Windows Server 2003

Implementing Common Desktop Management Scenarios with the Group Policy Management Console

Microsoft Corporation

Published: August 2003

Abstract

This white paper describes six scenarios for using IntelliMirror, and is intended for information technology managers and system administrators who are interested in using IntelliMirror technologies – and particularly Group Policy – to manage users' desktop environments. These scenarios are intended to be starting points from which you can develop settings tailored to your environment. These scenarios illustrate of the range of features manageable by using Group Policy. This white paper includes coverage of Windows Server 2003 and the Group Policy Management Console (GPMC).

Introduction

Group Policy Overview

The IntelliMirror® management technologies provide Active Directory-based change and configuration management of user and computer settings on computers running a member of the Microsoft® Windows® Server 2003 or Microsoft Windows® 2000 families of operating systems, or the Microsoft® Windows® XP Professional operating system. Group Policy provides the infrastructure for IntelliMirror by allowing you to specify settings for registry-based policy, security, software installation, scripts, folder redirection, Remote Installation Services, and Internet Explorer maintenance.

The Group Policy settings that you create are contained in a Group Policy object (GPO). By linking a GPO to selected Active Directory Service containers – sites, domains, and organizational units (OUs) – you can apply these settings to the users and computers in those Active Directory containers. Group Policy inheritance and precedence determine where and how you link GPOs. By default, options set in GPOs linked to higher levels of Active Directory containers – sites, domains and OUs – are inherited by all containers at lower levels, though inheritance does not occur across domains. Because lower-level GPOs apply last, they override higher-level GPOs and can provide lower-level OUs with a different set of Group Policy settings.

To manage GPOs, you use the Group Policy Management Console (GPMC) or its scripting interfaces. GPMC is a new tool, released at the launch of Windows Server 2003. It is important to note, however, that GPMC is a very effective tool for managing Group Policy in Windows 2000 domains and, with the exception of a few new features, does not require Windows Server 2003 to be running in your environment.

It is assumed that the reader of this white paper has an understanding of basic Group Policy principles.

About the Common Desktop Scenarios

Group Policy is a rich and flexible technology providing the capability to efficiently manage a large number of computer and user accounts through a centralized, "one-to-many" model. With this flexibility comes the potential for complexity. For example, Group Policy in Windows Server 2003 exposes almost 1,000 configurable settings. This can initially appear a daunting task – how does the administrator assess the relative importance of these settings, and what features enabled by Group Policy might be considered when deploying a solution?

This Common Desktop Scenarios white paper provides a structured, tested, and consistent set of pre-packaged GPOs and associated documentation, with the goal of lowering the "barrier of entry" for those assessing Group Policy.

The scenarios described in this white paper provide a good starting point from which you can begin evaluating and understanding Group Policy. By implementing these scenarios in a test environment, you should be able to:

- Quickly understand the scope of Group Policy and consider how to use a wide number of settings.
- List some of the important solutions enabled by Group Policy.
- Gain familiarity with some of the new functionality introduced with GPMC, particularly the backup/import of GPOs and Group Policy reports.
- Reach conclusions about how to implement Group Policy in your production environment.

Note The approach taken in this white paper has significant differences to previously released versions. These differences primarily reflect the new features available in GPMC and are described fully later in this document.

How to Use the Common Desktop Scenarios

The GPOs provided with this white paper were created using the Backup capability of GPMC. This new tool provides a single entry point for management of Group Policy in your environment and can manage both Windows 2000 and Windows Server 2003 domains. You can download the Group Policy Management Console (GPMC) from the Microsoft Web site. You can import these GPOs into your environment as a first step toward implementing the common scenarios. The details of each scenario are described in this document and further documented in a spreadsheet, as well as in HTML-based reports generated using the Group Policy Reports capability of GPMC for each of the GPOs.

In many cases, a scenario might deliver a specific computer/user configuration that is close to the required environment for your production environment and might not need significant changes. In other cases, it might be necessary to substantially modify the GPOs provided to ensure alignment with your business goals.

The GPOs can be implemented and validated in a test environment, modified (where necessary) to map to your specific needs, and – after appropriate testing – copied or imported into a production environment.

The mere act of importing the scenario GPOs into your domain has no immediate impact on computers or users. To affect target accounts, the GPOs must be linked to an appropriate Scope of Management (SOM) – a site, domain, or OU which you want to manage using these GPOs. This means that the reader with limited test resources might choose to import the GPOs into a production environment and – before applying to a set of computer or user accounts – link to a SOM that has a more limited number of accounts, effectively forming a controlled pilot program. After completing the pilot program and testing any required changes, the GPOs can be linked to broader SOMs. This approach is most effective when computers and users are targeted through OUs, and the majority of this white paper assumes that this is the targeting mechanism used (unless noted otherwise).

Overview of the Scenarios

The following is a list of the scenarios along with typical examples.

Lightly Managed

Use this scenario for power users or developers who require considerable control over their computer. You can also use this scenario in an organization where tightly managed desktops are not acceptable to users or where desktop management is highly delegated. Along with the other scenarios, the Lightly Managed scenario supports increased security and promotes consistency of user experience, both of which can be beneficial even where a tightly managed desktop is not appropriate.

The Lightly Managed scenario has the following characteristics:

- Is the least managed of all of the scenarios.
- Allows users to customize most settings that affect them but prevents them from making harmful system changes.
- Includes settings that reduce help desk costs and user downtime.
- Supports *free-seating*, which means users can sit down at any computer and access all their resources, applications, and data as if they were sitting at their own computer. This also simplifies your file-backup scenarios, because users' files are all stored on designated file servers.
- Typically has a core set of applications assigned to either the user or the computer, which are always available. Users can also install applications that have been published for them, which they can choose to install.

Mobile

The Mobile scenario is relevant to mobile/laptop computers and their users. This scenario pays particular attention to the disconnected user who frequently needs to work offline and occasionally resynchronize with the corporate network.

The Mobile scenario has the following characteristics:

- Can be used by users who are away from the office most of the time, who log on using low-speed, dial-up links, but who also occasionally log on using high-speed network links.
- Can also be used by users who are away from the office only occasionally and who log on by using remote access or remote network links.
- Allows users continuous access to their data and configuration settings whether the computer is connected to or disconnected from the network.
- Partially supports free-seating (can optionally support full free-seating) to facilitate centralized data backup and to enable users to access important data and settings from additional computers.
- Allows users to disconnect from the network without logging off or shutting down.

Multi-User

Use this scenario in a university computer laboratory or library where users can save some customizations, such as desktop wallpaper and color scheme preferences, but are not allowed to change hardware or connection settings.

The Multi-User scenario has the following characteristics:

- Allows basic customization of the desktop environment. Users can save desktop configurations, but they cannot customize network, hardware, and system settings.
- Supports free-seating; users can log onto any computer and get their data and settings. No cached state is maintained on the computer when they leave.
- Users have restricted write access to the local computer and can only write data to their user profile and to redirected folders.
- Has a set of applications that are always available (assigned), as well as applications that can be installed and removed as necessary (published).
- Is highly secure.

AppStation

The AppStation scenario is used when you require highly restricted configurations with only a few applications. Use this scenario in vertical applications such as marketing, claims and loan processing, and customer-service scenarios.

The AppStation scenario has the following characteristics:

- Allows minimal customization by the user.
- Allows users to access a small number of applications appropriate to their job role.
- Does not allow users to add or remove applications.
- Supports free-seating.
- Provides a simplified desktop and Start menu.
- Users have restricted write access to the local computer and can only write data to their user profile and to redirected folders.
- Is highly secure.

TaskStation

Use the TaskStation scenario when you need the computer dedicated to running a single application, such as on a manufacturing floor, as an entry terminal for orders, or in a call center.

The TaskStation scenario is similar to the AppStation scenario, with the following changes:

- It has only one application installed, which automatically starts when the user logs on.
- No desktop or Start menu is present.

