Lesson 19: Configuring Group Policy Processing

MOAC 70-411: Administering Windows Server 2012

Microsoft
Official Academic Course

WILEY

Overview

- Exam Objective 4.2: Configure Group Policy Processing
- Understanding Group Policy Processing

Understanding Group Policy Processing

Lesson 19: Configuring Group Policy Processing

Group Policies and GPOs

- Group policies are defined using group policy objects (GPOs).
- GPOs are the collection of configuration instructions that the computer processes.
- To assign a group policy, it is linked to an Active Directory container (site, domain, or organizational unit).

Scoping a GPO

Mechanisms for scoping a GPO:

- A GPO link to a site, domain, or organizational unit (OU)
- The GPO link enabled or disabled
- Enforced option of the GPO
- The Block Inheritance option of an OU
- Security group filtering
- WMI filtering
- Loopback policy processing
- Preferences targeting (discussed in Lesson 22)

Configuring Processor Order and Precedence

1. When a computer first starts up, it establishes a secure link between the computer and a domain controller.
2. The computer obtains a list of GPOs that are applied to the computer.
3. Computer configuration settings are applied synchronously (one by one) during computer startup before the Logon dialog box is presented to the user.
4. When the computer configuration settings have been applied and the startup scripts have been applied, users have the Ctrl+Alt+Del option to log on.

Configuring Processor Order and Precedence

5. A user is authenticated and the user profile is loaded.
6. The computer obtains a list of GPOs that are applied to the user. Again, GPO processing is hidden from the user.
7. After the user policies run, any logon scripts defined by GPOs run. Scripts are executed asynchronously.
8. The login script defined for the user in Active Directory user properties is executed.
9. The user’s desktop is displayed.

Understanding Group Policy Inheritance

A computer and user can be affected by multiple GPOs. GPOs are processed in the following order:

1. Local group policy
2. Site
3. Domain
4. OU

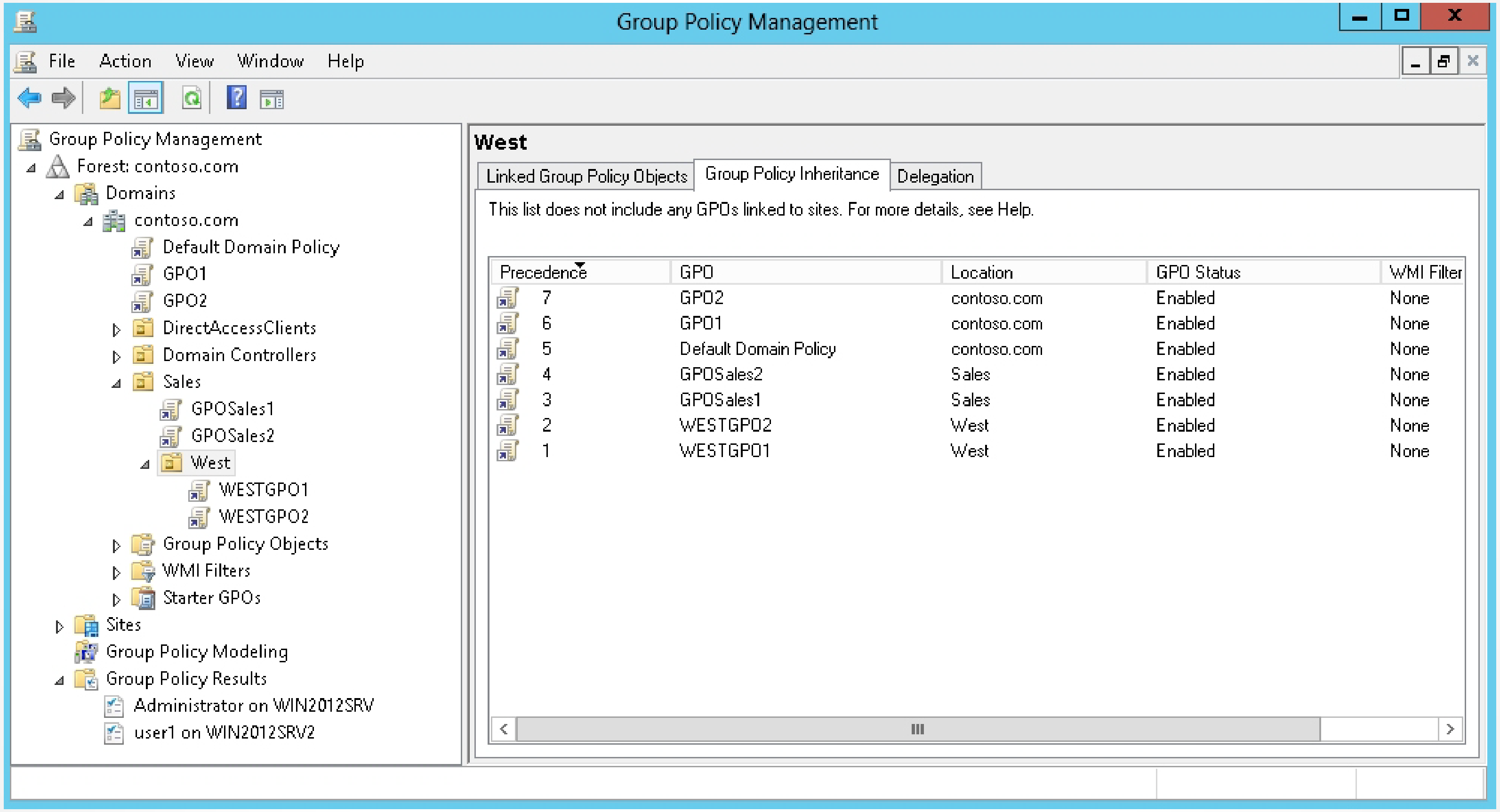
A Group Policy uses ***inheritance*** in which settings are inherited from the container above.

Understanding Group Policy Inheritance

When Active Directory is installed, two domain GPOs are created by default:

- ***Default Domain Policy***: Linked to the domain. It affects all users and computers in the domain including domain controllers. It specifies the password, account lockout, and Kerberos policies.
- ***Default Domain Controller Policy***: Linked to the Domain Controllers organization unit, which then affects the domain controllers. It contains the default user rights assignments.

Understanding Group Policy Inheritance

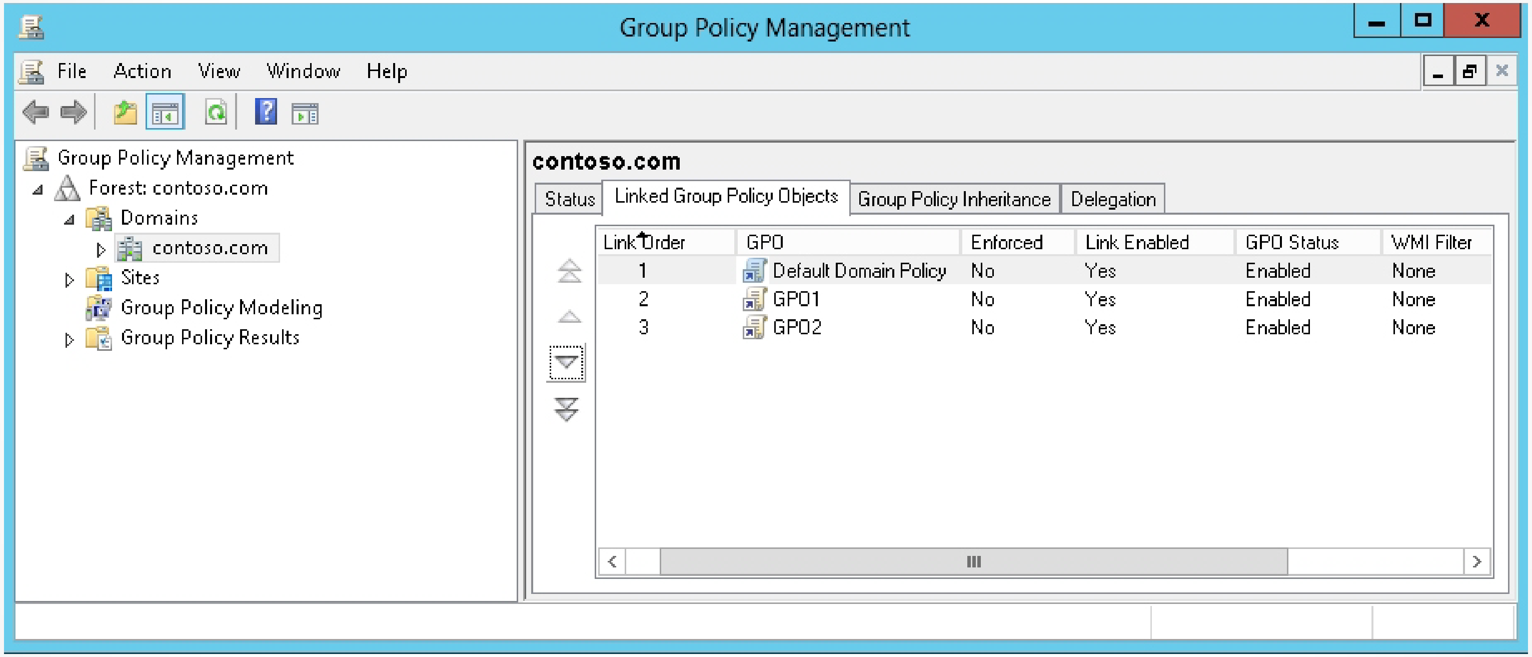


This list does not include any GPOs linked to sites. For more details, see Help.

Precedence	GPO	Location	GPO Status	WMI Filter
7	GPO2	contoso.com	Enabled	None
6	GPO1	contoso.com	Enabled	None
5	Default Domain Policy	contoso.com	Enabled	None
4	GPOSales2	Sales	Enabled	None
3	GPOSales1	Sales	Enabled	None
2	WESTGPO2	West	Enabled	None
1	WESTGPO1	West	Enabled	None

Displaying GPOs for a domain

Change the Precedence of a GPO



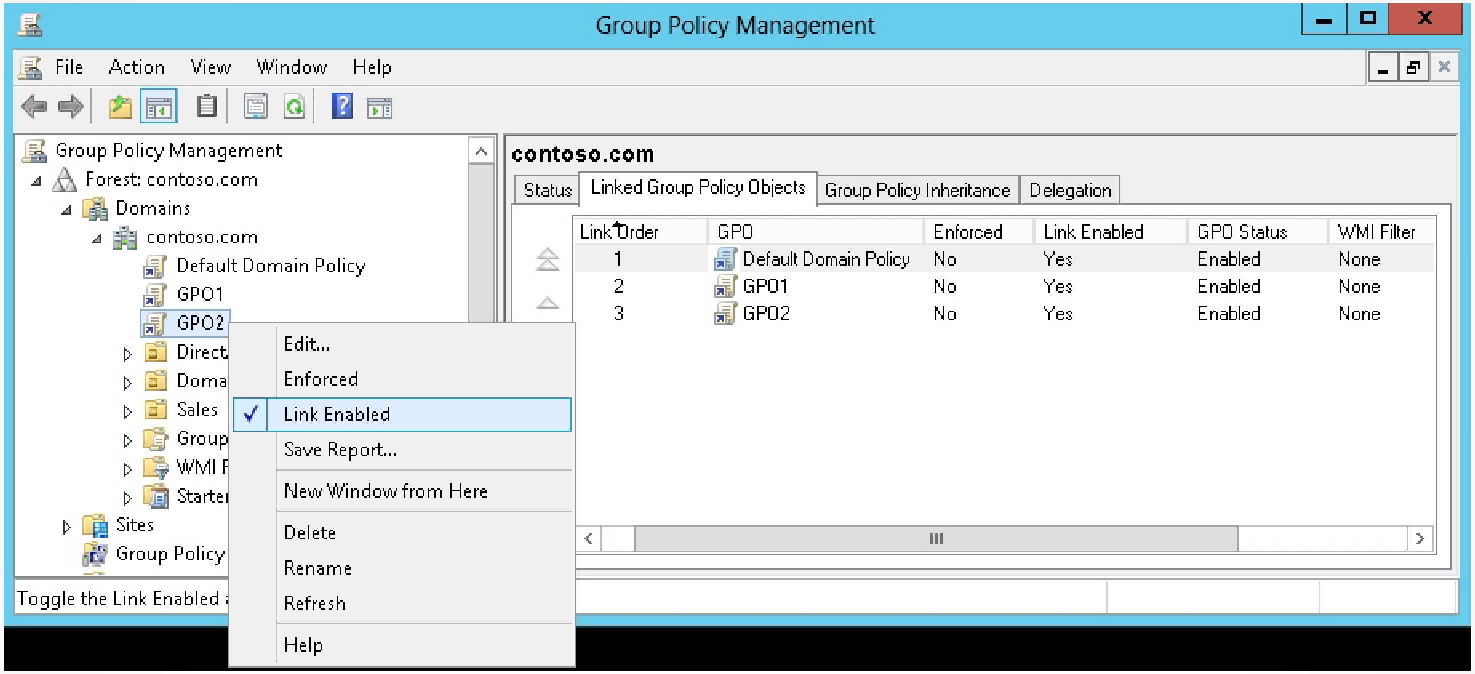
Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter
1	Default Domain Policy	No	Yes	Enabled	None
2	GPO1	No	Yes	Enabled	None
3	GPO2	No	Yes	Enabled	None

Changing the precedence

Managing Group Policy Links

To disable a group policy for a container, you right-click the GPO for the container and click the *Link Enabled* link.

