

Windows 2000 Server

## Step-by-Step Guide to Understanding the Group Policy Feature Set

---

Operating System

### Abstract

Group Policy is the central component of the Change and Configuration Management features of the Microsoft® Windows® 2000 operating system. Group Policy specifies settings for groups of users and of computers, including registry-based policy settings, security settings, software installation, scripts (computer startup and shutdown, and log on and log off), and folder redirection.

This paper is a technical step-by-step guide of the capabilities of Group Policy. It is intended for IT managers, system administrators, and others who are interested in using Group Policy to manage users' desktop environments.

### Introduction

This document is part of a set of step-by-step guides that introduce IT managers and system administrators to the features of the Windows 2000® operating system. This document presents a brief overview of Group Policy, and shows how to use the Group Policy snap-in to specify policy settings for groups of users and of computers. It includes information on:

- Configuring the Group Policy snap-in.
- Creating and managing Group Policy objects.
- Setting options for registry-based policy, scripts, and loopback policy.
- Using security groups with Group Policy.
- Linking multiple Group Policy Objects.
- Blocking and enforcing Group Policy.

### Group Policy and the Active Directory

In Windows 2000, administrators use Group Policy to enhance and control users' desktops. To simplify the process, administrators can create a specific desktop configuration that is applied to groups of users and computers. The Windows 2000 Active Directory™ service enables Group Policy. The policy information is stored in Group Policy objects (GPOs), which are linked to selected Active Directory containers: sites, domains, and organizational units (OUs).

A GPO can be used to filter objects based on security group membership, which allows administrators to manage computers and users in either a centralized or a de-centralized manner. To do this, administrators can use filtering based on security groups to define the scope of Group Policy management, so that Group Policy can be applied centrally at the domain level, or in a decentralized manner at the OU level, and can then be filtered again by security groups. Administrators can use security groups in Group Policy to:

- Filter the scope of a GPO. This defines which groups of users and computers a GPO affects.
- Delegate control of a GPO. There are two aspects to managing and delegating Group Policy: managing the group policy links and managing who can create and edit GPOs.

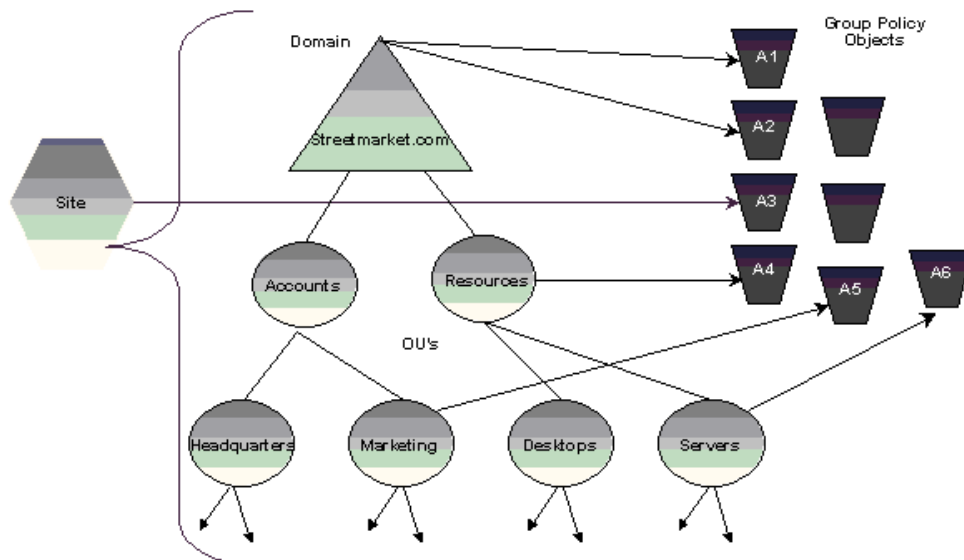
Administrators use the Group Policy Microsoft Management Console (MMC) snap-in to manage policy settings. Group Policy includes various features for managing these policy settings. In addition, third parties can extend Group Policy to host other policy settings. The data generated by Group Policy is stored in a Group Policy object (GPO), which is replicated in all domain controllers within a single domain.

The Group Policy snap-in includes several MMC snap-in extensions, which constitute the main nodes in the Group Policy snap-in. The extensions are as follows:

- **Administrative templates.** These include registry-based Group Policy, which you use to mandate registry settings that govern the behavior and appearance of the desktop, including the operating system components and applications.
- **Security settings.** You use the Security Settings extension to set security options for computers and users within the scope of a Group Policy object. You can define local computer, domain, and network security settings.
- **Software installation.** You can use the Software Installation snap-in to centrally manage software in your organization. You can assign and publish software to users and assign software to computers.
- **Scripts.** You can use scripts to automate computer startup and shutdown and user logon and logoff. You can use any language supported by Windows Scripting Host. These include the Microsoft Visual Basic® development system, Scripting Edition (VBScript); JavaScript; PERL; and MS-DOS®-style batch files (.bat and .cmd).
- **Remote Installation Services.** You use Remote Installation Services (RIS) to control the behavior of the Remote Operating System Installation feature as displayed to client computers.
- **Internet Explorer maintenance.** You use Internet Explorer Maintenance to manage and customize Microsoft® Internet Explorer on Windows 2000-based computers.
- **Folder redirection.** You use Folder Redirection to redirect Windows 2000 special folders from their default user profile location to an alternate location on the network. These special folders include My Documents, Application Data, Desktop, and the **Start** Menu.

Figure 1 below shows how Group Policy objects use the Active Directory hierarchy for deploying Group Policy.

## Group Policy and the Active Directory



**Server OU GPOs applied = A3, A1, A2, A4, A6**  
**Marketing OU GPOs applied = A3, A1, A2, A5**

If your browser does not support inline frames, [click here](#) to view on a separate page.

### Figure 1 The Hierarchy of Group Policy and the Active Directory

Group Policy objects are linked to site, domain, and OU containers in the Active Directory. The default order of precedence follows the hierarchical nature of the Active Directory: sites are first, then domains, and then each OU. A GPO can be associated with more than one Active Directory container or multiple containers can be linked to a single GPO.

### Prerequisites and Initial Configuration

#### Prerequisites

This Software Installation and Maintenance document is based on Step-by-Step to a Common Infrastructure for Windows 2000 Server Deployment [Parts One](#) and [Two](#).

Before using this guide, you need to build the common infrastructure as described in the document above. This infrastructure specifies a particular hardware and software configuration. If you are not using the common infrastructure, you must take this into account when using the guide.

#### Group Policy Scenarios

Note that this document does not describe all of the possible Group Policy scenarios. Please use this instruction set to begin to understand how Group Policy works and begin to think about how your organization might use Group Policy to reduce its TCO. Other Windows 2000 features, including Security Settings and Software Installation and Maintenance, are built on Group Policy. To learn how to use Group Policy in those specific scenarios, refer to the white papers and Windows 2000 Server online help on Windows 2000 Security and Software Installation and Maintenance, which are available on the Windows 2000 Web site.

#### Important Notes

The example company, organization, products, people, and events depicted in this guide are fictitious. No association with any real company, organization, product, person, or event is intended or should be inferred.

This common infrastructure is designed for use on a private network. The fictitious company name and DNS name used in the common infrastructure are not registered for use on the Internet. Please do not use this name on a public network or Internet.

The Active Directory™ service structure for this common infrastructure is designed to show how Windows 2000 Change and Configuration Management works and functions with Active Directory. It was not designed as a model for configuring an Active Directory service for any organization—for such information see the Active Directory documentation.

#### Group Policy Snap-in Configuration

Group Policy is tied to the Active Directory service. The Group Policy snap-in extends the Active Directory management tools using the Microsoft Management Console (MMC) snap-in extension mechanism.

The Active Directory snap-ins set the scope of management for Group Policy. The most common way to access Group Policy is by using the Active Directory User and Computers snap-in, for setting the scope of management to domain and organizational units (OUs). You can also use the Active Directory Sites and Services snap-in to set the scope of management to a site. These two tools can be accessed from the Administrative Tools program group; the Group Policy snap-in extension is enabled in both tools. Alternatively, you can create a custom MMC console, as described in the next section.

#### Configuring a Custom Console

The examples in this document use the custom MMC console that you can create by following the procedure in this section. You need to create this custom console before attempting the remaining procedures in this document.