Kiosk

Use this scenario in a public area, such as in an airport where passengers check in and view their flight information. Because the computer is normally unattended, it needs to be highly secure.

The Kiosk scenario has the following characteristics:

- Is a public workstation.
- Runs only one application.
- Uses only one user account and automatically logs on. The system automatically resets to a default state at the start of each session.
- Runs unattended.
- Is highly secure.
- Is simple to operate, with no logon procedure.
- Does not allow users to make changes to the default user or system settings.
- Does not save data to the disk.
- Is always on (the user cannot log off or shut down the computer).

A workstation that uses the Kiosk scenario is similar to a TaskStation, but users are anonymous in that they all share a single user account that automatically logs on at computer startup. This is achieved by modifying the Kiosk machine in a manner described later in this document. Users cannot customize their environment and user states are not preserved.

Although user sessions are usually anonymous, a user can log on to an application-specific account, such as to a Web-based application through Internet Explorer (assuming Internet Explorer is the "kiosk application" launched at startup).

The dedicated application could be a Line of Business (LOB) application, an application hosted in Internet Explorer, or another application, such as one available in Microsoft Office. The default application should not be Windows Explorer or any other shell-like application. Windows Explorer allows more access to the computer than is appropriate for a Kiosk computer. Be sure the command prompt is disabled and Windows Explorer cannot be accessed from any application you use for this purpose.

Applications used for kiosk scenarios should be carefully checked to ensure they do not contain "back doors" that allow users to circumvent system policies. For example, they should not allow users access to applications that access the file system. Ideally, you should only use applications that comply with The Application Specification for Windows 2000, are Certified for Windows, and that check for Group Policy settings before giving users access to prohibited features. For more information, see the "The Application Specification for Windows 2000" at the Microsoft Web site. Older applications will not normally be Group Policy-aware, so try to disable any features that allow users to bypass administrative policy.

The registry entries **Run** and **RunOnce** are disabled in the Kiosk scenario through associated policy settings.

> **Important** Applications that use the **RunOnce** entry to finish an installation or upgrade will fail when the **Do not process the Run Once list** Group Policy setting is enabled.

Please see the "Scenario Comparison" table in Appendix A for a comparison of features across scenarios.

Understanding and Using the Scenarios

The scenarios are implemented through the use of GPOs provided in the .MSI package with this white paper. By linking appropriate combinations of GPOs to OUs for computer and user settings, you can be implement each of the scenarios in your environment. This section describes the general characteristics of the GPOs and how they can be linked to OUs.

How the Scenarios Are Designed

Separate GPOs for Computer and User Policy Settings

Most scenarios are directly associated with two GPOs – one for computer configuration and another for user configuration. For example, the **Lightly Managed** scenario is directly associated with the **Lightly Managed (Machine)** GPO for computer configuration and the **Lightly Managed (User)** GPO for user configuration. This approach simplifies troubleshooting, makes the application of GPOs somewhat more intuitive, and is a Group Policy best practice.

Base GPOs for Common Settings

Many of the scenarios share a considerable number of policy settings and associated values. This version of the Common Scenarios white paper introduces the concept of the "base GPO," which is more relevant in a real-world, production environment than the monolithic GPOs packaged with previous versions.

The base GPOs (two each for **Lightly Managed** and **Highly Managed**) contain Group Policy settings common to other "child" scenarios (see the next section). The GPOs for these child scenarios extend these base GPOs by enabling, disabling, or changing the values of a relatively small number of settings tailored to their specific requirements.

Scenario/GPO Relationships

To implement any of the scenarios, the GPOs must be linked to Scope of Management (SOM) containers - a site, domain or OU. Most of the GPOs packaged with the white paper are designed to be linked to OUs, rather than sites or domains.

> **Note** The GPOs provided are intended to assemble common policy settings and their relationships are technically independent of any OU hierarchy you might implement. For scenarios that require more than one GPO you might either link separate GPOs in a chain of OUs (Group Policy inheritance) or link multiple GPOs to a single OU (Group Policy precedence) – these options are covered in more detail later in this white paper.

The following diagram illustrates the relationships between GPOs.

Machine Policy GPOs

Lightly Managed

Mobile – No differences from Lightly Managed GPO, so no *machine* GPO exists for Mobile

Highly Managed

AppStation - No differences from Highly Managed GPO, so no *machine* GPO exists for AppStation

Multi-User – GPO provided

TaskStation – GPO provided

Kiosk – GPO provided

User Policy GPOs

Lightly Managed

Mobile – GPO provided

Highly Managed

AppStation - GPO provided

Multi-User – GPO provided

TaskStation – GPO provided

Kiosk – GPO provided

If your browser does not support inline frames, click here to view on a separate page.

For example, the AppStation scenario shares many of its Group Policy settings with the Highly Managed GPOs, as follows:

- On the machine side of policy for the AppStation scenario, the settings are identical in all regards to that of the Highly Managed scenario and, as such, there is no AppStation-specific GPO for machine policy settings. To implement machine settings appropriate to the AppStation scenario, it is only necessary to ensure that the Highly Managed (Machine) GPO is linked to a SOM containing the target machines.
- By comparison, some differences exist for user policy settings between Highly Managed and AppStation. For this reason, a GPO is provided for the user policy settings in the AppStation scenario, which contains differences from the Highly Managed user GPO. To implement user settings for the AppStation scenario, it is necessary that both the Highly Managed (User) and AppStation (User) GPOs are linked – directly or otherwise - to a SOM containing the target users. This can be achieved through either Group Policy inheritance or precedence when GPOs are linked to the same container.

The AppStation scenario is an exception - most scenarios are implemented through two GPOs – one for computer configuration and another for user configuration (the AppStation scenario uses only user configuration). In addition, most are associated with the base scenarios, **Lightly Managed** and **Highly Managed**, through Group Policy inheritance and/or precedence. With these issues in mind, the GPOs listed in Table 1 are effective for each scenario.

Table 1 Scenario GPOs

Scenario Name	Base GPO Name	Scenario-Specific GPO Name
Lightly Managed		
Computer	Lightly Managed (Machine)	N/A (no changes from base)
User	Lightly Managed (User)	N/A (no changes from base)

Mobile		
Computer	Lightly Managed (Machine)	N/A (no changes from base)
User	Lightly Managed (User)	Mobile (User)
AppStation		
Computer	Highly Managed (Machine)	N/A (no changes from base)
User	Highly Managed (User)	AppStation (User)
Multi-User		
Computer	Highly Managed (Machine)	Multi-User (Machine)
User	Highly Managed (User)	Multi-User (User)
TaskStation		
Computer	Highly Managed (Machine)	TaskStation (Machine)
User	Highly Managed (User)	TaskStation (User)
Kiosk		
Computer	Highly Managed (Machine)	Kiosk (Machine)
User	Highly Managed (User)	Kiosk (User)