Managing Group Policy Links



Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter
1	Default Domain Policy	No	Yes	Enabled	None
2	GPO1	No	Yes	Enabled	None
3	GPO2	No	Yes	Enabled	None

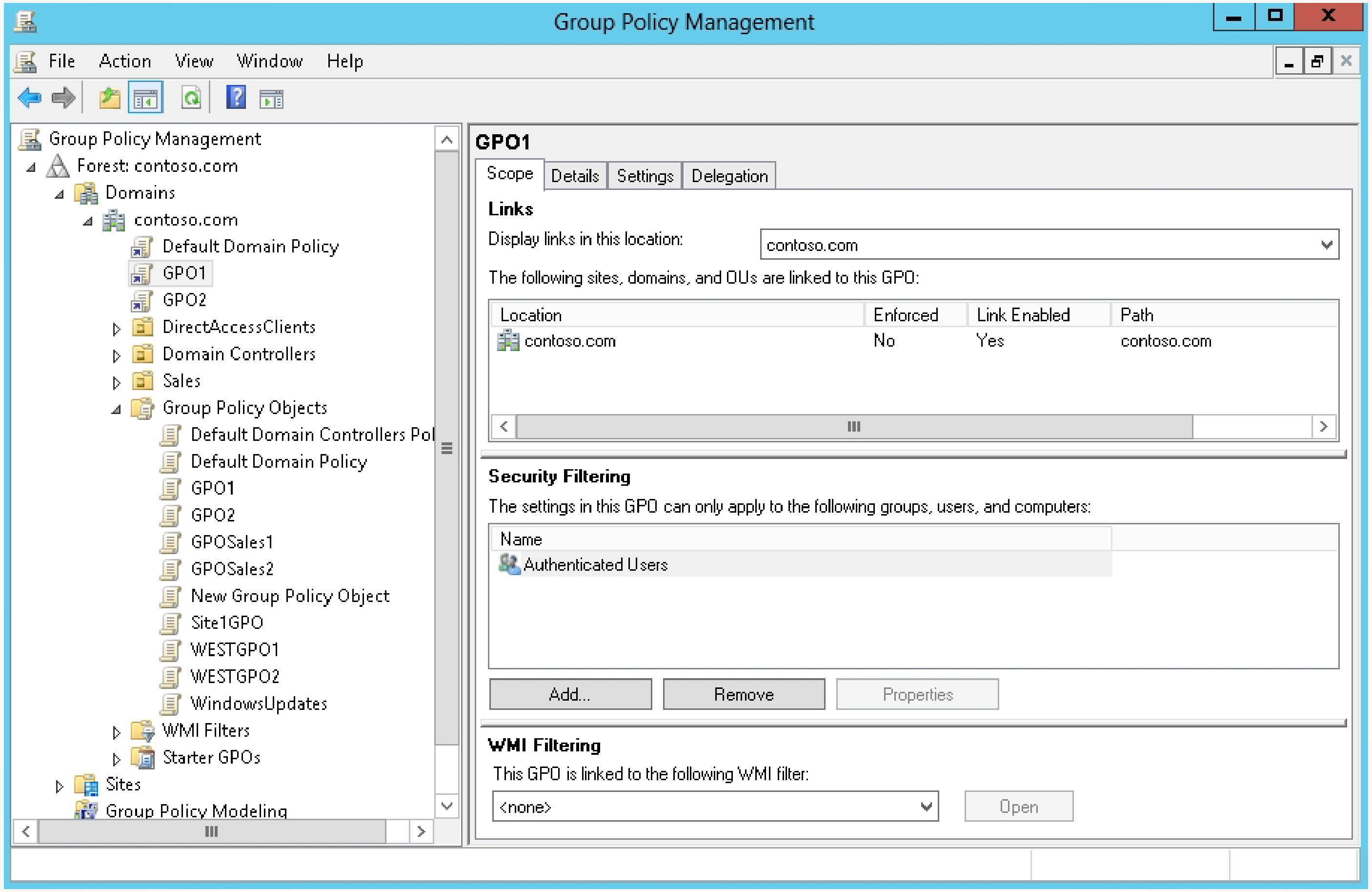
Showing a link is enabled for a GPO

Managing Group Policy Links

After a GPO is created, you can:

- View the containers that a GPO is linked to by clicking the GPO in Group Policy Management and viewing the Scope tab.
- Delete a link to a container for a GPO without deleting the GPO by right-clicking the GPO for a container and clicking *Delete*. When it asks whether to delete the link, click *OK*.
- Disable the link or delete a link for a container by right-clicking the container in the Scope tab and clicking the *Link Enabled* option or the *Delete Link(s)* option.

Managing Group Policy Links



GPO1

Links

Display links in this location: contoso.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
contoso.com	No	Yes	contoso.com

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

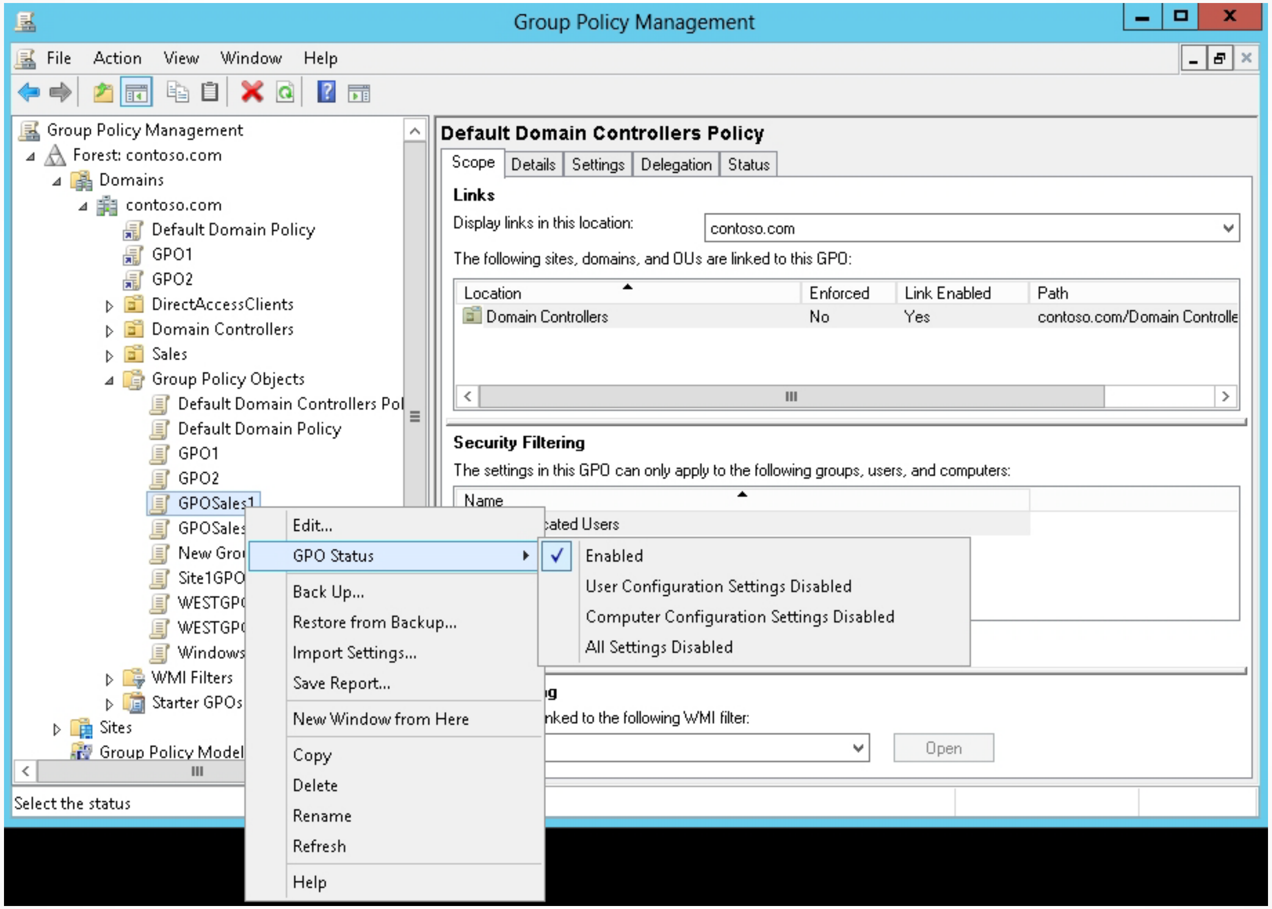
Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter: <none>

Showing the containers a GPO is linked to

Managing Group Policy Links



Default Domain Controllers Policy

Links

Display links in this location: contoso.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
Domain Controllers	No	Yes	contoso.com/Domain Controlle

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
cated Users

ıg

nked to the following WMI filter:

Select the status

Configuring the GPO status

Using Filtering with Group Policies

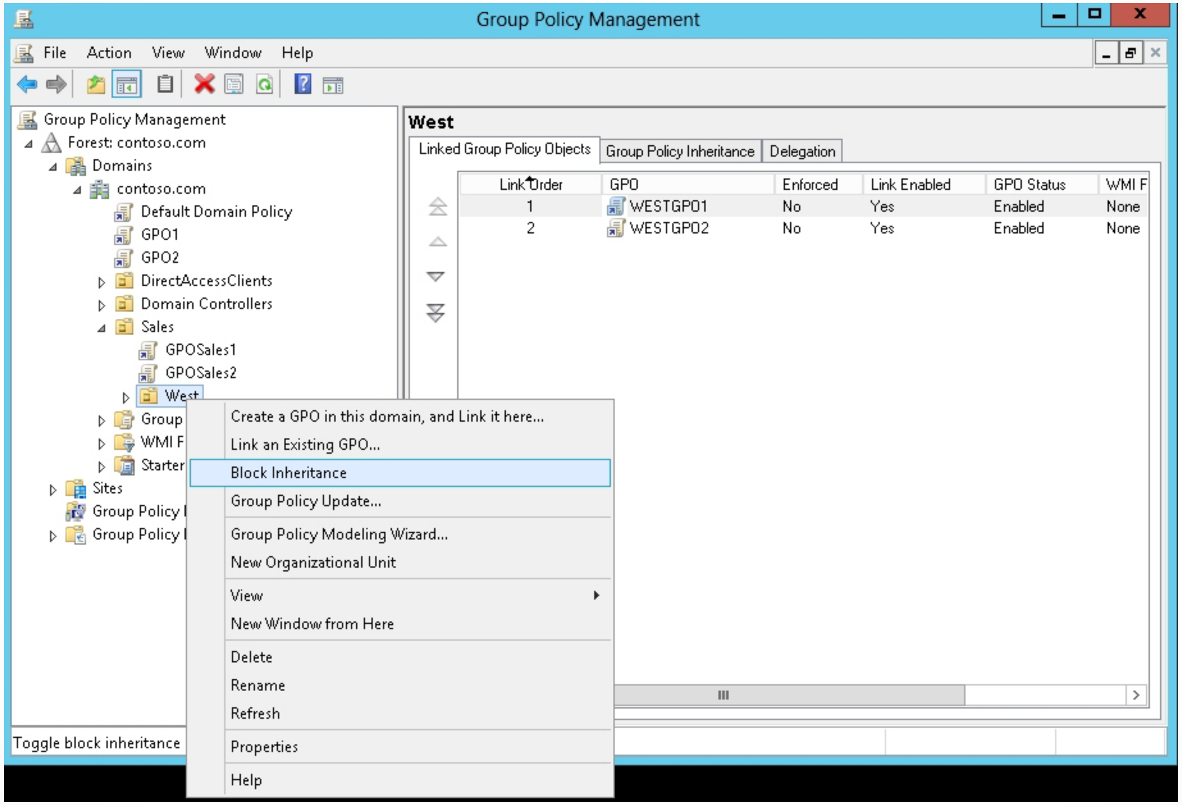
The exceptions to the processing of group policies can be modified with these options:

- Block inheritance
- Enforced

Configuring Blocking of Inheritance

- By default, group policies flow down to the lower containers and objects.
- To prevent the inheritance of policy settings, block all Group Policy settings from the GPOs linked to parent containers in the Group Policy hierarchy.
- GPOs linked directly to the container and GPOs linked to lower containers are unaffected.

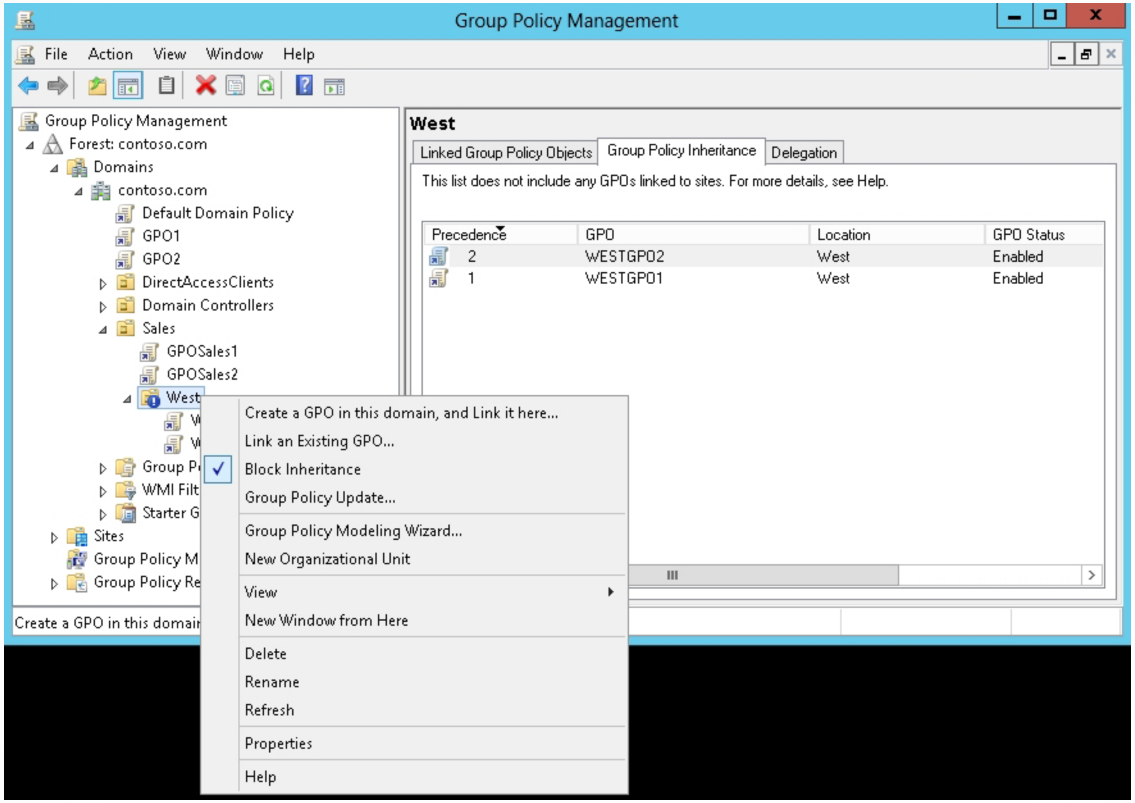
Block the Inheritance of GPOs



Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI F
1	WESTGPO1	No	Yes	Enabled	None
2	WESTGPO2	No	Yes	Enabled	None

Selecting the Block Inheritance option

Block the Inheritance of GPOs



This list does not include any GPOs linked to sites. For more details, see Help.