**Note** If you want more experience building MMC consoles, run through the procedures outlined in "Step-by-Step Guide to Microsoft Management Console"

##### To configure a custom console

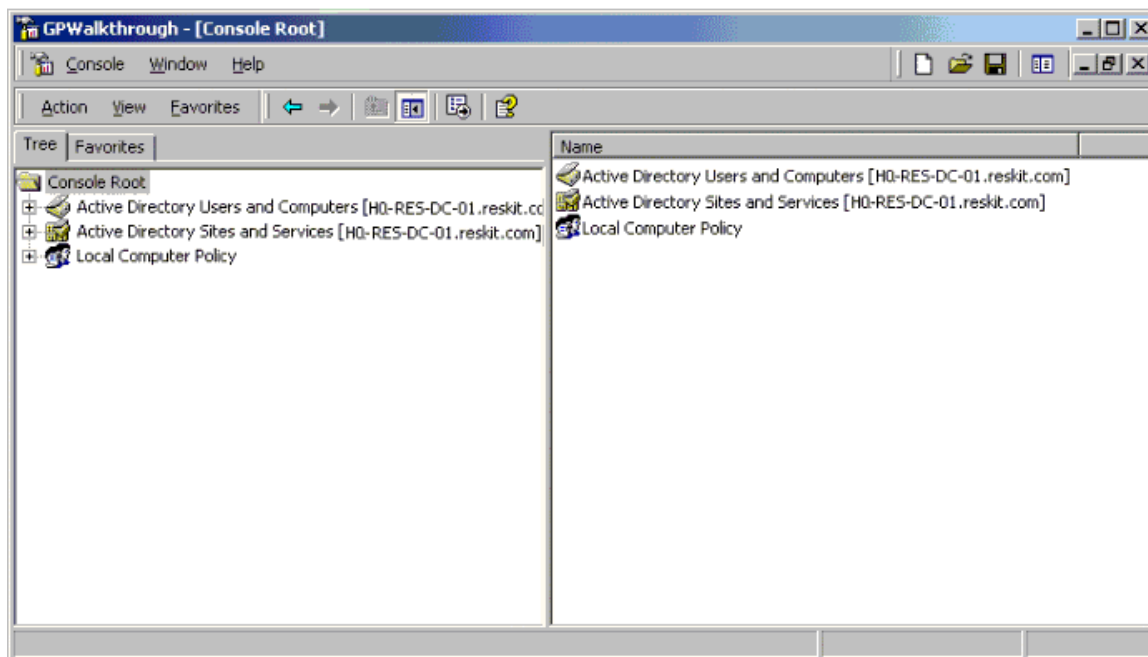
1. Log on to the **HQ-RES-DC-01** domain controller server as an administrator.
2. Click **Start**, click **Run**, type **mmc**, and then click **OK**.

3. On the **Console** menu, click **Add/Remove Snap-in**.
4. In the **Add/Remove Snap-in** dialog box, click **Add**.
5. In the **Add Standalone Snap-in** dialog box, in the **Available standalone snap-ins** list box, click **Active directory users and computers**, and then click **Add**.
6. Double-click **Active directory sites and services snap-in** from the **Available standalone snap-ins** list box.
7. In the **Available standalone snap-ins** list box, double-click **Group Policy**.
8. In the **Select Group Policy** object dialog box, **Local computer** is selected under **Group Policy object**. Click **Finish** to edit the local Group Policy object. Click **Close** in the **Add standalone snap-in** dialog box.
9. In the **Add/Remove Snap-in** dialog box, click the **Extensions** tab. Ensure that the **Add all extensions** check box is checked for each primary extension added to the MMC console (these are checked by default). Click **OK**.

#### To save console changes

1. In the MMC console, on the **Console** menu, click **Save**.
2. In the **Save As** dialog box, in the **File** name text box, type **GPWalkthrough**, and then click **Save**.

The console should appear as in Figure 2 below:



If your browser does not support inline frames, [click here](#) to view on a separate page.

**Figure 2 Group Policy MMC Console**

## Accessing Group Policy

You can use the appropriate Active Directory tools to access Group Policy while focused on any site, domain, or OU.

#### To open Group Policy from Active Directory Sites and Services

1. In the **GPWalkthrough** MMC console, in the console tree, click the + next to **Active Directory Sites and Services**.
2. In the console tree, right-click the site for which to access Group Policy.
3. Click **Properties**, and click **Group Policy**.

#### To open Group Policy from Active Directory Users and Computers

1. In the console tree in the **GPWalkthrough** MMC console, click the + next to **Active Directory Users and Computers**.
2. In the console tree, right-click either the **reskit** domain or the OU for which to access Group Policy.
3. Click **Properties**, and click **Group Policy**.

To access Group Policy scoped to a specific computer (or the local computer), you must load the Group Policy snap-in into the MMC console namespace targeted at the specific computer (or local computer). There are two major reasons for these differences:

- Sites, domains, and OUs can have multiple GPOs linked to them; these GPOs require an intermediate property page to manage them.
- A GPO for a specific computer is stored on that computer and not in the Active Directory.

## Scoping a Domain or OU

To scope the domain or OU, use the GPWalkthrough MMC console that you saved earlier.

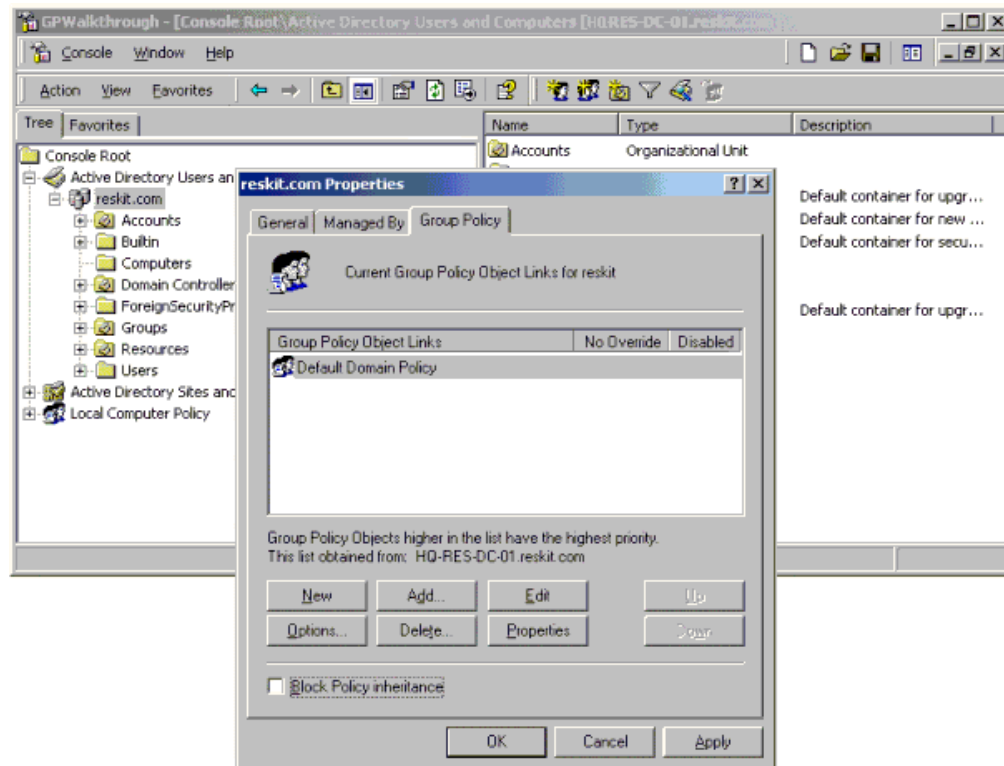
#### To scope Group Policy for a domain or OU

1. Click **Start**, point to **Programs**, click **Administrative Tools**, and click **GPWalkthrough** to open the MMC console you created earlier.
2. Click the + next to **Active Directory Users and Computers** to expand the tree.
3. Click the + next to **reskit.com** to expand the tree.
4. Right-click either the domain (reskit.com) or an OU, and click **Properties**.
5. Click the **Group Policy** tab as shown in Figure 3 below.

This displays a property page where the GPOs associated with the selected Active Directory container can be managed. You use this

property page to add, edit, delete (or remove), and disable GPOs; to specify No Override options; and to change the order of the associated GPOs. Selecting **Edit** starts the Group Policy snap-in. More information on using the Group Policy property page and the Group Policy snap-in can be found later in this document.

**Note** The Computers and Users containers are not organizational units; therefore, you cannot apply Group Policy directly to them. Users or computers in these containers receive policies from GPOs scoped to the domain and site objects only. The domain controller container is an OU, and Group Policy can be applied directly to it.



If your browser does not support inline frames, [click here](#) to view on a separate page.

**Figure 3 Group Policy Link Management**

### Scoping Local or Remote Computers

To access Group Policy for a local or a remote computer, you add the Group Policy snap-in to the MMC console, and focus it on a remote or local computer. To access Group Policy for the local computer, use the GPWalkthrough console created earlier in this document, and choose the **Local Computer Policy** node. You can add other computers to the console namespace by adding another Group Policy snap-in to the GPWalkthrough console, and clicking the **Browse** button when the **Select Group Policy** object dialog box is displayed.

**Note** Some of the Group Policy extensions are not loaded when Group Policy is run against a local GPO.

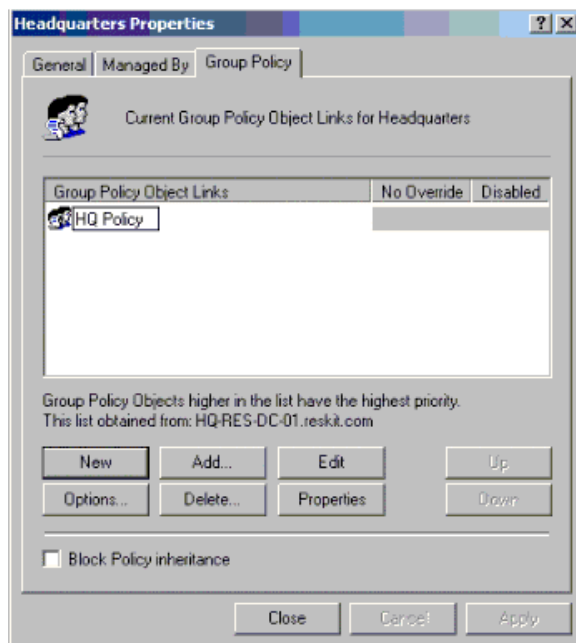
### Creating a Group Policy Object

The Group Policy settings you create are contained in a Group Policy Object (GPO) that is in turn associated with selected Active Directory objects, such as sites, domains, or organizational units (OUs).