Purpose of the Highly Managed GPOs

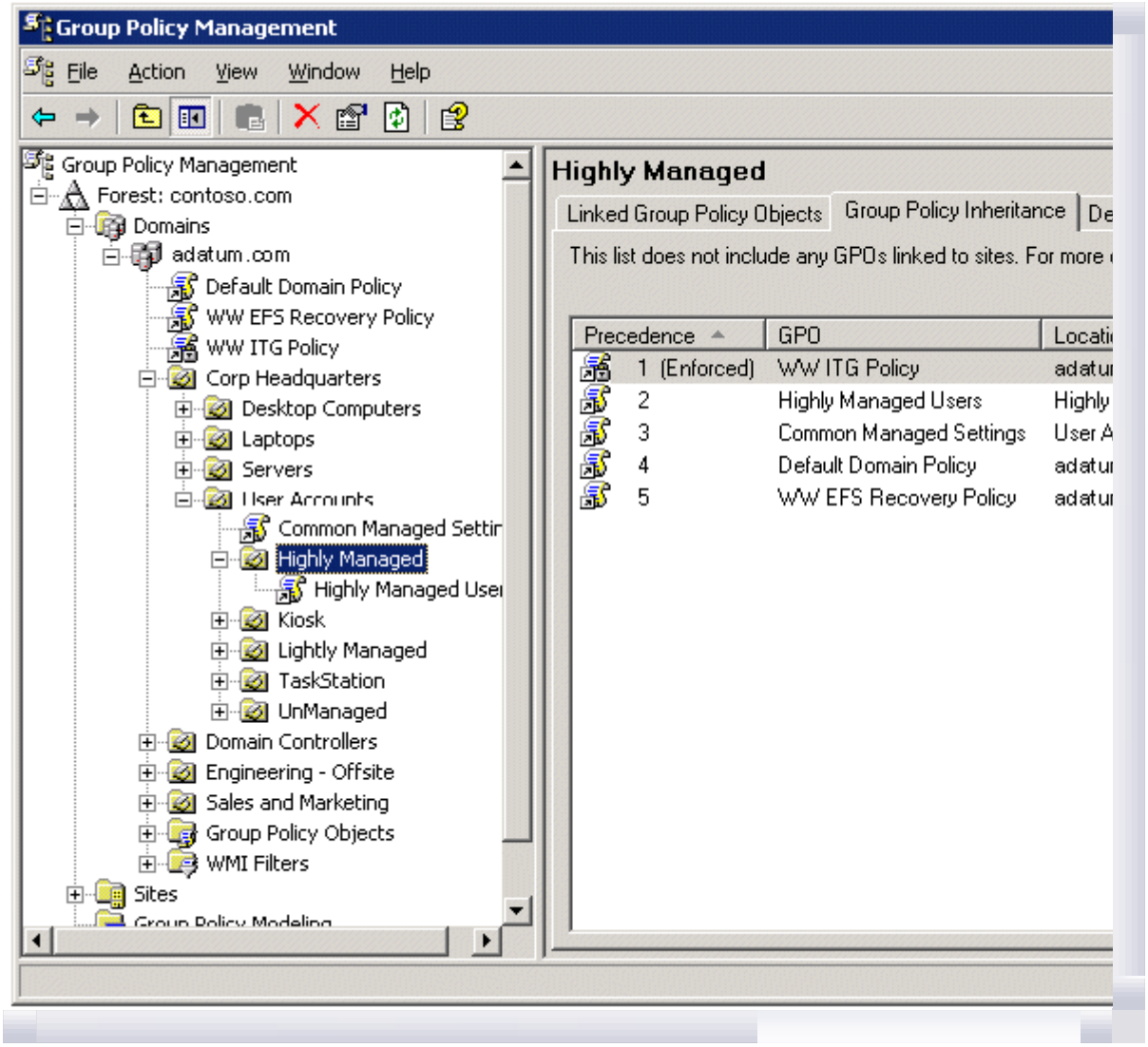
The Highly Managed scenario is a virtual scenario – its purpose is to provide a set of settings common to other scenarios (specifically, the Multi-User, AppStation, TaskStation, and Kiosk scenarios). As such, the Highly Managed GPOs are not intended (or tested) to operate in their own context. Instead, the other scenarios are enabled by ensuring that the Highly Managed GPOs affect accounts through Group Policy inheritance or precedence. In short, no computer or user account should exist in OUs designed specifically for a Highly Managed scenario.

Creating a Test Environment

In previous versions of this white paper, a considerable number of scripts were necessary to create and configure the GPOs provided with the white paper. With the advent of GPMC – and specifically its Import functionality – these scripts are no longer necessary. The GPOs have been backed up and provided with this white paper, which allows you to import them directly into your environment.

To assist in creation of this environment, a script included with GPMC, CreateEnvirommentFromXML.wsf, is used to create a hierarchy of OUs, create GPOs, and link the GPOs to the OUs appropriately. A script called CreateCommonScenarios.cmd is provided with this white paper to call this script with the appropriate parameters.

After successfully running the script, you will have OUs and linked GPOs configured similar to those shown in Figure 1.



If your browser does not support inline frames, click here to view on a separate page.

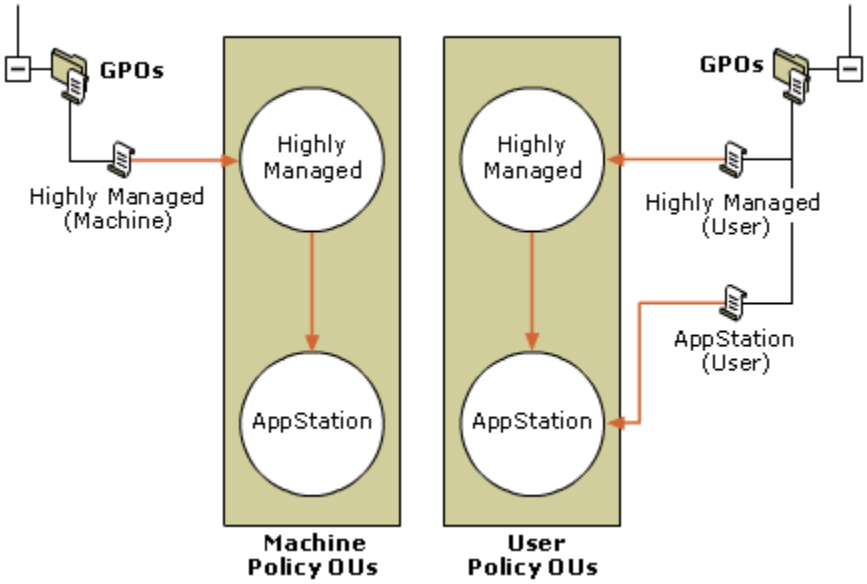
Figure 1 GPMC Screenshot of Scenario GPOs

Linking GPOs to OUs to Create Scenarios

There are two broad approaches available for using the GPOs to create scenarios in your environment. To illustrate these options, the AppStation scenario is used, which is an extension of the Highly Managed scenario (many of the AppStation settings are defined by the Highly Managed GPOs).

Linking GPOs to a Hierarchy of OUs (Group Policy Inheritance)

With this option, create an OU hierarchy where the AppStation OUs (one each for Computer and User accounts) are children to the Highly Managed OUs. Figure 2 illustrates how the GPOs would be linked.



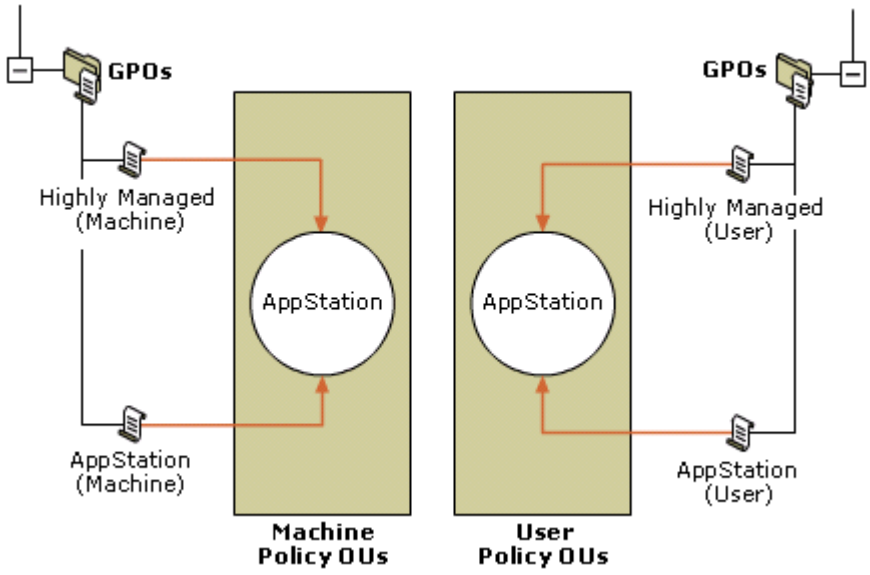
If your browser does not support inline frames, click here to view on a separate page.