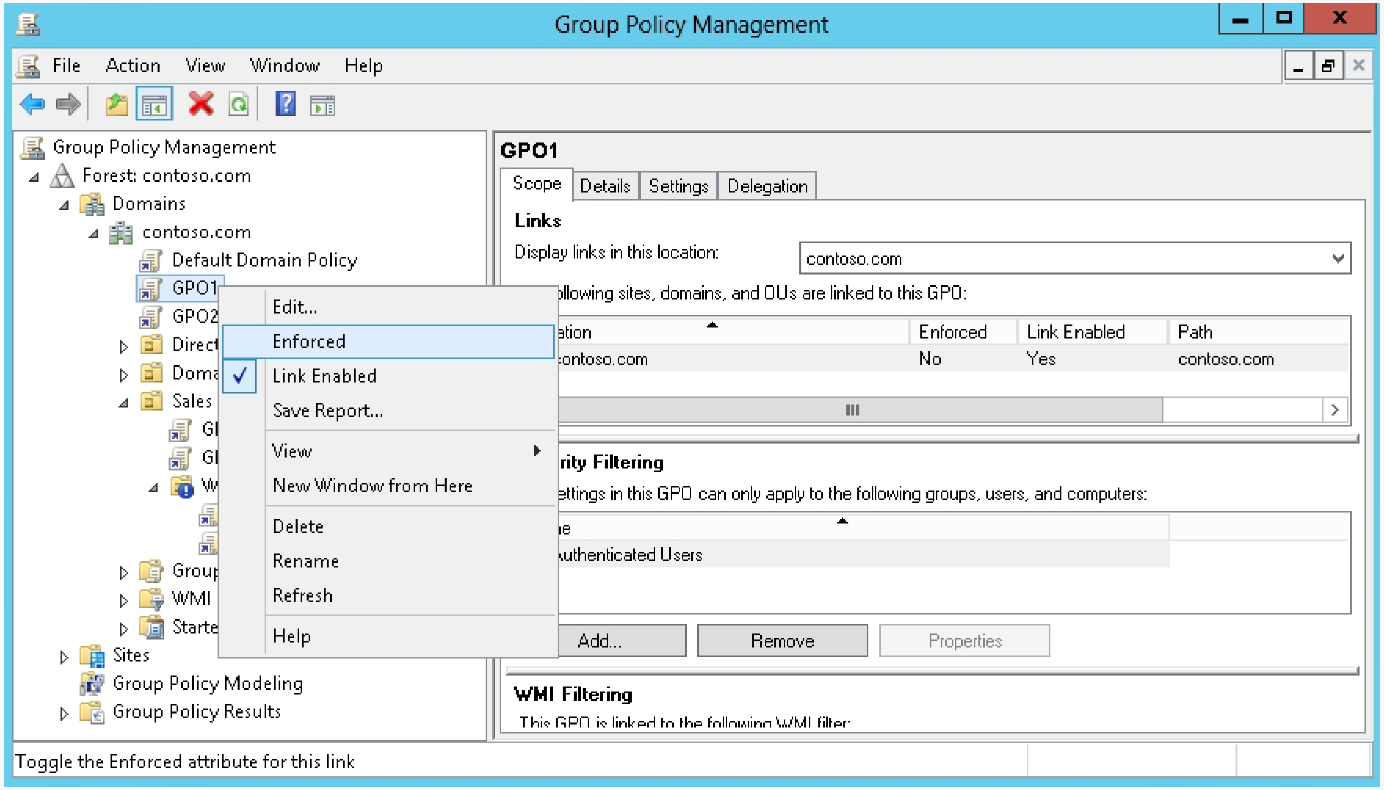
Precedence	GPO	Location	GPO Status
2	WESTGPO2	West	Enabled
1	WESTGPO1	West	Enabled

A GPO with the Block Inheritance option enabled

Configuring Enforced Policies

- By enforcing a GPO link, the GPO takes the highest precedence, which will prevail over any conflicting policy settings in other GPOs.
- An enforced link applies to child containers even when those containers are set to Block Inheritance.

Enforce a GPO



GPO1

Links

Display links in this location: contoso.com

llowing sites, domains, and OUs are linked to this GPO:

ation	Enforced	Link Enabled	Path
ontoso.com	No	Yes	contoso.com

rity Filtering

ettings in this GPO can only apply to the following groups, users, and computers:

e
uthenticated Users

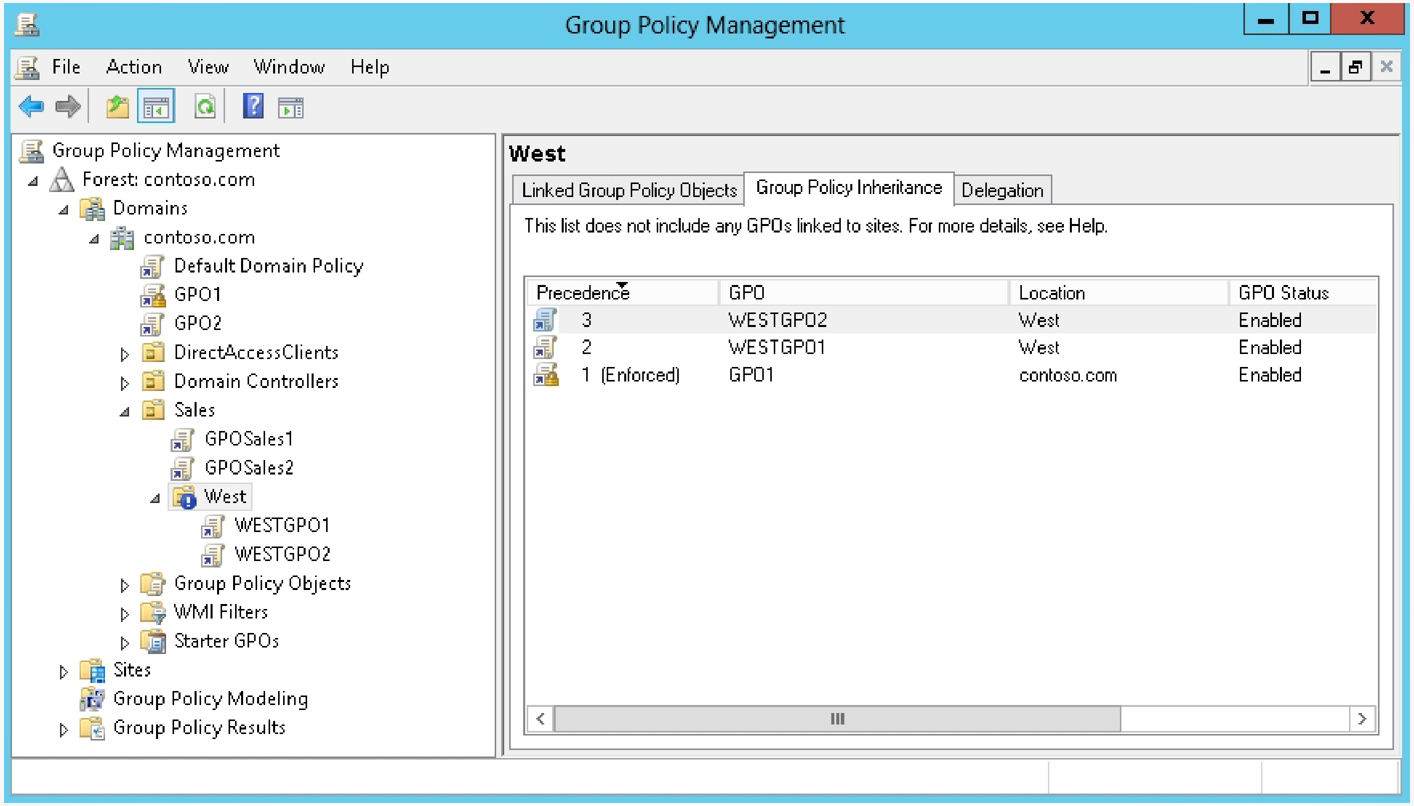
WMI Filtering

This GPO is linked to the following WMI filter:

Toggle the Enforced attribute for this link

Enforcing a GPO

Enforce a GPO



This list does not include any GPOs linked to sites. For more details, see Help.

Precedence	GPO	Location	GPO Status
3	WESTGPO2	West	Enabled
2	WESTGPO1	West	Enabled
1 (Enforced)	GPO1	contoso.com	Enabled

Showing the effect of enforcing a GPO

Configuring Security Filtering/WMI Filtering

For granular control over who or what receives a group policy, use these filters:

- **Security group filtering**: Uses a security access list (ACL) to determine who can modify or read a policy and who or what a GPO is applied to.
- **WMI filtering**: Uses the WMI Query Language (WQL) to control who or what a GPO is applied to.

Using Security Filtering

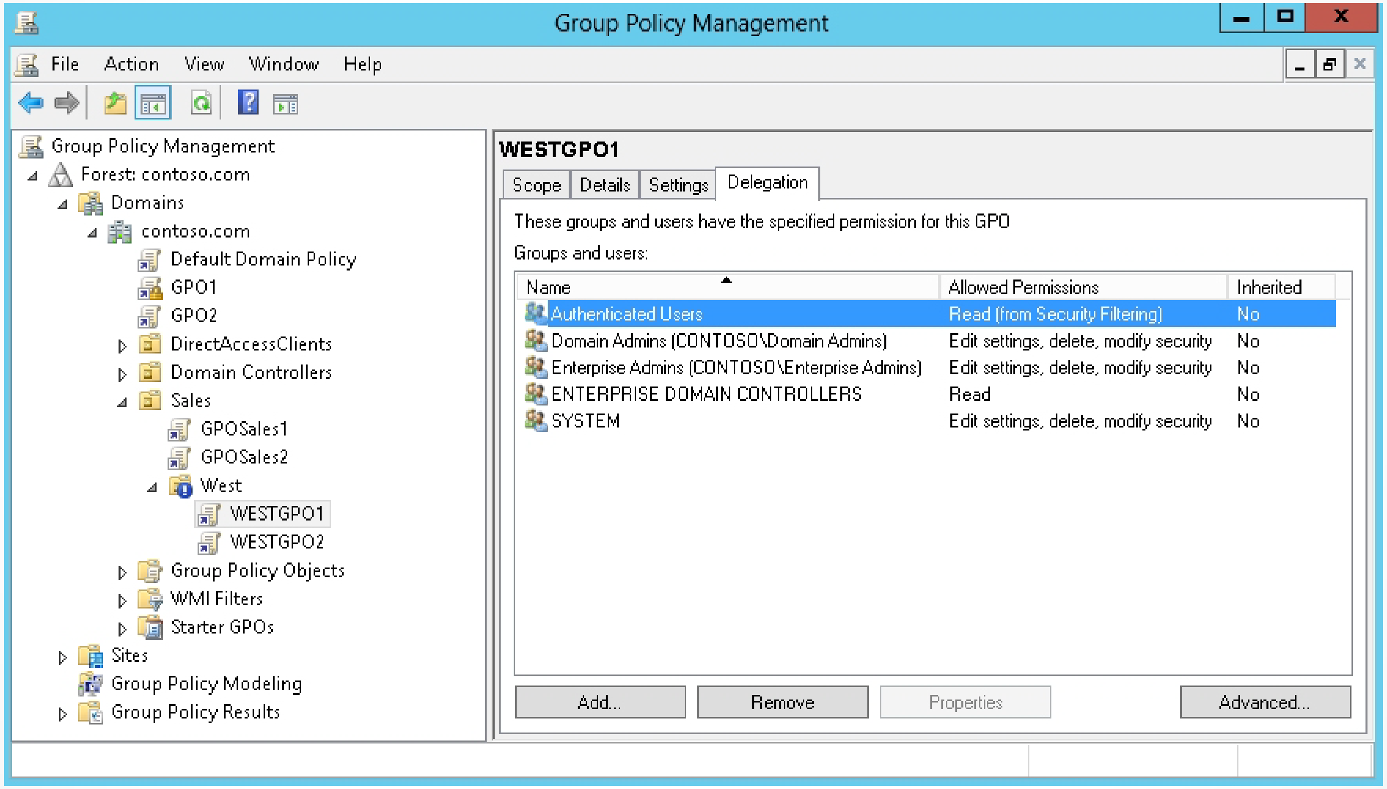
Security group filtering specifies which users, computers, or groups based on ACL receive a GPO.