#### To create a Group Policy Object (GPO)

1. Open the **GPWalkthrough** MMC console.
2. Click the + next to **Active Directory Users and Computers**, and click the **reskit.com** domain.
3. Click the + next to **Accounts** to expand the tree.
4. Right-click **Headquarters**, and select **Properties** from the context menu.
5. In the **Headquarters Properties** page, click the **Group Policy** tab.
6. Click **New**, and type **HQ Policy**.

The **Headquarters Properties** page should appear as in Figure 4 below:



**Figure 4 Headquarters Properties**

At this point you could add another GPO for the Headquarters OU, giving each one that you create a meaningful name, or you could edit the HQ Policy GPO, which starts the Group Policy snap-in for that GPO. All Group Policy functionality is derived from the snap-in extensions. In this exercise, all of these extensions are enabled. It is possible—using standard MMC methods—to restrict the extension snap-ins that are loaded for any given snap-in. For information on this capability, see the Windows 2000 Server Online Help for Microsoft Management Console.

There is also a Group Policy that you can use to restrict the use of MMC snap-in extensions. To access this policy, navigate to the System\Group Policy node under Administrative Templates. Use the Explain tab to learn more about the use of these policies.

If you have more than one GPO associated with an Active Directory folder, verify the GPO order; a GPO that is higher in the list has the highest precedence. Note that GPOs higher in the list are processed last (this is what gives them a higher precedence). GPOs in the list are objects; they have context menus that you use to view the properties of each GPO. You can use the context menus to obtain and modify general information about a GPO. This information includes Discretionary Access Control Lists (DACLS, which are covered in the Security Group Filtering section of this document), and lists the other site, domain, or OUs to which this GPO is linked.

7. Click **Close**

**Best Practice** You can further refine a GPO by using user or computer membership in security groups and then setting DACLS based on that membership. This is covered in the Security Group Filtering section below.

## Managing Group Policy

To manage Group Policy, you need to access the context menu of a site, domain, or OU, select **Properties**, and then select the **Group Policy** tab. This displays the Group Policy Properties page. Please note the following:

- This page displays any GPOs that have been associated with the currently selected site, domain, or OU. The links are objects; they have a context menu that you can access by right-clicking the object. (Right-clicking the white space displays a context menu for creating a new link, adding a link, or refreshing the list.)
- This page also shows an ordered GPO list, with the highest priority GPO at the top of the list. You can change the list order by selecting a GPO and then using the **Up** or **Down** buttons.
- To associate (link) a new GPO, click the **Add** button.
- To edit an existing GPO in the list, select the GPO and click the **Edit** button, or just double-click the GPO. This starts the Group Policy snap-in, which is how the GPO is modified. This is described in more detail later in this document.
- To permanently delete a GPO from the list, select it from the list and click the **Delete** button. Then, when prompted, select **Remove the link and delete the Group Policy object permanently**. Be careful when deleting an object, because the GPO may be associated with another site, domain, or OU. If you want to remove a GPO from the list, select the GPO from the links list, click **Delete**, and then when prompted, select **Remove the link from the list**.
- To determine what other sites, domains, or OUs are associated with a given GPO, right-click the GPO, select **Properties** from the context menu, and then click the **Links** tab in the GPO **Properties** page.
- The **No override** check column marks the selected GPO as one whose policies cannot be overridden by another GPO.  
**Note** You can enable the No Override property on more than one GPO. All GPOs that are marked as No override will take precedence over all other GPOs not marked. Of those GPOs marked as No override, the GPO with the highest priority will be applied after all the other similarly marked GPOs.
- The **Disabled** check box simply disables (deactivates) the GPO without removing it from the list. To remove a GPO from the list, select the GPO from the links list, click **Delete**, and then select **Remove the link from the list** in the **Delete** dialog box.
- It is also possible to disable only the User or Computer portion of the GPO. To do this, right-click the GPO, click **Properties**, click either **Disable computer configuration settings** or **Disable user configuration settings**, and then click **OK**. These options are available on the GPO **Properties** page, on the **General** tab.
- The **Block policy inheritance** check box has the effect of negating all GPOs that exist higher in the hierarchy. However, it cannot block any GPOs that are enforced by using the **No override** check box; those GPOs are *always* applied.

**Note** Policy settings contained within the local GPO that are not specifically overridden by domain-based policy settings are also always applied. Block Policy Inheritance at any level will not remove local policy.

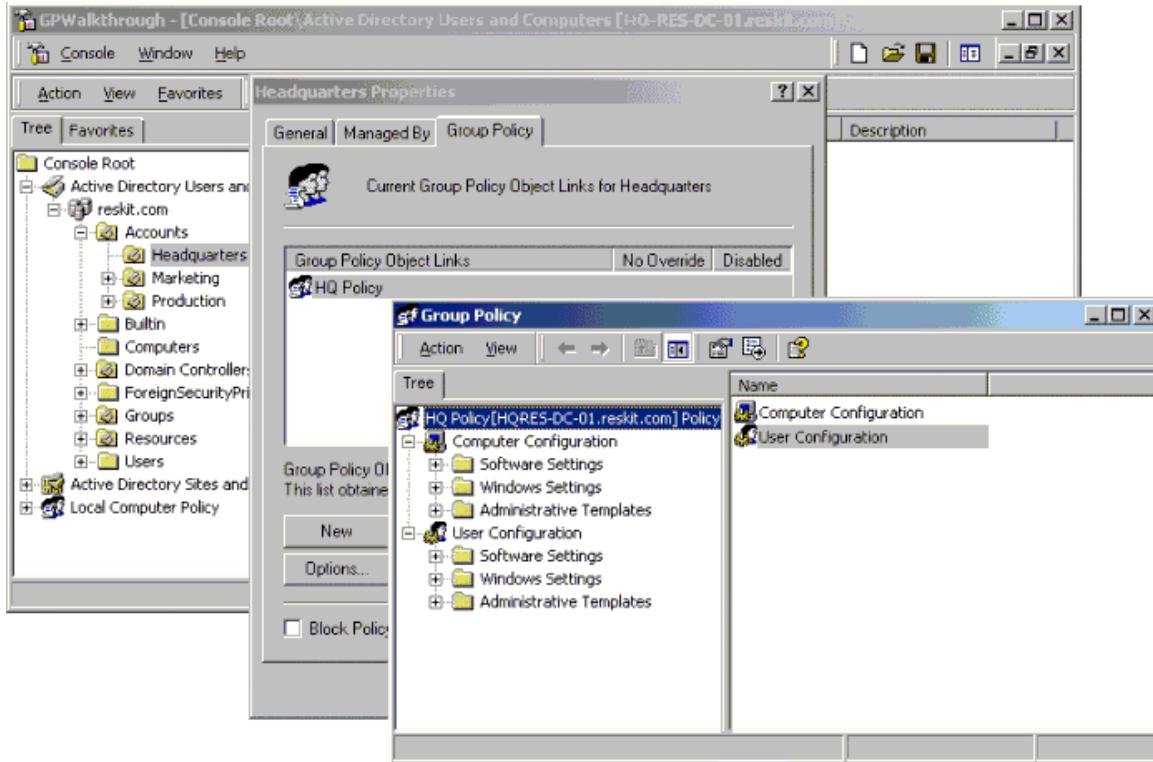
## Editing a Group Policy Object

You can use the custom console to edit a GPO. You will need to log on to the HQ-RES-DC-01 server as an Administrator, if you have not already done so.

**To edit a Group Policy Object (GPO)**

1. Click **Start**, point to **Programs**, click **Administrative Tools**, and then select **GPWalkthrough**.
2. Click the + next to **Active Directory Users and Computers**, click the **reskit.com** domain, and then click the **Accounts** OU.
3. Right-click **Headquarters**, select **Properties**, and then click the **Group Policy** tab. **HQ Policy** in the **Group Policy object links** list box should be highlighted.
4. Double-click the **HQ Policy** GPO (or click **Edit**).

This opens the Group Policy snap-in focused on a GPO named HQ Policy, which is linked to the OU named Headquarters. It should appear as in Figure 5 below:

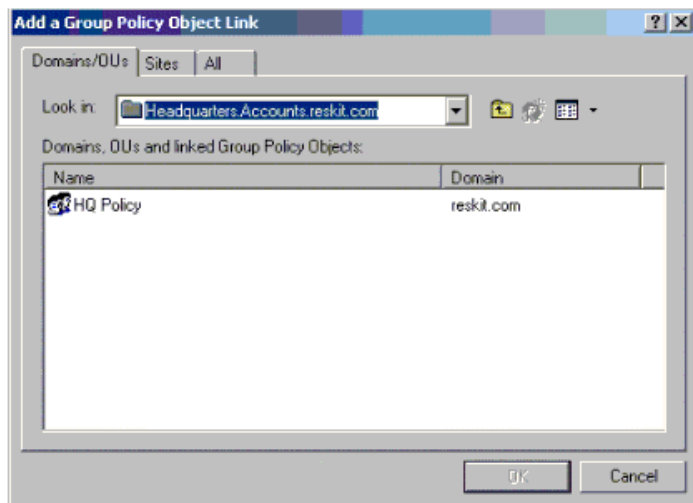


If your browser does not support inline frames, [click here](#) to view on a separate page.

**Figure 5 HQ Policy**

**Adding or Browsing a Group Policy Object**


The **Add a Group Policy Object Link** dialog box shows GPOs currently associated with domains, OUs, sites, or all GPOs without regard to their current associations (links). The **Add a Group Policy Object Link** dialog box is shown in Figure 6 below.



If your browser does not support inline frames, [click here](#) to view on a separate page.