Figure 2 Linking Scenario GPOs Using Inheritance

Note that because the machine policy for the AppStation scenario does not differ from that of the Highly Managed scenario, no AppStation (Machine) GPO exists. Technically, it is not necessary to place AppStation affected computers in the AppStation OU because they might reside in the Highly Managed OU and be affected by the same settings. However, for clarity and to easily accommodate the potential for future differences between Highly Managed and AppStation GPOs (on the machine side), there might be value in retaining the AppStation OU. After the appropriate GPOs are linked to these OUs, the computer and user accounts would be moved into the appropriate AppStation OUs.

Linking GPOs Directly to OUs (Group Policy Precedence)

In this approach, you only create two OUs (one each for Computer and User accounts). For each, both the Highly Managed and AppStation GPOs are linked directly to the OU. This is illustrated by Figure 3.



If your browser does not support inline frames, click here to view on a separate page.

Figure 3 Linking Scenario GPOs Using Precedence

After linking the GPOs, it is important to ensure that the precedence of the GPOs is such that the AppStation GPOs take priority over Highly Managed GPOs. GPMC provides a simple and intuitive interface for enforcing this

precedence. This is achieved by selecting a container, such as an OU, in the GPMC tree view and using the **Linked Group Policy Objects** tab in the right pane to adjust ordering of GPOs linked to that container.

After creating the OUs and GPO links, move the computer and user accounts into the appropriate AppStation OUs.

Differences with Earlier Versions of the Common Scenarios

An earlier version of this white paper focused on Windows 2000 domains. Since that time, a number of Group Policy enhancements have become available, most notably GPMC. The following areas differ between the Windows 2000 and Windows Server 2003 common scenarios.

Base GPOs

As described earlier, the base GPOs (Lightly Managed and Highly Managed) are a new concept in this version of the white paper.

GPMC-Based GPO Deployment

GPMC provides a significant number of features – Backup, Import, Copy and so on – that significantly simplify managing GPOs. This white paper takes full advantage of these new capabilities by providing backed-up copies of GPOs which can easily be imported into your test environment.

Environment Creation Script (CreateCommonScenarios.cmd)

GPMC includes a series of example scripts which illustrate the automation of common Group Policy operations. One such script is CreateEnvironmentFromXML.wsf which uses an XML file to recreate an environment (typically OUs, GPOs, and GPO links) in your domain. An XML file (CommonScenarios.xml) is included with this white paper to facilitate the use of the script to largely automate the creation of your environment.

A command file – CreateCommonScenarios.cmd – is packaged with this white paper to streamline the installation of a sample environment.

It is important to note that while the script must be run from either a Windows XP or Windows Server 2003 computer, the domain in which it creates the sample environment can be either a Windows 2000 or Windows Server 2003 domain.

Group Policy Reports Documentation

GPMC provides a new way to report the contents of GPOs – Group Policy Reports. These are HTML reports that document all aspects of each GPO. Reports for each of the GPOs are provided with this CommonScenarios.msi as a documentation tool. When you make changes to the GPOs, GPMC can help you document the changes by using Group Policy Reports.

New Group Policy Settings

Windows Server 2003 delivers a number of new settings not just for that operating system but also for Windows XP Professional. Many of these settings are used in the updated scenario GPOs.

Consolidated Spreadsheet of Group Policy Settings

The Windows 2000 and Windows XP versions of the scenarios installed one spreadsheet for each scenario. This revised version includes a consolidated spreadsheet – CommonScenarios.xls - and each scenario is listed in a separate column. Using Microsoft Excel column filtering, this can be a helpful way to quickly compare GPO settings.

Deploying the Scenarios

This section describes the steps necessary to implement the scenarios. As a prerequisite, it is assumed that you have created a fully operational Active Directory domain and have validated the integrity and operation of the underlying DNS infrastructure. Group Policy is dependent on a well-configured, reliable Active Directory environment.

The following steps are necessary to implement the scenarios:

1. Run the CommonScenarios.msi package to copy the GPOs, scripts, and associated documentation (such as this white paper) to your administrative workstation.
2. Create an appropriate OU environment.
3. Use GPMC to import the scenario GPOs into your environment.
4. Link the GPOs to OUs.

Two options are available to cover steps 2 - 4:

1. Automatically create an OU hierarchy, GPOs, and GPO links using a script provided with this white paper (CreateCommonScenarios.cmd).
2. Manually implement each step (create OUs, import GPOs, and so on). This is a more flexible approach but will take a little longer to implement.

On completion of these steps – and regardless of the approach taken (scripted or manual) - you will perform the following steps to complete configuration and testing of the scenarios:

- Configure specific scenario features (see the "Configuring Specific Features" section)
- Create Computer and User accounts for use within the scenarios.
- Test scenarios.

Test and Production Environment Considerations

Before installing the scenarios into your environment (described in the next section), you should understand the options available for testing. There are two primary ways in which you can incorporate the GPOs into your environment for testing; by linking the GPOs to test OUs in your production domain or by using a separate test domain (either in the same or a different forest).

Using Test OUs in Your Production Environment

Where a separate test domain (the preferred approach) is not feasible, the scenario GPOs can be imported to a production environment and linked to OUs created in that domain specifically for test purposes. These OUs should be well-segmented from those used for regular production purposes. The benefit of this approach is that you need not create infrastructure to support a separate domain (domain controllers, networking, and so on). The disadvantage is that misconfiguration of accounts, GPOs, or GPO links can directly affect the production environment.

Using a Separate Test Domain

With this approach, you use a domain that is separate from that of your production environment (trusts may or may not exist between the test and production environments). This can allow you to run a more realistic test by modeling the test domain on your existing domain, so you can test domain-wide settings and other interactions as needed. A significant benefit of using this approach is that the impact of errors through inappropriately linked or filtered GPOs is significantly less than is evident in a production environment. The primary drawback of this approach is that you need to set up domain controllers and other supporting infrastructure (networking, DNS, and so on) that implements the test domain. If possible, use this approach.

Cross-Forest and Cross-Domain Considerations

The two domains used for test and production purposes might or might not be in the same forest. Further, if they are in separate forests, a forest trust might or might not exist, because a forest trust can only be established between Windows Server 2003 forests.

Where a trust exists between the domains (for example, where the test and production domains are in the same forest and the default transitive trusts exist), an administrator with the appropriate rights in each domain can use GPMC to copy GPOs between domains. This can be as simple as dragging and dropping GPOs between domains using the GPMC graphical user interface. Note that if the GPOs in your test environment include security principals (for example, group names) or UNC paths (for example, when specifying your Folder Redirection parameters), migration tables will help you handle any changes you might need to make across domain boundaries. The Migration Table Editor – part of GPMC – provides a simple interface for editing migration tables. For more information, see the "Migrating GPOs Across Domains with GPMC" white paper at the Microsoft Web site.

Where a trust does not exist, the follow options are available:

- Create your OU structure and use the GPMC **Import** function to create new GPOs in the production environment. The backup from which you import GPOs might be that provided with this white paper or – if you have already tailored the GPOs to your needs – from a backup set that you created.
- Use the CreateEnvironmentFromXML.wsf script (a sample script installed with GPMC – see GPMC Help for more information) to create the default OU environment in your production domain and, if necessary, rename OUs and GPOs to better reflect naming/structural conventions in your production environment.
- Use the Stored User Names and Password feature of Windows XP to store credentials for a user in a non-trusted domain.