Filtering GPO Scopes

Here are the ways to filter GPO scopes:

- Remove the Allow Apply group policy permission from a group such as Authenticated Users.
- Remove the Authenticated Users group access control entry (ACE), add other groups or users, and assign the Allow Apply group policy permission.
- Add ACE for another group, user, or computer and assign the Deny Apply group policy permission. Like NTFS permissions, the Deny settings always supersede any Allow settings granted to a user through membership in another group or to the user directly.

Configure a Security Group Filtering



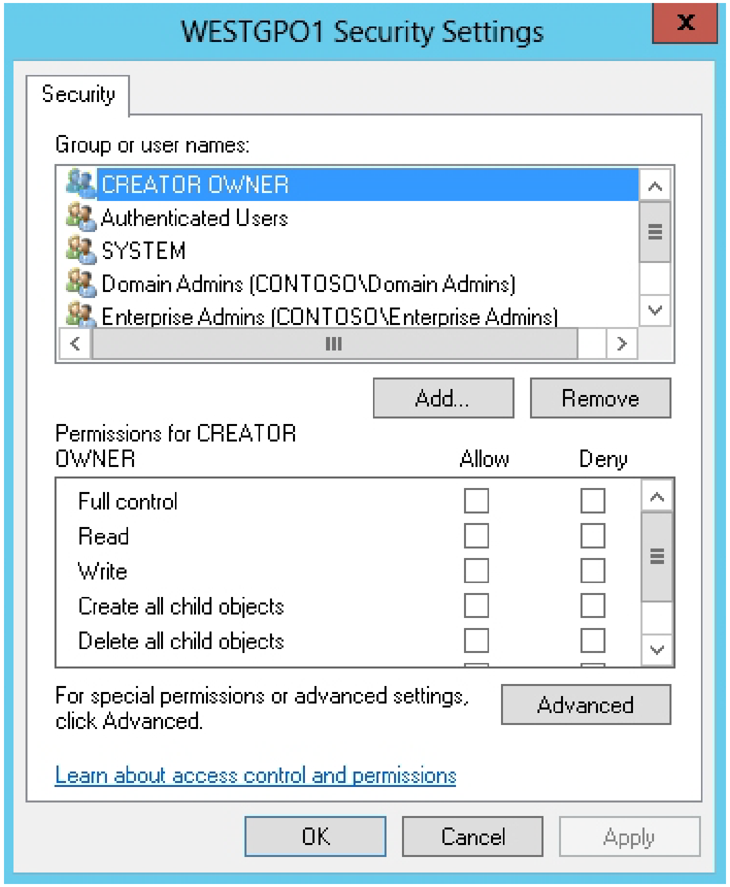
These groups and users have the specified permission for this GPO

Groups and users:

Name	Allowed Permissions	Inherited
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (CONTOSO\Domain Admins)	Edit settings, delete, modify security	No
Enterprise Admins (CONTOSO\Enterprise Admins)	Edit settings, delete, modify security	No
ENTERPRISE DOMAIN CONTROLLERS	Read	No
SYSTEM	Edit settings, delete, modify security	No

Showing current groups and users that have permissions to a GPO

Configure a Security Group Filtering



WESTGPO1 Security Settings
Security

Group or user names:

- CREATOR OWNER
- Authenticated Users
- SYSTEM
- Domain Admins (CONTOSO\Domain Admins)
- Enterprise Admins (CONTOSO\Enterprise Admins)

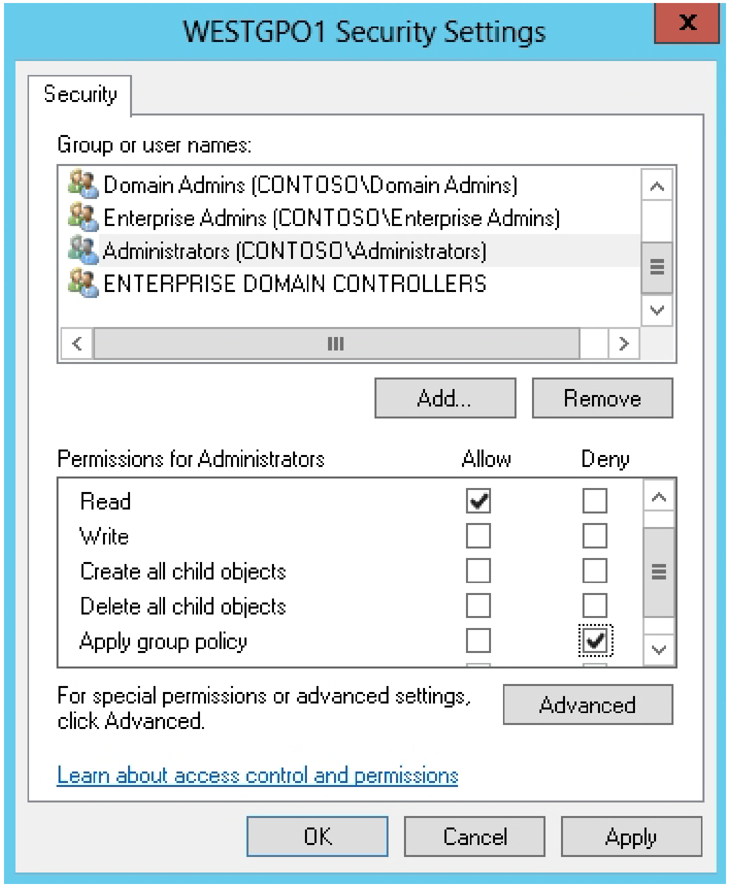
Permissions for CREATOR OWNER	Allow	Deny
Full control	□	□
Read	□	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□

For special permissions or advanced settings, click Advanced.

Advanced
Learn about access control and permissions
OK
Cancel
Apply

Showing the ACL for a GPO

Configure a Security Group Filtering



WESTGPO1 Security Settings

Group or user names:

- Domain Admins (CONTOSO\Domain Admins)
- Enterprise Admins (CONTOSO\Enterprise Admins)
- Administrators (CONTOSO\Administrators)
- ENTERPRISE DOMAIN CONTROLLERS

Permissions for Administrators	Allow	Deny
Read	☑	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□
Apply group policy	□	☑

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

Clicking the Deny Apply group policy permission

WMI Filtering

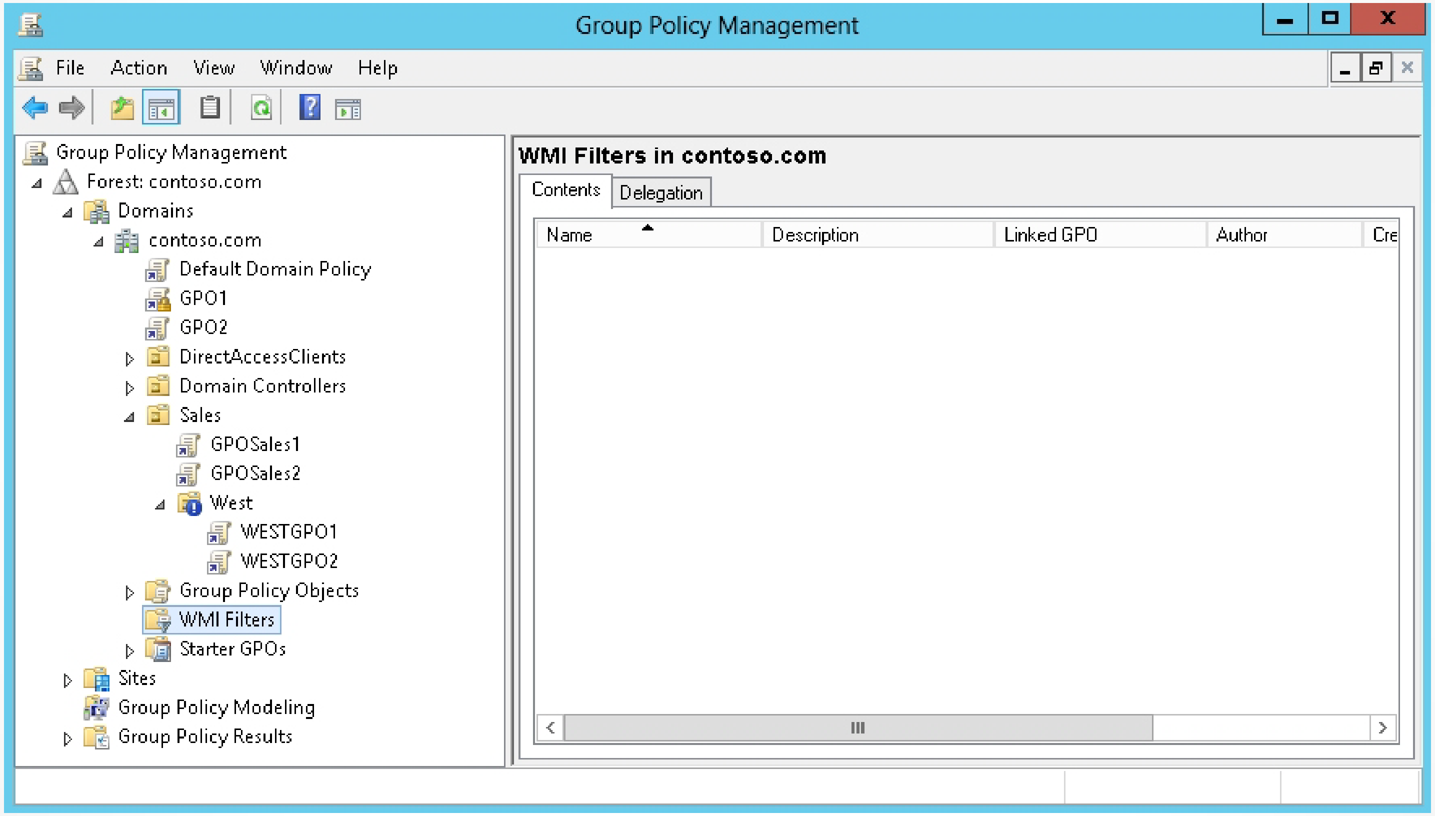
- ***Windows Management Instrumentation (WMI)***: A component that extends the Windows Driver Model through an operating system interface that provides information and notification on hardware, software, operating systems, and services.
- ***WMI filtering***: Configures a GPO to be applied to certain users or computers based on specific hardware, software, operating systems, and services.

Using WMI Filtering

To use WMI filters:

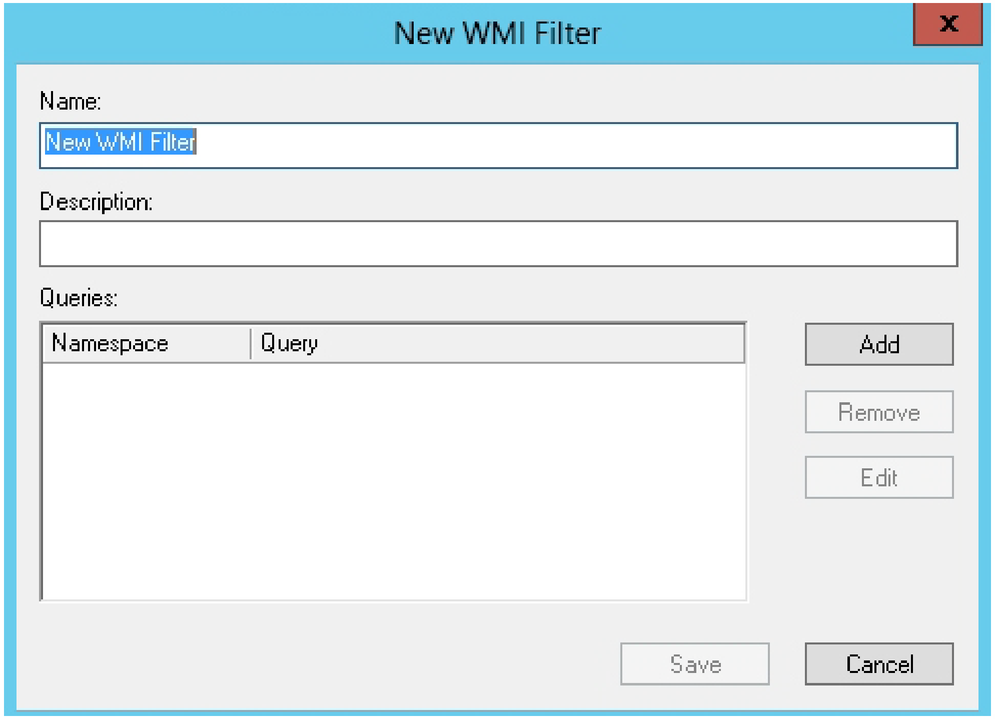
- You need to have one domain controller running Windows Server 2003 or higher.
- WMI filters will be applied only to computers running Windows XP Professional or newer, or Windows Server 2003 or newer.
- All filter criteria must have an outcome of true for the GPO to be applied.
- Only one WMI filter can be configured per GPO. After a WMI filter has been created, it can be linked to multiple GPOs.