**Figure 6 Add a Group Policy Object Link**

- GPOs are stored in each domain. The **Look In** drop-down box allows you to select a different domain to view.
- In the **Domains/OUs** tab, the list box displays the sub-OUs and GPOs for the currently selected domain or OU. To navigate the hierarchy, double-click a sub-OU or use the **Up one level** toolbar button.
- To add a GPO to the currently selected domain or OU, either double-click the object, or select it and click **OK**.

- Alternatively, you can create a new GPO by clicking the **All** tab, right-clicking in the open space, and selecting **New** on the context menu, or by using the **Create New GPO** toolbar button.  The **Create New GPO** toolbar button is only active in the **All** tab. To create a new GPO and link it to a particular site, domain, or OU, use the **New** button on the Group Policy Property page.

**Note** It is possible to create two or more GPOs with the same name. This is by design and is because the GPOs are actually stored as GUIDs and the name shown is a friendly name stored in the Active Directory.

- In the **Sites** tab, all GPOs associated with the selected site are displayed. Use the drop-down list to select another site. There is no hierarchy of sites.
- The **All** tab shows a flat list of all GPOs that are stored in the selected domain. This is useful when you want to select a GPO that you know by name, rather than where it is currently associated. This is also the only place to create a GPO that does not have a link to a site, domain, or OU.
- To create an unlinked GPO, access the **Add a Group Policy Link** dialog box from any site, domain, or OU. Click the **All** tab, select the toolbar button or right-click the white space, and select **New**. Name the new GPO, and click **Enter**, and then click **Cancel**—do not click **OK**. Clicking **OK** links the new GPO to the current site, domain, or OU. Clicking **Cancel** creates an unlinked GPO.

## Registry-Based Policies

The user interface for registry-based policies is controlled by using Administrative Template (.adm) files. These files describe the user interface that is displayed in the **Administrative Templates** node of the Group Policy snap-in. These files are format-compatible with the .adm files used by the System Policy Editor tool (poedit.exe) in Microsoft Windows NT 4.0. With Windows 2000, the available options have been expanded.

**Note** Although it is possible to add any .adm file to the namespace, if you use an .adm file from a previous version of Windows, the registry keys are unlikely to have an effect on Windows 2000, or they actually set preference settings and mark the registry with these settings; that is, the registry settings persist.

By default, only those policy settings defined in the loaded .adm files that exist in the approved Group Policy trees are displayed; these settings are referred to as *true policies*. This means that the Group Policy snap-in does *not* display any items described in the .adm file that set registry keys *outside* of the Group Policy trees; such items are referred to as Group Policy *preferences*. The approved Group Policy trees are:

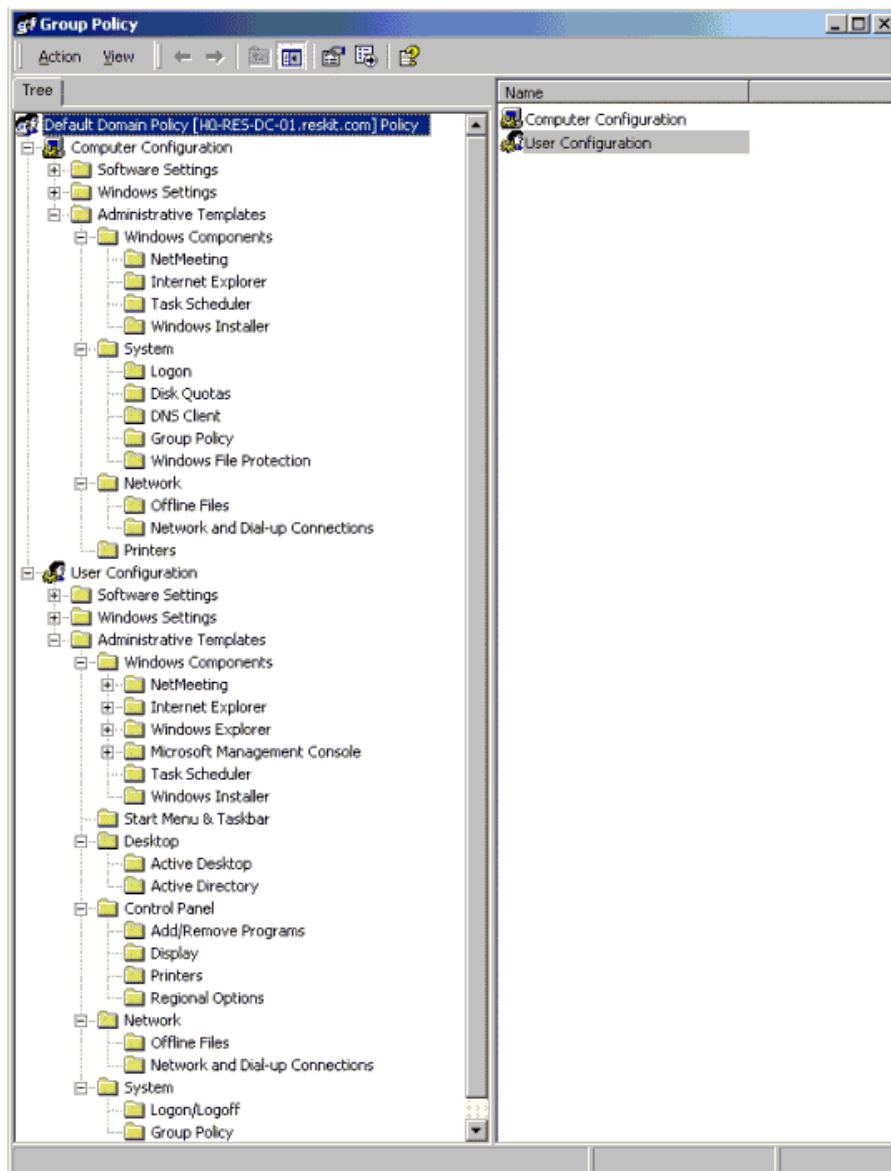
```
\Software\Policies
\Software\Microsoft\Windows\CurrentVersion\Policies
```

A Group Policy called **Enforce Show Policies Only** is available in **User Configuration\Administrative Templates**, under the **System\Group Policy** nodes. If you set this policy to **Enabled**, the **Show policies only** command is turned on and administrators cannot turn it off, and the Group Policy snap-in displays only true policies. If you set this policy to **Disabled** or **Not configured**, the **Show policies only** command is turned on by default; however, you can view preferences by turning off the **Show policies only** command. To view preferences, you must turn off the **Show policies only** command, which you access by selecting the **Administrative Templates** node (under either **User Configuration** or **Computer Configuration** nodes), and then clicking the **View** menu on the Group Policy console and clearing the **Show policies only** check box. Note that it is not possible for the selected state for this policy to persist; that is, there is no preference for this policy setting.

In Group Policy, preferences are indicated by a red icon to distinguish them from true policies, which are indicated by a blue icon.

Use of non-policies within the Group Policy infrastructure is strongly discouraged because of the persistent registry settings behavior mentioned previously. To set registry policies on Windows NT 4.0, and Windows 95 and Windows 98 clients, use the Windows NT 4.0 System Policy Editor tool, Poedit.exe.

By default the System.adm, Inetres.adm, and Conf.adm files are loaded and present this namespace as shown in Figure 7 below:



If your browser does not support inline frames, [click here](#) to view on a separate page.

### Figure 7 User Configuration

The .adm files include the following settings:

- System.adm: Operating system settings
- Inetres.adm: Internet Explorer restrictions
- Conf.adm: NetMeeting settings

### Adding Administrative Templates

The .adm file consists of a hierarchy of categories and subcategories that together define how options are organized in the Group Policy user interface.

#### To add administrative templates (.adm files)

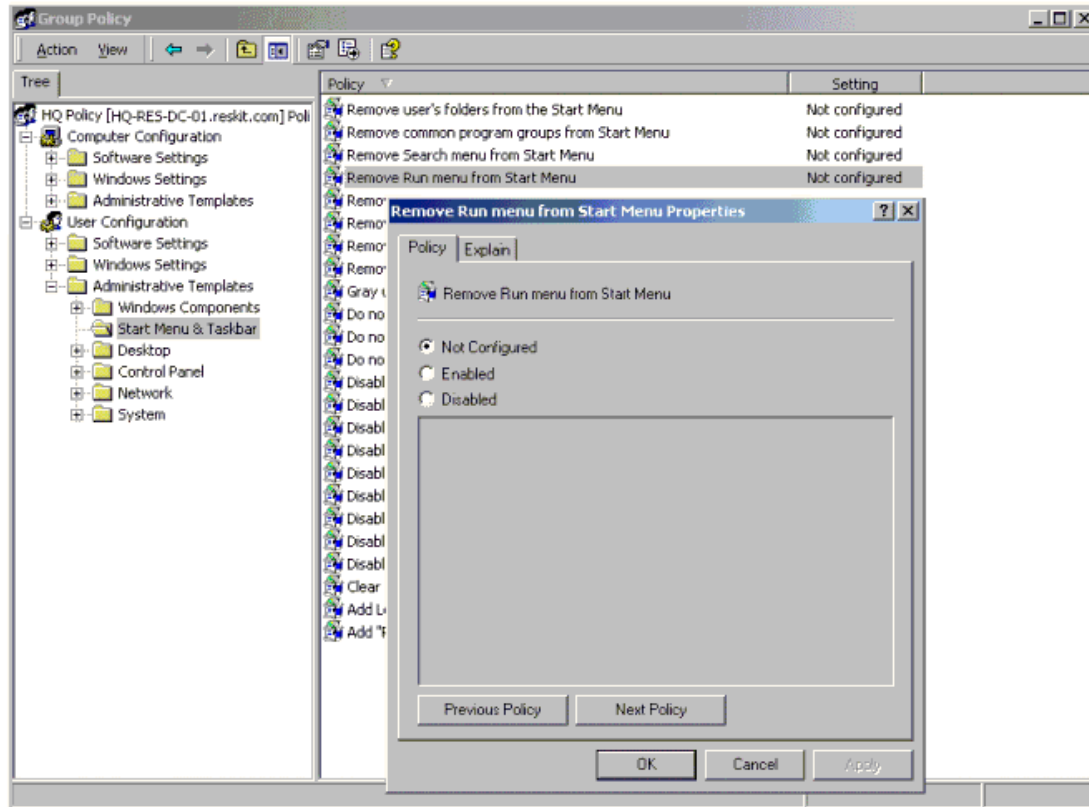
1. In the Group Policy console double-click **Active Directory Users and Computers**, select the domain or OU for which you want to set policy, click **Properties**, and then click **Group Policy**.
2. In the **Group Policy** properties page, select the Group Policy Object you want to edit from the **Group Policy objects links** list, and click **Edit** to open the Group Policy snap-in.
3. In the Group Policy console, click the plus sign (+) next to either **User Configuration** or **Computer Configuration**.  
The .adm file defines which of these locations the policy is displayed in, so it doesn't matter which node you choose.
4. Right-click **Administrative Templates**, and select **Add/Remove Templates**. This shows a list of the currently active templates files for this Active Directory container.
5. Click **Add**. This shows a list of the available .adm files in the %systemroot%\inf directory of the computer where Group Policy is being run. You can choose an .adm file from another location. Once chosen, the .adm file is copied into the GPO.