Test Environment Recommendation

Where adequate resources are available (domain controllers, networking infrastructure, and so on), it is strongly recommended that the GPOs are imported into a test domain. Using a separate domain provides you with a relatively safe environment in which to assess the GPOs and also allows more flexibility in regards to testing domain-wide Group Policy settings.

Installing the Common Scenario Scripts and GPOs

Packaged with this white paper is a series of scripts and GPO backups that form the basis of your deployment of the common scenarios. The CommonScenarios.msi file installs these components – including the white paper itself – into the "%programfiles%\Microsoft\Group Policy Common Scenarios" folder and creates menu options on the Start Menu for some of these components (for example, a link to the white paper and its associated spreadsheet). After running this package, the following directory structure is created:

%programfiles%\Microsoft\Group Policy Common Scenarios

\Documentation (Common Scenarios white paper and spreadsheet)

\GPO-Backups (GPMC-originated backups of the scenario GPOs)

\GPO-Reports (GPMC-originated reports for each GPO in HTML format)

\Environment (XML representation of example OU structure for scenarios)

\Scripts (scripts used to create example environment)

It is assumed that the computer on which this directory is created already has GPMC installed (the supplied scripts include calls to GPMC scripting interfaces). GPMC requires either Windows XP Professional or Windows Server 2003 (see GPMC documentation for further details about requirements). The directory in which the common scenarios files are installed is hereafter referred to as the **<installdir>**, (typically %programfiles% \Microsoft\Group Policy Common Scenarios).

In addition to installing the files, a **Group Policy Common Scenarios** menu on the user's **Start/Programs** menu is created. This menu provides access to the white paper, the spreadsheet, a shortcut to the Group Policy Reports directory, and a command line configured to start in the %programfiles%\Microsoft\Group Policy Common Scenarios\Scripts directory.

After you run the installer, you must import the GPOs associated with the scenarios into your domain. There are two options to achieve this: a quick method to create an overall common scenarios test environment (a sample OU structure, GPOs, and GPO links), and a more manual process where creation of OUs, GPOs and GPO links are separate steps.

Deployment Option 1: Quick Setup Using CreateCommonScenarios.cmd

A script is included to assist with installing a representative OU structure, GPOs, and GPO links into your environment. This script is named **CreateCommonScenarios.cmd** and is installed into the **<installdir>\Scripts** directory. The script calls a sample script installed by GPMC – (CreateEnvironmentFromXML.wsf) which is installed in the **%programfiles%\GPMC\Scripts** directory.

CreateCommonScenarios.cmd initiates the following tasks:

- Creates an example OU hierarchy, representing locations for computer and user accounts
- Creates the scenario GPOs, including default permissions
- Links the scenario GPOs to the appropriate OUs

Running CreateCommonScenarios.cmd

To run the script, do the following:

1. Click **Start**, click **Programs**, click **Group Policy Common Scenarios**, and then click **Common Scenarios Scripts Command Prompt**.
2. From the command prompt, type **CreateCommonScenarios**, and then press **Enter**.

Results of Running the Script

By running the script against your domain, you create a self-contained test environment with the appropriate OUs and GPOs linked to those OUs. Note that might still need to create or edit GPOs linked at the domain level, especially where account policy settings are modified but this is specific to your domain and outside the scope of the scenario GPOs. To avoid potential conflict with your existing environment, no domain-level policy settings are implemented through the scenarios.

Modifying the Behavior of CreateCommonScenarios.cmd

The CreateCommonScenarios.cmd script is a wrapper for the CreateEnvironmentFromXML.wsf script, which is installed with GPMC. In some cases you might need to change the default behavior of this script. For example, if you want to modify the domain controller against which the script is run. Any parameters passed directly to the CreateCommonScenarios.cmd script are passed on to the CreateEnvironmentFromXML.wsf script. For more information about the parameters supported by the CreateEnvironmentFromXML.wsf script, see GPMC Help.

Deployment Option 2: Manual Deployment Steps Using the GPMC GUI

This method is more time-consuming but allows you greater control over your OU design and GPO links.

Create an Appropriate OU Test Environment

You need to create OUs for the users and computers you want to manage within your domain. If your environment requires a more complex OU structure than that described in this document, refer to the "Designing the Active Directory Logical Structure" chapter of the *Designing and Deploying Directory and Security Services* book in the *Windows Server 2003 Deployment Kit*. For more information, see the Microsoft Web site.

Use GPMC to Import GPOs

The GPOs provided with this white paper can also be imported into your environment manually, using a GPMC sample script, as follows:

cscript %programfiles%\gpmc\scripts\ImportAllGPOs.wsf <installdir>\GPO-Backups

Note "Cscript" can be omitted if you have previously configured cscript as the default scripting environment for your machine. More specifically, if you have previously run:

cscript //hh:cscript

this will set cscript as the default environment, in which case the following command would work:

%programfiles%\gpmc\scripts\ImportAllGPOs.wsf <installdir>\GPO-Backups

The ImportAllGPOs.wsf script will result in all the GPOs provided in the <installdir>GPO-Backups directory being created in your environment and their settings imported. On completion of this step you will then need to link the GPOs to the OUs you have created.

The same result can be achieved through the GPMC MMC-snap-in, do the following:

1. Create empty GPOs (no policy settings) in your environment by right-clicking the Group Policy Object node and selecting **New** from the context menu. Create one GPO for each of the Common Scenario GPOs, using the names documented in the "How the Scenarios Are Designed" section of this white paper.
2. In GPMC, right-click each GPO and then click **Import**. Go to the <installdir>\GPO-Backups directory and import policy settings from the appropriate backed-up GPO.

Link GPOs to OUs

To apply the settings of a GPO to the users and computers of a domain, site, or OU, you need to add a link to that GPO. You can add one or more GPO links to each domain, site, or OU by using GPMC. Keep in mind that creating and linking GPOs is a sensitive privilege that should be delegated only to administrators who are trusted and understand Group Policy.

To link an existing GPO

1. In GPMC, right-click a domain or OU, and then click **Link an Existing GPO here**.
2. In the **Select GPO** dialog box, click the GPO which you want to link, and then click **OK**. In the left pane, the GPO is displayed beneath the domain or OU to which it is linked.

You can simultaneously link multiple GPOs to an Active Directory object by holding down the **CTRL** key while selecting GPOs.

Post-Installation Configuration

After you have created an environment in which you wish to host your scenario GPOs – either automatically by using the CreateCommonScenarios.cmd script or manually – you must carry out a number of additional steps to finalize the configuration of certain aspects of your environment. This section describes each of these steps.

Configure Scenario Features

Configuration for Roaming User Profiles and Redirected Folders require you to enter UNC paths specific to your environment (into the user objects within the Active Directory and to the appropriate GPOs, respectively). See

the "Configuring Specific Features" section for more details.

Create Computer and User Accounts

Using the Active Directory Users and Computers snap-in, create a sufficient number of user accounts to allow you to test each of the scenarios.

It is important to note that any one scenario is implemented through the combination of user and computer accounts, each of which should be affected by GPOs associated with the same scenario. For example, to achieve the TaskStation scenario, a user in the CommonScenarios/Users/TaskStation OU might log on to a computer in the CommonScenarios/Computer/TaskStation OU. Any "cross matching" of user and computer scenarios is untested and might cause unforeseen results.

Migrating the Scenarios to a Production Environment

After testing and potentially customizing the Common Scenario environment, you might wish to move into a production environment. The following approaches can be used:

- **Manual creation in production environment.** With this approach, you create each of the OUs from either GPMC or Active Directory Users and Computers. The GPOs are either copied (if a trust exists between the source and target environments) or created/imported (where file-based GPO backups are used). Then link the GPOs to the OUs and move the users/computers into the OUs as appropriate.
- **Use the CreateXMLFromEnvironment and CreateEnvironmentFromXML scripts.** The CreateXMLFromEnvironment script – included with GPMC as a sample script – allows the administrator to create an XML file representing all the policy-related objects (OUs, GPOs, and GPO links). Optionally, you can specify a starting OU rather than the entire domain. The script creates a representation of the OU and its linked GPOs in the specified XML file. This file can then be used by the CreateEnvironmentFromXML script to create a mirrored OU structure and associated GPOs and links in the target environment. When planned carefully, these two scripts can help create an initial framework in your production environment.