Use WMI with GPOs



Opening the WMI Filters node

Use WMI with GPOs



New WMI Filter

Name:

New WMI Filter

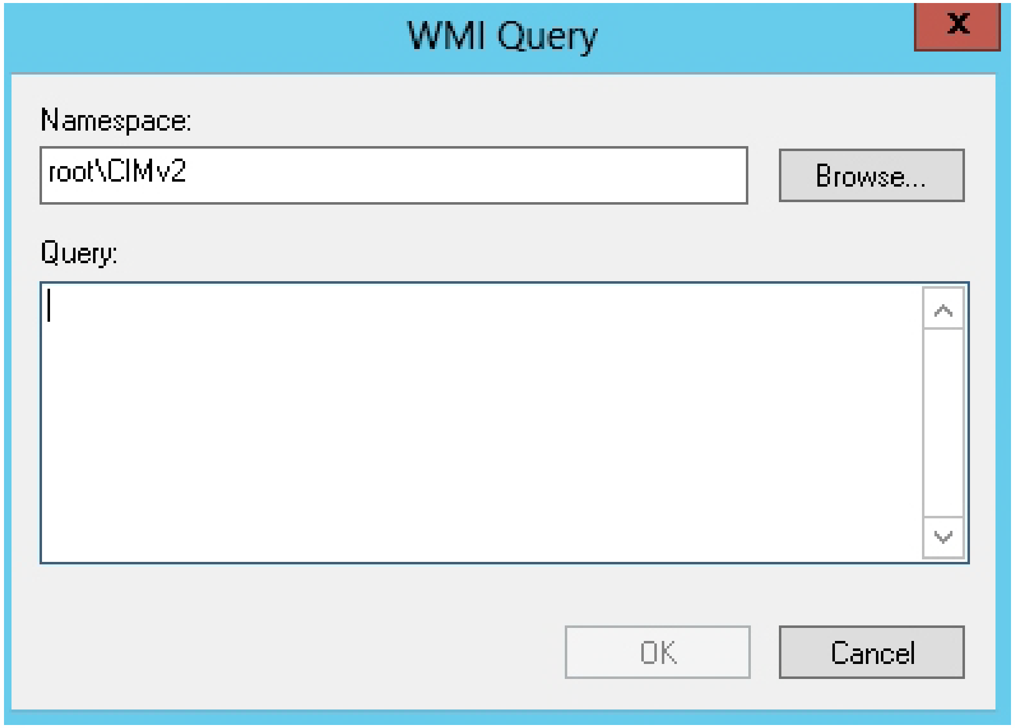
Description:

Queries:

Namespace	Query

Opening the New WMI Filter dialog box

Use WMI with GPOs

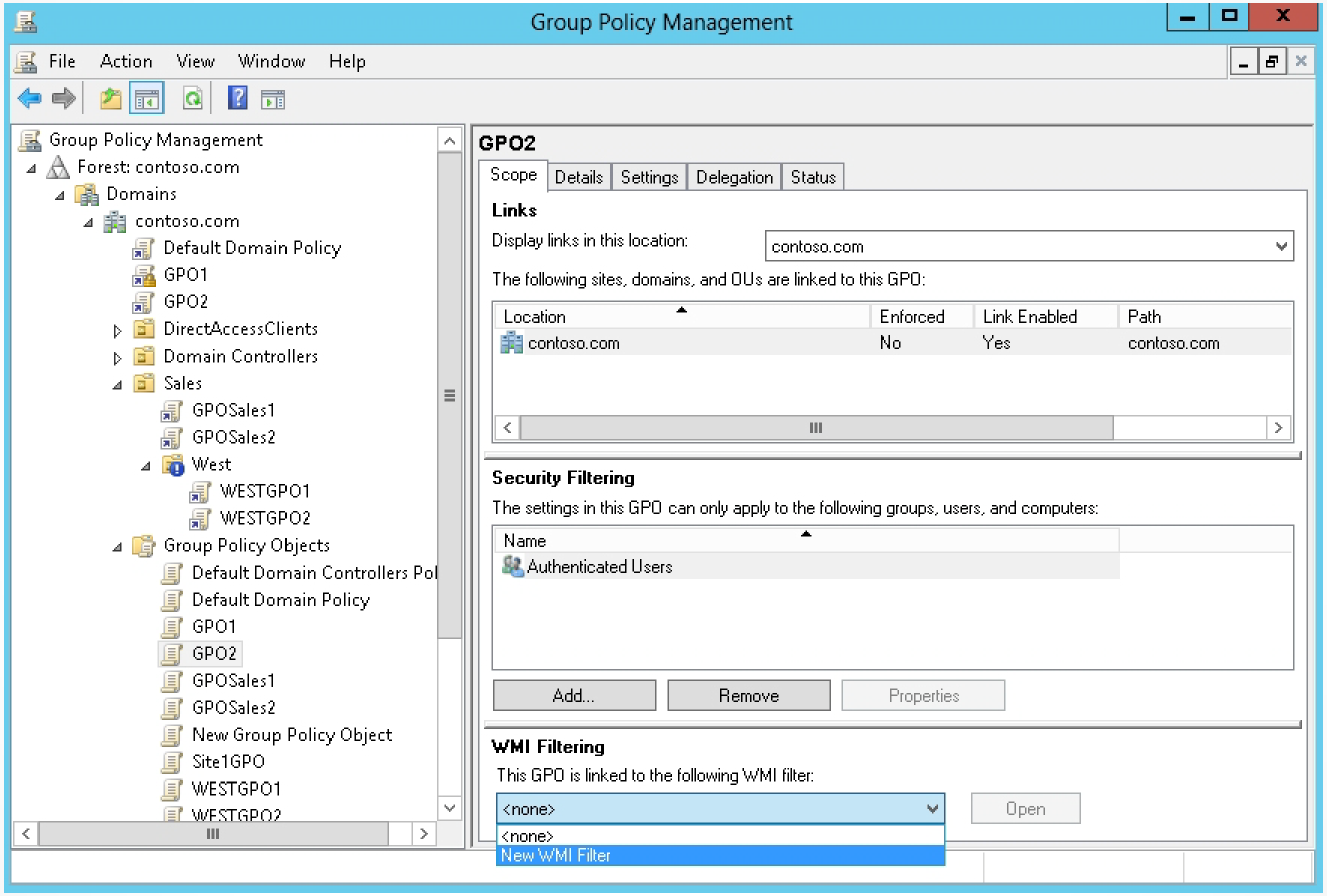


Namespace: root\CIMv2

Query:

Opening the WMI Query dialog box

Use WMI with GPOs



- Group Policy Management
  - Forest: contoso.com
    - Domains
      - contoso.com
        - Default Domain Policy
        - GPO1
        - GPO2
        - DirectAccessClients
        - Domain Controllers
        - Sales
          - GPOSales1
          - GPOSales2
          - West
            - WESTGPO1
            - WESTGPO2
        - Group Policy Objects
          - Default Domain Controllers Pol
          - Default Domain Policy
          - GPO1
          - GPO2
          - GPOSales1
          - GPOSales2
          - New Group Policy Object
          - Site1GPO
          - WESTGPO1
          - WESTGPO2

GPO2

Links

Display links in this location: contoso.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
contoso.com	No	Yes	contoso.com

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter:

<none>

Selecting the name of the WMI filter on the Scope tab

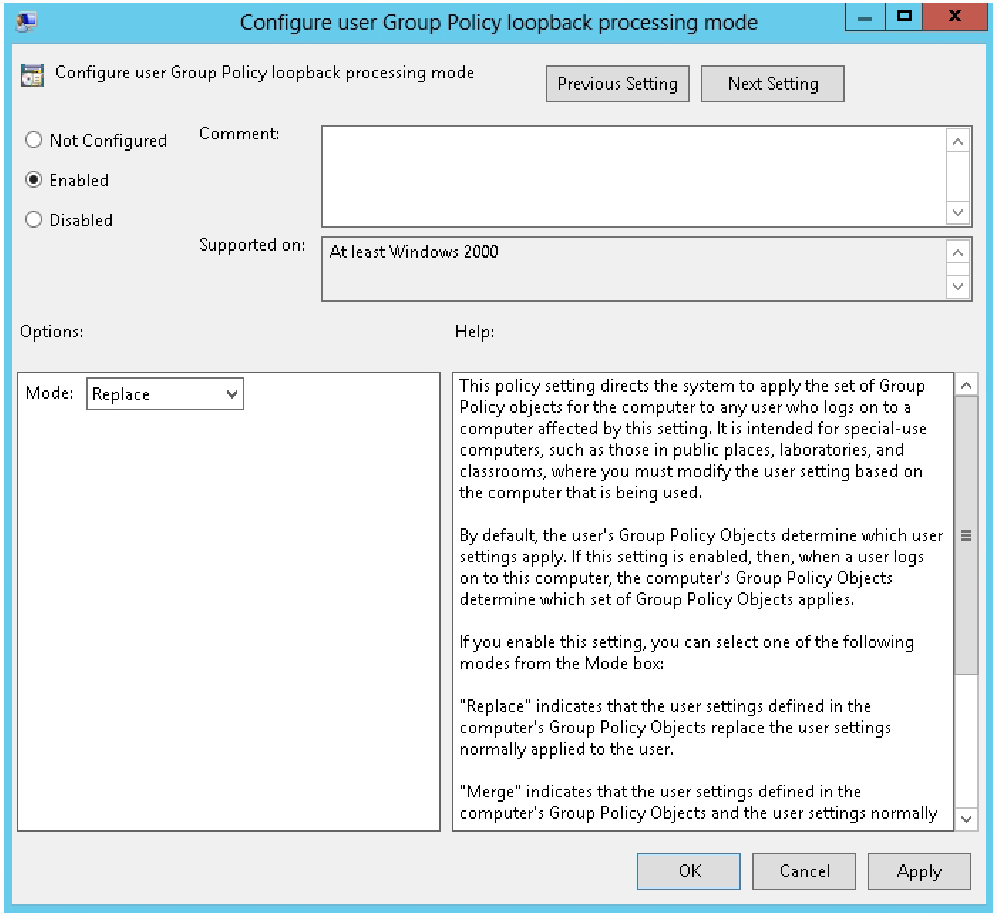
Configuring Loopback Processing

- Group Policy ***loopback processing*** is used to assign user policies to computer objects.
- No matter who logs on to a computer, the user policies are applied to the computer.

Configuring Loopback Processing

- The loopback policy is enabled using the Group Policy Management Editor, specifically the Computer Configuration\Administrative Templates\System\Group Policy\Configure user Group Policy Loopback processing mode.
- After you enable the setting, you have two modes to choose from that specify the loopback processing mode:
  - Replace mode
  - Merge mode

Configuring Loopback Processing



Configure user Group Policy loopback processing mode

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows 2000

Mode: Replace

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

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

If you enable this setting, you can select one of the following modes from the Mode box:

"Replace" indicates that the user settings defined in the computer's Group Policy Objects replace the user settings normally applied to the user.

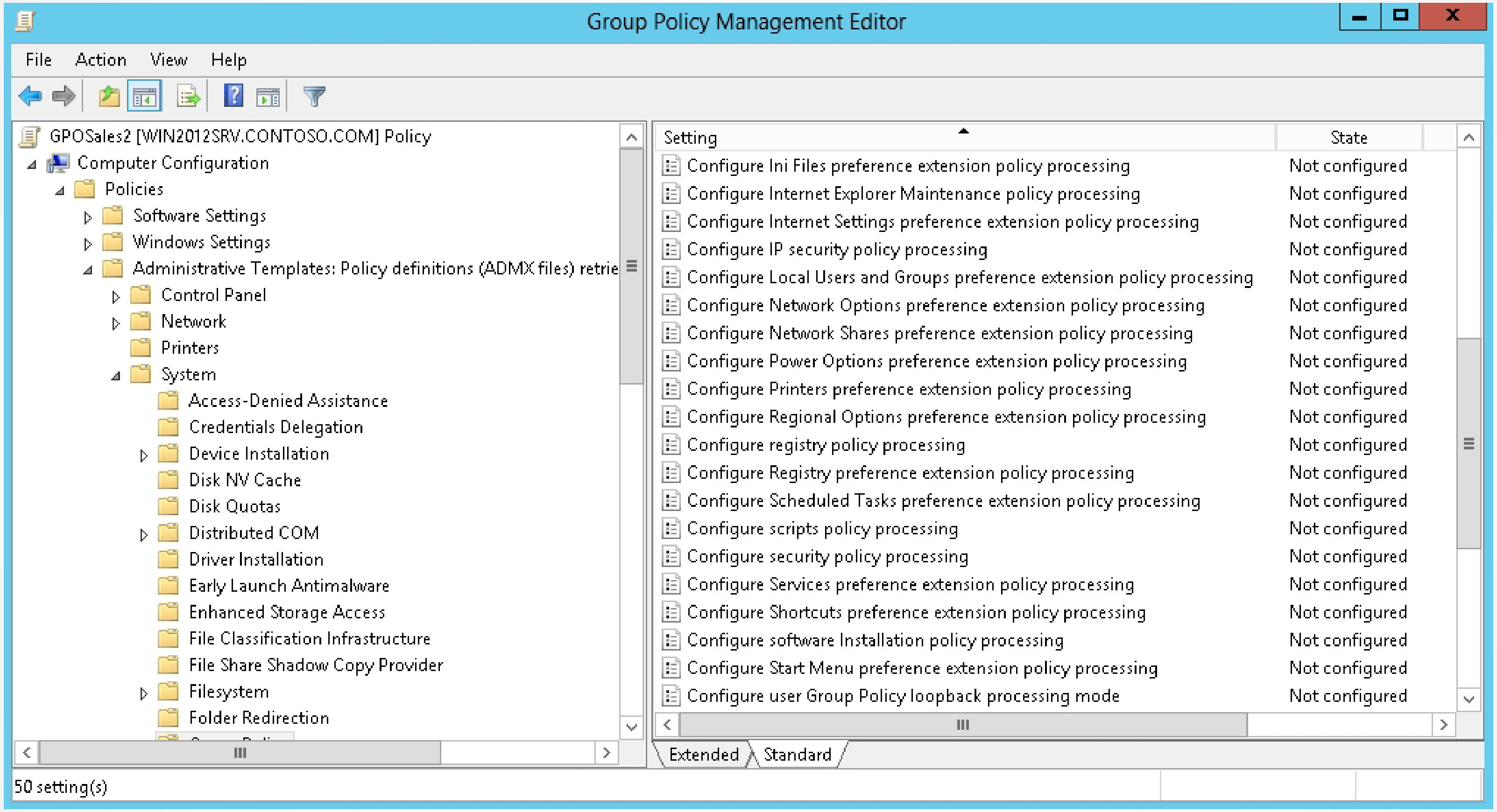
"Merge" indicates that the user settings defined in the computer's Group Policy Objects and the user settings normally

Configuring the Group Policy loopback processing mode

Configuring Client-Side Extension Behavior

- ***Client-side extensions (CSEs)*** are processes that interrupt the settings in a GPO and make the changes to the local computer or the currently logged-on user.
- CSEs are triggered when a Group Policy client pulls the GPOs from the domain.
- Each major category of policy setting has CSEs.