#### To set registry-based settings using administrative templates

1. In the GPWalkthrough console, double-click **Active Directory Users and Computers**, double-click the **reskit.com** domain, double-click **Accounts**, right-click the **Headquarters** OU, and then click **Properties**.
2. In the **Headquarters Properties** dialog box, click **Group Policy**.
3. Double-click the **HQ Policy** GPO from the **Group Policy object links** list to edit the HQ Policy GPO.



4. In the Group Policy console, under the **User Configuration** node, click the plus sign (+) next to **Administrative Templates**.
5. Click **Start Menu & Taskbar**.  
Note that the details pane shows all the policies as **Not configured**.
6. In the details pane, double-click the **Remove Run menu from Start menu** policy.  
This displays a dialog box for the policy as shown in Figure 8 below.



If your browser does not support inline frames, [click here](#) to view on a separate page.

**Figure 8 Remove Run menu from Start Menu**

7. In the **Remove Run menu from Start menu** dialog box, click **Enabled**.  
Note the **Previous Policy** and **Next Policy** buttons in the dialog box. You can use these buttons to navigate the details pane to set the state of other policies. You can also leave the dialog box open and click another policy in the details pane of the Group Policy snap-in. After the details pane has the focus, you can use the **Up** and **Down** arrow keys on the keyboard and press **Enter** to quickly browse through the settings (or **Explain** tabs) for each policy in the selected node.
8. Click **OK**.  
Note the change in state in the **Setting** column, in the details pane. This change is immediate; it has been saved to the GPO. If you are in a replicated domain controller (DC) environment, this action sets a flag that triggers a replication cycle.

If you log on to a workstation in the **reskit.com** domain with a user from the **Headquarters** OU, you will note that the **Run** menu has been removed.

At this point, you may want to experiment with the other available policies. Look at the text in the **Explain** tab for information about each policy.

## Scripts

You can set up scripts to run when users log on or log off, or when the system starts up or shuts down. All scripts are Windows Scripting Host (WSH)-enabled. As such, they may include Java Scripts or VB Scripts, as well as .bat and .cmd files. Links to more information on the Windows Scripting Host are located in the More Information section at the end of this document.

## Setting up a Logon Script

Use this procedure to add a script that runs when a user logs on.

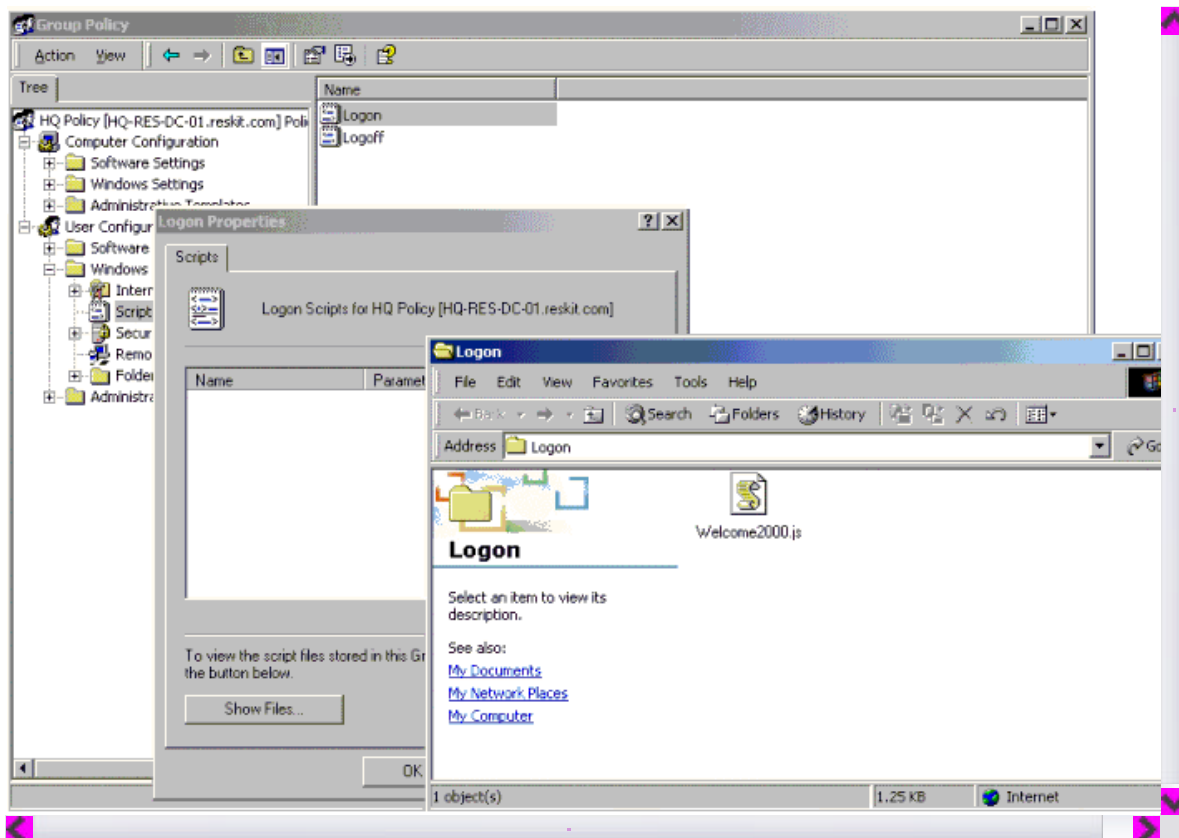
**Note** This procedure uses the Welcome2000.js script described in Appendix A of this document, which includes instructions for creating and saving the script file. Before performing the procedure for setting up logon scripts, you need to create the Welcome2000.js script file and copy it to the HQ-RES-DC-01 domain controller.

### To set up logon scripts

1. In the GPWalkthrough console, double-click **Active Directory Users and Computers**, right-click the **reskit.com** domain, click **Properties**, and then click **Group Policy**.
2. In the **Group Policy** properties page, select the **Default Domain Policy** GPO from the **Group Policy objects links** list, and click **Edit** to open the Group Policy snap-in.
3. In the Group Policy snap-in, under **User Configuration**, click the + next to **Windows Settings**, and then click the **Scripts (Logon/Logoff)** node.
4. In the details pane, double-click **Logon**.
  - o The **Logon Properties** dialog box displays the list of scripts that run when affected users log on. This is an ordered list, with the script that is to run first appearing at the top of the list. You can change the order by selecting a script and then using the **Up** or **Down** buttons.

- To add a new script to the list, click the **Add** button. This displays the **Add a Script** dialog box. Browsing from this dialog allows you to specify the name of an existing script located in the current GPO or to browse to another location and select it for use in this GPO. The script file must be accessible to the user at logon or it does not run. Scripts in the current GPO are automatically available to the user. You can create a new script by right-clicking the empty space and selecting **New**, then selecting a new file.
 

**Note** If the View Folder Options for this folder are set to Hide file extensions for known file types, the file may have an unwanted extension that prevents it from being run.
  - To edit the name or the parameters of an existing script in the list, select it and click the **Edit** button. This button does not allow the script itself to be edited. That can be done through the **Show Files** button.
  - To remove a script from the list, select it and click **Remove**.
  - The **Show Files** button displays an Explorer view of the scripts for the GPO. This allows quick access to these files or to the place to copy support files to if the script files require them. If you change a script file name from this location, you must also use the **Edit** button to change the file name, or the script cannot execute.
5. Click on the **Start** menu, click **Programs**, click **Accessories**, click **Windows Explorer**, navigate to the **Welcome2000.js** file (use Appendix A to create the file), and then right-click the file and select **Copy**.
  6. Close Windows Explorer.
  7. In the **Logon Properties** dialog box, click the **Show Files** button, and paste the Welcome2000.js script into the default file location. It should appear as in Figure 9 below:



If your browser does not support inline frames, [click here](#) to view on a separate page.

