for example, a custom dictionary. Program vendors decide what data to store in the User profile folder.
Cookies	User information and preferences.

Desktop	Desktop items, including files, shortcuts, and folders.
Favorites	Shortcuts to favorite locations on the Internet.
Local Settings	Application data, History, and Temporary files. Application data roams with the user by way of roaming user profiles.
My Documents	User documents.
My Pictures	User picture items.
NetHood	Shortcuts to My Network Places items.
PrintHood	Shortcuts to printer folder items.
Recent	Shortcuts to the most recently used documents and accessed folders.
SendTo	Shortcuts to document-handling utilities.
Start Menu	Shortcuts to program items.
Templates	User template items.

NTuser.dat file

The NTuser.dat file is the registry portion of the user profile. For more information on the Windows 2000 registry, see the Windows 2000 Resource Kits.

All Users

Although they are not copied to user profile folders, the settings in the All Users folder are used to create the individual user profiles.

Windows 2000 supports two program group types:

- Common program groups are always available on a computer, no matter who is logged on.
- Personal program groups are private to the user who creates them.

Common program groups are stored in the All Users folder under the Documents and Settings folder. The All Users folder also contains settings for the Desktop and **Start** menu.

Notes

- The My Documents, My Pictures, Favorites, Start Menu, and Desktop folders are, by default, the only folders displayed in Windows Explorer. The NetHood, PrintHood, Local Settings, Recent, and Templates folders are hidden and do not appear in Windows Explorer. To view these folders and their contents in Windows Explorer, on the **Tools** menu, point to **Folder options**, click the **View** tab, and then click **Show hidden files and folders**.
- On computers running Windows 2000 with the NTFS file system, only members of the Administrators group can create, delete, or modify the common program groups.

Settings saved in a user profile

A user profile contains configuration preferences and options for each user: a snapshot of a user's desktop environment.

The following table is a sample of the settings contained in a user profile.

Source	**Parameters saved**
Windows Explorer	All user-definable settings for Windows Explorer.
My Documents	User-stored documents.
My Pictures	User-stored picture items.
Favorites	Shortcuts to favorite locations on the Internet.
Mapped network drive	Any user-created mapped network drives.
My Network Places	Links to other computers on the network.
Desktop contents	Items stored on the Desktop and Shortcut elements.
Screen colors and fonts	All user-definable computer screen colors and display text settings.
Application data and registry hive	Application data and user-defined configuration settings.
Printer settings	Network printer connections.
Control Panel	All user-defined settings made in Control Panel.
Accessories	All user-specific program settings affecting the user's Windows environment, including Calculator, Clock, Notepad, and Paint.
Windows 2000–based programs	Any program written specifically for Windows 2000 can be designed so that it tracks program settings on a per-user basis. If this information exists, it is saved in the user profile.
Online user education bookmarks	Any bookmarks placed in the Windows 2000 Help system.

Note

- The My Documents, My Pictures, Favorites, Start Menu, and Desktop folders are, by default, the only folders displayed in Windows Explorer. The NetHood, PrintHood, Recent, and Templates folders are hidden and do not appear in Windows Explorer. To view these folders and their contents in Windows Explorer, from the **Tools** menu, point to **Folder options**, click the **View** tab, and then click **Show hidden files and folders**.

Using user profiles

This section covers:

- Using roaming user profiles
- Preconfigured user profiles

- Local user profiles

Using roaming user profiles

With roaming user profiles, users can log on to any computer running Windows 2000 within their domain. After the roaming user profile has been authenticated within the directory service, the user profile stored on the server is copied to the local computer. All of the users' settings and documents that are stored on the server in the roaming user profile are copied to the local computer. For more information on implementing roaming user profiles, see To create a roaming user profile.

From Active Directory, you can assign a server location for user profiles. If you enter a user profile path into a user's domain account, a copy of the user's local user profile is saved both locally and in the user profile path location when the user logs off. The next time that user logs on, the user profile in the user profile path location is compared to the copy in the local user profile folder, and the most recent copy of the user profile is opened. The local user profile becomes a roaming user profile because of the centralized domain location. The users' settings and documents are available wherever the user logs on.

If the server is not available, the local cached copy of the roaming user profile is used. If the user has not logged on to the computer before, a new local user profile is created. In either case, if the centrally stored user profile is not available at logon, it is not updated when the user logs off. If the user profile is not downloaded because of server problems, it is not loaded when the user logs off.

Preconfigured user profiles

Although you can use any account to create a preconfigured user profile, it is often more convenient and efficient to use a reference computer. For example, if you plan to create and preconfigure three different roaming or mandatory user profiles for your sales, payroll, and production departments, create three different reference accounts called Sales Profile, Payroll Profile, and Prod Profile. Then, log on with each account to create the appropriate user profile for each user group. After you log back on as Administrator, use the Active Directory console to modify the user's individual accounts or the appropriate group account, and then copy the user profiles to the appropriate server. For information on how to copy user profiles, see To copy the user profile to the server.

Local user profiles

For new installations of Windows 2000, the local user profile is stored under the user name in the %userprofile%\Documents and Settings folder. For Windows 2000 upgrade installations, the local profile is stored under the user name in the %systemroot%\profiles folder. When no preconfigured server-based roaming user profile exists for a user, the first time a user logs on to a computer, a user profile folder is created for the user name. The contents of Default User are then copied to the new user profile folder. The user profile, along with the common program group settings in the All Users folder, creates the user's desktop. When the user logs off, any changes made to the default settings during the session are saved to the new user profile folder. The user profile in Default User remains unchanged.

If the user has a user account on the local computer in addition to a domain user account, or more than one domain user account, the local user profile is different for each account because different user profiles are generated for each user who logs on. When the user logs off, changed settings are saved to only one user profile, depending on which account the user logged on to.

Resources

- Updated technical information
- Windows 2000 Resource Kit