Configuring Client-Side Extension Behavior



- GPOSales2 [WIN2012SRV.CONTOSO.COM] Policy
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Templates: Policy definitions (ADMX files) retrie
        - Control Panel
        - Network
        - Printers
        - System
          - Access-Denied Assistance
          - Credentials Delegation
          - Device Installation
          - Disk NV Cache
          - Disk Quotas
          - Distributed COM
          - Driver Installation
          - Early Launch Antimalware
          - Enhanced Storage Access
          - File Classification Infrastructure
          - File Share Shadow Copy Provider
          - Filesystem
          - Folder Redirection

Setting	State
Configure Ini Files preference extension policy processing	Not configured
Configure Internet Explorer Maintenance policy processing	Not configured
Configure Internet Settings preference extension policy processing	Not configured
Configure IP security policy processing	Not configured
Configure Local Users and Groups preference extension policy processing	Not configured
Configure Network Options preference extension policy processing	Not configured
Configure Network Shares preference extension policy processing	Not configured
Configure Power Options preference extension policy processing	Not configured
Configure Printers preference extension policy processing	Not configured
Configure Regional Options preference extension policy processing	Not configured
Configure registry policy processing	Not configured
Configure Registry preference extension policy processing	Not configured
Configure Scheduled Tasks preference extension policy processing	Not configured
Configure scripts policy processing	Not configured
Configure security policy processing	Not configured
Configure Services preference extension policy processing	Not configured
Configure Shortcuts preference extension policy processing	Not configured
Configure software Installation policy processing	Not configured
Configure Start Menu preference extension policy processing	Not configured
Configure user Group Policy loopback processing mode	Not configured

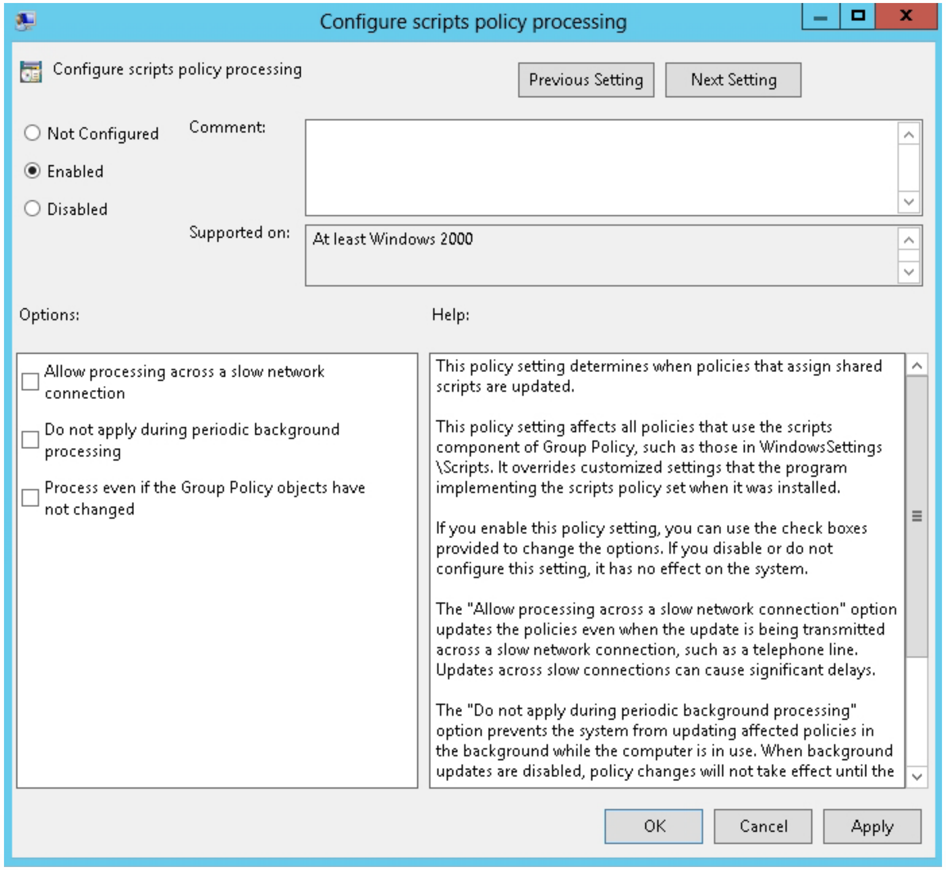
50 setting(s)

Displaying some of the available client-side extensions

Configuring Client-Side Extension Behavior

You can configure the behavior of CSEs by using Group Policy, specifically \Computer Configuration\Policies\Administrative Template\System\Group Policy\.

Configuring Client-Side Extension Behavior



Configure scripts policy processing

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000

Options:

□ Allow processing across a slow network connection

□ Do not apply during periodic background processing

□ Process even if the Group Policy objects have not changed

Help:

This policy setting determines when policies that assign shared scripts are updated.

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

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

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

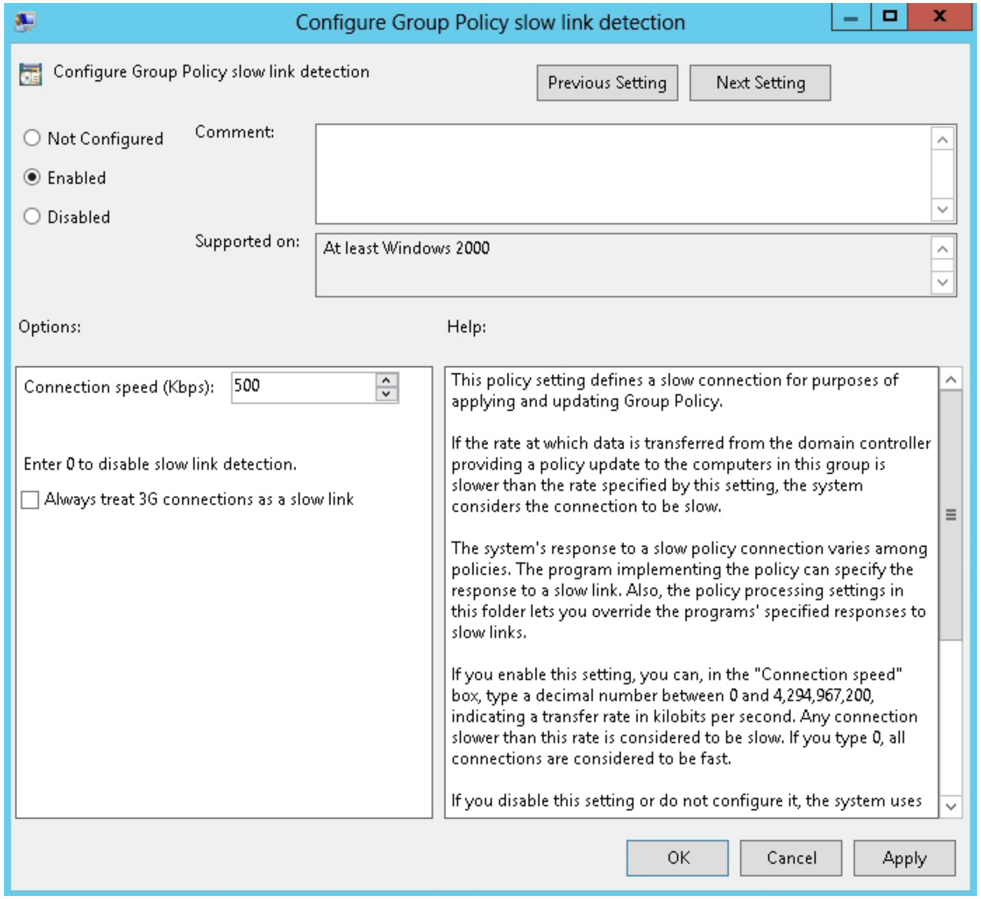
The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. When background updates are disabled, policy changes will not take effect until the

Configuring scripts policy processing

Configuring/Managing Slow-Link Processing

- Group policies executed over slow network links can affect the performance of the client computer, between a site and the corporate office of a site, or the computer being configured via a GPO.
- A link is considered slow if the link is less than 500 kilobits per second (kbps).
- The Configure Group Policy slow-link detection is used to define what is considered a slow-link connection.

Configuring/Managing Slow-Link Processing



Configure Group Policy slow link detection

○ Not Configured

● Enabled

○ Disabled

Supported on: At least Windows 2000

Connection speed (Kbps): 500

Enter 0 to disable slow link detection.

□ Always treat 3G connections as a slow link

This policy setting defines a slow connection for purposes of applying and updating Group Policy.

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

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

If you enable this setting, you can, in the "Connection speed" box, type a decimal number between 0 and 4,294,967,200, indicating a transfer rate in kilobits per second. Any connection slower than this rate is considered to be slow. If you type 0, all connections are considered to be fast.

If you disable this setting or do not configure it, the system uses

Defining the maximum speed of a slow link

Troubleshooting GPOs

Windows Server 2012 provides the following tools for performing Result Set of Policy (RSoP) analysis:

- The Group Policy Results Wizard
- The `GPResult.exe` command
- The Group Policy Modeling Wizard

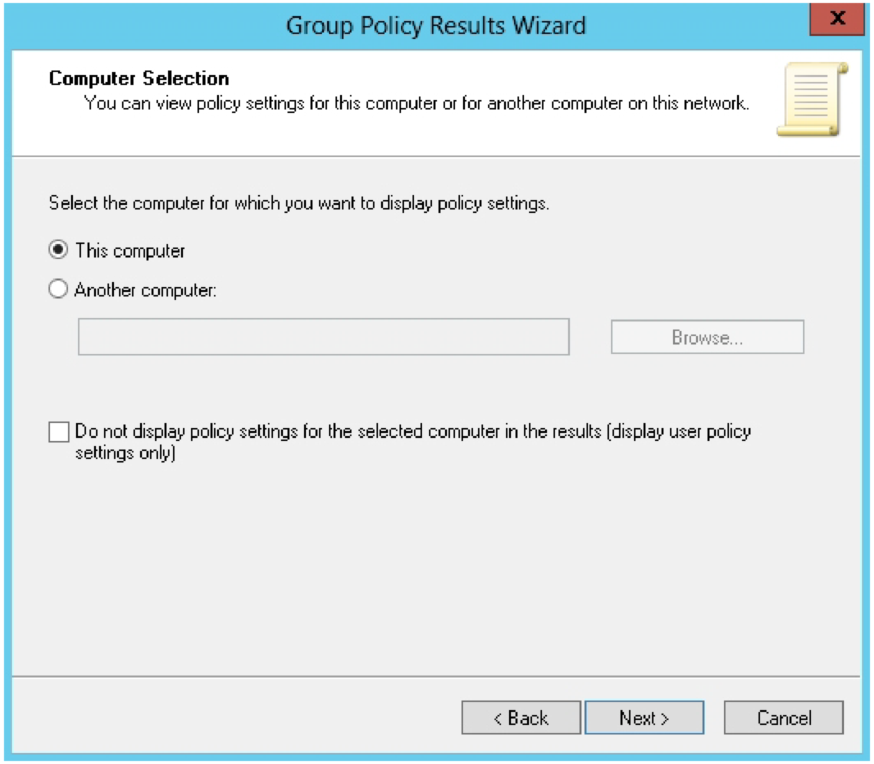
Troubleshooting GPOs

The ***Group Policy Results Wizard*** helps you analyze the cumulative effect of GPOs and policy settings on a user or computer.

To run the Group Policy Results Wizard, the following must be true:

- The target computer must be online.
- You must have administrative credentials on the target computer.
- The target computer must run Windows XP or newer.
- WMI must be running on the target computer and ports 135 and 445 must be available to access WMI on the target computer.

Run the Group Policy Results Wizard



Computer Selection

You can view policy settings for this computer or for another computer on this network.

Select the computer for which you want to display policy settings.

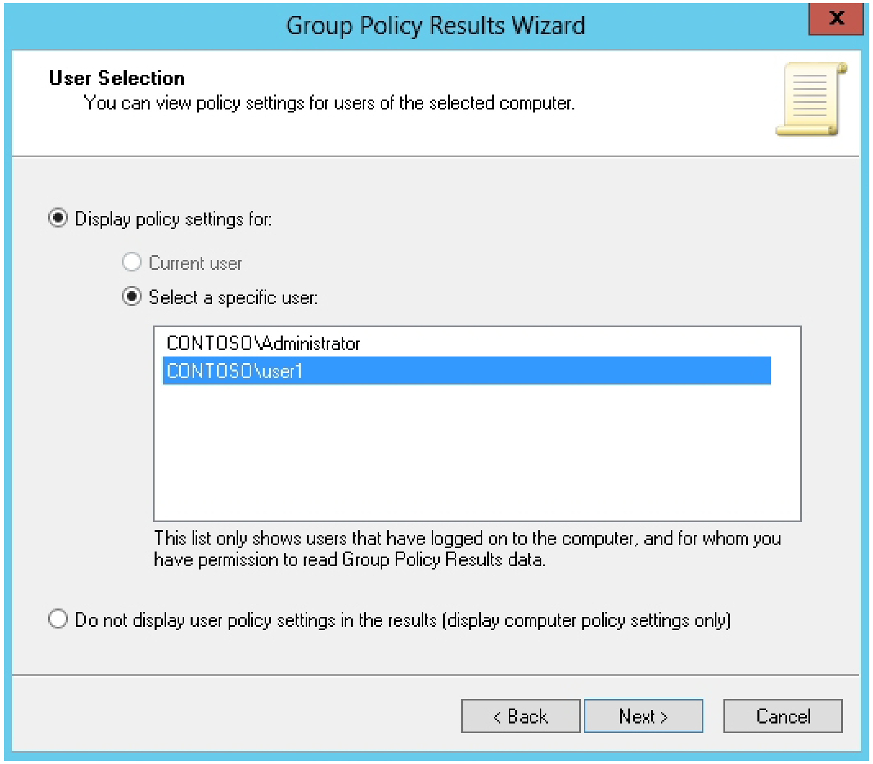
● This computer

○ Another computer:

□ Do not display policy settings for the selected computer in the results (display user policy settings only)

Viewing the Computer Selection page

Run the Group Policy Results Wizard



Group Policy Results Wizard

User Selection

You can view policy settings for users of the selected computer.