For more information about managing GPOs across domains, see the "Migrating GPOs Across Domains with GPMC" white paper at the Microsoft Web site.

Removing the Scenarios from Your Environment

Removing the scenarios from your environment is a relatively simple task. Use the following steps to remove them:

- Move computer and user accounts that you need to retain into alternative OUs, as necessary. Reconfigure user objects, as appropriate, to modify Roaming User Profile paths.
- Validate that each scenario GPO is linked to the expected SOMs (using the **Scope** tab within GPMC). This step is important to ensure that no unexpected cross-domain or other links exist.
- Delete each scenario GPO.
- Validate that the scenario OUs are empty, and then use Active Directory Users and Computers to remove those OUs.
- If you added the domain GPO, validate, unlink, and delete that GPO as appropriate.

If you have used the CreateCommonScenarios.cmd script to create your sample environment, then the CreateEnvironmentFromXML.wft sample script was called implicitly. This script has an **/undo** switch that removes the environment described by the XML file passed as an argument. See GPMC online Help for further details on this script.

In addition to these issues, please refer to the section "Switching Between Scenarios" for more factors that might also be relevant when removing scenarios (for example, "tattooing" the registry with security settings).

Configuring Specific Features

This section describes the various features configured in the common scenarios GPOs.

Roaming User Profiles

A user profile is a group of settings and files that define the user's environment. A profile includes program items, screen colors, network connections, window sizes and positions, and so on. Roaming User Profiles (RUP) enable the server-based storage of user profiles, which means that users can move between computers and see an identical environment. The RUP is downloaded to the user when s/he logs on and, by default, is stored back on the server when the user logs off. This feature is one component of the concept of "free-seating" – the capability for users to roam between computers yet maintain an identical environment.

Scenarios in Which Roaming User Profiles are Used

Due to the order in which logon, profile creation/loading, and the application of GPOs occurs, it is not possible to specify the location of a user profile using Group Policy. For this reason, specifying the user profile location is a distinct and separate step from the application of GPOs. Therefore, to ensure that a user is configured correctly, it is important to move that user into the appropriate OU and, additionally, configure the user object as described below.

The common scenarios leverage Roaming User Profiles as follows:

- **Used:** Lightly Managed, Highly Managed, Multi-User, AppStation, and TaskStation
- **Optionally Used:** Mobile User
- **Not Used:** Kiosk

Roaming User Profiles Configuration Steps

For the purposes of illustration, this document assumes a server named **CommonServer** is available to store user profiles. The following steps are necessary to create a share for user profiles and configure user accounts appropriately.

1. On the CommonServer computer, create a folder called ***profiles***.
2. Share this folder as ***profiles$***.
3. Set share permissions to **Full Control** for the **Everybody** group (security will be enforced by NTFS permissions when the user profile folders are created).
4. Ensure that caching for this folder is disabled (only use caching for folders where you do not store profiles).
5. For each account for which Roaming User Profiles is required, set the profile path in the user object to \\CommonServer\profiles$\%user name% (the Active Directory Users and Computers MMC snap-in is the most common way to edit this parameter). At the time the user profile is created, the %user name% environment variable will be resolved to the name of the user.

Roaming User Profile Notes

It is a best practice to allow the user-specific accounts (in the **Profiles** folder) to be automatically created at the time the user profile is first established. This ensures that the appropriate set of NTFS permissions and ownership are set on the folder.

> **Important:** Roaming User Profiles have their own caching mechanism, which can interfere with Offline Files synchronization and can lead to unexpected behavior and loss of data. Therefore, make sure that caching is disabled for the shares where you store profiles.

Redirected Folders

Folder Redirection allows the contents of a folder in the user's profile to be redirected to a location on the network. For example, you can move My Documents, which is typically part of the user's profile and cached on the local drive, to a folder in the user's home directory on the network. Enabling this feature is useful because the My Documents and Application Data folders often contain large amounts of data. Enabling Folder Redirection helps speed up logon and logoff time because the contents of the redirected folders are not copied along with the rest of the user profile.

In most cases when you use Folder Redirection, you will combine it with Offline Files so that users can access cached copies of the redirected folders when disconnected from the network. In fact, with Windows XP, all redirected folders are also cached locally by default (this is not the case with Windows 2000).

If you have a high volume of users that use a single computer, consider enabling the **At logoff, delete local copy of user's offline files** Group Policy setting to prevent the local hard drive from filling up with cached files from multiple users. This setting is located under Computer Configuration\Administrative Templates\Network\Offline Files.

> **Caution** You should use this policy setting with caution. If a user has been working offline and has not synchronized their changes, their changes will be lost at logoff when their offline files are deleted.

When you implement Folder Redirection, the destination folders are automatically created, and security is configured on these folders automatically. You can change the security of redirected folders by checking or clearing **Grant the user exclusive rights to *foldername,*** which is located in this path: User Configuration\Windows Settings\Folder Redirection*foldername* - **Settings** tab.

For example, if you redirect the My Documents folder to \\CommonServer\Docs*%User name%*, do not create a **User Name** folder in advance. If the folder exists in advance and the current user is not the owner of the folder and its contents, the redirection process fails. If the folder does not exist prior to folder redirection, however, it is created and the user is made the owner of that folder. If you use the **Create a folder for each user under the root path** option in the **Target Folder Location** dropdown box, Folder Redirection

automatically appends %user name% to the root path you specify.

Important: If you must create the folder in advance, ensure that the user is the owner of the folder and its contents. To change the ownership of a file or folder, use Windows Explorer or the Subinacl.exe utility that is available on the *Microsoft Windows Server 2003 Resource Kit* companion CD. For more information, see the Microsoft Web site.

Note: When Group Policy Folder Redirection settings go out of scope, by default, they leave the redirection in place. The **Settings** tab has an option that allows you to redirect the folders to the local computer; however, avoid using this option. The default setting is the safest because no data is moved when a Folder Redirection policy falls out of scope. Any new Folder Redirection policy then redirects as appropriate.

Scenarios in Which Folder Redirection is Used

The common scenarios leverage Folder Redirection as follows:

- **My Documents and Application Data Redirection:** Lightly Managed, Highly Managed, Mobile, Multi-User, AppStation and TaskStation
- **None:** Kiosk

Redirected Folders Configuration Steps

Because a server name is specified when configuring redirected folders, the GPOs provided with this CommonScenarios.msi do not specify Folder Redirection properties. To fully implement the scenarios in your environment, you must carry out the following steps.

1. On the CommonServer computer, create a folder called ***redirected***.
2. Share this folder as ***redirected*$** (the full share name would therefore be \\*CommonServer**redirected$*).
3. Set share permissions for the *redirected*$ share to **Full Control** for the **Everyone** group (security will be enforced by NTFS permissions when the user profile folders are created).
4. For both the **Lightly Managed (User)** and **Highly Managed (User)** GPOs, do the following:
   a. In GPMC, right-click the GPO, and then click **Edit**.
   b. Within the Group Policy Object Editor, go to *User Configuration/Windows Settings/Folder Redirection*.
   c. Right-click the **My Documents** node and click **Properties**.
   d. In the **Properties** dialog box, change the **Setting** list to **Basic – Redirect everyone's folder to the same location**.
   e. Leave the **Target Folder Location** list set to **Create a folder for each user under the root path**.
   f. Set the **Root Path** field to \\CommonServer\redirected$, and then click **OK**. Folder Redirection automatically appends %user name% to the path specified.
   g. Right-click the **Desktop** node and click **Properties**.
   h. In the **Properties** dialog box, change the **Setting** dropdown box to **Basic – Redirect everyone's folder to the same location**.
   i. Leave the **Target Folder Location** list set to **Create a folder for each user under the root path**.
   j. Set the **Root Path** field to \\CommonServer\redirected$\, and then click **OK**. Folder Redirection automatically appends %user name% to the path specified.
   k. Close the GPO.