**Figure 9 Welcome2000.js**

8. Close the **Logon** window.
9. Click the **Add** button in the **Logon Properties** dialog box.
10. In the **Add a Script** dialog box, click **Browse**, and then in the **Browse** dialog box, double-click the **Welcome2000.js** file.
11. Click **Open**.
12. In the **Add a Script** dialog box, click **OK** (no script parameters are needed), and then click **OK** again.

You can then logon to a client workstation that has a user in the **Headquarters OU**, and verify that the script is run when the user logs on.

## Setting Up a Logoff or Computer Startup or Shutdown Script

You can use the same procedure outlined in the preceding section to set up scripts that run when a user logs off or when a computer starts up or is shut down. For logoff scripts, you would select **Logoff** in step 4.

## Other Script Considerations

By default, Group Policy scripts that run in a command window (such as .bat or .cmd files) run hidden, and legacy scripts (those defined in the user object) are by default visible as they are processed (as was the case for Windows NT 4.0), although there is a Group Policy that allows this visibility to be changed. The policy for users is called **Run logon scripts visible** or **Run logoff scripts visible**, and is accessed in the **User Configuration\Administrative Templates** node, under **System\Logon/Logoff**. For computers, the policy is **Run startup scripts visible** and can be accessed in the **Computer Configuration\Administrative Templates** node, under **System\Logon**.

## Security Group Filtering

You can refine the effects of any GPO by modifying the computer or user membership in a security group. To do this, you use the **Security** tab to set Discretionary Access Control Lists (DACLS) for the properties of a GPO. DACLS are used for performance reasons,

the details of which are contained in the Group Policy technical paper referenced earlier in this document. This feature allows for tremendous flexibility in designing and deploying GPOs and the policies they contain.

By default, all GPOs affect all users and machines that are contained in the linked site, domain, or OU. By using DACLs, the effect of any GPO can be modified to exclude or include the members of any security group.

You can modify a DACL using the standard Windows 2000 **Security** tab, which is accessed from the **Properties** page of any GPO.

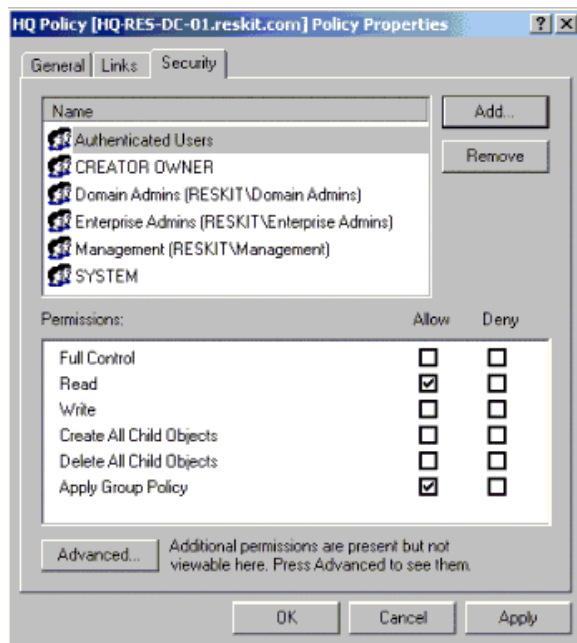
**To access a GPO Properties page from the Group Policy Properties page of a Domain, or OU**

1. In the GPWalkthrough console, double-click **Active Directory Users and Computers**, double-click the **reskit.com** domain, double-click **Accounts**, right-click the **Headquarters** OU, and then click **Properties**.
2. In the **Headquarters Properties** dialog, click **Group Policy**.
3. Right-click the **HQ Policy** GPO from the **Group Policy Object Links** list, and select **Properties** from the context menu.
4. In the **Properties** page, click the **Security** tab. This displays the standard **Security** properties page.

You will see security groups and users based on the Common Infrastructure. For more information, see the Windows 2000 step-by-step guide, A Common Infrastructure for Change and Configuration Management. Make sure that you have completed the appropriate steps in that document before continuing.

5. In the **Security** property page, click **Add**.
6. In the **Select Users, Computers, and Groups** dialog box, select the **Management** group from the list, click **Add**, and click **OK** to close the dialog.
7. In the **Security** tab of the **HQ Policy Properties** page, select the **Management** group, and view the permissions. By default, only the **Read** Access Control Entry (ACE) is set to **Allow** for the Management group. This means that the members of the Management group do not have this GPO applied to them unless they are also members of another group (by default, they are also Authenticated Users) that has the **Apply Group Policy** ACE selected.

At this point, *everyone* in the Authenticated Users group has this GPO applied, regardless of having added the Management group to the list, as shown in Figure 10 below..



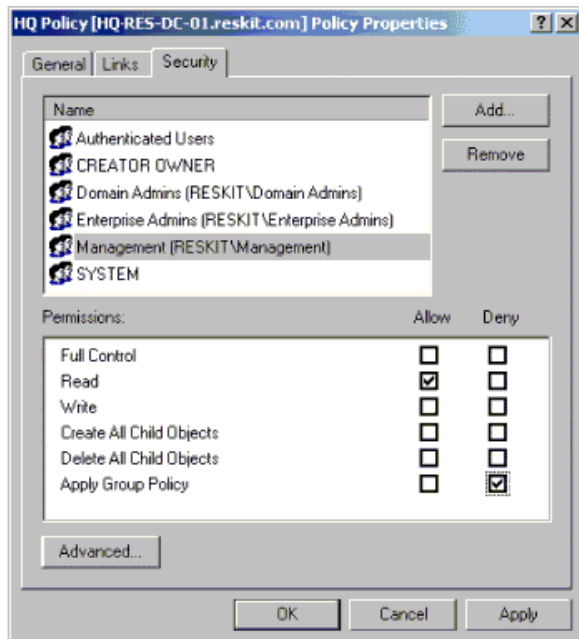
**Figure 10 Authenticated Users**

8. Configure the GPO so that it applies to the members of the Management group *only*. Select **Allow** for the **Apply Group Policy** ACE for the Management group, and then remove the **Allow Group Policy** ACE from the Authenticated Users group.

By changing the ACEs that are applied to different groups, administrators can customize how a GPO affects the users or computers that are subject to that GPO. **Write** access is required for modifications to be made; **Read** and **Allow Group Policy** ACEs are required for a policy to affect a group (for the policy to apply to the group).

Use the **Deny** ACE with caution. A **Deny** ACE setting for any group has precedence over any **Allow** ACE given to a user or computer because of membership in another group. Details of this interaction may be found in the Windows 2000 Server online Help by searching on Security Group.

Figure 11 belows shows an example of the security settings that allow everyone to be affected by this GPO *except* the members of the Management group, who were explicitly *denied* permission to the GPO by setting the **Apply Group Policy** ACE to **Deny**. Note that if a member of the Management group were also a member of a group that had an explicit **Allow** setting for the **Apply Group Policy** ACE, the **Deny** would take precedence and the GPO would not affect the user.



**Figure 11 Security Settings**

Variations on the above may include:

- Adding additional GPOs with different sets of policies and having them apply only to groups other than the Management group.
- Creating another group with members of the existing groups in them, and then using those groups as filters for a GPO.

**Note** You can use these same types of security options with the Logon scripts you set up in the preceding section. You can set a script to run only for members of a particular group or for everyone except the members of a specific group.

Security group filtering has two functions: the first is to modify which group is affected by a particular GPO, and the second is to delegate which group of administrators can modify the contents of the GPO by restricting **Full Control** to a limited set of administrators (by a group). This is recommended because it limits the chance of multiple administrators making changes at any one time.

### Blocking Inheritance and No Override

The **Block inheritance** and **No override** features allow you to have control over the default inheritance rules. In this procedure, you set up a GPO in the Accounts OU, which applies by default to the users (and computers) in the Headquarters, Production, and Marketing OUs.

You then establish another GPO in the Accounts OU and set it as **No override**. These settings apply to the children OUs, even if you set up a contrary setting in a GPO scoped to that OU.

You then use the **Block inheritance** feature to prevent Group policies set in a parent site, domain, or OU (in this case, the Accounts OU) from being applied to the Production OU.

A description of how to disable portions of a GPO to improve performance is also included.

### Setting Up the Environment

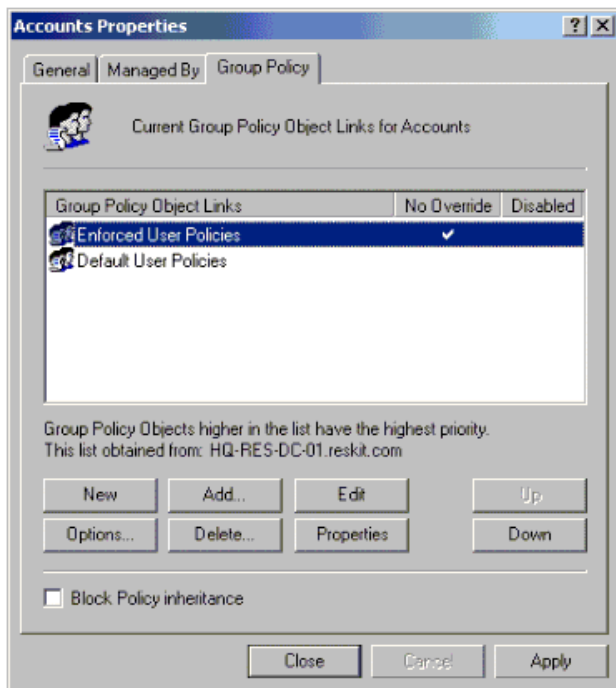
You must first set up the environment for the procedures in this section.