● Display policy settings for:

○ Current user

● Select a specific user:

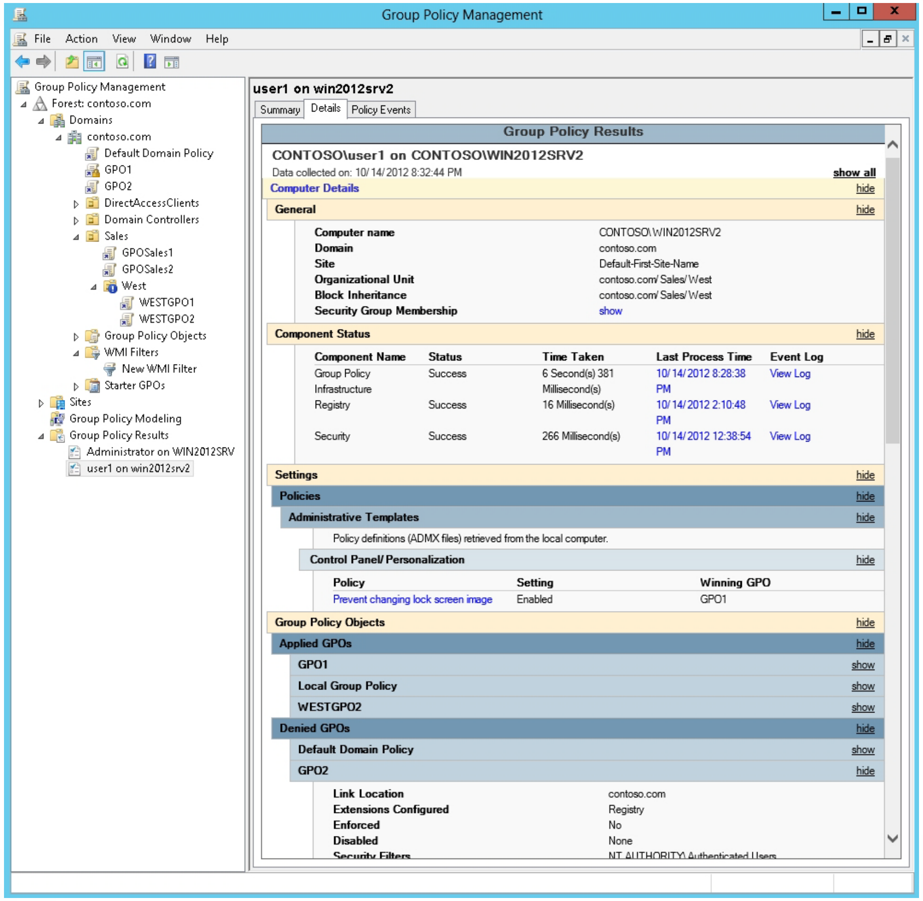
CONTOSO\Administrator
CONTOSO\user1

This list only shows users that have logged on to the computer, and for whom you have permission to read Group Policy Results data.

○ Do not display user policy settings in the results (display computer policy settings only)

Viewing the User Selection page

Run the Group Policy Results Wizard



user1 on win2012srv2

Group Policy Results

CONTOSO\user1 on CONTOSO\WIN2012SRV2

Data collected on: 10/ 14/ 2012 8:32:44 PM

Computer Details

General

Computer name	CONTOSO\ WIN2012SRV2
Domain	contoso.com
Site	Default-First-Site-Name
Organizational Unit	contoso.com/ Sales/ West
Block Inheritance	contoso.com/ Sales/ West
Security Group Membership	show

Component Status

Component Name	Status	Time Taken	Last Process Time	Event Log
Group Policy Infrastructure	Success	6 Second(s) 381 Millisecond(s)	10/ 14/ 2012 8:28:38 PM	View Log
Registry	Success	16 Millisecond(s)	10/ 14/ 2012 2:10:48 PM	View Log
Security	Success	266 Millisecond(s)	10/ 14/ 2012 12:38:54 PM	View Log

Settings

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

Control Panel/ Personalization

Policy	Setting	Winning GPO
Prevent changing lock screen image	Enabled	GPO1

Group Policy Objects

Applied GPOs

GPO1

Local Group Policy

WESTGPO2

Denied GPOs

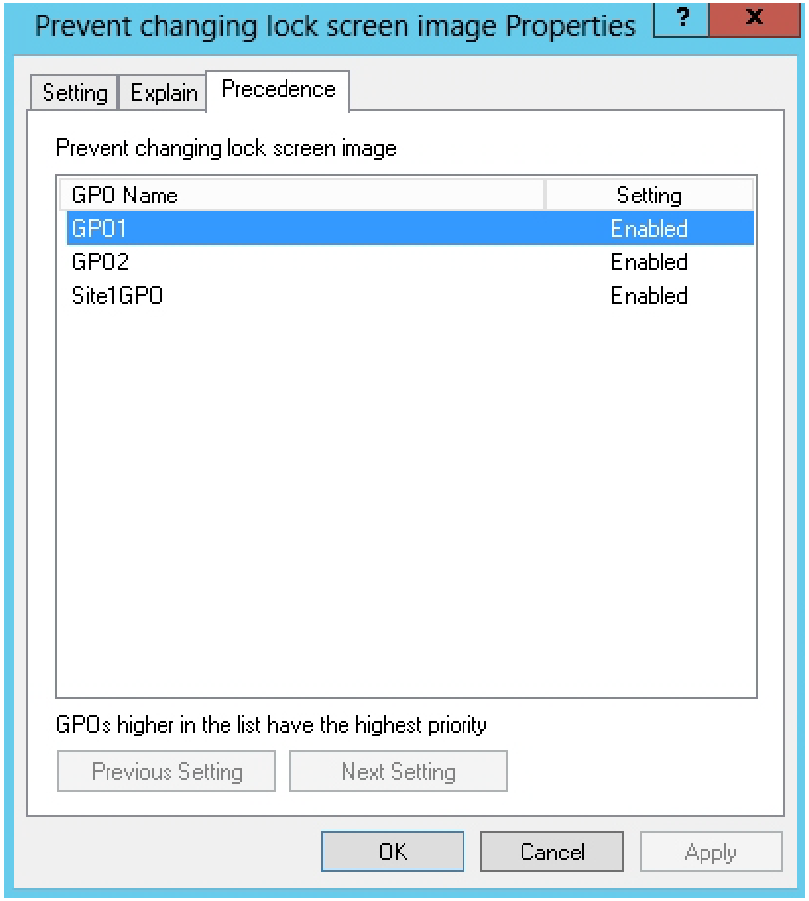
Default Domain Policy

GPO2

Link Location	contoso.com
Extensions Configured	Registry
Enforced	No
Disabled	None
Security Filters	NT AUTHORITY\ Authenticated Users

Viewing the Details tab for Group Policy Results

Run the Group Policy Results Wizard



Prevent changing lock screen image Properties

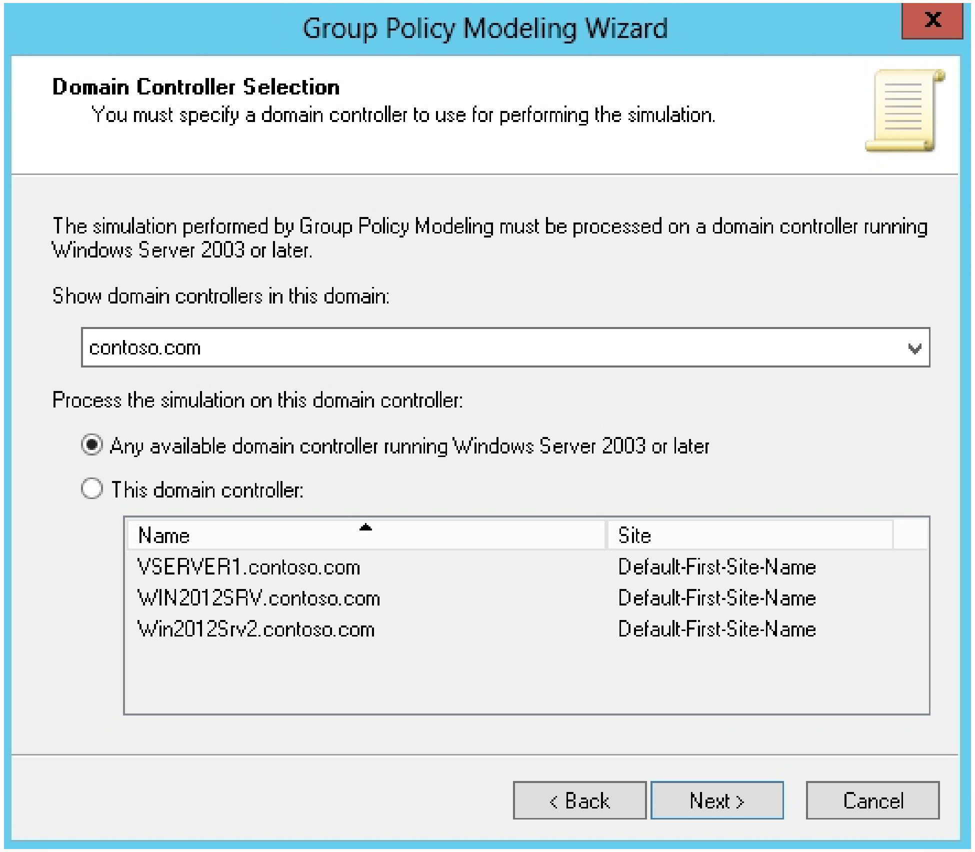
Prevent changing lock screen image

GPO Name	Setting
GPO1	Enabled
GPO2	Enabled
Site1GPO	Enabled

GPOs higher in the list have the highest priority

Using the Resultant Set of Policy console

Run the Group Policy Modeling Wizard



Domain Controller Selection

You must specify a domain controller to use for performing the simulation.

The simulation performed by Group Policy Modeling must be processed on a domain controller running Windows Server 2003 or later.

Show domain controllers in this domain:

contoso.com

Process the simulation on this domain controller:

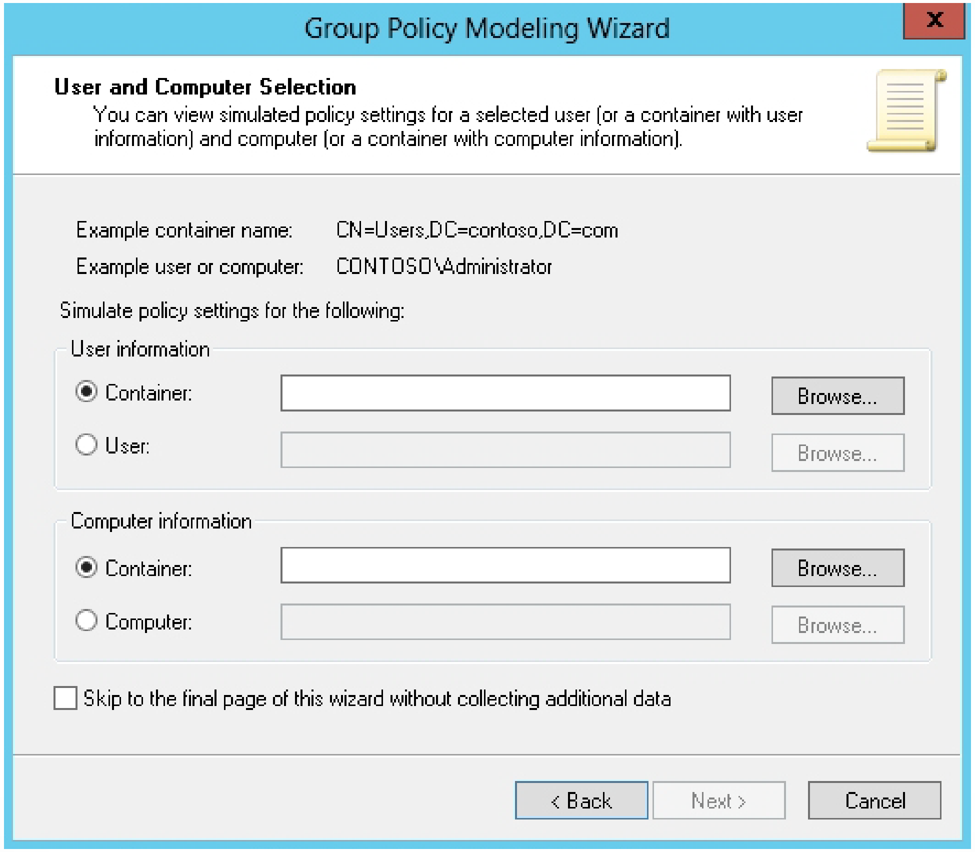
● Any available domain controller running Windows Server 2003 or later

○ This domain controller:

Name	Site
VSERVER1.contoso.com	Default-First-Site-Name
WIN2012SRV.contoso.com	Default-First-Site-Name
Win2012Srv2.contoso.com	Default-First-Site-Name

Selecting the domain controller

Run the Group Policy Modeling Wizard



User and Computer Selection

You can view simulated policy settings for a selected user (or a container with user information) and computer (or a container with computer information).