Redirected Folders Notes

The steps above ensure that all scenarios – except the Kiosk scenario – implement redirected folders. Because the Kiosk scenario is a child of the Highly Managed scenario, it is necessary to disable the Folder Redirection setting specified in the Highly Managed (User) GPO. This is achieved – through the supplied Kiosk GPOs – by redirecting the appropriate folders back to the local user profile location; this is, in essence, the same as disabling Folder Redirection.

Internet Explorer Configuration

There are two types of Internet Explorer Group Policy settings: the standard Windows registry settings and a collection of registry settings and files used to configure Internet Explorer. The standard settings are located in the Group Policy Object Editor under Administrative Templates\Windows Components\Internet Explorer, and the configuration settings are located in User Configuration\Windows Settings\Internet Explorer Maintenance.

The Internet Explorer Maintenance settings can be set in two modes: **policy mode** or **preference mode**. Policy mode is enforced and automatically resets any settings users might change (if they have the appropriate permissions) when Group Policy is applied.

> **Note** Like all registry-based Group Policy settings, Internet Explorer Maintenance policy mode settings reapply only when the GPO changes. Unlike most registry-based Group Policy settings, configuring an Internet Explorer Maintenance setting does not prevent the user from changing that setting.

Preference mode sets initial default values that the user can change, subject to other Group Policy settings that affect the user. The preference settings are only applied again when the administrator makes changes to the preference settings. To allow users to change these preferences, they must be able to access Internet Options on the Tools menu. You allow users access by configuring settings in the Group Policy Object Editor under Computer (or User) Configuration\Administrative Templates\Windows Components\Internet Explorer.

You cannot use policy and preference modes together in a single GPO. If you need both modes, you must use two separate GPOs. The included scenarios are configured using policy mode, so you might need to create an additional GPO using preference mode for your environment.

Kiosk Scenario Configuration

The Kiosk scenario uses a single account that is a member of the Domain Users group (all new accounts in a domain are added to this group) with no special privileges. To enable the use of this account with no user intervention, the AutoLogon feature is used. At startup, the operating system logs on automatically using the account and password specified in the registry key below.

Kiosk User Account Configuration

The account used by the Kiosk scenario should be configured as follows:

- Password never expires
- User cannot change password

To configure the account for auto logon, the TweakUI tool (part of the Windows XP PowerToys) can be used to specify the user name and password. For more information about the PowerToys, see http://www.microsoft.com/windowsxp/pro/downloads/powertoys.asp.

Specifying the Kiosk Application

The packaged GPOs specify Internet Explorer as the auto launch application for both the TaskStation and Kiosk scenarios. This is handled by enabling the \User Configuration\Administrative Templates\System\Custom User Interface Group Policy setting. The value used for this policy (for both scenarios) is:

%programfiles%\internet explorer\iexplore.exe –k

This has the result of automatically launching Internet Explorer (in full screen mode because of the –k switch) when a user logs on. In effect, the policy is used to replace Windows Explorer as the shell. By updating the Custom User Interface Group Policy setting, you can dictate the application to be launched in the TaskStation and Kiosk scenarios in your own environment.

Resetting Kiosk Settings to a Default State

In some cases, you might want to reset the Kiosk environment to a known state. Although Kiosk users are prevented from making most changes to a Kiosk-based computer, a few application-specific settings cannot easily be managed by using Group Policy settings. For example, if a user resizes the Internet Explorer window, the window starts up in that size for all subsequent users.

You can use a mandatory user profile to reset the Kiosk settings. To do this, use the following procedure:

1. Log on to the user account and configure the appropriate settings.
2. Log off of the user account and then log on as an Administrator.
3. Copy the profile to a local or network directory and then rename the profile root to OldName.man.
4. Modify the user object and specify this directory as the profile path.

After you carry out this procedure, if a Kiosk user logs on, the computer settings reflect the settings defined in the mandatory profile.

Disk Maintenance

Applications used on a Kiosk-based computer can write data to the disk drive. To prevent the disk drive from filling up, set a disk quota that leaves at least 100 megabytes (MB) free on the system disk.

You should consider using the disk quota in conjunction with a scheduled script that removes older temporary files each night. If the Kiosk application creates a lot of temporary files, the script might also need to run disk defragmentation to maintain system performance.

Disabling Logoff Capability for Kiosk Users

Kiosk users cannot log off the Kiosk account by pressing **Ctrl+Alt+Del** or by using the **Start** menu. When the computer starts up, it automatically logs on to the Kiosk account.

> **Important** In the Kiosk scenario, Kiosk users are prevented from logging off; however, in the Kiosk GPOs provided with this white paper, logoff capability is enabled because it makes testing easier. Therefore, before deploying the scenario, you need to disable the logoff feature.

A disadvantage of disabling the logoff feature is that an administrator cannot easily log on to the computer. The administrator cannot restart the computer from the console because shutdown and restart are disabled for the kiosk user. To resolve this, you can use one of the following solutions:

Solution 1

1. Restart the computer by doing one of the following:
   - Execute a remote restart using **shutdown.exe**.
   - Perform a hardware reset or power off of the computer (this solution is not recommended because it could lead to data loss or system malfunction).
2. When the computer restarts, hold down the **Shift** key to bypass the automatic logon feature and access the standard logon dialog box.

Solution 2

In this option, the logon feature remains enabled. The administrator logs off from the Kiosk account and then holds down the Shift key to bypass the automatic logon feature. The disadvantage to this method is that a user could do the first part of this operation. Although they would be unable to log on, this would leave the logon dialog box displayed and render the Kiosk computer unusable until it is restarted.

Switching Between Scenarios

Joining a particular scenario is relatively simple – move the appropriate computer and user accounts into OUs to which the appropriate scenario GPOs have been linked. For example, if a user is to experience the Multi-User scenario, his or her account must exist in an OU to which the Multi-User (User) GPO has been linked and must log on to a computer in an OU to which the Multi-User (Computer) GPO has been linked.

In general, moving between scenarios is simply a matter of moving computers and users into the appropriate OUs. However, you might need to do some additional work to complete the transition between scenarios related to security settings and Roaming User Profiles.

Note that moving users between OUs requires a logon to ensure that this is reflected and that the appropriate GPOs are applied. Similarly, moving a computer to a different OU requires that the computer is restarted for the new OU to be recognized.

Security Settings

A number of security settings "tattoo" the registry – once applied through a GPO, they remain active even when the GPO is moved out of scope for the target computer or user (by unlinking the GPO, moving the account from an affected OU, or disabling the GPO). Therefore, simply switching a computer or user account to an OU associated with a different scenario will result in some settings from the original scenario remaining. This is particularly evident when transitioning to a scenario with fewer security settings than the original.

There are a number of options to address this issue:

- Ensure that the GPOs associated with the new scenario explicitly disable/enable security settings that have been set in the GPOs associated with the original scenario. For example, if a security setting is configured in a GPO for the original scenario, the GPO for the new scenario must configure that security setting, even if the security setting isn't directly relevant to the new scenario. While this makes for a more deterministic application of these settings (the eventual result of the security setting is independent of the configuration in the original scenario), this does result in all GPOs needing to include the superset of all possible security settings, which can be cumbersome to manage and track.
- Temporarily move the computer and user accounts to a "clean up" OU that explicitly sets all security settings to a default state. After these have been implemented (allowing Group Policy to refresh by waiting at least 120 minutes or by using the **gpupdate** command), the accounts are moved to the appropriate OUs for the new scenario. One drawback with this approach is the potential for a delay to ensure that the temporary policy settings are applied to the computer and user accounts. Additionally, it is necessary for the user account be used to log on at least once to ensure that the "clean up" GPOs associated with user-

based security settings are applied.