#### To set up the GPO environment

1. Open the saved MMC GP console GPWalkthrough, and then open the **Active Directory User and Computers** node.
2. Double-click the **reskit.com** domain, and then double-click the **Accounts OU**.
3. Right-click the **Accounts OU**, and select **Properties** from the context menu, and click the **Group Policy** tab.
4. Click **New** to create a new GPO called **Default User Policies**.
5. Click **New** to create a new GPO called **Enforced User Policies**.
6. Select the **Enforced Users Policies** GPO, and click the **Up** button to move it to the top of the list.

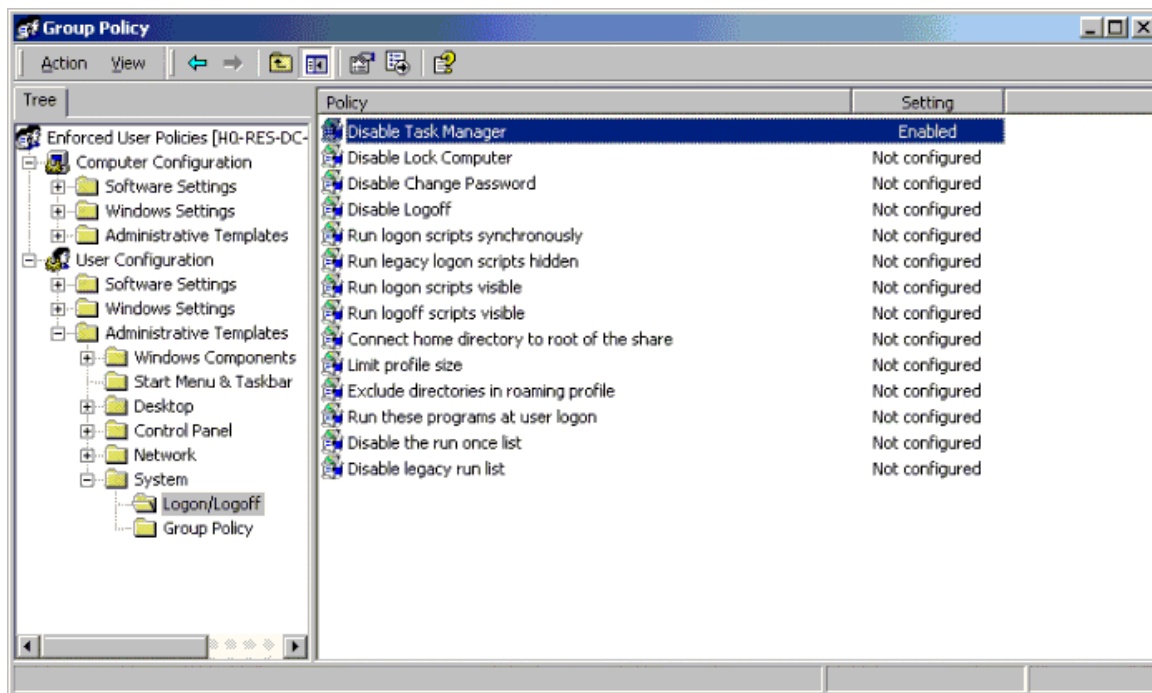
The **Enforced Users Policies** GPO should have the highest precedence. Note that this step only serves to demonstrate the functionality of the **Up** button; an enforced GPO always takes precedence over those that are not enforced.

7. Select the **No override** setting for the **Enforced User Policies** GPO by double-clicking the **No override** column or using the **Options** button. The **Accounts Properties** page should now appear as in Figure 12 below:



**Figure 12 Enforced User Policies**

8. Double-click the **Enforced User Policies** GPO to start the Group Policy snap-in.
9. In the Group Policy snap-in, under **User Configuration**, click **Administrative Templates**, click **System**, and then click **Logon/Logoff**.
10. In the details pane, double-click the **Disable Task Manager** policy, click **Enabled** in the **Disable Task Manager** dialog box, and then click **OK**.  
For information on the policy, click the **Explain** tab. Note that the setting is now **Enabled** as in Figure 13 below.



If your browser does not support inline frames, [click here](#) to view on a separate page.

**Figure 13 Task Manager**

11. Click the **Close** button to exit the Group Policy snap-in.
12. In the **Accounts Properties** dialog box, on the **Group Policy** tab, double-click the **Default User Policies** GPO from the **Group Policy objects links** list.
13. In the Group Policy snap-in, in the **User Configuration** node, under **Administrative Templates**, click the **Desktop** node, click the **Active Desktop** folder, and then double-click the **Disable Active Desktop** policy on the details pane.
14. Click **Enabled**, click **OK**, and click **Close**.
15. In the **Accounts Properties** dialog box, click **Close**.

You can now log on to a client workstation as any user in any of the OUs under the Accounts OU. Note that you cannot run the Task Manager—the tab is unavailable from both CTRL+SHIFT+ESC and CTRL+ALT+DEL. In addition, the Active Desktop cannot be enabled. When you right-click on **Desktop** and select **Properties**, you will see that the **Web** tab is missing.

As an extra step, you can reverse the setting of the **Disable Task Manager** policy in a GPO that is linked to any of the child OUs of the

Accounts OU (Headquarters, Production, Marketing). To do this, change the radio button for that policy.

**Note** Doing this has no effect while the Enforced User Policies GPO is enabled in the Accounts OU.

### Disabling Portions of a GPO

Because these GPOs are used solely for user configuration, the computer portion of the GPO can be turned off. Doing so reduces the computer startup time, because the Computer GPOs do not have to be evaluated to determine if any policies exist. In this procedure, no computers are affected by these GPOs. Therefore, disabling a portion of the GPO has no immediate benefit. However, since these GPOs could later be linked to a different OU that may include computers, you may want to disable the computer side of these GPOs.

#### To disable the Computer portion of a GPO

1. Open the saved MMC console GPWalkthrough, and then double-click the **Active Directory User and Computers** node.
2. Double-click the **reskit.com** domain.
3. Right-click the **Accounts** OU, select **Properties** from the context menu, and click the **Group Policy** tab.
4. In the **Accounts Properties** dialog box, click the **Group Policy** tab, right-click the **Enforced User Policies** GPO, and select **Properties**.
5. In the **Enforced User Policies Properties** dialog box, select the **General** tab, and then select the **Disable computer configuration settings** check box. In the **Confirm Disable** dialog box click **Yes**.  
Note that the **General** properties page includes two check boxes for disabling a portion of the GPO.
6. Repeat steps 4 and 5 for the **Default Users Policies** GPO.

### Blocking Inheritance

You can block inheritance so that one GPO does not inherit policy from another GPO in the hierarchy. After you block inheritance, only those settings in the Enforced User Policies affect the users in this OU. This is simpler than reversing each individual policy in a GPO scoped at this OU.

#### To block inheritance of Group Policy for the Production OU

1. Open the saved MMC console GPWalkthrough, and then double-click the **Active Directory User and Computers** node.
2. Double-click the **reskit.com** domain, and then double-click the **Accounts** OU.
3. Right-click the **Production** OU, select **Properties** from the context menu, and then click the **Group Policy** tab.
4. Select the **Block policy inheritance** check box, and click **OK**.

To verify that inherited settings are now blocked, you can logon as any user in the Production OU. Notice that the Web tab is present in the Display setting properties page. Also, note that the task manager is still disabled, as it was set to No Override in the parent OU.

### Linking a GPO to Multiple Sites, Domains, and OUs

This section demonstrates how you can link a GPO to more than one container (site, domain, or OU) in the Active Directory. Depending on the exact OU configuration, you can use other methods to achieve similar Group Policy effects; for example, you can use security group filtering or you can block inheritance. In some cases, however, those methods do not have the desired effects. Whenever you need to explicitly state which sites, domains, or OUs need the same set of policies, use the method outlined below:

#### To link a GPO to multiple sites, domains, and OUs

1. Open the saved MMC console GPWalkthrough, and then double-click the **Active Directory User and Computers** node.
2. Double-click the **reskit.com** domain, and double-click the **Accounts** OU.
3. Right-click the **Headquarters** OU, select **Properties** from the context menu, and then click the **Group Policy** tab.
4. In the **Headquarters Properties** dialog box, on the **Group Policy** tab, click **New** to create a new GPO named **Linked Policies**.
5. Select the **Linked Policies** GPO, and click the **Edit** button.
6. In the Group Policy snap-in, in the **User Configuration** node, under **Administrative Templates** node, click **Control Panel**, and then click **Display**.
7. On the details pane, click the **Disable Changing Wallpaper** policy, and then click **Enabled** in the **Disable Changing Wallpaper** dialog box and click **OK**.
8. Click **Close** to exit the Group Policy snap-in.
9. In the **Headquarters Properties** page, click **Close**.

Next you will link the **Linked Policies** GPO to another OU.

1. In the GPWalkthrough console, double-click the **Active Directory User and Computers** node, double-click the **reskit.com** domain, and then double-click the **Accounts** OU.
2. Right-click the **Production** OU, click **Properties** on the context menu, and then click the **Group Policy** tab on the **Production Properties** dialog box.
3. Click the **Add** button, or right-click the blank area of the **Group Policy objects links** list, and select **Add** on the context menu.
4. In the **Add a Group Policy Object Link** dialog box, click the down arrow on the **Look in** box, and select the **Accounts.reskit.com** OU.
5. Double-click the **Headquarters.Accounts.reskit.com** OU from the **Domains, OUs, and linked Group Policy objects** list.
6. Click the **Linked Policies** GPO, and then click **OK**.