Example container name: CN=Users,DC=contoso,DC=com

Example user or computer: CONTOSO\Administrator

Simulate policy settings for the following:

User information

● Container: Browse...

○ User: Browse...

Computer information

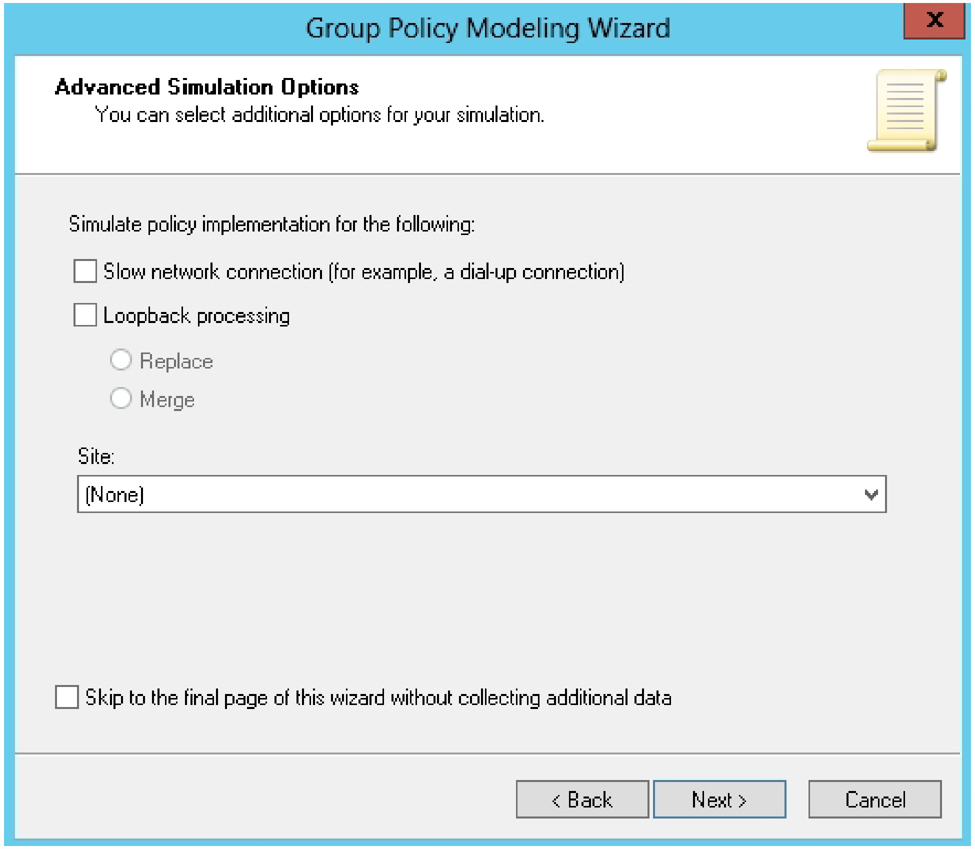
● Container: Browse...

○ Computer: Browse...

□ Skip to the final page of this wizard without collecting additional data

Selecting the user and computer to model

Run the Group Policy Modeling Wizard



Advanced Simulation Options

You can select additional options for your simulation.

Simulate policy implementation for the following:

□ Slow network connection (for example, a dial-up connection)

□ Loopback processing

○ Replace

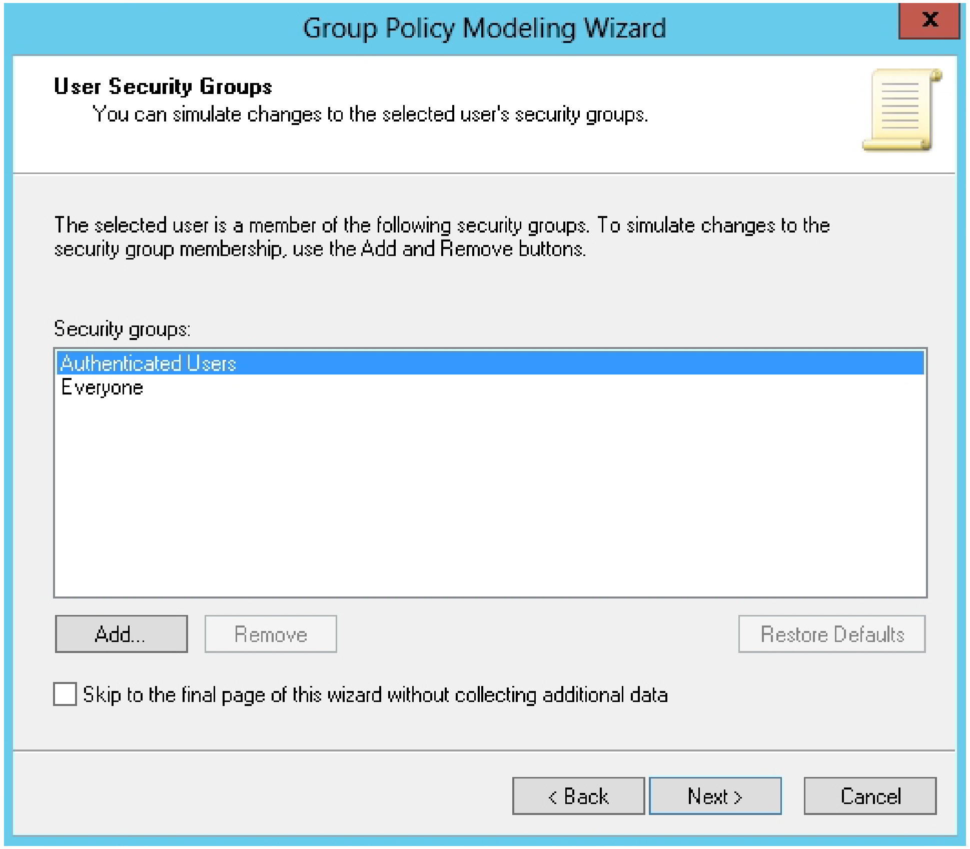
○ Merge

Site: (None)

□ Skip to the final page of this wizard without collecting additional data

Selecting advanced simulation options

Run the Group Policy Modeling Wizard



Group Policy Modeling Wizard

User Security Groups

You can simulate changes to the selected user's security groups.

The selected user is a member of the following security groups. To simulate changes to the security group membership, use the Add and Remove buttons.

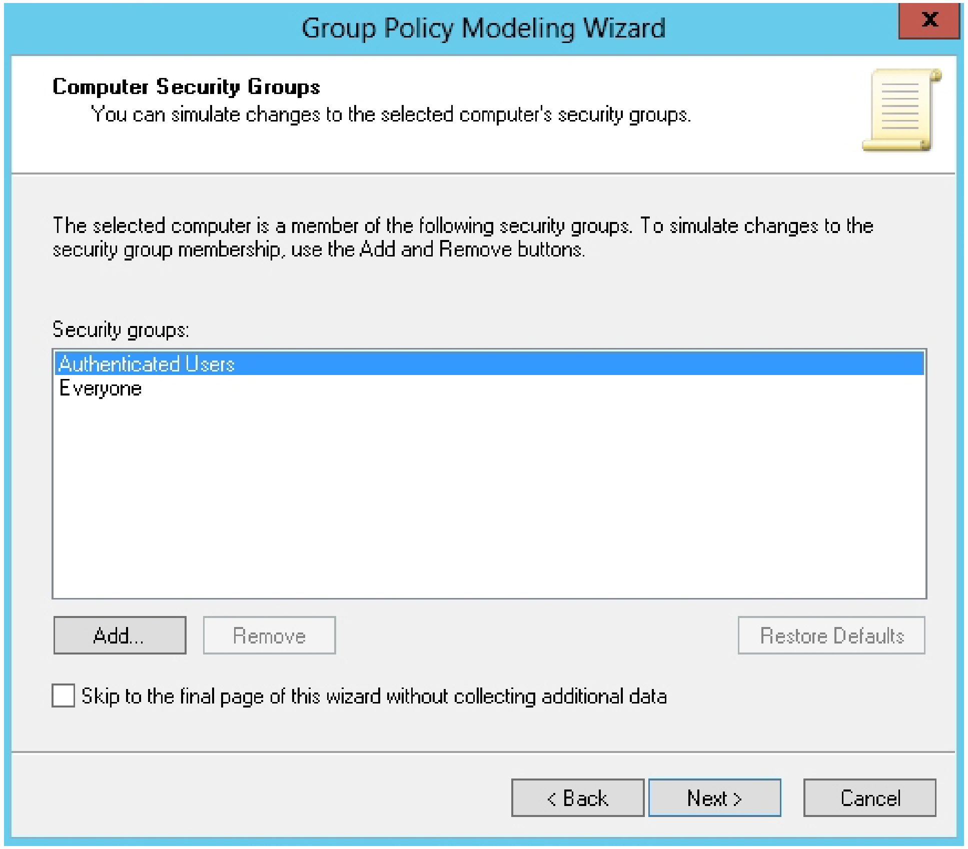
Security groups:

Authenticated Users
Everyone

□ Skip to the final page of this wizard without collecting additional data

Changing the user security groups

Run the Group Policy Modeling Wizard



Computer Security Groups

You can simulate changes to the selected computer's security groups.

The selected computer is a member of the following security groups. To simulate changes to the security group membership, use the Add and Remove buttons.

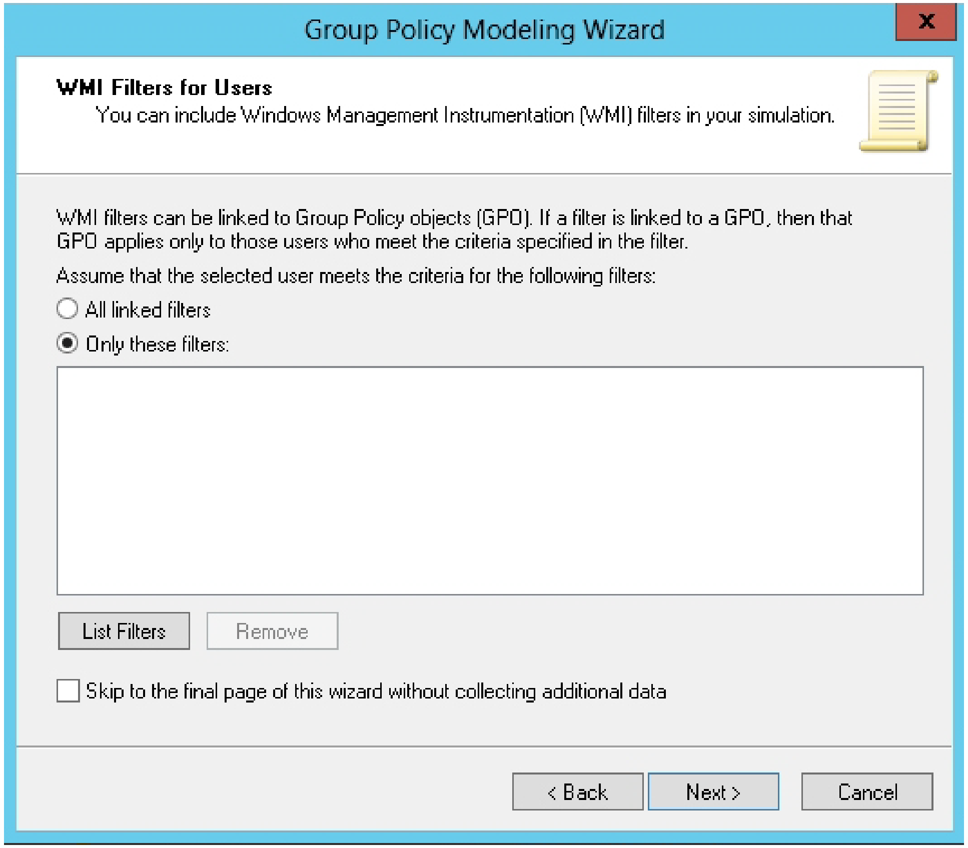
Security groups:

Authenticated Users
Everyone

□ Skip to the final page of this wizard without collecting additional data

Changing the computer security groups

Run the Group Policy Modeling Wizard



Group Policy Modeling Wizard

WMI Filters for Users

You can include Windows Management Instrumentation (WMI) filters in your simulation.

WMI filters can be linked to Group Policy objects (GPO). If a filter is linked to a GPO, then that GPO applies only to those users who meet the criteria specified in the filter.

Assume that the selected user meets the criteria for the following filters:

○ All linked filters

● Only these filters:

□ Skip to the final page of this wizard without collecting additional data

Changing WMI Filters for Users

Lesson Summary

- Group policies are defined using group policy objects (GPOs), which are the collection of configuration instructions that are processed by the computer.
- To assign a group policy, it is linked to an Active Directory container (site, domain, or organizational unit).
- GPOs are processed in the following order: local group policy, site, domain, and OU.
- By default, a group policy uses inheritance, whereas settings are inherited from the container above.
- When Active Directory is installed, there are two domain GPOs created by default: Default Domain Policy and Default Domain Controller Policy.
- The exceptions to the processing of group policies can be modified with the Block inheritance and Enforced options.

Lesson Summary

- Windows Management Instrumentation (WMI) filtering configures a GPO to be applied to certain users or computers based on specific hardware, software, operating systems, and services.
- Loopback processing allows the Group Policy processing order to circle back and reapply the computer policies after all user policies and logon scripts run.
- Client-side extensions (CSEs) are processes that interrupt the settings in a GPO and make the changes to the local computer or the currently logged-on user.
- Windows Server 2012 provides the following tools for performing RSoP analysis: the Group Policy Results Wizard, the `GPResult.exe` command, and the Group Policy Modeling Wizard.