- As an administrator on the target machine, manually remove the security settings that no longer apply. This is clearly the most labor-intensive approach, requires significant knowledge of how each security setting is implemented, and is generally not an option with a significant number of computers.

Roaming User Profiles

The Roaming User Profile attribute for a user (the location of the roaming profile, if set) is stored in the user account object within Active Directory. Due to the order in which profiles are applied, as related to the application of Group Policy, this parameter cannot be set through Group Policy. As such, if a user moves between scenarios where the use of Roaming User Profiles changes (for example, where the initial scenario uses a Roaming User Profile but the target scenario does not), then it is necessary to update the user object to reflect this change.

Extending the Scenarios

You can use the common scenarios GPOs as a starting point for your own custom scenarios. For more information about the features and capabilities of Group Policy, see the *Designing a Managed Environment* book in the *Windows Server 2003 Deployment Kit*. For more information, see the Microsoft Web site.

Software Distribution Through Group Policy

The scenarios do not implement any form of software distribution, although this is a feature of Group Policy. By creating .MSI packages and associating them with targeted GPOs, it is possible to manage applications using Group Policy, including support for initial deployment, transforms, and "self-healing" installations (detection and automatic repair of missing components such as DLLs). Group Policy enables you to automatically install and maintain software installation on target computers or make it available for user installation.

Software Restriction Policies

Software restriction policies, new with Windows XP and Windows Server 2003, provide a policy-driven mechanism that enables you to identify the programs that are running on computers in your domain, and to control their ability to run. By using software restriction policies, you can:

- Control what programs run on your system. For example, you can apply a rule that does not allow certain file types to run in the mail attachment directory of your e-mail program if you are concerned about users receiving viruses through e-mail.
- Run only digitally signed scripts.
- Allow users to run only specific files on multi-user computers. For example, if you have multiple users who use a single computer, you can set up software restriction policies and Access Control List settings so that users cannot make changes to the computer.
- Decide who can add trusted publishers to a computer.
- Control whether software restriction policies affect all users or only certain users who use a computer.
- Prevent any files from running on a local computer. For example, if you are aware of a known virus, you can disallow a hash of that virus so that the computers in your domain cannot run that program.

Creating Default OUs for New Machine and User Accounts

By default, all new computer or user accounts are created in the Computer or User containers, respectively. Because these are not OUs, it is not possible to link GPOs to them. However, using two new tools provided with Windows Server 2003, you can specify that all new accounts will be created in specific OUs. You do this by first creating OUs for new user and computer accounts and then running Redirusr.exe (for user accounts) and/or Redircmp.exe (for computer accounts) once for each domain. From this point, all new user and computer accounts will be placed in the targeted OUs. These tools are included on the Windows Server 2003 CD. You can run either of these tools or both of them.

For more details, see article 324949, "Redirecting the Users and Computers Containers in Windows Server 2003 Domains,".

Appendix A: GPO Scenario Policy Settings

The Group Policy settings for each scenario (GPOs for both computer and user policy settings) are documented in the accompanying spreadsheet, CommonScenarios.xls. Using Excel's column-filtering capability, the spreadsheet allows you to easily browse through the settings associated with each scenario.

In addition, HTML-based GPO reports are provided in the **<installdir>\GPO-Reports** directory. One report exists for each GPO provided with CommonScenarios.msi and provides a good deal of information about each GPO.

Scenario Comparison Table

Table 2 lists the feature characteristics of each scenario.

Table 2 Scenario Features

	Lightly Managed	Mobile	Multi-User	AppStation	TaskStation	Kiosk
Number of users	Multiple	1	Multiple	Multiple	Multiple	1 (anonymous)
User profile type	Roaming	Roaming	Roaming	Roaming	Roaming	Local
Profile persistence at logoff	Cached	Cached	Removed at logoff	Cached	Removed at logoff	N/A
Folder Redirection	My Documents and AppData	My Documents and AppData	My Documents and AppData	My Documents and AppData	My Documents and AppData	No
User can customize	Almost all settings	Some or most settings	Some settings	Few settings	None	None
Task bar and Start Menu	Yes	Yes	Yes	Yes	No	No
Assigned Applications	Multiple	Multiple	Multiple	Few	1 (usually computer assigned)	1 (computer assigned)
Published applications	Yes	Yes	Yes	No	No	No
Security context	User or Power User	User or Power User	User	User	User	User
Based on security template	Secure Workstation	Secure Workstation	Highly Secure Workstation	Highly Secure Workstation	Highly Secure Workstation	Highly Secure Workstation

Notes

- The scenarios are based on the security templates listed; however, in each scenario, the templates have been modified.
- The following significant modifications are made for compatibility reasons:
  - Mandatory digital signing of SMB traffic is disabled.
  - Mandatory encryption of secure channel communications is disabled.
  - LAN Manager Authentication Level is not specified.

Permissions Needed for Folder Redirection

When setting up folder redirection, it is recommended that you create the root share only on the server, and let the system create the folders for each user. For the best experience, set the share permissions to **Full Control** for the security groups you're redirecting, and set the NTFS permissions to **Full Control** on this folder, subfolders, and files.

If you must create folders for the users, ensure that you set the correct permissions. Tables 3, 4, and 5 below show the default and minimum permissions required for folder redirection.

Table 3 NTFS Permissions Needed for Root Folder

User account	Folder redirection defaults	Minimum permissions needed
Creator/owner	Full Control, this folder,	Full Control, this folder, subfolders, and files

	subfolders, and files	
Local Administrator	Full Control, this folder, subfolders, and files	Full Control, this folder, subfolders, and files
Everyone	Full Control, this folder, subfolders, and files	List Folder/Read data, Create Files/Write Data, Create Folders/Append Data - This Folder only
Local System	Full Control, this folder, subfolders, and files	Full Control, this folder, subfolders, and files

Table 4 Share level (SMB) Permissions Required for Root Folder

User account	Folder redirection defaults	Minimum permissions needed
Everyone	Full Control	Everyone - no permissions. Use security group that matches the users who will need to put data on share.

Table 5 NTFS Permissions Required for each User's Redirected Folder

User account	Folder redirection defaults	Minimum permissions needed
%User Name%	Full Control, owner of folder	Full Control, owner of folder
Local System	Full Control	Full Control
Everyone	Traverse Folder, Read Attributes, Read Extended Attributes, and Read Permissions	Everyone - no permissions

Appendix B: Running CommonScenarios.msi

This white paper comes with a number of supporting files – spreadsheets, GPO backups, and HTML-based Group Policy reports. These are installed by the installation package CommonScenarios.msi.

When you install this package, the files listed in Table 6 are copied into the **%programfiles% \Microsoft\CommonScenarios** directory and a new menu – **Group Policy Common Scenarios** – is created on **Start/Programs**.

Table 6 Files Installed by CommonScenarios.msi Package

Directory	FileName	Description
\Documentation	CommonScenariosWS2003.doc	This white paper.
\Documentation	CommonScenariosWS2003.xls	Spreadsheet listing each setting specified for all scenarios.
\Environment	CommonScenarios.xml	File representing sample environment for common scenarios and for use by CreateEnvironmentFromXML script.
\GPO-Backups	[GUID]	One subdirectory for each GPO included in the common scenarios.
\GPO-Reports	[GPO Name].htm	HTML-based report for each GPO (generated from GPMC).
\Scripts	CreateCommonScenarios.cmd	Command file to install a sample OU structure, create the common scenarios GPOs, and link GPOs.