You have now linked a single GPO to two OUs. Changes made to the GPO in either location result in a change for both OUs. You can test this by changing some policies in the **Linked Policies** GPO, and then logging onto a client in each of the affected OUs, **Headquarters** and **Production**.

### Loopback Processing

This section demonstrates how to use the loopback processing policy to enable a different set of user type Group Policies based on the Computer being logged onto. This policy is useful when you need to have user type policies applied to users of specific computers. There are two methods for doing this. One allows for the policies applied to the user to be processed, but to also apply user policies based on the computer that the user has logged onto. The second method does not apply the user's settings based on where the user object is, but only processes the policies based on the computer's list of GPOs. Details on this method can be found in the Group Policy white paper referred to earlier.

#### To use the Loopback processing policy

1. In the GPWalkthrough console, double-click the **Active Directory User and Computers** node, double-click the **reskit.com** domain, and then double-click the **Resources** OU.

2. Right-click the **Desktop** OU, click **Properties** on the context menu, and then click the **Group Policy** tab on the **Desktop Properties** dialog box.
3. Click **New** to create a new GPO named **Loopback Policies**.
4. Select the **Loopback Policies** GPO, and click **Edit**.
5. In the Group Policy snap-in, under the **Computer Configuration** node, click **Administrative Templates**, click **System**, and then click **Group Policy**.
6. In the details pane, double-click the **User Group Policy loopback processing mode** policy.
7. Click **Enabled** in the **User Group Policy loopback processing mode** dialog box, select **Replace** in the **Mode** drop-down box, and then click **OK** to exit the property page.

Next, you will set several **User Configuration** policies by using the **Next Policy** navigation buttons in the policy dialog boxes.

1. In the Group Policy snap-in, under the **User Configuration** node, click **Administrative Templates**, and click **Start Menu & Taskbar**.
2. In the details pane, double-click the **Remove user's folders from the Start menu** policy, and then click **Enabled** in the **Remove user's folders from the Start menu** dialog box.
3. Click **Apply** to apply the policy, and click the **Next Policy** button to go on to the next policy, **Disable and remove links to Windows update**.
4. In the **Disable and Remove Links to Windows Update** dialog box, click **Enabled**, click **Apply**, and then click the **Next Policy** button.
5. In each of the following policies' dialog boxes, set the state of the policies as indicated on the list below:

Policy	Setting
Remove common program groups from Start Menu	Enabled
Remove Documents from Start Menu	Enabled
Disable programs on Settings Menu	Enabled
Remove Network & Dial-up Connections from Start menu	Enabled
Remove Favorites Menu from Start menu	Enabled
Remove Search Menu from Start menu	Enabled
Remove Help Menu from Start menu	Enabled
Remove Run Menu from Start menu	Enabled
Add Logoff on the Start Menu	Enabled
Disable Logoff on the Start Menu	Not configured
Disable and remove the Shut Down command	Not configured
Disable drag-and-drop context menus on the Start Menu	Enabled
Disable changes to Taskbar and Start Menu Settings	Enabled
Disable Context menus for the taskbar	Enabled
Do not keep history of recently opened documents	Enabled
Clear history of recently opened documents on exit	Enabled

6. Click **OK** when you have set the last policy from the list in step 5.
7. In the Group Policy console tree, navigate to the **Desktops** node under **User Configuration\Administrative Templates**, and set the following policies to **Enabled**:

Policy	Setting
Hide Remove My Documents from Start Menu	Enabled
Hide My Network Places icon on desktop	Enabled
Hide Internet Explorer icon on desktop	Enabled
Prohibit user from changing My Documents path	Enabled
Disable adding, dragging, dropping and closing the Taskbar's toolbars	Enabled
Disable adjusting desktop toolbars	Enabled
Don't save settings at exit	Enabled

8. Click **OK** when you have set the last policy from the list in step 7.
9. In the Group Policy console tree, navigate to the **Active Desktop** node under **User Configuration\Administrative Templates\Desktops**, set the **Disable Active Desktop** policy to **Enabled**, and then click **OK**.
10. In the Group Policy console tree, navigate to the **Control Panel** node under **User Configuration\Administrative Templates**, click the **Add/Remove Programs** node, double-click the **Disable Add/Remove Programs** policy, set it to **Enabled**, and then click **OK**.
11. In the Group Policy console tree, navigate to the **Control Panel** node under **User Configuration\Administrative Templates**, click the **Display** node, double click the **Disable display in control panel** policy, set it to **Enabled**, and then click **OK**.
12. In the Group Policy snap-in, click **Close**.
13. In the **Desktops Properties** dialog box, click **Close**.

At this point, all users who log on to computers in the **Desktops** OU have no policies that would normally be applied to them; instead, they have the user policies set in the **Loopback Policies** GPO. You may want to use the procedures outlined in the section on Security Group Filtering to restrict this behavior to specific groups of computers, or you may want to move some computers to another OU.

For the following example, a security group called **No Loopback** is created. To do this, use the **Active Directory Users and**

**Computers** snap-in, click the **Groups** container, click **New**, and create this global security group.

In this example, computers that are in the **No-Loopback** security group are excluded from this loopback policy, if the following steps are taken:

1. In the GPWalkthrough console, double-click **Active Directory Users and Computers**, double-click **reskit.com**, double-click **Resources**, right-click **Desktop**, and then select **Properties**.
2. In the **Desktop Properties** dialog box, click **Group Policy**, right-click the **Loopback Policies** GPO, and then select **Properties**.
3. In the **Loopback Policies Properties** page, click **Security**, and select **Allow** for the **Apply Group Policy** ACE for the **Authenticated Users** group.
4. Add the **No Loopback** group to the **Name** list. To do this, click **Add**, select the **No Loopback** group, and click **OK**.
5. Select **Deny** for the **Apply Group Policy** ACE for the **No Loopback** group, and click **OK**.
6. Click **OK** in the **Loopback Policies Properties** page.
7. Click **Close** in the **Desktop Properties** dialog box
8. In the GPWalkthrough console, click **Save** on the **Console** menu.

### Other Group Policy Scenarios

Now that you familiar with the methodologies for administrating Group Policy, you may want to set up some security policies, perform some software installation and maintenance, and redirect some user folders—such as the My Documents folder. These topics are covered in detail in the following step-by-step guides, available on the Windows 2000 Server Web site:

- Deploying Security Policies
- Software Installation and Maintenance
- User Data and Settings Management

### For More Information

For the latest information on the Microsoft Windows 2000 network operating system, visit the [Windows 2000 Web site](#) and the [Windows NT Forum on the Microsoft Network](#).

For specific help about installing and using Windows 2000, see the [Windows 2000 Professional Online Help](#) and [Windows 2000 Server Online Help](#).

For help in determining the best deployment practices for your company, see the [Windows 2000 Deployment and Planning Guide](#).

For additional information on Group Policy, refer to the [Windows 2000 Group Policy technical paper](#). This paper includes information about the Group Policy infrastructure and mechanics, the Group Policy snap-in and its capabilities, extending the Group Policy functionality, and using Group Policy on stand-alone computers. It also presents instructions for creating administrative templates (.adm files).

For more information on Windows Script Host, see the [Windows Script Host white paper](#).

For information about MMC, see the [Microsoft Management Console Overview white paper](#) and a [Step-by-Step Guide to the Microsoft Management Console](#).

For more information on .adm files, persistent registry settings, and using the Windows NT 4.0 System Policy Editor, see the [Windows 2000 Group Policy technical paper](#), and [Implementing Profiles and Policies for Windows NT 4.0](#).

### Appendix A: Welcome2000.js Sample Script

The code for the Welcome2000.js sample script is shown following the procedure for creating and saving the sample script file.

#### To create and save this sample script

1. Select and copy all the sample code presented in this section, beginning with the line with `// Script Sample for Windows Scripting Host`, and ending with the line with `}`.
2. Click **Start**, click **Run**, type **notepad**, and then click **OK**.  
This starts the Windows Notepad application.
3. In **Notepad**, click **Edit**, and click **Paste**.
4. On the **File** menu, click **Save**, type **Welcome.js** in the **File name** text box, save as type text, and click **OK**.

The Welcome2000.js script code is shown next.

```
// Script Sample for Windows Scripting Host
//
// Define constant values.
//
var MB_ICONINFORMATION = 0x40;
var MB_ICONQUESTION = 0x20;
var MB_ICONYESNO = 0x04
var IDYES = 6;
var IDTIMEOUT = -1;

var POPUP_WAIT = 5; // close popup after 5 seconds.

//
// Create ActiveX Controls
//
var Shell = WScript.CreateObject("WScript.Shell")
var Env = Shell.Environment("PROCESS")

//
// Set greeting message.
//
var strTitle = "Sample Login Script";

var strMsg = "Welcome \"\" + Env("UserName")
strMsg += "\" to the \"" + Env("UserDomain") + "\" domain\r\n\r\n"

Shell.Popup(strMsg, POPUP_WAIT, strTitle, MB_ICONINFORMATION);

//
// Launch Internet Explorer if user wants.
```



```
//
strMsg = "Do you want to visit the Windows 2000 web site?";
var strURL;

strURL = "http://www.microsoft.com/windows";

var intAnswer = Shell.Popup(strMsg,
POPUP_WAIT,
strTitle,
MB_ICONQUESTION | MB_ICONYESNO );

if (intAnswer == IDYES) {
Shell.Run(strURL);
}
}
```

---

[Send feedback to Microsoft](#)

[© 2004 Microsoft Corporation. All rights reserved.](#)